Lars Vincent van de Wiel Lydersen

Practical security of quantum cryptography

Thesis for the degree of Philosophiae Doctor

Trondheim, September 2011

Norwegian University of Science and Technology
Faculty of Information Technology, Mathematics
and Electrical Engineering
Department of Electronics and Telecommunications

NTNU – Trondheim
Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the degree of Philosophiae Doctor

Faculty of Information Technology, Mathematics and Electrical Engineering
Department of Electronics and Telecommunications

ISBN 978-82-471-3012-4 (printed ver.)
ISBN 978-82-471-3013-1 (electronic ver.)
ISSN 1503-8181

Doctoral theses at NTNU, 2011:227

Printed by NTNU-trykk

Abstract

The peculiar properties of quantum mechanics enable possibilities not allowed by classical physics. In particular, two parties can generate a random, secret key at a distance, even though an eavesdropper can do anything permitted by the laws of physics. Measuring the quantum properties of the signals generating the key, would ultimately change them, and thus reveal the eavesdropper's presence. This exchange of a random, secret key is known as quantum cryptography.

Quantum cryptography can be, and has been proven unconditionally secure using perfect devices. However, when quantum cryptography is implemented, one must use components available with current technology. These are usually imperfect. Although the security of quantum cryptography has been proven for components with certain imperfections, the question remains: can quantum cryptography be implemented in a provable, unconditionally secure way, using components available with current technology? This thesis contains both a theoretical, and an experimental contribution to the answer of this question. On the experimental side, components used in, and complete quantum cryptography systems have been carefully examined for security loopholes. In particular, it turned out that two commercial quantum cryptography systems contained loopholes, which would allow an eavesdropper to capture the full secret key, without exposing her presence. Furthermore, this detector control attack could be implemented with current technology. The attack is applicable against a variety of quantum cryptography implementations and protocols.

The theoretical contribution consists of security proofs for quantum cryptography in a very general setting. Precisely, the security is proven with arbitrary individual imperfections in the source and detectors. These proofs should make it possible to use a wide array of imperfect devices in implementations of quantum cryptography.

Finally, a secure detection scheme is proposed, immune to the detector control attack and compatible with those security proofs. Therefore, if this scheme is implemented correctly, it offers provable security.

Publications contained in this thesis are referenced in bold (i.e. [**57**]) throughout the text.

Acknowledgements

First and foremost I give my deepest gratitude to my supervisor Professor *Johannes Skaar*. Throughout this work, I never experienced that he did not have time for discussions of virtually any topic. I admire his ability to tackle large and complex problems, and solve them as abstract logical puzzles rather than detailed brute-force calculations. He is one of the best lecturers I have ever met, and his passion for the beauty of electromagnetism is apparent for any of his students. My teaching style is heavily influenced by his lectures, and I have been honored enough to teach electromagnetism during his sabbatical.

My co-supervisor, Doctor *Vadim Makarov* has been the main supervisor in the experimental parts of this thesis. He is very creative, and combined with his extreme thoroughness, he is an excellent experimentalist. His different way of thinking, lifestyle and approach to life has caused numerous situations I thought I would never experience, and it has really enriched these years.

I have also had an excellent collaboration with the other PhD-students in the group, *Øystein Marøy* and *Qin Liu*.

This work has been conducted partly in Trondheim at the Department of Electronics and Telecommunications, and partly in Kjeller at the University Graduate Center. Furthermore we have had a very fruitful collaboration with the excellent Max Planck Institute for the Science of Light in Erlangen, Germany, led by Professor *Gerd Leuchs*. I always felt very welcome during my visits, and want to thank *Carlos Wiechers*, *Christoffer Wittmann* and *Bettina Heim* in particular. One of the experiments was conducted at the Group of Applied Physics in Geneva, Switzerland. Also here, I felt truly welcome and particularly want to thank the group leader *Nicolas Gisin* in addition to *Nino Valenta*, *Hugo Zbinden* and *Claudio Barreiro*. I also want to thank *Gregoire Ribordy*, *Matthieu Legré* and *Patrick Trinkler* at ID Quantique.

While this work was financed by the Department of Electronics and Telecommunications, I also received financial support from the University Graduate Center and the Research Council of Norway (grant no. 180439/V30 and project no. 199854).

Over the years I have had many great colleagues, many of whom I consider good friends: *Åsmund Monsen, Magne Saxegaard, Erik Folven, Espen Eberg, Jos*

Boshker, Jon Olav Grepstad, Øyvind Berle and *Mariam Kaynia.* I certainly think we solved numerous critical worldwide issues during lunch.

Finally, I want to thank my family for their support, and last but not least I thank my dear *Camilla* for her unconditional and never ending support.

Contents

1 Introduction 1
1.1 The playing field of cryptography . . . 2
1.2 Symmetric cryptography . . . 2
1.3 Asymmetric cryptography . . . 4
1.4 Quantum cryptography . . . 5
1.5 Motivation for this work . . . 7

2 The principles of quantum key distribution 9
2.1 The BB84 protocol . . . 9
2.2 Example of an attack . . . 11
2.3 Privacy amplification . . . 13

3 Theoretical security 15
3.1 Provable security . . . 16
3.2 Security definition for QKD . . . 17
3.3 Koashi's framework for proving security . . . 18

4 Implementations of QKD 21
4.1 Components for QKD . . . 21
4.1.1 Qubit source . . . 21
4.1.2 Quantum channel . . . 22
4.1.3 Detector . . . 22
4.2 System architectures . . . 26
4.2.1 Polarization encoding . . . 26
4.2.2 Phase encoding . . . 27
4.2.3 Plug-and-play architecture . . . 29
4.2.4 Distributed-phase-reference protocols . . . 33
4.3 QKD networks . . . 35

5 Practical security 37
5.1 Finite key length . . . 37

5.2 Photon-number splitting attack 38
5.2.1 Scarani-Acín-Ribordy-Gisin 2004 protocol 39
5.2.2 Decoy states protocol 40
5.3 Trojan-horse attack 40
5.4 Phase-remapping attack 41
5.5 Detector efficiency mismatch 42
5.6 Detector control attacks 44
5.7 Device-independent QKD 46

6 Thoughts on the future 49

7 Conclusion and future work 53

8 Publication list 55

9 Contributions in papers 59

Bibliography 63

Papers

A Security of quantum key distribution with bit and basis dependent detector flaws 81

B Security of quantum key distribution with arbitrary individual imperfections 101

C Hacking commercial quantum cryptography systems by tailored bright illumination 111

D Avoiding the blinding attack in QKD 121

E Thermal blinding of gated detectors in quantum cryptography 125

F After-gate attack on a quantum cryptosystem 145

G Secure gated detection scheme for quantum cryptography 161

H Tailored bright illumination attack on distributed-phase-reference protocols 171

I Device calibration impacts security of quantum key distribution 179

J Superlinear threshold detectors in quantum cryptography 187

K Controlling an actively-quenched single photon detector with bright light 197

L Controlling a superconducting nanowire single-photon detector using tailored bright illumination 205

M Comment on “Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography” 215

Chapter 1

Introduction

The word cryptography originates from Greek and is composed by the words *kryptos* which means hidden, and *graphein* which means writing. Placed together: cryptography is the art of writing messages such that their content is hidden for anyone but the intended receiver. The importance of cryptography cannot be sufficiently emphasized. Without the cracking of the Enigma during the second world war, the world history could have taken a very different turn. Without the invention of public key cryptography in the seventies, it would be unreasonably difficult to communicate privately on the internet. Just imagine if all your non-face-to-face communication such as phone calls, text-messages and internet activity were openly available!

From the ancient Greece through the wars of the medieval times, the second world war, and to today's online banking, cryptography is the tool that more or less permitted the public transport of important information. However, within the field of cryptography, there has always been a constant battle between the code makers who invent the cryptographic schemes, and those who break them. Every time a new scheme has been proposed, there has been an extensive effort to break it. Some try to break the schemes to identify security loopholes, in order to improve security. Others try to break the schemes to eavesdrop the communication with evil intentions.

Adding a new chapter to the constant battle between the makers and the breakers[1], a new flavor emerged 20 years ago, sprouting from quantum physics. Previously, the security of cryptographic schemes has been based on trusted couriers or mathematical complexity, while in quantum cryptography the security is rooted in the laws of quantum mechanics. Even the very best code breakers cannot break the laws of physics, so it seems that the code makers got the final word?

[1] For an entertaining introduction into the dramatic history of cryptography, I highly recommend "The Code Book" by Simon Singh [1].

1.1 The playing field of cryptography

Before entering the field of cryptography, and quantum cryptography in particular, let us establish some terminology and game rules. The task of finding weaknesses or breaking a cryptographic scheme is called *cryptanalysis*. The information which is to be encrypted is usually called the plaintext, or just the message. The encrypted message is usually called the ciphertext. The goal of all cryptographic schemes is that one party, commonly named *Alice* wants to send information to the receiving party, commonly called *Bob* through some public channel. The goal of the eavesdropper *Eve*, is to obtain the information through her access to the public channel, in many cases preferably without alerting Alice and Bob.

Encryption and decryption involves the use of secret[2] keys, which in a computer context is just a string of ones and zeroes. In fact, an encryption device or algorithm should only have the secret key and the message as inputs, and only output the ciphertext. Likewise, the decryption device or algorithm should only have the ciphertext and the secret key as inputs, and only output the message. The security of the scheme should not rely on keeping details of the devices or algorithms private. In fact, this is stated in *Kerckhoffs' principle* for cryptographic devices: a cryptosystem should be secure even if everything about the system, except the key, is public knowledge. Security based on the secrecy of the devices is often dubbed "security through obscurity," and does not really offer any security[3]. The eavesdropper could simply buy a copy of the system and examine it. Even when the systems are not sold, the history has shown that the details of a scheme eventually become known to the eavesdropper. As Claude Shannon phrased it: "The enemy knows the system".

1.2 Symmetric cryptography

One of the first known ciphers is *Caesar's cipher*, used by Julius Caesar to communicate with his generals during his military campains. Caesar's cipher is an example of a mono-alphabetic substitution cipher: to encrypt the plaintext, each letter is replaced with a letter a predetermined number of characters higher in the alphabet. For instance, if the secret key is "f", the letters of the plaintext is replaced according to a→f, b→g, c→h and so forth. The ciphertext is decrypted by replacing each letter with the letter the same number of characters lower in the alphabet. The encryption is easily broken: the plaintext can be found by trying all 25 shifts in the alphabet, where only one shift will produce a meaningful message.

[2] Secret means unknown to any but Alice and Bob, and therefore Eve in particular.

[3] A simple example of security through obscurity is hiding the key to your front door under the doormat. If the burglar knows the location of the key, the scheme is not secure any more.

Still, Caesar's cipher is a prime example of a *symmetric* ciphers.

In symmetric key cryptography, also called *private key* cryptography, Alice and Bob agree on a secret, private, and preferably random keystring[4]. This key can then be used to encrypt and decrypt messages in some cryptographic scheme (for instance the secret key "f" using Caesar's cipher in the above example).

The most important symmetric cipher is the *one-time pad*, invented by Gilbert Vernam in 1917 [2]. On a character by character basis, the encryption and decryption works just as in Caesar's cipher: each letter is shifted a number of characters up and down the alphabet. However, in the one-time pad, the shift is changed for each letter. For instance the code "fpt" would result in the word "the" being encrypted as "zwx". Now a brute-force attack would consist of trying each letter in the alphabet on each of the three places. This would produce all possible three letter words, hence Eve could just as well try to guess the plaintext. In fact, the unconditional security (see Section 3.1) of the one-time pad was proved from information-theoretic principles by Shannon in 1949 [3]. The result is simple to derive, and is repeated in Section 3.1.

In the binary alphabet, the encryption and decryption algorithm of the one-time pad is a bitwise *exclusive or* (XOR) operation[5] on the message/cipher bits, and equally many bits of secret key. Note that the key can not be reused, so the one-time pad encryption consumes a number of secret bits equal to the number of bits in the message. In fact, history has shown that reusing a key for the one-time pad can be fatal: due to reuse of keys, Soviet spies were exposed, captured and executed in the United States during the cold war[6]. As a matter of fact, not only did Shannon prove the unconditional security of the one-time pad, but he also proved that any unconditionally secure encryption scheme consumes at least as many bits of secret key as the message. Therefore the symmetric ciphers suffer from the key distribution problem: how much key is needed? And once Alice and Bob cannot meet to "refill" their key, how do you distribute the secret key?

The key distribution problem has led to the development of less key-consuming ciphers such as DES [4], RC4, and AES [5, 6] which are widely used in computers today. However, from Shannon's proof we know that these ciphers do not offer unconditional security: their security is merely based on the fact that they have not been broken yet, and that it is believed that they are very difficult to break.

[4] If the keystring is not random, it reduces the time it takes to find the keystring by a brute-force attack, since Eve can start with the most probable keystrings. An everyday example of this is the dictionary attack, where the attacker assumes that the password/key is a word.

[5] The XOR operation is equal to adding modulo 2 bitwise. Another way of thinking about the XOR operation when used to encrypt in the one-time pad, is that it inverts the message bit if the secret key bit is 1 or leaves it untouched if the secret key bit is 0.

[6] Julius and Ethel Rosenberg were exposed by the VENONA eavesdropping project, and later executed.

1.3 Asymmetric cryptography

The other main class of non-quantum cryptographic schemes is called *asymmetric key*, or *public key* cryptography, and does not suffer from the key-distribution problem[7]. In asymmetric cryptography, Alice and Bob use different keys: one for encryption and a different key for decryption. The first publication on public key cryptography came in 1976 by Whitfield Diffie and Martin Hellman [7]. Two years later came the now so widely used Rivest-Shamir-Adleman (RSA) algorithm [8]. The principle is that Bob generates a key pair, consisting of an encryption key, also called the public key, and a decryption key, also called the private key. The encryption key is made available to Alice, for instance by making it publicly available. Alice uses the public key to encrypt the message. Once the ciphertext is received by Bob he uses his private key to decrypt the message.

Public key cryptography solves the key distribution problem, because the encryption key can be made publicly available. In this scheme, the eavesdropper obtains the encryption key and the ciphertext. Finding the decryption key based on the the encryption key is a factorization problem which takes an exponential amount of time[8] using currently known algorithms on a classical (i.e. non-quantum) computer. By selecting the key size, the average time required to find the private key can be made arbitrarily large. However, there is a hitch: it is unknown whether more efficient factorization algorithms exist. Therefore, the security of public key cryptography is based on computational complexity and assumptions about the non-existence of more efficient algorithms.

Unfortunately an algorithm which is polynomial in time exists for quantum computers [9, 10]. This makes public key cryptography insecure in the presence of a scalable quantum computer[9]. Even without quantum computers, public cryptography offers no *forward secrecy*: Eve could capture and store the public key and the ciphertext until sufficient computational power to decrypt the message is available.

So it seems that solving the key distribution problem comes at the cost of the provable security?

[7] Of course Alice and Bob need to authenticate in any cryptographic scheme: This requires Alice and Bob to know some (not necessarily secret) information about each other, like the hash of each others public key.

[8] Exponential amount of time means that the factorization time consumed by a classical computer scales exponentially with the size of argument.

[9] Currently, the number 15 has been factorized on a magnetic resonance quantum computer [11]. Also recently, a Canadian company started offering quantum computers based on quantum annealing [12]. Even though there have been discussions whether quantum annealing can be used to implement general quantum algorithms [13], the company recently announced selling a quantum computer to Lookheed Martin [14].

1.4 Quantum cryptography

This is where quantum cryptography comes to a rescue! The strange laws of quantum mechanics allow Alice and Bob to generate a secret, random key at a distance, therefore solving the key distribution problem! Afterwards, the key can be used in an unconditionally secure symmetric encryption scheme, like the one-time pad. I will here give a brief overview of the history of quantum cryptography; for a more complete story, see for instance the reviews by Gisin [15] and Scarani [16].

In 1984 Charles Bennett and Gilles Brassard suggested the use of elementary particles to generate a secret random key at a distance [17]. The intuition comes from the laws of quantum mechanics: in general, a measurement of a property of a particle, can change the same property. This makes it impossible to copy a quantum particle [18]. To exploit this for key distribution, Alice sends random bits encoded in the properties of such elementary particles to Bob. These random bits can later be used as a secret key. Any attempt at eavesdropping will we caught: measuring the particles will change them, and reveal Eve's presence to Alice and Bob. If the particles were received undisturbed, the laws of quantum mechanics guarantee that no one has knowledge of the bits in the key. Therefore, the security of the key is not based on computational complexity, but rather on the laws of physics.

The term quantum cryptography is somewhat inaccurate, since there is no encryption involved. A more correct term is *quantum key distribution* (QKD), which is the term I will use throughout this thesis[10].

The protocol proposed in 1984 is now known as the BB84 protocol from the names of its inventors. Alice sends a random bit in a random basis corresponding to sending one out of four non-orthogonal quantum states to Bob. Bob performs a measurement in a random basis. Afterwards they compare their bases, and if they used the same bases Bob's measurement result should correspond to Alice's random bit. If they used different bases the bits are discarded. Their remaining random bits is a private secret key. To check for eavesdropping, they publicly compare a fraction of their keys to check for errors. A full review of BB84 is given in Section 2.1.

Independently, and without knowledge of Bennett and Brassard's findings, Arthur Ekert proposed to use entangled states to perform key distribution [19]. His intuition came from the fact that measuring each of the two particles in an entangled state gives correlated measurement results, even if the two particles are measured at a distance. These strong quantum correlations will necessarily

[10] Although some prefer to call it *quantum key growing*, since the authentication of Alice and Bob requires a small initial key.

violate the Bell inequalities [20]. Any measurement on an entangled state brings "local reality" [21] to the properties of the particle such that further measurements will not violate the Bell inequalities. Therefore, the violation of Bell inequalities means that no eavesdropping has taken place. This makes it is possible to reveal any eavesdropper. In fact, one could even let the eavesdropper produce the entangled states.

The protocol proposed by Ekert is named E91 or simply the Ekert protocol. Here Alice and Bob each have one particle from an entangled state. Both Alice and Bob measure their respective particles in one out of three different bases. Again, the same basis choice gives perfectly correlated results, and these bits are the key. The other bits where their bases differ, are used to check for the eavesdropper by verifying the violation of a Bell inequality. Later Bennett, Brassaird and Mermain claimed that prepare-and-measure protocols such as BB84, and entanglement based protocols such as the Ekert protocol are equivalent [16, 22].

In 1992 Bennett showed that it is possible to perform QKD using only two non-orthogonal states [23] in the so-called B92 protocol.

The first experimental demonstration of a QKD system was conducted by Bennett et al. in 1992 [24]. This lab-bench experiment had a 32 cm free-space quantum channel, with the quantum states encoded in the polarization of photons. After this demonstration, the interest for QKD rapidly increased, as did the experimental activity. Soon QKD was demonstrated in an optical commercial telecomcable over 23 km [25]. Currently, the distances has been increased to 250 km for an optical fibre [26], and 144 km in free space [27]. Today there exist several commercial companies which supply QKD systems.

Theory also came a long way since 1984. An important discovery was privacy amplification [28], which makes it possible to remove Eve's partial knowledge about the secret key by discarding some of the key during public discussion. Afterwards the first security proofs were established [29–32], proving the unconditional security of BB84 using perfect devices. In turn, people started considering the security of QKD with models of real devices [33–35]. Unfortunately, the early security analysis used an insufficient security definition (see Section 3.2). In 2005, a new composable security definition was found [36, 37], and subsequently most of the existing security proofs were updated or patched.

Even though QKD has been proven secure, it is a considerable challenge to implement it. The presence of side channels was realized already during the first experimental demonstration [24], when noise from the Pockels cells power supplies revealed the secret key, making the system "secure against any eavesdropper who happened to be deaf!" [38].

One imperfection which received considerable attention was the use of a coherent source at Alice, which frequently sends more than one photon in each pulse.

This allows the photon-number-splitting attack [39, 40], where Eve blocks single photons from Alice, and takes a photon for herself from the pulses containing multiple photons. Although covered by security proofs [33, 34][**41**], the impact on the key rate and communication distance is devastating. Therefore, new protocols emerged [42–45] to allow implementations with only a modest reduction in key rate from an imperfect source.

A host of other security loopholes have also been identified [46–56][**57**][58,59] in the implementations. From Eve's point of view, the most successful class of attacks is the detector control attacks [**57, 60**]. Exploiting the detector response to bright illumination, they allow Eve to capture the full secret key, without causing errors in the key. Furthermore, the eavesdropping device is implementable with off-the-shelf components. Detector control has been demonstrated in two commercial quantum key distribution systems [**57**], and a full eavesdropper has been used to capture the full secret key of an experimental QKD system at the National University of Singapore [58]. The search for implementation loopholes is often referred to as *quantum hacking*.

Even with very general security proofs [33][**41**], it seems to be challenging to make implementations within the assumptions of the proofs. In parallel with the success of quantum hacking, the idea of device independency was established. In device-independent QKD (DI-QKD) [19, 61, 62] the number of assumptions on the devices is reduced to a minimum. However, the remaining assumptions are challenging to implement. In particular, the proofs depend on a loophole-free Bell test, which requires a high detection probability at Bob. Otherwise, the correlations seen at Alice and Bob can originate from a pre-programmed computer. Although there are proposals to circumvent the detection loophole [63–65] at a distance [66], it seems experimentally challenging and promises at best moderate key rates. Therefore, it remains an open question if we will ever see DI-QKD outside the laboratory [67].

1.5 Motivation for this work

When I entered this field in 2006, I got the impression that QKD was quite mature. There were several startup companies producing QKD systems, and quite general security proofs incorporated a wide array of imperfections. However, a loophole not covered by the existing security proofs was found by our group. Therefore my motivation was that, by weeding out some remaining loopholes, practical QKD could deliver its provable, unconditional security. During my PhD, I have been given the opportunity to test commercial QKD systems to see if they actually comply with the assumptions in the security proofs. This is a very important task: all mature security technologies, for instance RSA public-key cryptography [68], did not become practically secure before the implementation had received massive scrutiny from independent researchers, and loopholes were closed. Therefore, if QKD is to mature, it is crucial that the security of the practical devices is tested by independent researchers, in order to obtain a reasonable level of security.

Chapter 2

The principles of quantum key distribution

There are numerous techniques in various quantum key distribution protocols, but they all rely on the same fundamental principle from quantum mechanics: in general, a measurement of a quantum state necessarily perturbs the quantum state. In particular, the no-cloning theorem [18] shows that it is impossible to copy a quantum bit (qubit). Therefore, by generating and measuring qubits in a suitable way, any eavesdropper must necessarily change the states of the qubits by measuring them, and therefore reveal her presence.

In this chapter, the first and most important protocol, the BB84 protocol is presented. Several other protocols have been proposed and implemented, mainly to increase practical performance, or to simplify the implementation. Some of those protocols will be presented in subsequent chapters.

2.1 The BB84 protocol

The BB84 protocol is the QKD protocol which was first proposed [17], implemented [24], and proved unconditionally secure [29, 31]. It has the advantage of being intuitive and easy to understand, but it might not be the optimal protocol to implement in practice.

QKD protocols require Alice and Bob to share a quantum channel, capable of transporting qubits, and a classical channel, for instance the internet. Eve is allowed to do anything allowed by physics with the qubits in the quantum channel. The classical channel is authenticated[1] by Alice and Bob. Therefore, while Eve

[1] Unconditionally secure authentication schemes exists. However, breaking the authentication after the secret key is generated does not compromise the security of the key. Therefore, authentication schemes that guarantee the security for a limited amount of time are sufficient.

can read all the information in the classical channel, she can not change this information. To authenticate the classical channel, previously generated secret key is used[2]. Therefore QKD is often referred to as *secret growing*.

BB84 protocol:

1. Alice generates N random classical bits, and for each bit she randomly chooses the $Z = \{|0\rangle, |1\rangle\}$ or the $X = \{|-\rangle, |+\rangle\}$ basis, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. For each bit, she generates a qubit and sends it to Bob. If the bit value is 0, she sends $|0\rangle$ or $|-\rangle$, and if the bit value is 1, she sends $|1\rangle$ or $|+\rangle$.

2. Bob measures the N qubits in a random basis; either the Z or the X basis. Bob's measurement result will be equal to Alice's bit value if they used the same basis. If they used opposite bases, Bob's measurement result will be random. This initial key is often called the *raw key*.

3. Alice and Bob publicly announce their basis choices over the classical channel, and discard the bits where they used different bases. With a high probability, they have about $N/2$ bits left, commonly called the *sifted key*.

4. Alice randomly selects a fraction of the remaining bits, and publicly announces the bit values. Bob compares Alice's bit values with his measurement results to check for Eve's presence. From this set, they can estimate the quantum bit error rate (QBER). If it is sufficiently low they continue the protocol with the remaining m-bit key (how low is sufficiently low will be discussed in Chapters 3 and 5). Otherwise, they discard the key and start over again.

5. The last step is called *reconciliation*. Using the QBER estimate Alice sends Bob error correcting data to obtain equal keys. The QBER enables Alice and Bob to upper bound Eve's information about the key. Then, Eve's information about the key is removed by discarding parts of the key. This is called *privacy amplification* (see Section 2.3). In this step, the m-bit erroneous, partly secure key is reduced to an n-bit flawless, unconditionally secure key.

[2] For the first run, a pre-established (small) secret key is used for authentication. At first this might appear as a drawback for QKD, but absolutely all (including all classical) cryptographic schemes require authentication to avoid the man-in-the-middle attack. In this attack, Eve poses as Alice to Bob, and as Bob to Alice, but in fact both Alice and Bob communicate only with Eve. To avoid this attack, all protocols require some preshared information about the parties. In QKD this is a random, secret key. In classical cryptography there exists schemes where the preshared information is publicly available (i.e. the MD5 or SHA1 hash of a public key), but these schemes are not unconditionally secure.

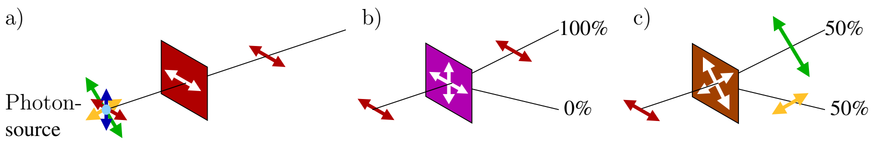


Figure 2.1: The components used for a simple polarization encoded BB84 scheme. a) A photon source is followed by a linear polarizer to generate a qubit with the desired polarization, in this case a horizontally polarized photon. b) When a horizontally polarized photon propagates through a horizontally oriented polarizing beam splitter (PBS), it is deterministically found in the exit of the beam splitter corresponding to the horizontal polarization. c) When a horizontally polarized photon propagates through a +45° oriented PBS, the photon has 50% probability to be found in each exit (but the photon will only be detected in one of them!). Furthermore, if the photon is found in the ±45° exit of the PBS, the photon will have a ±45° polarization afterwards. Therefore, the measurement has changed the state of the photon.

During the reconciliation step Alice's key was selected as the reference key, and Alice sent information to Bob such that he could correct his key. The procedure could have been done in the opposite direction, often referred to as *reversed reconciliation*.

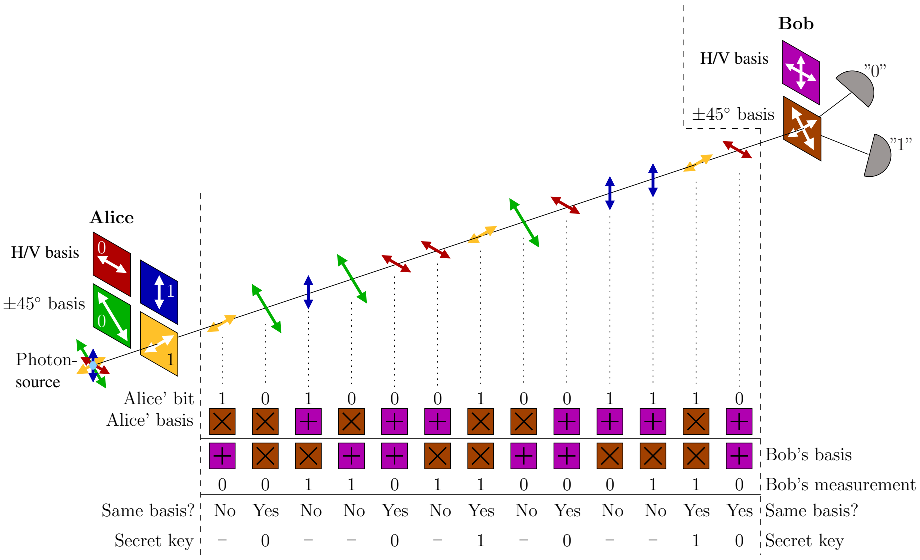
The protocol can be illustrated in a simple way by using the polarization of photons as qubits. As we will see in Chapter 4, photons are used as qubits in implementations. Figure 2.1 shows how to generate, encode and measure photons as qubits. Figure 2.2 illustrates the BB84 protocol for a polarization encoded QKD scheme.

2.2 Example of an attack

Let us briefly examine why a simple attack strategy fails. The most intuitive would be for Eve to collect the qubit, copy it, and send one copy to Bob. After the basis is revealed she could measure her copy in the same basis, and obtain the bit correct value. But the no-cloning theorem [18] makes it impossible to copy the qubit, so this strategy is physically impossible.

Let us see what happens if Eve tries to measure the qubits sent by Alice. Since she does not know the basis used by Alice and Bob[3], she randomly uses the Z or X basis. For half the bits she will guess the correct basis, and then she measures the

[3] For BB84, Alice and Bob discard the bits where they used different bases, so it is only necessary to consider the case where Alice and Bob used the same basis.

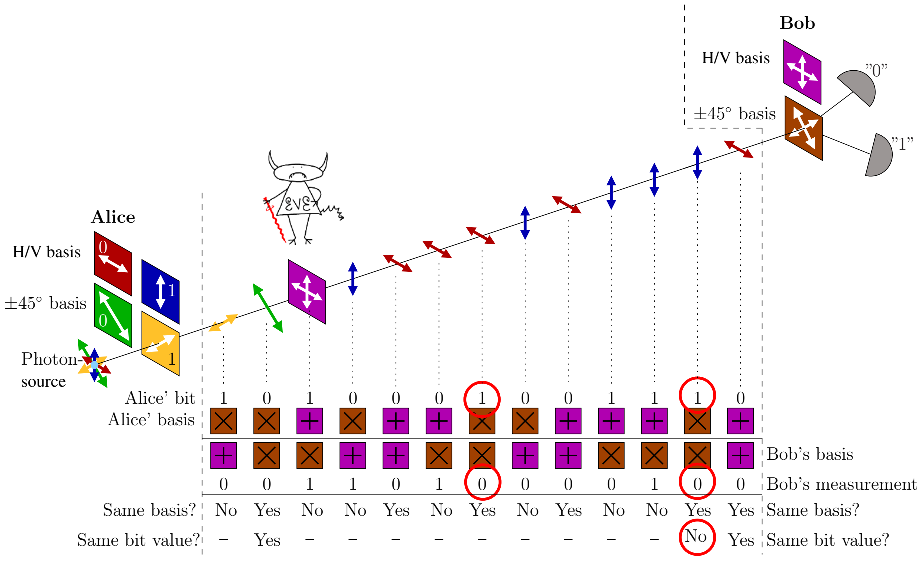


Alice' bit	1	0	1	0	0	0	1	0	0	1	1	1	0
Alice' basis	×	×	+	×	+	+	×	×	+	+	+	×	+
Bob's basis	+	×	×	+	+	×	×	+	+	×	×	×	+
Bob's measurement	0	0	1	1	0	1	1	0	0	0	1	1	0
Same basis?	No	Yes	No	No	Yes	No	Yes	No	Yes	No	No	Yes	Yes
Secret key	–	0	–	–	0	–	1	–	0	–	–	1	0

Figure 2.2: The BB84 protocol illustrated with photons. Here, the horizontal/vertical (H/V) basis corresponds to the Z basis and the ±45° basis corresponds to the X basis.

correct bit value. These qubits are unaffected by Eve's measurement, and Bob's measurement results will correspond to Alice bit values. No QBER is introduced. For the other half of the bits, Eve will use the opposite from Alice's and Bob's basis. For these bits, the probability to measure the same bit value as Alice is 50%. The qubit is passed on to Bob in the wrong basis, so regardless of Eve's measurement result, Bob will have a 50% probability of measuring the opposite of Alice's bit value. In other words, Eve's attack will introduce 50% QBER for half of the bits, a total of 25% QBER. Figure 2.3 illustrates this attack for the polarization encoded scheme presented in Figure 2.2.

This type of attack is called an *intercept-resend* attack because Eve fully measures the qubits from Alice. For such attacks, Eve always has more information about Alice's bits than Bob has. Therefore, obviously the QBER accepted by Alice and Bob must be lower than 25%. The acceptable QBER depends on the assumptions about Alice's and Bob's devices, and will be discussed in detail in Chapters 3 and 5. Note that Eve could achieve an arbitrarily low QBER by attacking just a fraction of the qubits. Therefore, a non-zero QBER means that Eve might have some information about the key.



Alice' bit	1	0	1	0	0	0	1	0	0	1	1	1	0	
Alice' basis	×	×	+	×	+	+	×	×	+	+	+	×	+	
	+	×	×	+	+	×	×	+	+	×	×	×	+	Bob's basis
	0	0	1	1	0	1	0	0	0	0	1	0	0	Bob's measurement
Same basis?	No	Yes	No	No	Yes	No	Yes	No	Yes	No	No	Yes	Yes	Same basis?
Same bit value?	–	Yes	–	–	–	–	–	–	–	–	–	No	Yes	Same bit value?

Figure 2.3: Eve's attempt at a simple intercept-resend attack. She always uses the same H/V basis (Z basis) to measure the photons, since this is equally likely to be the correct basis choice as any other choice. For the bits where Eve's basis choice is different from the one of Alice and Bob, she will introduce errors in the key. Therefore, when Alice and Bob estimate the QBER (using a fraction of the key, in this case 3 bits) her presence is revealed.

2.3 Privacy amplification

Let's assume that after error correction, Alice and Bob have a flawless, private key where parts of the key is known to Eve. It turns out that it is possible for Alice and Bob to sacrifice parts of the key to obtain a smaller key on which Eve has no information. The procedure is called *privacy amplification* [28].

An intuitive algorithm goes as follows: Alice announces that two of the bits are to be replaced with a single bit. The bit value of this bit is the XOR of the two bit values. If Eve knew each bit value independently with 75% probability, she knows the correct XOR value with probability $0.75^2 + 0.25^2 = 0.625$. Thus Eve's information about this bit is less than her information about each of the previous bits.

In practice, a different algorithm is used. The only privacy amplification algorithm that preserves composability (see Section 3.2) is two-universal hashing. A hash function maps all 2^n n-bit inputs to all 2^m m-bit outputs. Since

$m < n$ there exists a probability that two different inputs produce the same output. The family of two-universal hash functions $\mathcal{F}$ has the property that for all $f \in \mathcal{F}$, and all $x, x' \in (\mathbb{Z}_2)^n$, the probability of a collision is upper-bounded as $p(f(x) = f(x')) \leq 1/2^m$. Therefore, Alice and Bob randomly choose a function $f \in \mathcal{F}$, and obtain the secret key $s = f(x)$, where x is the key after error correction. If Eve has a slightly different key x', the probability that she obtains the same key $f(x')$ is equal or less than $1/2^m$, so any guess is equally probable to be the key as $f(x')$.

Chapter 3

Theoretical security

So far the security of QKD has been based on the fact that Eve cannot measure the qubits without introducing errors in the key. However, quantum physics allows more powerful interactions than a projective measurement! Normally, Eve's attack is classified as follows [69]:

- In *individual attacks* (also called *incoherent attacks*) Eve treats every quantum system from Alice equally. One example of an individual attack is the intercept-resend attack considered in Section 2.2. A more general attack is to let each quantum system from Alice interact with an individual probe[1], and measure the probe later. In different definitions of individual attacks, it varies whether the measurement of the probe must happen before or after sifting [16]. Note that for the BB84 protocol, the best individual attack has been found [70].

- A stronger class of attacks is *collective attacks.* As for the individual attacks, Eve may let the each system from Alice interact with a probe. After the interactions, Eve has a number of probes. In this class of attacks Eve can wait arbitrarily long, for instance until the key is used in some application like the one-time pad. Then she can do a collective measurement on all the probes simultaneously.

- The most powerful class of attacks is called *coherent attacks*, or *general attacks.* Here Eve can have any interaction with the system from Alice and perform any measurement at any time. She could for instance entangle multiple bits, and/or use the same probe for many bits.

[1] A probe is a quantum system in a well-defined state, typically a number of quantum bits each prepared in the state $|0\rangle$.

The *exponential de Finetti theorem* [71, 72] proves that in the asymptotic limit of infinite keys, and if Bob's signals have a sufficiently low dimension, any coherent attack is not better than the best collective attack. Therefore, under such circumstances, it suffices to prove the security against collective attacks. However, the prerequisites are not always fulfilled for devices with imperfections. To apply the de Finetti theorem, the (entanglement based) protocol must be invariant to a permutation of Alice's and Bob's N particle pairs after they have been distributed. This is clearly not the case for collective errors, for instance in the case of afterpulses (see Section 4.1.3). In general, the dimension of Bob's signals will be of infinite dimension, and therefore the de Finetti theorem does not apply. In some cases, this can be solved by proving the existence of a squash operator [73–76], such that one can assume that Eve only sends single qubits to Bob. However, in the presence of certain imperfections, for instance detector efficiency mismatch (see Section 5.5), no squash operator has been found[2].

3.1 Provable security

Provable secure means that the security is proven without restricting the eavesdropper in computational power, time or physical access to the communication channel. The only requirement is that the attacker obeys the laws of physics, and that the protocol is correctly implemented[3].

Since it is straightforward, let us prove that the one-time pad (see Section 1.2) is unconditionally secure. Assume a n-bit message $M \in (\mathbb{Z}_2)^n$ where $P(M = m)$ follows some probability distribution. Furthermore, assume a random, secret key $K \in (\mathbb{Z}_2)^n$ where all keys are equally probable: $P(K = k) = 1/2^n$. Let the ciphertext be denoted by $c \in (\mathbb{Z}_2)^n$. Since all possible keys k map m into all possible ciphers c in $(\mathbb{Z}_2)^n$, the conditional probability on the cipher c given the message m is equal to $P(C = c|M = m) = 1/2^n$. In turn the probability of a specific ciphertext c for any message m is found as

$$P(C = c) = \sum_m P(C = c|M = m)P(M = m) = \sum_m P(M = m)\frac{1}{2^n} = \frac{1}{2^n}. \quad (3.1)$$

[2] Squash operators have been found for BB84 for specific measurement setups for Bob: when Bob's detectors are identical and his basis selector is simply a Hadamard transform on each photon of the received pulse [74, 77], or if Bob's measurement operators are symmetric under the cyclic group C_4 [76].

[3] As a trivial example: Alice or Bob should not reveal the secret key, nor the secret message to Eve. Although trivial, in practice this kind of information leakage is a highly relevant problem.

Then, Bayes' theorem gives

$$\begin{aligned} P(M=m|C=c) = \frac{P(C=c|M=m)P(M=m)}{P(C=c)} &= \frac{1/2^n P(M=m)}{1/2^n} \\ = P(M=m), \end{aligned} \tag{3.2}$$

which means that the probability of a given message m is the same if the ciphertext is known. In other words: the ciphertext reveals nothing about the plaintext.

3.2 Security definition for QKD

One would like to prove that a QKD protocol gives a random, secret key to Alice and Bob, while zero information about the key is given to Eve. This means that the best attempt Eve could do to find the key is to try to guess. Unfortunately, Eve could always attack a few bits, and the privacy amplification could fail, leaving Eve with a tiny information about the key. In practice, the security is defined such that the information left to the eavesdropper is quantified, and can be made arbitrarily small. The first security definition was the following: "A QKD protocol is *ϵ-secure* if, for any security parameters $\epsilon > 0$ and $s > 0$ chosen by Alice and Bob, and for any eavesdropping strategy, either the scheme aborts, or it succeeds with probability at least $1 - O(2^{-s})$, and guarantees that Eve's mutual information with the final key is less than ϵ. The key must also be exponentially close to uniformly distributed [78, 79]." The security definition is very intuitive: the protocol should normally succeed, and Eve's mutual information with the key can be made arbitrarily small. Under this security definition the achievable secret key rate R is given by [80]

$$R \geq I(A,B) - \min\left\{I(A,E), I(B,E)\right\}, \tag{3.3}$$

where $I(\,\cdot\,,\,\cdot\,)$ denotes the mutual information [81] two parties (A stands for Alice, B for Bob, and E for Eve).

This definition is insufficient because it considers the information *after* the parties (including Eve) have measured their quantum systems. Quantum mechanics is often counterintuitive, and it turns out that if Eve is given one extra bit of information before she measures her probe, this could unlock *more* than one bit of information [82]. This extra information could easily come from some known-plaintext attack[4]. This security criterion also lacks *composability.* If an ϵ-secure task[5] uses an ϵ'-secure key, what is the security parameter of the composite process?

[4] In a known-plaintext attack, the eavesdropper knows a part of the encrypted plaintext. For instance, the header of an e-mail is very similar for all e-mails. Then, the one-time pad encrypted header reveals parts of the secret key.

[5] The one-time pad is a 0-secure task.

A suitable security definition was found in 2005 [37]. The success criterion corresponds to the original one, but Eve's knowledge about the key is not based on measurement data any more. Let ρ_{ABE} be the general quantum state of Alice, Bob and Eve. Further let $\rho_S = 1/|S| \sum_S |s\rangle\langle s| \otimes |s\rangle\langle s|$ be a classical quantum extension of the final secret key bits s. Then, the key is ϵ-secure if

$$\frac{1}{2}\|\rho_{ABE} - \rho_S \otimes \rho_E\|_1 \leq \epsilon, \tag{3.4}$$

where $\frac{1}{2}\|\rho - \sigma\|_1 = \frac{1}{2}\mathrm{tr}|\rho - \sigma|$ is the trace distance between the quantum states ρ and σ, with $|A| = \sqrt{A^\dagger A}$. The trace distance has the property that no physical process can increase the trace distance between two quantum states [83]. Therefore, there is no operation that will increase Eve's entanglement with the key, and thus knowledge about the key after a measurement of her quantum system.

For this security definition, ϵ is the distinguishability advantage: the probability that Eve can use her information to distinguish the QKD system from a perfect QKD system is less than ϵ.

This security definition is composable [84], so if an ϵ-secure key is used for an ϵ'-secure task, the composed task is $(\epsilon + \epsilon')$-secure. Due to the late arrival of this suitable security definition, many of the security proofs and security frameworks are formulated for the obsolete security definition. Luckily, patches have been found for most security proofs and frameworks, making them valid also with the new definition. Note that the expression for the secret key rate, Equation (3.3) remains valid for security proofs restricted to individual attacks.

3.3 Koashi's framework for proving security

It is often complicated to prove the security of QKD-protocols directly. Therefore, the security proofs are usually constructed as follows: first the security is proved for an abstract, virtual protocol. Then, the actual protocol is shown to be a special case of the virtual protocol.

The security of QKD has been proven using several different frameworks [29–32, 85, 86]. For QKD with imperfections, most proofs use a virtual protocol based on entanglement. The contributions in this thesis use the framework from Koashi [85, 87]. The idea and principle behind this framework is sketched below. Note that this sketch is not complaint with the new security definition. Luckily, it has been proved that the results are also valid with the new security definition [88] (see Section 3.2). Nevertheless, the information-theoretic approach is sketched here because it is more intuitive and easier to understand than the trace-distance based approach.

Koashi's security proof is based on the uncertainty principle. Assume that N qubits are measured in either the X or the Z basis, and let X_N and Z_N be the stochastic variables corresponding to the measurement result in each basis. The entropic uncertainty relation [89] can then be formulated as:

$$H\left(X_N\right) + H\left(Z_N\right) = N, \tag{3.5}$$

where $H(\,\cdot\,)$ denotes the entropy of the measurement result in a basis. The idea is to use the entropic uncertainty relation (3.5) to upper bound Eve's information about the key[6].

In this protocol, Alice and Bob share N bipartite states (for instance EPR-pairs). The protocol is symmetric with respect to the basis choices, so without lack of generality, assume that Alice and Bob use the Z basis[7] to generate the key, and in particular, let Alice's measurement result be the raw key.

The amount of privacy amplification required can be found from the following virtual experiment: assume that Alice measures the raw key in the X basis instead of the Z basis. Bob's task is to predict the result of Alice's virtual X basis measurement. Since Bob does not actually do this prediction, Bob can do anything permitted by the laws of nature, including a virtual measurement on his parts of the bipartite states. If the uncertainty about Alice's virtual X basis measurement $H(A)$ can be bounded from Bob's virtual measurement result $B = b$, $H(A|B = b) \leq K$, then the entropic uncertainty relation (3.5) predicts that no one, including Eve can predict the outcome of Alice's Z basis measurement with uncertainty less than $H(Z_N) \geq N - K$. Since these $N - K$ bits are unknown to Eve, they can be used to generate a secret key. However, Bob must ensure that he has an identical raw key as Alice. Let δ_{bit} be the error rate in the Z basis, and let $h(\,\cdot\,)$ denote the binary entropy function. Then Alice can use $Nh(\delta_{\text{bit}})$-bits of pre-established secret key to securely send Bob error correcting data such that they obtain identical raw keys. The net secret key rate is therefore

$$R \geq N\left(1 - h\left(\delta_{\text{bit}}\right)\right) - K. \tag{3.6}$$

For perfect devices, Bob can for instance try to predict Alice's virtual X basis measurement by measuring his parts of the bipartite states in the X basis. Then, if δ_{phase} is the error rate in the X basis, the number of bits where his and Alice's measurement results differ should be $N\delta_{\text{phase}}$, and his uncertainty about Alice's

[6] Recently a quantum version of the uncertainty relations has been found [90, 91], relating the uncertainty not only to the measurement outcome of Eve, but also to the quantum states possessed by Eve.

[7] Since protocol is symmetric with respect to the basis choice, one can simply label Alice's and Bob's basis choice as the Z basis, and the opposite basis as the X basis.

virtual X basis measurement is given by $K \geq Nh(\delta_{\text{phase}})$. Therefore, the net key rate for perfect devices is given by

$$R \geq 1 - h(\delta_{\text{bit}}) - h(\delta_{\text{phase}}). \tag{3.7}$$

If the QBER in the bases are equal ($\delta = \delta_{\text{phase}} = \delta_{\text{bit}}$), the rate becomes

$$R \geq 1 - 2h(\delta). \tag{3.8}$$

$R > 0$ requires $\delta < 0.11 = 11\%$. This is a bound for the QBER in the absence of imperfections.

Chapter 4

Implementations of QKD

The most important ingredient when implementing QKD is suitable quantum bits. They should be easy to generate, easy to transport while preserving their quantum state, and easy to measure. In practice the photon is the particle that best suits these requirements. In this chapter, we discuss the main components in a QKD setup, and discuss some architectures for QKD systems. Finally, QKD networks are discussed. Note that continuous-variable QKD [92, 93] is not presented here, since it is unrelated to the work presented in this thesis.

4.1 Components for QKD

4.1.1 Qubit source

In most setups, lasers are used as a qubit source because they are practical, small and low-cost. However, a laser is not a single photon source: it emits approximately coherent states. Without a phase reference, the output state from a laser can be expressed as a Poissonian mixture of the different number states:

$$\rho = \sum_{n=0}^{\infty} \frac{e^{-\mu}\mu^n}{n!} |n\rangle\langle n|, \tag{4.1}$$

where μ is the mean number of photons in the pulse.

Since Alice frequently sends more than one photon, this imperfection has led to the development of more sophisticated protocols to battle the photon-number splitting attack (see Section 5.2).

There are sources which send out multiphoton pulses less frequently than a laser, so-called sub-Poissonian sources. The development of these sources for quantum cryptography has slowed down, due to the development of the decoy state protocol [43–45], which negates the loss of key due to multiphoton pulses.

However, the sub-Poissonian sources might find a new application in quantum repeaters [94].

A third class of sources is entangled photon sources, for instance used in the Ekert and the BBM QKD protocols [19,22], and an essential ingredient in photon-based quantum computing [10]. Entangled photon sources have developed rapidly in the recent years. Traditionally, entangled photons have been generated through parametric down-conversion, requiring a powerful pump laser. However, now it seems that entangled light emitting diodes are within reach [95,96].

In prepare and measure schemes, Alice's basis and bit choice is usually encoded in the polarization or phase of the photon. In a polarization encoded scheme, the encoder is simply a polarizer, while in a phase encoded scheme, the encoder is usually an interferometer (see Sections 4.2.1–4.2.2).

4.1.2 Quantum channel

The requirements for the quantum channel are that it should preserve the quantum state (avoid decoherence from the environment), and have low loss. In practice, two channels have the desirable properties: optical fiber and free-space.

Optical fiber technology is mature: optical fibers have been developed and used in telecommunication for four decades. The loss α of an optical fiber is usually measured in dB/km. The probability for a single photon to be transmitted through an optical fiber of length l, is given by $10^{-(\alpha l)/10}$. The loss depends heavily on the wavelength of the photons, and is minimal in the two "telecom windows": $\alpha \simeq 0.34\,\mathrm{dB/km}$ for 1330 nm, and $\alpha \simeq 0.2\,\mathrm{dB/km}$ for 1550 nm. Since loss is critical for the transmission range and key rate, the 1550 nm wavelength is usually used for QKD.

Due to birefringent effects, optical fibers have significant depolarization. Therefore, phase-encoding is usually used for fiber-based QKD systems.

Free-space links have negligible decoherence. However, atmospheric fluctuations make it challenging to predict the arrival point of a photon over large distances. Another disadvantage of the free-space link is that it requires a line-of-sight between Alice and Bob.

There are "atmospheric transmission windows" that have small loss, for instance 780–850 nm and 1520–1600 nm typically have loss $\alpha < 0.1\,\mathrm{dB/km}$ in clear weather [97].

4.1.3 Detector

There are excellent reviews of single photon detectors [98,99], so this section only contains a brief review of the detector technologies relevant to this thesis: avalanche photodiodes (APDs) [100], and superconducting nanowire single photon detectors (SNSPDs) [101, 102].

The detector performance has four important figures: detection efficiency, dark count rate (false detection events), detector dead time (or maximum detection rate) and timing jitter.

With a few notable exceptions [103–105], both APD based and SNSPD based single photon detectors are threshold detectors. Then, the detector output is binary and distinguishes between “zero” or “one or more photons”.

Avalanche photodiodes

In an APD, an absorbed photon creates an electron-hole pair. If an electric field is present, the electron and the hole will propagate in opposite directions, and in the case of a sufficiently large electric field, the particles can generate energies larger than the ionization energy of semiconductor. Then, a collision with the lattice causes more electron-hole pairs, and in total an avalanche of charge carriers. Therefore, by applying a sufficiently large bias voltage V_{APD} across the APD, the absorption of a single photon is amplified to a large macroscopic current.

When the APD is (reversely) biased above the breakdown voltage V_{br} in the Geiger mode, the current caused by an avalanche is self-sustained. To reset the APD, the voltage of the APD is reduced below the breakdown voltage, such that the avalanche stops. This is called quenching [106]. It can be done passively, where the current trough the APD lowers the voltage, or actively, where an external circuit forces the voltage down after an avalanche. Gating the APDs can be seen as a special case of active quenching, where the voltage is reduced periodically regardless of the presence of an avalanche. Figure 4.1 shows the bias operation of the APD.

For light in the 400–1000 nm range, silicon APDs can be used [100]. They typically have a detection efficiency of around 50%, and a dark count rate of about 100 Hz. Furthermore, their dead time allows count rates up to at least 10 MHz. Typical jitter is 350 ps FWHM for thick APDs optimized for longer wavelengths, 50 ps FWHM for thinner ones with peak sensitivity around 500 nm [100].

With fiber-based QKD, the 1550 nm wavelength is the most interesting due to the low loss at this wavelength. While it is possible to use silicon APDs combined with up-conversion [107], InGaAs/InP heterostructure APDs are usually used at this wavelength. The drawback of these composite semiconductor devices is that they have more impurities, resulting in higher dark count rates. Therefore, they are only biased to the Geiger mode when a photon is expected, in so-called *gates* (see Figure 4.2).

The temperature is an important parameter for the APD. At a lower temperature, the dark count probability is reduced. However, during an avalanche carriers

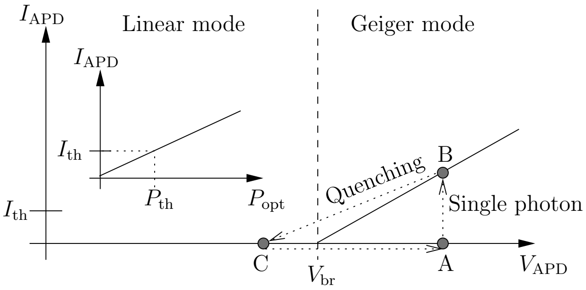


Figure 4.1: The operating principles of an APD. First the APD is biased at a point (A) above the breakdown voltage V_{br}. When a single photon arrives, it causes an electron-hole pair which amplifies to a macroscopic current (B). A photon arrival is signaled when the current exceeds the comparator threshold I_{th}. Afterwards, the current is stopped through quenching (C), before the voltage is brought back above the breakdown voltage again. For a bias below the breakdown voltage, the current through the APD depends linearly on the optical power incident on the APD.

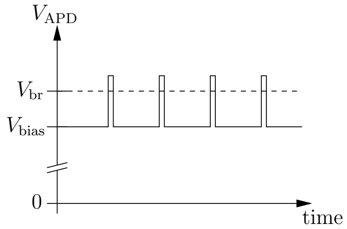


Figure 4.2: Gating an APD to reduce dark counts. When the APD is gated, the voltage at the APD is only above the breakdown voltage at times when a photon is expected.

are trapped in impurities in the semiconductor. If a gate is applied a short time after an avalanche, there is a high dark count probability due to decay of trapped carries. This is called an afterpulse. At a lower temperature, it takes a longer time for the trapped carries to decay, and therefore low temperature effectively reduces the gate repetition rate. There is an intermediate solution: the gates are applied at a high repetition rate, but a number of gates is removed after a detection event, so-called afterpulse blocking [108]. For example, Clavis2 QKD system by manufacturer ID Quantique uses a pair of InGaAs/InP APDs. They are cooled to −50 °C, and about 3 ns long gates are applied at a frequency of 5 MHz. Their quantum

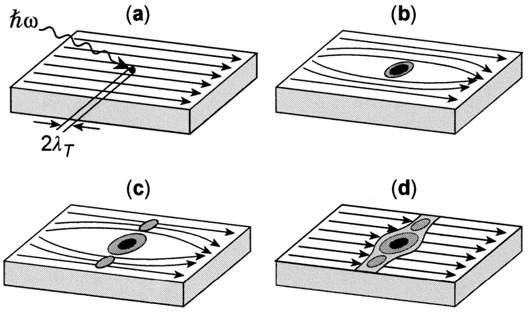


Figure 4.3: Single photon detection using a superconducting nanowire. (a) A photon is absorbed in the superconducting nanowire, and causes a normally conducting hot-spot. (b) The bias current circumvents the hot-spot, increasing the current density outside the hot-spot. (c) The current density on each side of the hot-spot exceeds the critical current density, and a larger piece of the cross-section is now normally conductive. (d) The normally resistive region covers a whole cross-section of the nanowire, which now has a non-zero resistance. Reprinted from Reference [113], ©2003 IEEE.

efficiency is about 10%. After a detection event, 50 gates are removed from both APDs, corresponding to a deadtime of 10 μs, effectively limiting the count rate to less than 100 kHz. The timing jitter for these detectors is about 500 ps FWHM, although the system only registers timing as the gate number.

Faster APD based detectors have been developed using rapid gating techniques [109–112]. These detectors use very short gates, and bias the APD only slightly above the breakdown voltage in the gate. Therefore, the current in the avalanche, and thus afterpulses are significantly reduced. They also use more sophisticated comparator techniques, some of which give photon-number resolving capabilities [103].

Superconducting nanowire single photon detectors

A SNSPD [101, 102] consists of a superconducting nanowire, typically shaped to fill a square in order to achieve good coupling between the optical fiber and the nanowire. During operation, the nanowire must be cooled to the superconducting state, typically at a temperature of about 4 K. Then, it is biased with a current I_b slightly lower than the critical current I_c where nanowire goes normally conductive. Note that since the nanowire is superconducting, there is no voltage drop across it. When a photon is absorbed by the nanowire, it causes a normally conductive hot-spot (see Figure 4.3). This reduces the superconducting cross-section of the nanowire, such that the current density in the rest of the cross-section increases, and exceeds the critical current density. Then, the whole cross-section goes normally resistive, which makes the voltage over the nanowire increase. Afterwards, the current drops, the nanowire cools back to the superconducting state, and the current rises to the original value making the detector ready for the next photon.

The longest-distance experiments [26, 114–116] use SNSPDs, due to their low dark count rates ($< 1\,\text{Hz}$) and low timing jitter ($< 60\,\text{ps}$ FWHM). The deadtime is typically 10 ns, and the quantum efficiency is typically in the order of 1%. However, using an integrated optical cavity, a quantum efficiency of 57% has been reported [117].

4.2 System architectures

4.2.1 Polarization encoding

Polarization encoding was used in the first experimental QKD system [24]. Alice used a laser and two Pockels cells to generate the four different states in the BB84 protocol. The quantum channel was 32 cm free space. Bob's receiver consisted of a Pockels cell to select the basis, followed by a polarizing beam splitter and two photomultiplier tubes. There is one important remark about this implementation: Alice's and Bob's bit and basis choice must be applied to the Pockels cells. This is called *active basis choice*: true random numbers must be input to the apparatuses.

Generating a sufficient amount of random numbers is challenging. True quantum random number generators[1] still have a bit rate less than 100 Mbit/s [120, 121][2]. Therefore, *passive basis choice* implementations were invented [124], with one example in Figure 4.4. In a passive basis choice BB84 implementation, a beam splitter is used to randomly choose the basis: the single photon can only take one of the exits of the beam splitter. Since one of the exits contains the X basis measurement, and the other contains the Z basis measurement, this results in a random basis choice. In passive basis choice implementations, Bob cannot verify that the basis choice was random. Therefore, passive basis choice offers a lower level of security than active basis choice. I will use the term passive not only for BB84, but for all implementations where Bob does not input any randomness into his measurement device.

[1] There are quantum random number schemes, which are faster, but contain a mixture of quantum and chaotic randomness [118, 119].

[2] An natural question is: how can one verify that a sequence of numbers is truly random? The answer is that this is impossible for a finite sequence of numbers, because this sequence could always repeat itself [122]. Interestingly, quantum physics offers not only a technique to generate random numbers (single photon source followed by a 50/50 beam splitter and two detectors), but also, a way to verify that the numbers are truly random [122, 123].

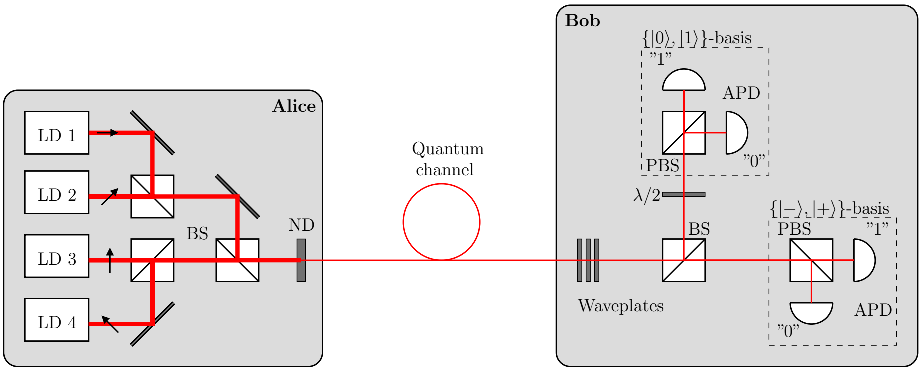


Figure 4.4: A polarization encoded implementation with passive basis choice. Alice randomly fires one of the four laser diodes before reducing the energy of the pulse to the single photon level. Bob must use waveplates in order to revert the transformation by the quantum channel. A beam splitter (BS) is used to randomly select the basis at Bob's side. LD: laser diode; ND: neutral density filter (attenuator); PBS: polarizing beam splitter; $\lambda/2$: half-wave plate; APD: avalanche photodiode.

After the initial demonstration [24], distances increased to 1 km [125], and later to 23 km in an existing fiber under lake Geneva [25]. The experiments revealed that the depolarization in the fiber is a challenge. In contrast, free-space has negligible impact on the polarization. Therefore, polarization encoding has been used in several free-space experiments [27, 126–128].

4.2.2 Phase encoding

It was quickly realized [23, 129] that in optical fibers, the phase of the photon is stable, and therefore suitable for encoding the qubit state. Figure 4.5 shows an example of a phase encoded implementation, consisting of a large Mach-Zehnder interferometer where Alice and Bob controls the phase shift in each arm. Alice selects the bit and basis by applying one out of four random phase shifts $\varphi_A \in \{0,\pi/2,\pi,3\pi/2\}$ to her phase modulator. The quantum channel consists of two optical fibers between Alice and Bob. Bob randomly selects one out of two phase shifts $\varphi_B \in \{0, \pi/2\}$ to select between the two bases. If the phase difference $\varphi_A - \varphi_B$ is equal to 0 or π, the photon will be detected deterministically at a single output from Bob's fiber coupler. If $\varphi_A - \varphi_B$ is equal to $\pi/2$ or $3\pi/2$, the photon will be detected at a random output. This is summarized in Table 4.1. From the table, it is easy to realize that a phase encoded system is topologically

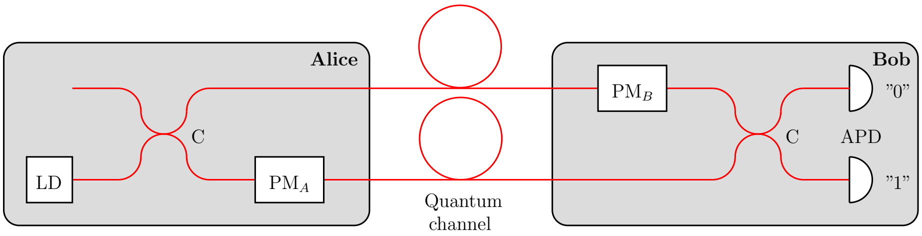


Figure 4.5: A phase encoded implementation using active basis choice. Alice randomly chooses a phase shift $\varphi_A \in \{0,\pi/2,\pi,3\pi/2\}$ to encode one of the four states. Bob randomly chooses a phase shift $\varphi_B \in \{0,\pi/2\}$ to select his measurement basis. This setup is topologically equal to the polarization encoded system in Figure 4.4. LD: laser diode; C: fiber-optic coupler; PM$_A$: Alice's phase modulator; PM$_B$: Bob's phase modulator; APD: avalanche photodiode.

Alice bit	Alice basis	φ_A	Bob basis	φ_B	$\varphi_A - \varphi_B$	Bob measurement
0	Z	0	Z	0	0	0
0	Z	0	X	$\pi/2$	$-\pi/2$	?
0	X	$\pi/2$	Z	0	$\pi/2$	?
0	X	$\pi/2$	X	$\pi/2$	0	0
1	Z	π	Z	0	π	1
1	Z	π	X	$\pi/2$	$\pi/2$	?
1	X	$3\pi/2$	Z	0	$3\pi/2$	?
1	X	$3\pi/2$	X	$\pi/2$	π	1

Table 4.1: The relation between Alice's and Bob's bit and basis choices, Bob's measurement result and the settings of the phase modulators in an interferometric implementation.

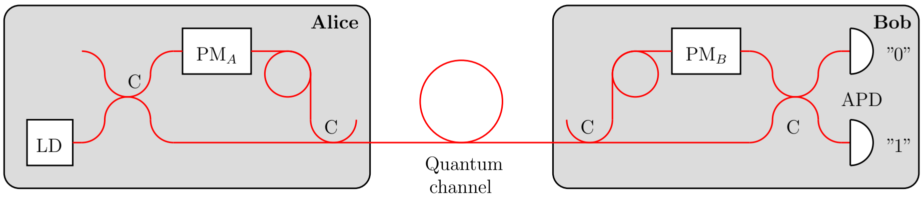


Figure 4.6: An active basis choice phase encoded implementation, using two asymmetric Mach-Zehnder interferometers. Alice randomly chooses a phase shift $\varphi_A \in \{0,\pi/2,\pi,3\pi/2\}$ to encode one of four states. Bob randomly chooses a phase shift $\varphi_B \in \{0,\pi/2\}$ to select measurement basis. LD: laser diode; C: fiber-optic coupler; PM$_A$: Alice's phase modulator; PM$_B$: Bob's phase modulator; APD: avalanche photodiode.

equal to a polarization encoded system.

The implementation as shown in Figure 4.5 is impractical. Optical fibers are expensive, so two fibers would double the bill. More importantly, it would be a tremendous challenge to keep such a long interferometer stable. There is however a way to transport the modes of both fibers through a single fiber by using an asymmetric interferometer to time-multiplex them into two pulses. Then the two pulses are split in another asymmetric interferometer at Bob. Figure 4.6 shows an implementation using two Mach-Zehnder interferometers, but note that there are also implementations based on Faraday-Michelson interferometers [130].

Despite this configuration being tremendously more stable than the one in Figure 4.5, still the main challenge of the double interferometer architecture is to keep the interferometers balanced: after alignment they usually only stay balanced for minutes [131]. Therefore, tracking methods have been developed [108, 132]. This double interferometer architecture has been used in numerous experiments, including an experimental QKD system producing over 1 Mbit/s secret key rate over 50 km [133].

4.2.3 Plug-and-play architecture

As mentioned, the main challenge in an interferometric implementation is phase drift in the interferometers. However, there is a beautiful solution to the problem. In plug-and-play systems (see Figure 4.7), the pulses are first passing through Bob's interferometer as bright pulses, and are sent from Bob to Alice. Alice uses her phase modulator to encode the bit and basis choice, and uses a Faraday mirror [134] to send the pulses back to Bob. The pulses are attenuated to single photon

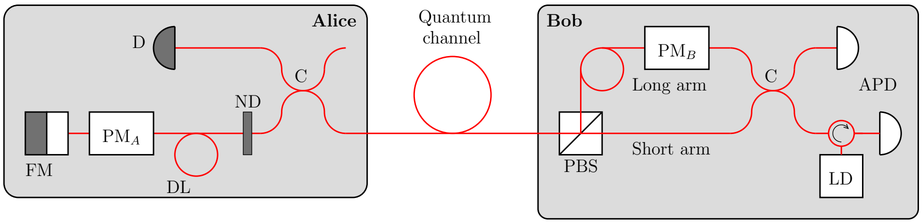


Figure 4.7: A plug-and-play QKD system. The laser in Bob sends a train of pulses through his interferometer without activating his phase modulator (PM$_B$). The pulses travel to Alice, where a classical detector (D) is used to synchronize Alice's phase modulator (PM$_A$) to one of the two pulses from Bob's interferometer. An optical delay line (DL) is used to store the whole train of pulses to avoid Raileigh backscattering hitting Bob's detectors. Upon return, the pulses travel through the opposite arms of the interferometer thereby automatically compensating drift in the interferometer. FM: Faraday mirror; C: fiber-optic coupler; ND: neutral density filter (attenuator); PBS: polarizing beam splitter; APD: avalanche photodiode.

level at the exit of Alice's system. Using this design, the birefringence (i.e. polarization transformation) of the fiber is reverted when the photon travels back to Bob. Furthermore, the polarization is exploited to make the photon travel the opposite arm in Bob's interferometer when it returns. Given that the interferometer is stable for the round trip time of the photon, phase drift in the interferometer is automatically compensated. Therefore, this is called the plug-and-play architecture: it works on any uncharacterized[3], previously deployed fiber. Since the pulses are sent from Bob to Alice and back to Bob again, this is also often referred to as a send-return system. Although this allows Eve to tamper with the signals before they enter Alice's system, including this in the model of Alice shows that it barely reduces the key rate [135].

There have been many QKD experiments using the plug-and-play systems [136–138]. In fact it is the architecture used in several commercial systems, such as the QKD systems from ID Quantique (see Figure 4.8) and the QPN 5505 by MagiQ Technologies. In the SwissQuantum QKD network (see Figure 4.9), three links from ID Quantique ran autonomously from April 2009 to January 2011, thus the plug-and-play architecture seems to be very stable.

[3] The loss of the fiber must be upper bounded to calculate the secure key rate, but this should be possible with the knowledge of the length and type of fiber.

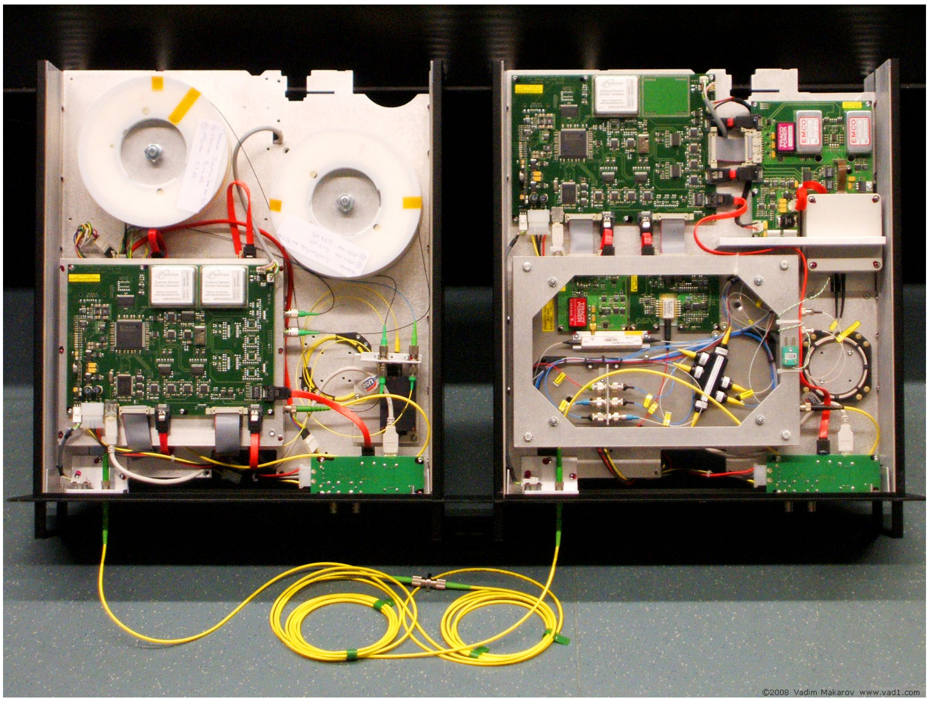


Figure 4.8: Clavis2, a research QKD system by commercial vendor ID Quantique. This system is an implementation of the plug-and-play architecture presented in Figure 4.7. Alice is at the left while Bob is at the right. Printed with permission from ID Quantique. Photo ©2008 Vadim Makarov.

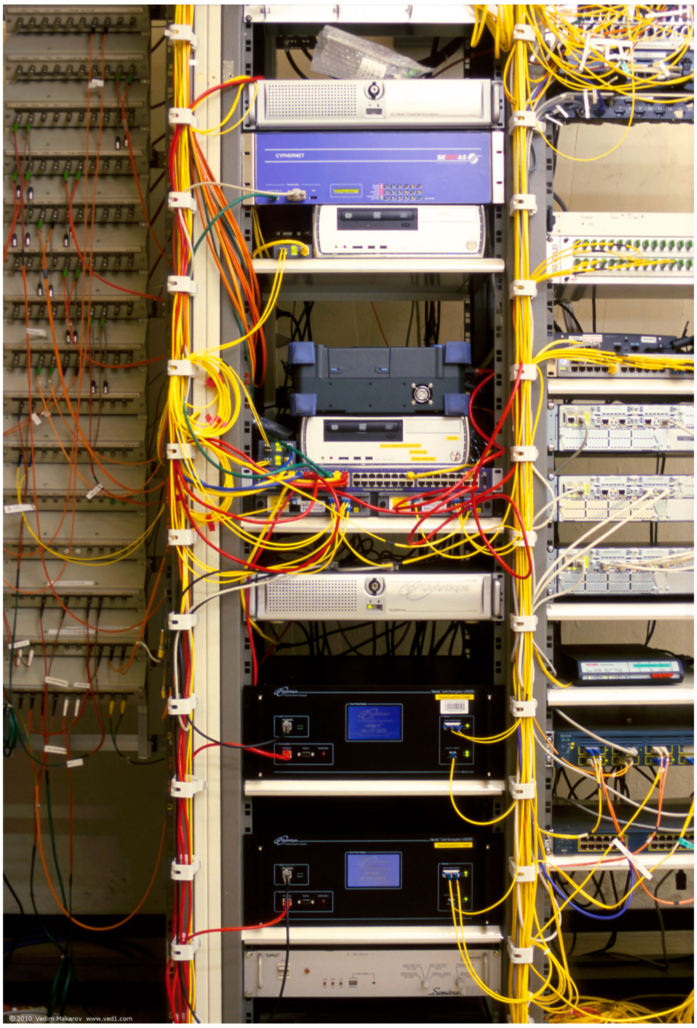


Figure 4.9: The node located at the University of Geneva (UNIGE) in the SwissQuantum network. The bottom of the rack contains two commercial Vectis QKD systems by ID Quantique, each connected to different nodes through pairs of fibers (one dark fiber for faint pulses and synchronization data, classical post-processing and encrypted data on another). The node also contains a key management server, and several different classical encryptors which use the secret key generated by the QKD systems. Photo by ©2010 Vadim Makarov.

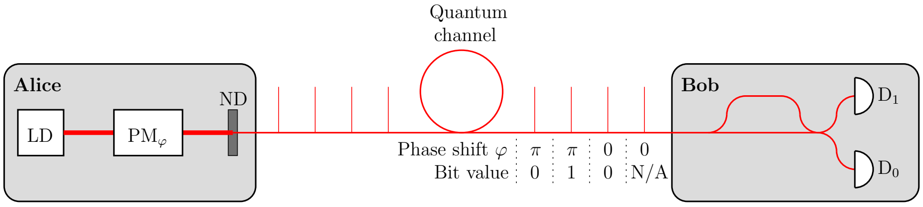


Figure 4.10: An implementation of the DPS protocol. Alice consists of a laser source (LD), followed by a phase modulator (PM$_\varphi$). The bit values of the key are encoded into the phase difference between two consecutive pulses: 0 (π) phase difference corresponds to the bit value 0 (1). Bob consists of an asymmetric interferometer, with the length difference of the two arms corresponding to the length difference between two pulses sent by Alice. The figure shows an example of bit values coded into the pulse train. Note that the phase shifts must be read from right to left according to the pulse's arrival to Bob. ND: neutral density filter (attenuator); D$_{0/1}$: single photon detector for the bit value 0/1.

4.2.4 Distributed-phase-reference protocols

While some protocols have been motivated by increased security in practical implementations, others have been motivated by a simpler implementation. This is the case for the distributed-phase-reference protocols such as the differential phase shift (DPS) protocol [139, 140] and the coherent one way protocol (COW) [141, 142]. Note that although numerous restricted attacks have been studied on these protocols [143–146], there are no security proofs providing lower bounds on the secret key rate for these protocols. Therefore, it is difficult to compare their performance against discrete variable protocols[4].

Differential phase shift protocol

Figure 4.10 shows the implementation of the DPS protocol [140]. In this protocol, Alice emits a train of weak coherent pulses, each with a mean photon number less than one. The secret key is encoded in the phase difference between two pulses: 0 (π) phase difference corresponds to the bit value 0 (1). Bob detects the pulse train using an asymmetric interferometer, with the length difference in the two arms corresponding to the length difference between two pulses sent by Alice. After detecting a train of pulses, Bob will publicly announce his detection times. Then Alice knows which of Bob's detectors have clicked, and thus which bit value Bob

[4] Reference [16] contains a comparison using different security levels for different protocols.

must have detected for each pulse.

The DPS protocol has a passive Bob, so Eve may use a copy of Bob to obtain valid detection results. However, it is impossible for Eve to generate the same detections in Bob without causing errors. Since the mean photon number in each pulse is less than 1, there will be bit slots without a detection event. Imagine that Eve wants to cause a click in detector 0 at Bob. She can do this by sending two pulses with 0 phase difference. For these two pulses to interfere and cause a detection event in detector 0, the first pulse must enter the long arm and the second pulse must enter the short arm of Bob's interferometer. However, the pulses don't necessarily interfere: the first pulse may take the short arm, and/or the second pulse may take the long arm. This causes random detections at Bob, and thus errors in the key.

The DPS protocol is tailored for an easy implementation and a high key rate. For instance, compared to BB84, one does not have to discard half the key owing to different basis choices. The DPS protocol has been used in several long-distance experiments with various types of detectors [114, 147, 148].

Coherent one way protocol

Figure 4.11 shows the implementation of the COW protocol [141, 142]. Alice sends a train of pulses which will be grouped in pairs to encode the key. The position of the pulse within a pair encodes the bit value of the key. Bob simply measures the position of the pulse within a pair to determine the bit value. However, this alone does not provide any security against an eavesdropper. Therefore, an asymmetric interferometer followed by two monitoring detectors is coupled into the data line with coupling ratio $1 - t_B$. A typical value of t_B is 0.9. This interferometer is tailored to reveal eavesdropping attempts. Alice will occasionally send two adjacent pulses (for instance sending the bit value 1 followed by the bit value 0, or she might simply insert a decoy state, leaving a pulse in both slots of the pair), and then this monitoring measurement setup is equal to Bob's measurement setup in the DPS protocol. As described for the DPS protocol, Eve cannot fully control the detections in the monitoring detectors, and therefore any eavesdropping attempt will be revealed by additional clicks in monitoring detector 1 (DM_1).

Compared to the DPS protocol, the COW protocol uses two pulses per bit instead of one, so double the pulse repetition rate is needed for the same raw key rate. Still, the COW protocol has been used in a very long distance experiment, with a transmission distance over 250 km [26]. A COW implementation was also part of the SECOQC quantum key distribution network in Vienna [149].

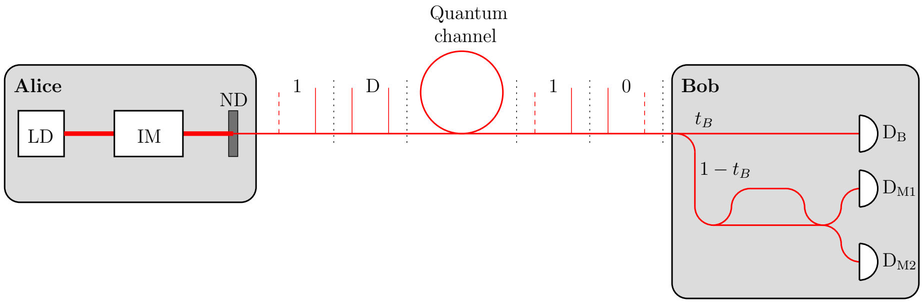


Figure 4.11: An implementation of the COW protocol. Alice consists of a laser source (LD), followed by an intensity modulator (IM). Similarly to the DPS protocol, Alice sends a train of pulses. In the COW protocol, the pulses are paired to encode the bits of the key. The position of the pulse within the pair determines the bit value. Additionally, Alice can send pulses in both slots of a pair as decoys (denoted as "D" in the figure) to measure the coherence of the channel. Bob consists of a fiber-optic coupler or beam splitter with splitting ratio $t_B : (1 - t_B)$, followed by a data detector ($\mathrm{D_B}$), used to measure the key. The other exit of the coupler is followed by an asymmetric interferometer to monitor the coherence of the channel, with a length difference equal to the length difference between two pulses sent by Alice. The figure shows an example of bit values coded into the pulse train. ND: neutral density filter (attenuator); $\mathrm{D_{M1/2}}$: monitoring detectors.

4.3 QKD networks

There are different approaches to create quantum networks, some of which have been implemented. In one approach, optical switches are used to connect the quantum channels of the different parties [150]. This does not increase the transmission distance, but rather decreases it since the optical switches introduce loss. A quantum router has also been proposed [151], based on wavelength division multiplexing. Then, each node is assigned to a wavelength. This makes it possible to connect all nodes with each other.

In a different approach, networks use trusted nodes [149, 152–154]. This does increase the transmission distance, since a trusted node can be used as a trusted repeater. There is already a proposal to use a satellite orbiting the earth as a trusted node [155]. Note however, that two nodes in this type of network must trust the nodes between them in order to communicate securely. Still, this type of network might be suitable for instance for companies which own buildings spaced suitably apart.

There is also an example of a combination, with parts of the network using optical switches, and parts of the network using trusted nodes [156].

Chapter 5

Practical security

In this chapter, the practical security of QKD systems is reviewed. In particular, a number of known attacks are reviewed as well as assumptions about the devices in the security proofs. There are some implicit assumptions in QKD [16, 67]:

a) The information that leaves Alice's and Bob's system is restricted to what the protocol allows.

b) Random numbers originate from true random number sources.

c) Alice and Bob use unconditionally secure authentication on the classical channel (such schemes exist, for instance Wegman-Carter authentication [157, 158]).

d) Eve must obey the laws of quantum physics.

5.1 Finite key length

Most security proofs consider the secret key rate in the asymptotic limit of an infinitely long key. Then, neither the error correcting code nor the privacy amplification has overhead. Practical systems however, can only perform post-processing (sifting, error correction and privacy amplification) on finite blocks of bits. There have been several investigations of finite key length QKD [159–161] with perfect devices. The latest results show that in order to obtain 50% of the asymptotic key rate, a block size of 10^6 bits is required [161], using a reasonable security parameter $\epsilon = 10^{-14}$. This is an interesting result. Very few QKD implementations have the key rate necessary to generate 10^6 bits in reasonable time at a useful distance. Therefore, only the highest key rate QKD systems have been reported incorporating finite key effects [133, 162, 163].

5.2 Photon-number splitting attack

As discussed in Section 4.1.1, most sources are not really single photon sources: some pulses contain multiple photons. This enables Eve to perform the photon-number splitting (PNS) attack [39]: Eve measures the number of photons in the pulse from Alice. This is a non-demolition measurement in the sense that it does not disturb the polarization or the phase of the photon(s). If the pulse contains more than one photon, she keeps one photon for herself, passing on at least one photon to Bob. If it contains a single photon, she does not send anything to Bob. When Bob announces his measurement bases, Eve measures her photons in the same bases to obtain identical measurement results. This gives Eve a perfect copy of the key. Note that it is not known how to implement the non-demolition photon-number measurement with current technology.

In this attack, Eve introduces loss. However, as discussed in Section 4.1.2 the channel is always lossy, so Eve can replace the channel by a lossless channel, and remove a fraction of pulses corresponding to the original loss. Let us do some napkin-math to see how the PNS attack upper bounds the key rate according to the transmission of the channel, when the source emits coherent states with mean photon number μ per pulse (a full derivation can be found for instance in References [33, 34, 40]). For a coherent state, the number of photons per pulse n is Poisson distributed:

$$p_n = \frac{\mu^n e^{-\mu}}{n!}. \tag{5.1}$$

The probability that the pulse contains a photon at all is given by

$$p_{n>0} = 1 - p_0 = 1 - e^{-\mu} \approx \mu, \tag{5.2}$$

for small μ. The probability that the pulse contains more than one photon is given by

$$p_{n>1} = 1 - p_1 - p_0 = 1 - \mu e^{-\mu} - e^{-\mu} \approx \frac{\mu^2}{2}. \tag{5.3}$$

Let us assume that Bob has perfect detectors, and that the channel transmission is given by t. Since the probability that the pulse contains at least one photon is given by μ, the detection probability at Bob is approximately given by $t\mu$. But we must assume that Eve knows the value of all the $\mu^2/2$ pulses containing multiple photons. Therefore, a simplified expression for the rate is given by

$$R = t\mu - \frac{\mu^2}{2}. \tag{5.4}$$

Optimizing μ to maximize R gives $\mu = t$, thus the rate scales as $R \propto t^2$ (as opposed to $R \propto t$ for a perfect single photon source). In practice, due to the errors caused by dark counts, R cannot be arbitrarily small. Therefore, the maximum transmission distance is substantially reduced by the threat of the PNS attack. Therefore, the frequent use of coherent sources in QKD caused a search for new protocols which were resistant to the PNS attack.

5.2.1 Scarani-Acín-Ribordy-Gisin 2004 protocol

The Scarani-Acín-Ribordy-Gisin 2004 (SARG04) protocol [42] is tailored to be robust against the PNS attack. For the raw key exchange, the protocol is identical to the BB84 protocol presented in Section 2.1. The difference is in the post-processing. In the SARG04 protocol, the key bit is encoded in the basis choice of Alice. Instead of announcing the basis, Alice announces a set of two states: the state she sent and a random state from the opposite basis. When Bob selects the opposite basis from Alice, he can have an unambiguous detection event such that he deterministically knows which of the two states Alice sent, and thus which basis she used.

Let the Z basis ($= \{0\rangle, |1\rangle\}$) represent bit value 0, and the X basis ($= \{-\rangle, |+\rangle\}$) represent bit value 1. Assume that Alice sent $|0\rangle$ (bit value 0) and announced $\{|0\rangle, |-\rangle\}$. If Bob measured in the Z basis he must have obtained the measurement result $|0\rangle$. However, the bit must be discarded since this result could have been caused by any of the states announced by Alice. Again, if Bob measured in the X basis and obtained the measurement result $|-\rangle$, the bit must be discarded. If Bob measured in the X basis and obtained the measurement result $|+\rangle$, this could only result from Alice sending $|0\rangle$. Therefore, Bob adds the bit value 0 to the key. Note that Bob does not announce his basis choice. In fact, Bob's basis choice contains the value of the key (Bob's basis is always the opposite from Alice's for unambiguous detection results).

To see why the SARG04 protocol is more resistant to the PNS attack than the BB84 protocol, assume that Eve has a copy of Bob's photon and the announcement from Alice. Eve's task is to use the photon to distinguish between the two non-orthogonal states. But it is impossible to perfectly distinguish between two non-orthogonal states. Therefore, the two photon states emitted by Alice do not always reveal the bit value.

In the SARG04 protocol, the probability that Bob has an unambiguous measurement result is 1/4, compared to 1/2 for the BB84 protocol. Still, the SARG04 protocol gives a higher bit rate at low channel transmittances, because the mean photon number in the coherent pulse can be much higher than for BB84. For an optimal mean photon number, one can show that the key rate scales with the transmittance as $R \propto t^{3/2}$ [16, 164].

5.2.2 Decoy states protocol

Another discovery countering the PNS attack is the decoy states protocol [43–45]. The difference between the original BB84 protocol and the decoy states protocol, is that in the decoy states protocol the photon number mixture of the source is varied[1] in order to estimate the fraction of detections at Bob, where Alice emitted single photons. In practice, an intensity modulator is added to Alice's setup, and Alice emits coherent states of various mean photon number. If an infinite number of intensities is used, Alice and Bob can obtain a perfect estimate of the single photon transmittance and error rate [45]. In practice, Alice usually emits signal states with mean photon number $\mu_s \approx 1$, and two different decoy states, one with a very low photon number $\mu_{d1} = \mu_d < 1$ and one which is vacuum $\mu_{d2} = \mu_v = 0$ [165].

The decoy states protocol fully negates the PNS attack, since Alice and Bob lower-bound the single photon transmittance, and upper-bound the error rate for single photons emitted by Alice. Since the probability that a single photon will pass the channel is given by the transmittance t, the rate scales as $R \propto t$. When the decoy states protocl was implemented for the 144 km free-space link between La Palma and Tenerife, the key rate increased one order of magnitude [27, 128]!

The decoy states protocol can be considered an as auxiliary protocol on top of the BB84 protocol, providing the transmittance and the error rate for single photons emitted by Alice. Therefore, other security proofs for the BB84 protocol simply assume that these parameters are available [87][**166**].

5.3 Trojan-horse attack

In the Trojan-horse attack [47, 48], Eve uses a powerful laser to interrogate the system of Alice and/or Bob. In particular, it turns out that the back-reflections passing the phase modulator in a phase encoded implementation reveal the setting of the phase modulator. In Alice's system, the phase modulator setting contains the bit and basis value. Therefore, this setting must be kept secret. Most implementations of Alice contain an attenuator at the exit of Alice's system, to attenuate brighter pulses to the single photon level. The same attenuation would apply twice to Eve's pulse in the Trojan-horse attack (one time when the pulse enters Alice's system, and one time on the reflected pulse). Therefore, the Trojan-horse attack can be countered by having sufficient attenuation at Alice's exit: then the required power in Eve's laser would destroy the optical fiber [47].

In a BB84 implementation, Bob's phase modulator setting contains the basis.

[1] In particular, the probability distributions of the photon number must be linearly independent. This is the case for coherent states of various mean photon number.

This is publicly announced, so protecting it is not crucial[2]. However, if the four-state Bob patch is used to counter the detector efficiency mismatch loophole (see Section 5.5), Bob's phase modulator setting must remain secret. Also, in the SARG04 protocol (see Section 5.2.1), the basis value is the key bit, and therefore Bob's phase modulator setting contains the secret key.

It is more difficult to avoid the Trojan-horse attack on Bob's apparatus [47]. An attenuator would consume most of the precious single photons from Alice. One solution could be a narrow bandpass filter and a circulator followed by a detector to measure the optical power exiting Bob's apparatus. In a plug-and-play system (see Section 4.2.3) this is difficult because Bob's entrance must remain bi-directional. Another solution could be a beam splitter and a power meter at Bob's entrance. However, if the security of a scheme is based partly on the output of a power meter in Bob's system, the output of this power meter must be included in the assumptions of the security proofs for the system.

5.4 Phase-remapping attack

In the plug-and-play system (see Section 4.2.3), Bob emits pulses which are sent to Alice, where Alice encodes her bit and basis choice by phase modulating one of the two pulses from Bob. However, there are two hatches in this scheme: 1) Eve could mess with the pulses before they enter Alice's system; 2) Alice's phase modulator does not switch infinitely fast between the different values. Eve could change the intensity and/or the photon number statistics of the pulse entering Alice, but this has been considered in security proofs [135]. However, the finite switching speed of Alice's phase modulator makes the encoding process dependent on the timing of the pulses. Therefore, in the phase-remapping attack [52], Eve adjusts the timing of the pulses from Bob such that they are phase shifted less than the value selected by Alice. Specifically, instead of a $\{0, \pi/2, \pi, 3\pi/2\}$ phase shift, the pulses get a $\{0, \delta, 2\delta, 3\delta\}$ phase shift. Then, Eve can intercept the pulse from Alice and better distinguish between the four phase settings. Therefore, she introduces less QBER when resending to Bob. In the limit where $\delta \to 0$, the phase-remapping attack introduces 14.6% QBER.

The phase-remapping attack has been implemented on a commercial QKD system [56]. Since it is an intercept-resend attack, Eve has full information about the secret key. The attack introduced a QBER of 19.7%, which is above the theoretical 11% limit for perfect devices. Still, there are protocols which allow a QBER up to 20% [79, 167] (with perfect devices), although they have not been implemented.

[2] Note however that it is crucial that Eve does not know the basis value *before* Alice's pulse enters Bob's apparatus. This can be ensured by a sufficiently long delay line at Bob's entrance.

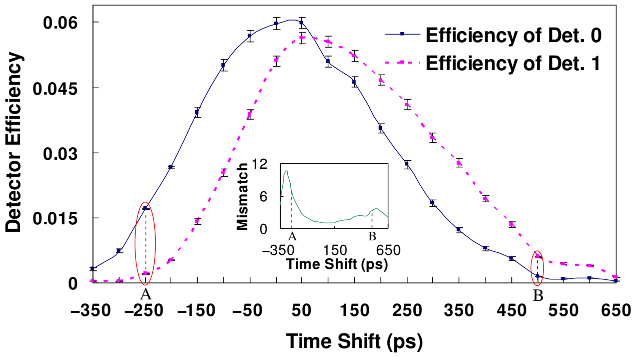


Figure 5.1: The detector efficiency curves for a commercial QKD system from ID Quantique. The points 'A' and 'B' shows the two timings referred to as t_0 and t_1, where the subscript refers to the detector that is much more efficient than the other. Reprinted from Reference [53], ©2008 The American Physical Society.

5.5 Detector efficiency mismatch

As discussed in Section 4.1.3, APD-based single photon detectors are usually gated in order to reduce dark counts. Since QKD systems require the detection of two different bit values, they require at least two detectors[3]. Then it is unavoidable that finite manufacturing precision in the detector and the electronics, and difference in optical path length will slightly misalign the two detector gates, and cause detector efficiency mismatch [49]. This is the case for the QKD systems from the commercial producer ID Quantique [53][**168**]. Figure 5.1 shows the measured detector efficiency curves for a well-designed commercial QKD system [53]. Furthermore, the calibration routine of a commercial QKD system can be tricked into setting a large detector efficiency mismatch [**168**].

When a QKD system has detector efficiency mismatch, the system can be attacked with the following faked-state attack [49, 169]: Eve measures the state from Alice in a random basis to obtain a measurement result. Then, she resends the opposite bit value from her measurement result in the opposite basis, timed to arrive at Bob's detectors when the detector corresponding to her measurement result has much higher detection efficiency than the other detector. As an example, if Eve measured the bit value 0 in the X basis, she would resend the bit value 1 in the Z basis, timed to arrive at t_0 (corresponding to timing A in Figure 5.1). Since the attack is an intercept-resend attack, Eve has full information about the key.

[3] It is possible to time-multiplex using a single detector, but that will not avoid detector efficiency mismatch due to the finite precision of the time-multiplexing.

Eve will however introduce a non-zero QBER. Let $\eta_0(t)$ ($\eta_1(t)$) be the efficiency curve of detector 0 (1). Let

$$\eta = \min_t \left\{ \frac{\eta_0(t)}{\eta_1(t)}, \frac{\eta_1(t)}{\eta_0(t)} \right\}, \tag{5.5}$$

where t labels the various modes, for instance the different temporal modes. Then Eve introduces less than 11% QBER if $\eta \leq 0.066$ [49]. However, Eve can launch the time-shift attack and the optimal individual attack simultaneously. Then, the information obtained from the time-shift attack can be used to improve the measurements of her probes. If $\eta \leq 0.25$, this combined attack gives Eve full information about the key while the QBER is kept below 11% [**166**]. The faked-state attack also applies to the SARG04, DPS and Ekert protocols [170].

The *time-shift attack* [50] is based on detector efficiency mismatch. In this attack, Eve randomly times the pulse from Alice to arrive at t_0 or t_1 in Bob. This partly reveals the bit value: if the pulse arrived at t_0 (t_1), and Bob announces receipt, the bit value is more likely to be 0 (1). In contrast to the faked-state attack [49], Eve does not get the full secret key. However, the time-shift attack has a very simple implementation, and does not introduce any extra QBER. The vulnerability was confirmed in a commercial QKD system [53]. In the experiment, Eve got an information-theoretical advantage in about 4% of her attempts. When Eve has an information-theoretical advantage, she may outperform a straight brute-force search for the secret key. In the time-shift experiment [53], the entropy of the 1297-bit key was reduced to 2^{1131}. If this key is used for the one-time pad, the decrease in entropy tremendously decreases the required computational power required to decrypt the message. On one hand, such a computational task is unfeasible now and for the foreseeable future. On the other hand, if we could trust computationally-bounded security, why use QKD? Also, by the security definition in Section 3.2, the security is clearly broken.

A frequently mentioned countermeasure against detector efficiency mismatch is four-state Bob [49, 50, 78]. In a phase-encoded implementation using four-state Bob, Bob randomly selects from four different phase modulator settings $\{0, \pi/2, \pi, 3\pi/2\}$ instead of only the usual two $\{0, \pi/2\}$. The extra π phase shift randomly maps the bit values 0 and 1 to the two detectors. QKD using four-state Bob has been proven secure if Bob only receives single photons [171]. The assumption that Bob only receives single photons is clearly unrealistic, but a decoy-detector scheme similar to decoy-states (see Section 5.2.2) can be used to estimate the fraction of single photons received by Bob [172].

There are however some drawbacks with the four-state Bob scheme. First of all, the phase-modulator value must now remain secret, and therefore Bob's system must be secured against the Trojan-horse attack. As discussed in Section 5.3, this is a difficult task. Also, the four-state Bob scheme does not secure against tailored bright illumination attacks [55][**57,60**], and in particular not against the after-gate attack [**173, 174**].

In another approach, the amount of privacy amplification necessary to remove Eve's knowledge about the key is quantified. There has so far not been found a squash model [74–77] working in the presence of detector efficiency mismatch, therefore existing security proofs using single qubits do not apply to systems having detector efficiency mismatch. However, there are several security proofs for QKD systems with detector efficiency mismatch [**41, 166**][171]. In the most general proof, with symmetry between the bases and with a perfect source, the secret key rate is given by [**41**]

$$R \geq -h(\mathrm{QBER}) + \eta(1 - h(\mathrm{QBER}), \tag{5.6}$$

where $h(\,\cdot\,)$ is the binary entropy function. Here η is the smallest detection probability for a non-vacuum state received by Bob's system. For gated systems, η is very close to zero at the beginning and end of the gate. Therefore, the secret key rate given by the security proofs will be zero. However, *bit-mapped gating* allows the user to calculate η from Equation (5.5) using only detector efficiencies in the central part of the gate [**175**]. Furthermore, it makes it possible to estimate η from system parameters measured in the laboratory.

5.6 Detector control attacks

From Eve's perspective, the detector control attack seems to be the most successful. The core of the attack is the following [**57, 60**]: Eve measures the quantum state from Alice in a random basis. Then a bright trigger pulse is resent to Bob when his detectors are in a state where they are only sensitive to bright illumination[4]. The power level of the pulse is adjusted such that Bob's detector always reports a detection event from the bright pulse, but never reports a detection event from a pulse with 3 dB less power. Therefore, in the detector control attack, when Eve used the same basis as Bob to measure the quantum state from Alice, Bob gets a detection event as if there were no eavesdropper. And if Eve used the opposite basis from Bob to measure the quantum state from Alice, her bright pulse will strike both of Bob's detectors with 3 dB less power, and neither detector will report a detection event: the bit is simply lost. Against an active-basis choice implementation, this introduces 50% total loss. In practice, this is no limitation for the attack: Eve

[4] Here, bright means containing a sufficient number of photons such that if the bright pulse is sent through a 50/50 beam splitter, each exit of the beam splitter will contain close to half the number of photons from the input pulse.

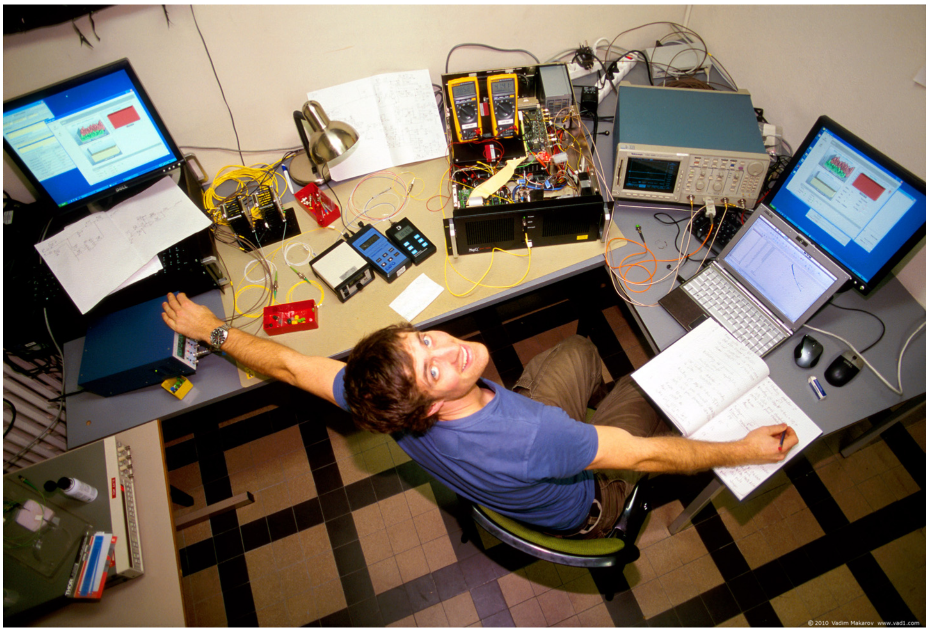


Figure 5.2: Photo of myself during an experiment at the Group of applied physics at the University of Geneva. In this experiment, we showed that the commercial QKD system QPN 5505 from MagiQ Technologies was vulnerable to bright illumination [**57**]. Photo ©2010 Vadim Makarov.

can place her intercept-unit close to Alice while compensating the loss in the remaining fiber by resending brighter states. This perfect detector control attack introduces zero QBER, captures the full secret key, and is implementable with current technology.

If a non-zero QBER, or higher loss than 50% can be tolerated, it suffices that the detectors click with a high probability when Eve used the correct basis, and with a low probability when Eve used the incorrect basis. For a full discussion of the constraints on the detector click probability, see Reference [**174**]. The detector control attack is applicable to the BB84, SARG04 and decoy-protocols, as well as distributed-phase-reference protocols like DPS and COW [**176**].

The question is if Bob's detectors can be caught in a state where they have such abrupt change in detection probability. For APD-based detectors, they actually have such response to bright illumination when they are biased below the breakdown voltage (see Section 4.1.3). Gated detectors are already biased below the breakdown voltage outside the gate. Therefore, by timing the bright trigger pulse after the gate, eavesdropping is possible, although introduces considerable QBER [**173, 174**]. It turns out that by shining bright illumination on the detectors, the bias voltage is lowered to a value below the breakdown voltage. This is called *blinding* the detectors, because they remain insensitive to single photons and have no dark counts. Both passively quenched [55], actively quenched [**60**], and gated detectors [**57, 177**] could be blinded and controlled through a variety of techniques. The detectors in two commercial QKD systems from two different vendors were blindable and controllable by bright illumination [**57**] (see Figure 5.2). Furthermore, a full eavesdropper[5] has been implemented and used to capture the full key of a 290 m quantum channel in an experimental QKD system [58]. Note that the QKD systems from some manufacturers might be immune to the simplest blinding schemes [178][**179**].

SNSPDs have been reported to exhibit multiphotonic processes [102]. Therefore, in some cases it might be possible to eavesdrop on QKD systems using SNSPDs simply by choosing an appropriate power level for the trigger pulses [**174**]. We have also shown that a SNSPD can be blinded permanently[6] by forcing it into the latched state [**180**]. In the latched state, the SNSPD had a suitable response to bright trigger pulses, allowing a detector control attack. Furthermore, the SNSPD can be controlled without forcing it into the latched state [**180**].

Since the detector control attack can be performed with less than 100 photons in the trigger pulse, an optical power meter seems to be unreliable to reveal the eavesdropper [**174**]. Furthermore, as discussed previously, any threshold in Bob's system must be included in a security proof[7]. It seems that one solution could be a calibrated light source inside Bob's system to test the single photon sensitivity at random times [58][**176**]. The details and implementation of such a scheme remain a potential study for the future.

5.7 Device-independent QKD

Many security proofs use a bottom-up approach, incorporating an increasing number of imperfections. There is also a top-down approach where the number of assumptions on the devices is reduced to a minimum. In device-independent QKD (DI-QKD) [19, 61, 62, 91], there are barely any assumptions on the devices: the

[5] Interestingly, but perhaps not surprisingly, the same implementation has been used to violate Bell inequalities even though one half of the EPR pairs were measured by the eavesdropper [65].

[6] Until the operator resets the bias current. Of course, a commercial QKD system using SNSPDs must have an automatic reset feature or avoid latching by other means.

[7] For instance, as a countermeasure against the detector control attack it has been suggested to monitor the photocurrent in the APDs and look for anomalously high values [181][**182**]. What is an anomalously high photocurrent? For this particular example, the countermeasure is also insufficient since a 100 photons in a trigger pulse does not cause any anomalously high value.

security is proven solely from the non-classical correlations in Alice's and Bob's data. However, three assumptions remain:

- No information can exit Alice's and Bob's measurement devices (only the particles whose properties are to be measured can enter the devices).
- Alice and Bob input true randomness into their devices.
- Alice's and Bob's measurement devices always output 0 or 1 whenever they both apply a basis choice, even if no photon has been detected.

Let us discuss these assumptions in detail. The first assumption is not only necessary for DI-QKD, but also QKD in general and any implementation of a security scheme. However, it is also equally difficult to test this assumption for a DI-QKD scheme as for a QKD scheme. For instance, one could imagine that the detectors emit an exotic particle, for instance the Higgs-boson, which reveals the key and thereby violates this assumption. Therefore, it is impossible to verify that this is the case for a real device, with 100% certainty.

As for the true randomness, this is equally important, and the assumption is equally strict for DI-QKD and for QKD. Without true randomness, Eve might be able to predict parts of the key.

The last of the assumptions, makes it a major challenge to implement DI-QKD. As discussed, all channels have substantial loss, and Bob's detectors have a finite detection efficiency. Therefore, using current and foreseeable technology, Bob will most of the time not get a click. Therefore, for DI-QKD, whenever Bob's detectors did not produce a click, Bob must simply select the bit value 0 or 1. Since Bob's selections will often be erroneous, in practice, the detection probability must be at least about 90%. This is the obstacle preventing DI-QKD from being implemented with current technology. Recently there has been a proposal to use a heralded photon amplifier, such that Bob only applies a basis choice if a photon entered his apparatus [66]. This eliminates the channel from the loss budget. Still, an implementation seems to be extremely challenging, and it is unlikely that an implementation would allow useful key rates at useful distances [66].

Chapter 6

Thoughts on the future

History has shown that one should be careful about predicting the future, especially when it comes to technology[1]. There have been predictions and discussions regarding the future for QKD [67, 183–189]. Here, I will present my perspective on the future of QKD.

QKD is often advertised as an alternative to public key cryptography, and the solution to the key distribution problem. I agree that QKD is superior to public key cryptography in terms of security, but I disagree that QKD should be compared with public key cryptography. I rather think that QKD should be compared with a trusted courier distributing a large symmetric key. In fact, a trusted courier must be used to distribute the QKD system. This courier (as well as the producer of the QKD system) must be trusted because otherwise, they may install a tap, leaking the secret key to Eve. Therefore, in terms of distribution, I see no difference between a courier transporting a several terabyte hard drive containing a secret key, and a courier transporting a QKD system. Either case requires the same level of trust.

A frequently used argument against a huge symmetric key, is that any adversary seeing the secret key makes all future communication insecure. However, I argue that the same is the case for QKD: if Eve sees the secret key which is used for authentication in future rounds of QKD, she may immediately call her helper Steve, who immediately inserts an eavesdropping station performing a man-in-the-middle attack[2]. Just as for the hard drive, an adversary seeing the secret key makes all future communication insecure.

Note that a courier must also bring the first initial secret key, used to authenticate the first round of QKD. While it has been claimed that this is a drawback

[1] Although there is a discussion whether the statement was made, the most famous example is Thomas J. Watson, a former president of International Business Machines (IBM), whom predicted a world market for about five computers in 1943.

[2] While this operation is very complicated, there is no inherent security in this complexity.

of QKD [187], this is the case with any encryption protocol: encryption without authentication is insecure. Alice must be sure that she is talking to Bob and not Eve, and the only way to do so is pre-shared information[3].

Therefore, it seems that the alternative to QKD is a trusted courier transporting a large symmetric key. Table 6.1 compares a 3 terabyte symmetric key with the best commercially available QKD system and the best experimental QKD systems. As far as I can see, this comparison favors sending a 3 terabyte symmetric key with the courier instead of a QKD system. Specifically, repeating this procedure every 290 days will make a bandwidth equal to the best experimental QKD system available, without the distance limitation, and with a small fraction of the cost.

However, one performance parameter omitted so far should be discussed in detail: lifetime. In some cases, it is very difficult to replace the hard drive, for instance if one of the parties is placed in a satellite [155]. Then it simply boils down to the lifetime of the device. Consumer hard drives are known to fail after 3–5 years, but one could easily imagine that with special focus it should be possible to produce more reliable hard drives. Meanwhile, compared to a single hard drive, a QKD system typically consists of a huge amount of components. For instance, although APDs seem to have low failure probabilities [191], their parameters are known to degrade over time. This would result in a reduction in the secret key rate. Therefore, it is not easy to compare the lifetimes of the two alternatives.

So far I have only considered point-to-point links in this comparison. However, when one starts to consider networks, the picture changes. The hard drive example has no reusable parts, so a pair of hard drives is required between each pair of participants in the network. Using QKD however, one could imagine a module

[3] In public key authentication schemes, Alice does not need to share a secret with Bob, but she must have Bob's public key. Bob's public key may be publicly available, but Alice must still make sure that it is really Bob's and not Eve's public key. On the internet, this is solved using trusted(?) third-parties (for instance VeriSign Inc.) to verify the identity of the owner of the Bob's key. The public keys of these third-parties are embedded in the browser.

	3 terabyte hard drive	Commercial QKD [190]	Experimental QKD
Price	800 €	80000 €+ dark fiber	? + dark fiber
Key rate at 50 km	N/A	3.5 kbps	1 Mbps [133]
Maximum distance	Unlimited	100 km	250 km [26]
Time to generate a 3 terabyte key at 50 km	24 hours?	233 years	290 days

Table 6.1: Comparison between a 3 terabyte symmetric key, the best commercially available QKD system and the best experimental QKD systems.

able to play the role of either Alice or Bob. Therefore, each participant only needs one such module. This is reflected in the huge difference in storage requirements: if there are N participants, and each pair of participants share b bits of secret key, each participant must store a total of $b(N-1)$ bits. As argued above, $b = 3\,\mathrm{TB}$ for the hard drives, while for QKD, b must just suffice to authenticate a couple of rounds of QKD. For large networks, the difference is huge!

It is my conclusion, that in order to compete with a pair of hard drives, QKD must increase the transmission distance, secret key rate, and move to networks. There is intense research going on to achieve this. However, it seems to me in terms of distance, we are approaching the limit with optical fiber as the quantum channel. Therefore, in order to increase the transmission distance, quantum repeaters [192, 193] will become necessary. It remains an open question whether quantum repeaters can become sufficiently stable to be used in QKD.

At the end of the day, there seems to be a small, but growing market for QKD systems. The current commercial systems combine the key generated from QKD with a symmetric key distributed using public key encryption[4]. Therefore, in order to break the security of the system, both key distribution schemes must be broken. One could argue that this gives a higher level of security. Regardless of whether QKD is the key distribution solution for the future, one thing is certain: as long as there are governments and industries using QKD for high security tasks, it is crucial that there are independent third parties scrutinizing the QKD systems to reveal loopholes in the implementations to improve the security.

[4] The keys are simply XOR-ed together. Then, the combined key is as secure as the most secure of the keys.

Chapter 7

Conclusion and future work

Assuming that Eve must obey the laws of quantum physics, QKD has been proven secure with perfect devices. However, when QKD is implemented, one must use actual devices available with current technology. In this setting, the security proofs with perfect devices are not valid any more, and the actual devices must be modeled and incorporated into practical security proofs. While there are already security proofs that model and incorporate certain imperfections, the actual devices do not necessarily comply with the existing proofs.

The contribution in this thesis is twofold: a theoretical part consisting of security proofs for practical devices, and an experimental part examining how actual devices comply with the models of the existing security proofs. Since the source in QKD had already received considerable attention when I entered this field, most of this work relates to the detectors.

For the theoretical part, the results are very general security proofs, which lower bound the asymptotic, secure key rate with arbitrary imperfections simultaneously in the source and the detectors [**41**]. Furthermore, a detection scheme compatible with these security proofs has been proposed in order to measure the detector parameters [**175**].

In the experimental part, the results show that commercial QKD systems contained flaws in their implementation, which would allow an eavesdropper to capture the full secret key, using off-the-shelf components without getting revealed by errors in the key [**57**]. This important work caused discussions [178][**179**], and got considerable media attention. Some of the media attention led the public to believe that QKD was insecure. But as stated in the beginning of this chapter, QKD is proven secure once and for all with perfect devices. In fact, spectacular security flaws are usually found and patched in some phase of most security technologies. One example is the widely adopted public key cipher RSA [68]. One could argue that QKD is in this phase now, and as such I believe that this work is a milestone. I believe that this work has led to increased awareness about imperfections in QKD, and therefore future implementations will be more secure.

There is still much work to be done. The long term goal should be to design and implement a practical QKD scheme which is provable secure, while having a useful key rate at a useful distance. On the theoretical side, this requires a security proof which quantifies the imperfections in the source and receiver. At the moment, there are proofs considering imperfections in both the source and the receiver, but unfortunately they handle loss such a way that in practice they would only allow very short transmission distances. This could possibly be improved by integrating the proofs with the decoy-state approach. Furthermore, while the imperfections are quantified, for an actual implementation to be provable secure, the imperfection parameters of the security proof must be measured or bounded. While we have proposed how to do this for the detectors, it is still an unanswered question for the source.

A bigger challenge is that most QKD systems contain collective errors, for instance the afterpulsing of the detectors and/or imperfect random number generators. This is yet to be tackled in a security proof.

Imperfections in the source and the receiver, and finite key effects have so far been studied separately: imperfections with the asymptotic infinite key, and finite key with perfect devices. Therefore, future security proofs incorporating imperfections should also incorporate the finite key size.

On the experimental side there is still work to do: implement and scrutinize a detector scheme where the detector parameters are verified to be within the model in the security proof. In the short term, this could involve designing and implementing a calibrated light source in Bob, to avoid detector control attacks.

For both the experimental and theoretical future, the biggest challenge remains: will it be possible to implement QKD in a way that is provable secure?

Chapter 8

Publication list

Journal publications

- L. Lydersen and J. Skaar, “Security of quantum key distribution with bit and basis dependent detector flaws,” Quantum Information & Computation **10**, 60–76 (2010).
- Ø. Marøy, L. Lydersen and J. Skaar, “Security of quantum key distribution with arbitrary individual imperfections,” Physical Review A **82**, 032337 (2010).
- L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” Nature Photonics **4**, 686–689 (2010).
- L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Avoiding the blinding attack in QKD,” Nature Photonics **4**, 801 (2010).
- L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Thermal blinding of gated detectors in quantum cryptography,” Optics Express **18**, 27938–27954 (2010).
- C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov and G. Leuchs, “After-gate attack on a quantum cryptosystem,” New Journal of Physics **13**, 013043 (2011).
- L. Lydersen, V. Makarov and J. Skaar, “Secure gated detection scheme for quantum cryptography,” Physical Review A **83**, 032306 (2011).
- L. Lydersen, J. Skaar and V. Makarov, “Tailored bright illumination attack on distributed-phase-reference protocols,” Journal of Modern Optics **58**, 680–685 (2011).

- N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov and G. Leuchs, “Device calibration impacts security of quantum key distribution,” accepted for publication in Physical Review Letters; arXiv: 1103.2327 [quant-ph].

- L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov and G. Leuchs, “Superlinear threshold detectors in quantum cryptography,” accepted for publication in Physical Review A; arXiv: 1106.2119 [quant-ph].

- S. Sauge, L. Lydersen, J. Skaar, A. Anisimov and V. Makarov, “Controlling an actively-quenched single photon detector with bright light,” submitted to Optics Express; arXiv: 0809.3408 [quant-ph].

- L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar and V. Makarov, “Controlling a superconducting nanowire single-photon detector using tailored bright illumination,” submitted to New Journal of Physics; arXiv: 1106.2396 [quant-ph].

- L. Lydersen, V. Makarov and J. Skaar, “Comment on ‘Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography’,” submitted to Applied Physics Letters; arXiv: 1106.3756 [quant-ph].

For a full, updated list of my journal publications including preprints, please visit `http://arxiv.org/a/lydersen_l_1`.

Conference contributions

Presenting author in bold.

- **L. Lydersen** and J. Skaar, “Security of QKD-systems with detector efficiency mismatch,” poster at Theory and Realisation of Practical Quantum Key Distribution, Waterloo, Canada, July 2007.

- **L. Lydersen** and J. Skaar, “Security of quantum key distribution with bit and basis dependent detector flaws,” poster at Information Security in a Quantum World, Waterloo, Canada, August 2008.

- **L. Lydersen** and J. Skaar, “Security of quantum key distribution with bit and basis dependent detector flaws,” poster at SECOQC conference, Vienna, Austria, October 2008.

- **Ø. Marøy**, L. Lydersen, and J. Skaar, “Security of quantum key distribution with imperfect equipment,” contributed talk at 18th International Laser Physics Workshop, Barcelona, Spain, July 2009.

- **L. Lydersen**, V. Makarov, Q. Liu, Ø. Marøy and J. Skaar, “Quantum key distribution and quantum hacking,” invited talk at Quantum Communication Workshop, Kjeller, Norway, February 2010.

- **V. Makarov**, L. Lydersen, Q. Liu, C. Wiechers, C. Wittmann, D. Elser, I. Gerhardt, S. Sauge, J. Skaar, A. Lamas-Linares and C. Kurtsiefer, “Perfect eavesdropping: 100% key, 0% QBER,” invited talk at Tropical QKD workshop 2010, Waterloo, Canada, June 2010.

- L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and **V. Makarov**, “Cracking commercial quantum cryptography,” invited talk at International Conference on Quantum Information and Computation, Stockholm, Sweden, October 2010.

- **L. Lydersen**, J. Skaar, Q. Liu and V. Makarov, “Practical quantum hacking,” invited talk at Post-Quantum Security Models, Paris, France, October 2010.

- **N. Jain**, L. Lydersen, C. Wittmann, C. Wiechers, D. Elser, C. Marquardt, V. Makarov and G. Leuchs, “How secure is quantum secure: Regenerative QKD in practice,” poster at Updating Quantum Cryptography and Communications, Tokyo, Japan, October 2010.

- **L. Lydersen**, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” poster at Updating Quantum Cryptography and Communications, Tokyo, Japan, October 2010.

- **C. Wiechers**, L. Lydersen, N. Jain, C. Wittmann, D. Elser, V. Makarov, C. Marquardt, J. Jose, J. Skaar and G. Leuchs, “Improving quantum key distribution systems by quantum hacking tests,” contributed talk at Quantum Optics V, Cozumel, Mexico, November 2010.

- **N. Jain**, L. Lydersen, C. Wittmann, C. Wiechers, D. Elser, C. Marquardt, V. Makarov and G. Leuchs, “Inducing a detector efficiency mismatch to hack a commercial quantum key distribution system,” contributed talk at CLEO/Europe-EQEC, Munich, Germany, May 2011.

Other

- D. R. Hjelme, L. Lydersen and V. Makarov, book chapter on quantum cryptography for the book "A Multidisciplinary Introduction to Information Security", to be published by CRC Press in 2011/2012, arXiv: 1108.1718 [quant-ph].

Chapter 9

Contributions in papers

This section summarizes my contribution to each of the papers contained in this thesis. The papers are labeled with the same letters as in this thesis. When I state that I performed the analysis or wrote whole or parts of a paper, I have had the main responsibility and made the major contribution to the task. However, usually the tasks have been conducted with substantial help, guidance and input from co-authors. Figure numbers in preprints refer to the figure number in the preprint version reprinted in this thesis.

Paper A

L. Lydersen and J. Skaar, "Security of quantum key distribution with bit and basis dependent detector flaws," Quantum Information & Computation **10**, 60–76 (2010).

My contribution: Analysis of the upper bound, and the example in Section 4.2. Writing Sections 1, 2 and 4.2, making all figures.

Paper B

Ø. Marøy, L. Lydersen and J. Skaar, "Security of quantum key distribution with arbitrary individual imperfections," Physical Review A **82**, 032337 (2010).

My contribution: Contributing to the concept to include both imperfections in the source and the detector simultaneously, and to the model of the system, especially the detectors.

Paper C

L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nature Photonics **4**, 686–689 (2010).

My contribution: My contribution is stated in the "Author contributions" section at the end of the paper: *"V.M. conceived the idea and planned the study. L.L. and V.M. conducted the Clavis2 experiment with the help of C. Wiechers, D.E. and C. Wittmann. L.L. and V.M. conducted the QPN 5505 experiment. L.L. and J.S. wrote the paper and Supplementary information, with input from all authors. J.S. and V.M. supervised the project."*

Paper D

L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Avoiding the blinding attack in QKD," Nature Photonics **4**, 801 (2010).

Note: this is a reply to correspondence [178] regarding Paper C [57].

My contribution: Writing the paper.

Paper E

L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," Optics Express **18**, 27938–27954 (2010).

My contribution: Conducting the main experiment with some guidance. Discovering the thermal blinding effect, analyzing the data, writing the paper, and making all figures.

Paper F

C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov and G. Leuchs, "After-gate attack on a quantum cryptosystem," New Journal of Physics **13**, 013043 (2011).

My contribution: Major participation in the main experiment, and performing an initial, minor part of the simulation.

Paper G

L. Lydersen, V. Makarov and J. Skaar, “Secure gated detection scheme for quantum cryptography,” Physical Review A **83**, 032306 (2011).

My contribution: Conceiving the main idea, performing the analysis, writing the paper, and making all figures.

Paper H

L. Lydersen, J. Skaar and V. Makarov, “Tailored bright illumination attack on distributed-phase-reference protocols,” Journal of Modern Optics **58**, 680–685 (2011).

My contribution: Conceiving the idea (possibly independently from V. Makarov who also had the same general idea), performing the analysis, writing the paper, and making all figures.

Paper I

N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov and G. Leuchs, “Device calibration impacts security of quantum key distribution,” accepted for publication in Physical Review Letters; arXiv: 1103.2327 [quant-ph].

My contribution: Major participation in one of the experiments (the data presented in figures 3 and 4), and verifying the theoretical equations (1)-(5).

Paper J

L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov and G. Leuchs, “Superlinear threshold detectors in quantum cryptography,” accepted for publication in Physical Review A; arXiv: 1106.2119 [quant-ph].

My contribution: Conceiving the idea. Designing and having a major participation in the experiment. Analyzing the data, developing the theory, writing the paper, and making all figures.

Paper K

S. Sauge, L. Lydersen, J. Skaar, A. Anisimov and V. Makarov, “Controlling an actively-quenched single photon detector with bright light,” submitted to Optics Express; arXiv: 0809.3408 [quant-ph].

My contribution: Repeating the experiment from the initial manuscript (which I did not co-author), and conducting additional experiments to verify the origin of the observed detector response. Analyzing the data, and making figures 2, 3 and 5.

Paper L

L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar and V. Makarov, “Controlling a superconducting nanowire single-photon detector using tailored bright illumination,” submitted to New Journal of Physics; arXiv: 1106.2396 [quant-ph].

My contribution: Conducting the latched detector control experiment in Section III together with V. Makarov. Writing Sections I, III, and V of the paper, and making all figures.

Paper M

L. Lydersen, V. Makarov and J. Skaar, “Comment on ‘Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography’,” submitted to Applied Physics Letters; arXiv: 1106.3756 [quant-ph].

Note: this is submitted as correspondence to a publication [181].

My contribution: Writing the paper.

Bibliography

[1] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Four Estate, London, 1999).

[2] G. S. Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communications,” Journal of the American Institute of Electrical Engineers **45**, 109–115 (1926).

[3] C. E. Shannon, “Communication theory of secrecy systems,” Bell System Technical Journal **28**, 656–715 (1949).

[4] National Bureau of Standards, “Data Encryption Standard,” U.S. Department of Commerce, Federal Information Processing Standards Publication. 46 (January 1977).

[5] J. Daemen and V. Rijmen, “The Block Cipher Rijndael,” in *Proceedings of the The International Conference on Smart Card Research and Applications* (Springer-Verlag, London, UK, 2000) pp. 277–284.

[6] National Bureau of Standards and Technology, “Advanced Encryption Standard,” U.S. Department of Commerce, Federal Information Processing Standards Publication. 197 (November 2001).

[7] W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory **22**, 644–654 (1976).

[8] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM **21**, 120–126 (1978).

[9] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM Journal on Computing **26**, 1484–1509 (1997).

[10] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O’Brien, “Quantum computers,” Nature **464**, 45–53 (2010).

[11] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," Nature **414**, 883–887 (2001).

[12] M. W. Johnson, M. H. S. Amin, S. Gildert, T. Lanting, F. Hamze, N. Dickson, R. Harris, A. J. Berkley, J. Johansson, P. Bunyk, E. M. Chapple, C. Enderud, J. P. Hilton, K. Karimi, E. Ladizinsky, N. Ladizinsky, T. Oh, I. Perminov, C. Rich, M. C. Thom, E. Tolkacheva, C. J. S. Truncik, S. Uchaikin, J. Wang, B. Wilson, and G. Rose, "Quantum annealing with manufactured spins," Nature **473**, 194–198 (2011).

[13] W. D. Oliver, "Quantum physics: Keep your feet on the ground," Nature **473**, 164–165 (2011).

[14] Zeeya Merali, "First sale for quantum computing," Nature News (2011), `http://www.nature.com/news/2011/110531/full/474018a.html`, visited 19th June 2011..

[15] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Reviews of Modern Physics **74**, 145–195 (2002).

[16] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Reviews of Modern Physics **81**, 1301 (2009).

[17] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, Bangalore, India, 1984) pp. 175–179.

[18] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802–803 (1982).

[19] A. K. Ekert, "Quantum Cryptography Based on Bell's Theorem," Physical Review Letters **67**, 661–663 (1991).

[20] J. S. Bell, "On the problem of hidden variables in quantum mechanics," Reviews of Modern Physics **38**, 447–452 (1966).

[21] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Physical Review **47**, 777–780 (1935).

[22] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without Bell’s theorem,” Physical Review Letters **68**, 557–559 (1992).

[23] C. H. Bennett, “Quantum cryptography using any 2 nonorthogonal states,” Physical Review Letters **68**, 3121–3124 (1992).

[24] C. H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin, “Experimental quantum cryptography,” Journal of Cryptology **5**, 3–28 (1992).

[25] A. Muller, H. Zbinden, and N. Gisin, “Quantum cryptography over 23 km in installed under-lake telecom fibre,” Europhysics Letters **33**, 335–339 (1996).

[26] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,” New Journal of Physics **11**, 075003 (2009).

[27] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, “Entanglement-based quantum communication over 144 km,” Nature Physics **3**, 481–486 (2007).

[28] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, “Generalized privacy amplification,” IEEE Transactions on Information Theory **41**, 1915–1923 (1995).

[29] D. Mayers, “Advances in cryptology,” in *Proceedings of Crypto’96*, Vol. 1109, edited by N. Koblitz (Springer, New York, 1996) pp. 343–357.

[30] H.-K. Lo and H. F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances,” Science **283**, 2050–2056 (1999).

[31] P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol,” Physical Review Letters **85**, 441–444 (2000).

[32] D. Mayers, “Unconditional security in quantum cryptography,” Journal of the ACM **48**, 351–406 (2001).

[33] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” Quantum Information & Computation **4**, 325–360 (2004).

[34] H. Inamori, N. Lütkenhaus, and D. Mayers, “Unconditional security of practical quantum key distribution,” European Physical Journal D **41**, 599–627 (2007).

[35] M. Koashi and J. Preskill, “Secure quantum key distribution with an uncharacterized source,” Physical Review Letters **90**, 057902 (2003).

[36] M. Ben-Or, M. Horodecki, D.W. Leung, D. Mayers, and J. Oppenheim, “The universal composable security of quantum key distribution,” in *Second Theory of Cryptography Conference*, Lecture Notes in Computer Science, Vol. 3378 (Springer, New York, 2005) pp. 386–406.

[37] R. Renner and R. Koenig, “Universally composable privacy amplification against quantum adversaries,” in *Second Theory of Cryptography Conference, TCC 2005*, LNCS, Vol. 3378, edited by J. Kilian (Springer Verlag, Berlin, 2005) pp. 407–425, arXiv:quant-ph/0403133.

[38] G. Brassard, “Brief history of quantum cryptography: a personal perspective,” in *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security* (2005) pp. 19–23.

[39] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on practical quantum cryptography,” Physical Review Letters **85**, 1330–1333 (2000).

[40] N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution,” Physical Review A **61**, 052304 (2000).

[41] Ø. Marøy, L. Lydersen, and J. Skaar, “Security of quantum key distribution with arbitrary individual imperfections,” Physical Review A **82**, 032337 (2010).

[42] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,” Physical Review Letters **92**, 057901 (2004).

[43] W.-Y. Hwang, “Quantum key distribution with high loss: Toward global secure communication,” Physical Review Letters **91**, 057901 (2003).

[44] X.-B. Wang, “Beating the photon-number-splitting attack in practical quantum cryptography,” Physical Review Letters **94**, 230503 (2005).

[45] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” Physical Review Letters **94**, 230504 (2005).

[46] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, “The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?” Journal of Modern Optics **48**, 2039–2047 (2001).

[47] A. Vakhitov, V. Makarov, and D. R. Hjelme, “Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography,” Journal of Modern Optics **48**, 2023–2038 (2001).

[48] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, “Trojan-horse attacks on quantum-key-distribution systems,” Physical Review A **73**, 022320 (2006).

[49] V. Makarov, A. Anisimov, and J. Skaar, “Effects of detector efficiency mismatch on security of quantum cryptosystems,” Physical Review A **74**, 022313 (2006); Erratum ibid. **78**, 019905 (2008).

[50] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, “Time-shift attack in practical quantum cryptosystems,” Quantum Information & Computation **7**, 73–82 (2007).

[51] A. Lamas-Linares and C. Kurtsiefer, “Breaking a quantum key distribution system through a timing side channel,” Optics Express **15**, 9388–9393 (2007).

[52] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, “Phase-remapping attack in practical quantum-key-distribution systems,” Physical Review A **75**, 032314 (2007).

[53] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, “Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems,” Physical Review A **78**, 042333 (2008).

[54] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, “Information leakage via side channels in freespace BB84 quantum cryptography,” New Journal of Physics **11**, 065001 (2009).

[55] V. Makarov, “Controlling passively quenched single photon detectors by bright light,” New Journal of Physics **11**, 065003 (2009).

[56] F. Xu, B. Qi, and H.-K. Lo, “Experimental demonstration of phase-remapping attack in a practical quantum key distribution system,” New Journal of Physics **12**, 113026 (2010).

[57] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” Nature Photonics **4**, 686–689 (2010).

[58] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," Nature Communications **2**, 349 (2011).

[59] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," New Journal of Physics **13**, 073024 (2011).

[60] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, "Controlling an actively-quenched single photon detector with bright light," arXiv:0809.3408 [quant-ph].

[61] J. Barrett, L. Hardy, and A. Kent, "No signaling and quantum key distribution," Physical Review Letters **95**, 010503 (2005).

[62] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," Physical Review Letters **98**, 230501 (2007).

[63] P. M. Pearle, "Hidden-variable example based upon data rejection," Physical Review D **2**, 1418–1425 (1970).

[64] A. A. Semenov and W. Vogel, "Fake violations of the quantum Bell-parameter bound," Physical Review A **83**, 032119 (2011).

[65] Q. Liu, I. Gerhardt, A. Lamas-Linares, J. Skaar, V. Makarov, and C. Kurtsiefer, "Violating a Bell inequality with classical states," arXiv:1106.3224 [quant-ph].

[66] N. Gisin, S. Pironio, and N. Sangouard, "Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier," Physical Review Letters **105**, 070501 (2010).

[67] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems," arXiv:0906.4547v1 [quant-ph].

[68] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," Notices of the American Mathematical Society **46**, 203–213 (1999).

[69] N. Lütkenhaus, "Estimates for practical quantum cryptography," Physical Review A **59**, 3301–3319 (1999).

[70] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. 1. Information bound and optimal strategy," Physical Review A **56**, 1163–1172 (1997).

[71] R. Renner, "Symmetry of large physical systems implies independence of subsystems," Nature Physics **3**, 645–649 (2007).

[72] R. Renner and J. I. Cirac, "de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," Physical Review Letters **102**, 110504 (2009).

[73] T. Moroder, M. Curty, and N. Lütkenhaus, "Detector decoy quantum key distribution," *presentation at Information Security in a Quantum World, Institute for Quantum Computing, University of Waterloo, Canada* (2008).

[74] T. Tsurumaru and K. Tamaki, "Security proof for quantum-key-distribution systems with threshold detectors," Physical Review A **78**, 032302 (2008).

[75] C.-H. F. Fung, H. F. Chau, and H.-K. Lo, "Universal squash model for optical communications using linear optics and threshold detectors," arXiv:1011.2982 [quant-ph].

[76] T. Tsurumaru, "Squash operator and symmetry," Physical Review A **81**, 012328 (2010).

[77] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, "Squashing models for optical measurements in quantum communication," Physical Review Letters **101**, 093601 (2008).

[78] P. M. Nielsen, C. Schori, J. L. Sørensen, L. Salvail, I. Damgård, and E. Polzik, "Experimental quantum key distribution with proven security against realistic attacks," Journal of Modern Optics **48**, 1921–1942 (2001).

[79] D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," IEEE Transactions on Information Theory **49**, 457–475 (2003).

[80] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Transactions on Information Theory **24**, 339–348 (1978).

[81] T. M. Cover and J. A. Thomas, *Elements of information theory*, 2nd ed. (Wiley, Hoboken, N.J., 2006).

[82] R. König, R. Renner, A. Bariska, and U. Maurer, “Small accessible quantum information does not imply security,” Physical Review Letters **98**, 140502 (2007).

[83] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, 2000).

[84] Jörn Müller-Quade and Renato Renner, “Composability in quantum cryptography,” New Journal of Physics **11**, 085006 (2009).

[85] M. Koashi, “Simple security proof of quantum key distribution via uncertainty principle,” arXiv:quant-ph/0505108v1.

[86] R. Renner, N. Gisin, and B. Kraus, “Information-theoretic security proof for quantum-key-distribution protocols,” Physical Review A **72**, 012332 (2005).

[87] M. Koashi, “Efficient quantum key distribution with practical sources and detectors,” arXiv:quant-ph/0609180v1.

[88] M. Koashi, “Simple security proof of quantum key distribution based on complementarity,” New Journal of Physics **11**, 045018 (2009).

[89] H. Maassen and J. B. M. Uffink, “Generalized entropic uncertainty relations,” Physical Review Letters **60**, 1103–1106 (1988).

[90] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, “The uncertainty principle in the presence of quantum memory,” Nature Physics **6**, 659–662 (2010).

[91] M. Tomamichel and R. Renner, “Uncertainty relation for smooth entropies,” Physical Review Letters **106**, 110506 (2011).

[92] T. C. Ralph, “Continuous variable quantum cryptography,” Physical Review A **61**, 010303 (1999).

[93] M. Hillery, “Quantum cryptography with squeezed states,” Physical Review A **61**, 022309 (2000).

[94] N. Sangouard, C. Simon, J. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin, “Long-distance entanglement distribution with single-photon sources,” Physical Review A **76**, 050301 (2007).

[95] A. J. Shields, “Semiconductor quantum light sources,” Nature Photonics **1**, 215–223 (2007).

[96] C. L. Salter, R. M. Stevenson, I. Farrer, C. A. Nicoll, D. A. Ritchie, and A. J. Shields, “An entangled-light-emitting diode,” Nature **465**, 594–597 (2010).

[97] S. Bloom, E. Korevaar, J. Schuster, and H. Willebrand, “Understanding the performance of free-space optics [Invited],” Journal of Optical Networking **2**, 178–200 (2003).

[98] V. Makarov, *Quantum cryptography and quantum cryptanalysis*, Doctoral thesis, Norwegian University of Science and Technology (2007).

[99] R. H. Hadfield, “Single-photon detectors for optical quantum information applications,” Nature Photonics **3**, 696–705 (2009).

[100] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, “Evolution and prospects for single-photon avalanche diodes and quenching circuits,” Journal of Modern Optics **51**, 1267–1288 (2004).

[101] G. N. Gol’tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, “Picosecond superconducting single-photon optical detector,” Applied Physics Letters **79**, 705–707 (2001).

[102] A. Verevkin, J. Zhang, R. Sobolewski, A. Lipatov, O. Okunev, G. Chulkova, A. Korneev, K. Smirnov, G. N. Gol’tsman, and A. Semenov, “Detection efficiency of large-active-area NbN single-photon superconducting detectors in the ultraviolet to near-infrared range,” Applied Physics Letters **80**, 4687–4689 (2002).

[103] B. E. Kardynal, Z. L. Yuan, and A. J. Shields, “An avalanche-photodiode-based photon-number-resolving detectors,” Nature Photonics **2**, 425–428 (2008).

[104] A. Divochiy, F. Marsili, D. Bitauld, A. Gaggero, R. Leoni, F. Mattioli, A. Korneev, V. Seleznev, N. Kaurova, O. Minaeva, G. Gol’tsman, K. Lagoudakis, M. Benkhaoul, F Lévy, and A. Fiore, “Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths,” Nature Photonics **2**, 302–306 (2008).

[105] O. Thomas, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Efficient photon number detection with silicon avalanche photodiodes,” Applied Physics Letters **97**, 031102 (2010).

[106] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, “Avalanche photodiodes and quenching circuits for single-photon detection,” Applied Optics **35**, 1956–1976 (1996).

[107] E. Diamanti, H. Takesue, T. Honjo, K. Inoue, and Y. Yamamoto, "Performance of various quantum-key-distribution systems using 1.55-μm up-conversion single-photon detectors," Physical Review A **72**, 052311 (2005).

[108] V. Makarov, A. Brylevski, and D. R. Hjelme, "Real-time phase tracking in single-photon interferometers," Applied Optics **43**, 4385–4392 (2004).

[109] N. Namekata, S. Adachi, and S. Inoue, "1.5 GHz single-photon detection at telecommunication wavelengths using sinusoidally gated InGaAs/InP avalanche photodiode," Optics Express **17**, 6275–6282 (2009).

[110] J. Zhang, R. Thew, C. Barreiro, and H. Zbinden, "Practical fast gate rate InGaAs/InP single-photon avalanche photodiodes," Applied Physics Letters **95**, 091103 (2009).

[111] Z. L. Yuan, A. W. Sharpe, J. F. Dynes, A. R. Dixon, and A. J. Shields, "Multi-gigahertz operation of photon counting InGaAs avalanche photodiodes," Applied Physics Letters **96**, 071101 (2010).

[112] J. Zhang, P. Eraerds, N. Walenta, C. Barreiro, R. Thew, and H. Zbinden, "2.23 GHz gating InGaAs/InP single-photon avalanche diode for quantum key distribution," in *Proceedings of the SPIE - The International Society for Optical Engineering, Vol. 7681, edited by M. A. Itzler and J. C. Campbell (2010) p. 76810Z.*

[113] R. Sobolewski, A. Verevkin, G. N. Gol'tsman, A. Lipatov, and K. Wilsher, "Ultrafast superconducting single-photon optical detectors and their applications," IEEE Transactions on Applied Superconductivity **13**, 1151–1157 (2003).

[114] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors," Nature Photonics **1**, 343–348 (2007).

[115] D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, R. J. Hughes, and J. E. Nordholt, "Practical long-distance quantum key distribution system using decoy levels," New Journal of Physics **11**, 045009 (2009).

[116] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, "Decoy-state quantum key distribution with polarized photons over 200 km," Optics Express **18**, 8587–8594 (2010).

[117] K. M. Rosfjord, J. K. W. Yang, E. A. Dauler, A. J. Kerman, V. Anant, B. M. Voronov, G. N. Gol'tsman, and K. K. Berggren, "Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating," Optics Express **14**, 527–534 (2006).

[118] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," Nature Photonics **2**, 728–732 (2008).

[119] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Optics Letters **35**, 312–314 (2010).

[120] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," Nature Photonics **4**, 711–715 (2010).

[121] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," Optics Express **18**, 13029–13037 (2010).

[122] V. Scarani, "Information science: Guaranteed randomness," Nature **464**, 988–989 (2010).

[123] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).

[124] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, "Quantum random-number generation and key sharing," Journal of Modern Optics **41**, 2435–2444 (1994).

[125] A. Muller, J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km," Europhysics Letters **23**, 383 (1993).

[126] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, "Quantum cryptography: A step towards global key distribution," Nature **419**, 450–450 (2002).

[127] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Free-space quantum key distribution with entangled photons," Applied Physics Letters **89**, 101122 (2006).

[128] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Physical Review Letters **98**, 010504 (2007).

[129] P. D. Townsend, J. G. Rarity, and P. R. Tapster, "Single photon interference in 10 km long optical fibre interferometer," Electronics Letters **29**, 634–635 (1993).

[130] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo, "Faraday-Michelson system for quantum cryptography," Optics Letters **30**, 2632–2634 (2005).

[131] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," Applied Physics Letters **84**, 3762–3764 (2004).

[132] Z. Yuan and A. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre," Optics Express **13**, 660–665 (2005).

[133] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Continuous operation of high bit rate quantum key distribution," Applied Physics Letters **96**, 161102 (2010).

[134] H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, "Interferometry with Faraday mirrors for quantum cryptography," Electronics Letters **33**, 586–588 (1997).

[135] Y. Zhao, B. Qi, and H.-K. Lo, "Quantum key distribution with an unknown and untrusted source," Physical Review A **77**, 052327 (2008).

[136] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "'Plug and play' systems for quantum cryptography," Applied Physics Letters **70**, 793–795 (1997).

[137] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Automated 'plug & play' quantum key distribution," Electronics Letters **34**, 2116–2117 (1998).

[138] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," New Journal of Physics **4**, 41–41 (2002).

[139] K. Inoue, E. Waks, and Y. Yamamoto, “Differential phase shift quantum key distribution,” Physical Review Letters **89**, 037902 (2002).

[140] K. Inoue, E. Waks, and Y. Yamamoto, “Differential-phase-shift quantum key distribution using coherent light,” Physical Review A **68**, 022317 (2003).

[141] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, “Towards practical and fast quantum cryptography,” arXiv:quant-ph/0411022v1.

[142] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, “Fast and simple one-way quantum key distribution,” Applied Physics Letters **87**, 194108 (2005).

[143] T. Tsurumaru, “Sequential attack with intensity modulation on the differential-phase-shift quantum-key-distribution protocol,” Physical Review A **75**, 062319 (2007).

[144] M. Curty, L.-L. Zhang, H.-K. Lo, and N. Lütkenhaus, “Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states,” Quantum Information & Computation **7**, 665–688 (2007).

[145] C. Branciard, N. Gisin, N. Lütkenhaus, and V. Scarani, “Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography,” Quantum Information & Computation **7**, 639–664 (2007).

[146] C. Branciard, N. Gisin, and V. Scarani, “Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography,” New Journal of Physics **10**, 013031 (2008).

[147] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, “Differential phase shift quantum key distribution experiment over 105 km fibre,” New Journal of Physics **7**, 232 (2005).

[148] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, “100 km differential phase shift quantum key distribution experiment with low jitter up-conversion detectors,” Optics Express **14**, 13073–13082 (2006).

[149] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser,

G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," New Journal of Physics **11**, 075001 (2009).

[150] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA Quantum Network," arXiv:quant-ph/0503058.

[151] T. Zhang, X.-F. Mo, Z.-F. Han, and G.-C. Guo, "Extensible router for a quantum key distribution network," Physics Letters A **372**, 3957–3962 (2008).

[152] R. Alléaume, F. Roueff, E. Diamanti, and N. Lütkenhaus, "Topological optimization of quantum key distribution networks," New Journal of Physics **11**, 075002 (2009).

[153] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, "Security of trusted repeater quantum key distribution networks," Journal of Computer Security **18**, 61–87 (2010).

[154] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD network," Optics Express **19**, 10387–10409 (2011).

[155] J. M. P. Armengol, B. Furch, C. Jacinto de Matos, O. Minster, L. Cacciapuoti, M. Pfennigbauer, M. Aspelmeyer, T. Jennewein, R. Ursin, T. Schmitt-Manderbach, G. Baister, J. Rarity, W. Leeb, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Quantum communications at ESA: Towards a space experiment on the ISS," Acta Astronautica **63**, 165–178 (2008).

[156] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Metropolitan all-pass and inter-city quantum communication network," Optics Express **18**, 27217–27225 (2010).

[157] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," Journal of Computer and System Sciences **18**, 143–154 (1979).

[158] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," Journal of Computer and System Sciences **22**, 265–279 (1981).

[159] V. Scarani and R. Renner, "Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing," Physical Review Letters **100**, 200501 (2008).

[160] L. Sheridan, T. P. Le, and V. Scarani, "Finite-key security against coherent attacks in quantum key distribution," New Journal of Physics **12**, 123019 (2010).

[161] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," arXiv:1103.4130 [quant-ph].

[162] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate," Optics Express **16**, 18790–18979 (2008).

[163] J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tanaka, and A. Tomita, "Experimental decoy state quantum key distribution with unconditional security incorporating finite statistics," arXiv:0705.3081 [quant-ph].

[164] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, "Security of two quantum cryptography protocols using the same four qubit states," Physical Review A **72**, 032301 (2005).

[165] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Physical Review A **72**, 012326 (2005).

[166] L. Lydersen and J. Skaar, "Security of quantum key distribution with bit and basis dependent detector flaws," Quantum Information & Computation **10**, 60–76 (2010).

[167] H. F. Chau, "Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate," Physical Review A **66**, 060302 (2002).

[168] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, "Device calibration impacts security of quantum key distribution," Physical Review Letters (in press).

[169] V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," Journal of Modern Optics **52**, 691–705 (2005).

[170] V. Makarov and J. Skaar, "Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols," Quantum Information & Computation **8**, 622–635 (2008).

[171] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, "Security proof of quantum key distribution with detection efficiency mismatch," Quantum Information & Computation **9**, 131–165 (2009).

[172] T. Moroder, M. Curty, and N. Lütkenhaus, "Detector decoy quantum key distribution," New Journal of Physics **11**, 045008 (2009).

[173] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, Ch. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem," New Journal of Physics **13**, 013043 (2011).

[174] L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "Superlinear threshold detectors in quantum cryptography," Physical Review A (in press).

[175] L. Lydersen, V. Makarov, and J. Skaar, "Secure gated detection scheme for quantum cryptography," Physical Review A **83**, 032306 (2011).

[176] L. Lydersen, J. Skaar, and V. Makarov, "Tailored bright illumination attack on distributed-phase-reference protocols," Journal of Modern Optics **58**, 680–685 (2011).

[177] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," Optics Express **18**, 27938–27954 (2010).

[178] Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Avoiding the detector blinding attack on quantum cryptography," Nature Photonics **4**, 800–801 (2010).

[179] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Reply to 'Avoiding the blinding attack in QKD'," Nature Photonics **4**, 801 (2010).

[180] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, "Controlling a superconducting nanowire single-photon detector using tailored bright illumination," arXiv:1106.2396 [quant-ph].

[181] Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography," Applied Physics Letters **98**, 231104 (2011).

[182] L. Lydersen, V. Makarov, and J. Skaar, "Comment on 'resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography'," arXiv:1106.3756 [quant-ph].

[183] R. Alléaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier, N. Lütkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, "SECOQC white paper on quantum key distribution and cryptography," arXiv:quant-ph/0701168.

[184] E. Klarreich, "Quantum cryptography: Can you keep a secret?" Nature **418**, 270–272 (2002).

[185] B. Schneier, "Crypto-gram: Qunatum cryptography," (2003), `http://www.schneier.com/crypto-gram-0312.html#6`, visited 19th April 2011.

[186] B. Schneier, "Schneier on security: Switzerland protects its vote with quantum cryptography," (2007), `http://www.schneier.com/blog/archives/2007/10/switzerland_pro.html`, visited 19th April 2011.

[187] K. G. Paterson, F. Piper, and R. Schack, "Quantum cryptography: a practical information security perspective," in *Quantum Communication and Security*, NATO Advanced Research Workshop, edited by S. Kilin, M. Żukowski, and J. Kowalik (IOS Press, Amsterdam, 2007) pp. 175–180.

[188] B. Schneier, "Quantum cryptography: As awesome as it is pointless," Wired (2008), `http://www.wired.com/politics/security/commentary/securitymatters/2008/10/securitymatters_1016`, visited 19th April 2011.

[189] D. Stebila, M. Mosca, and N. Lütkenhaus, "The case for quantum key distribution," in *Quantum Communication and Quantum Networking*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 36, edited by O. Akan *et al.* (Springer, Berlin, Heidelberg, 2010) pp. 283–296.

[190] ID Quantique Cerberis datasheet: `http://www.idquantique.com/images/stories/PDF/cerberis-encryptor/cerberis-specs.pdf`, visited 19th April 2011.

[191] G. M. Smith, K. A. McIntosh, J. P. Donnelly, J. E. Funk, L. J. Mahoney, and S. Verghese, “Reliable InP-based Geiger-mode avalanche photodiode arrays,” in *Advanced Photon Counting Techniques III*, Vol. 7320, edited by M. A. Itzler and J. C. Campbell (SPIE, 2009) p. 73200R.

[192] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, “Quantum repeaters: The role of imperfect local operations in quantum communication,” Physical Review Letters **81**, 5932–5935 (1998).

[193] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, “Quantum repeaters based on atomic ensembles and linear optics,” Reviews of Modern Physics **83**, 33–80 (2011).

Paper A

Security of quantum key distribution with bit and basis dependent detector flaws

Published in Quantum Information & Computation.

arXiv: 0807.0767 [quant-ph]

Quantum Information and Computation, Vol. 10, No. 1&2 (2010) 0060–0076
© Rinton Press

SECURITY OF QUANTUM KEY DISTRIBUTION WITH BIT AND BASIS DEPENDENT DETECTOR FLAWS

LARS LYDERSEN[a] JOHANNES SKAAR
Department of Electronics and Telecommunications, Norwegian University of Science and Technology
NO-7491 Trondheim, Norway
and
University Graduate Center, NO-2027 Kjeller, Norway

Received July 04, 2008
Revised September 3, 2009

We consider the security of the Bennett-Brassard 1984 (BB84) protocol for Quantum Key Distribution (QKD), in the presence of bit and basis dependent detector flaws. We suggest a powerful attack that can be used in systems with detector efficiency mismatch, even if the detector assignments are chosen randomly by Bob. A security proof is provided, valid for any basis dependent, possibly lossy, linear optical imperfections in the channel/receiver/detectors. The proof does not assume the so-called squashing detector model.

Keywords: Quantum cryptography, quantum key distribution, security proof, detection efficiency mismatch
Communicated by: H-K Lo & R Laflamme

1 Introduction

Quantum mechanics makes it possible to exchange a random bit string at a distance [1, 2, 3, 4]. In theory, the key distribution is secure, even if an eavesdropper Eve can do anything allowed by the currently known laws of nature [5, 6, 7, 8].

In practical QKD systems there will always be imperfections. The security of QKD systems with a large variety of imperfections has been proved [5, 9, 10, 11]. However, a QKD system is relatively complex, and loopholes and imperfections exist that are not covered by existing security proofs. A security loophole can be dealt with in two different ways: Either you modify the implementation, or you increase the amount of privacy amplification [12] required to remove Eve's information about the key. The first approach, to modify the implementation, may often be done without decreasing the rate of which secret key can be generated. It may however increase the complexity of the implementation, which in turn may lead to new loopholes. The advantages of the second approach, to increase the amount of privacy amplification, are that the apparatus can be kept as simple as possible, and that existing implementations can be made secure with a software update. A drawback is clearly the reduced key rate, which is considered as a critical parameter in commercial QKD systems.

One of the imperfections to be considered in this paper, is called detector efficiency mismatch (DEM) [13]. If an apparatus has DEM, Eve can control the efficiencies of Bob's

[a] Email: lars.lydersen@iet.ntnu.no

detectors by choosing a parameter t in some external domain. Examples of such domains can be the timing, polarization, or frequency of the photons [13, 14].

To be more concrete, consider DEM in the time-domain. In most QKD systems Bob's apparatus contains two single photon detectors to detect the incoming photons, one for each bit value. (Equivalently, two different detection windows of a single detector can be used for the two bit values (time-multiplexed detector).) Normally the detectors are gated in the time-domain to avoid high dark-counts. This means that electronic circuits are used to turn the detectors on and off, creating detection windows. Different optical path lengths, inaccuracies in the electronics, and finite precision in detector manufacturing may cause the detection windows of the two detectors to be slightly shifted, as seen in Fig. 1. The shift means that there exist times where the two detectors have different efficiencies.

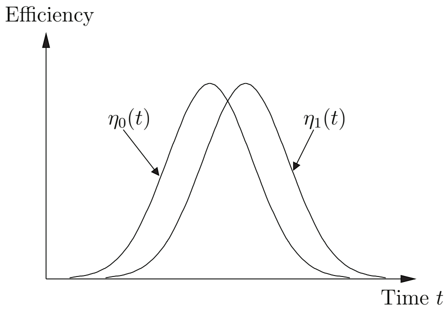


Fig. 1. An example of mismatched efficiency curves for two detectors in the time-domain. The functions $\eta_0(t)$ and $\eta_1(t)$ are the efficiencies of detector 0 and 1, respectively. The parameter t can be used to parametrize other domains as well.

Systems with DEM can be attacked with a faked-states attack [13]. The faked-states attack is an intercept-resend attack where Eve does not try to reconstruct the original state sent by Alice, but rather exploit the imperfections in Bob's apparatus to hide errors. The faked-states attack can be adapted to the Scarani-Acin-Ribordy-Gisin 2004 (SARG04), Ekert, and Differential Phase Shift Keying (DPSK) protocols, in addition to BB84 [15]. Another attack on systems with DEM is the time-shift attack [16]. In this attack Eve just selects the timing of each qubit randomly, thereby gaining information about the bit value when Bob announces which qubits were received and which were lost. The major advantage of the time-shift attack is that it does not introduce any quantum bit error rate (QBER). It has been demonstrated experimentally that the security of a commercially available QKD system can be compromised with a time-shift attack [17].

A frequently mentioned countermeasure for systems with DEM is called *four-state Bob* [18, 19, 13, 16]. In a phase-encoded QKD system, Bob chooses from four different phase settings $\{0, \pi/2, \pi, 3\pi/2\}$ instead of only two $\{0, \pi/2\}$. This will randomly assign the bit values 0 and 1 to the detectors (or the detection windows, in the case of one time-multiplexed detector) for each received state. Therefore Eve does not know which detector characteristics that corresponds to the 0 and 1 detectors.

However, as mentioned previously [13, 16] Eve may use a large laser pulse attack [20, 21, 22, 23] to read Bob's phase modulator settings. In a large pulse attack Eve uses a strong laser pulse to measure the reflections from either Alice's or Bob's apparatus. The setting of the phase modulator may give a signature on the reflections, enabling Eve to obtain the phase.

First assume that Eve is able to read Alice's modulator settings. Then Eve could obtain bit and/or basis information before the pulse enters Bob's apparatus, and therefore the security would be seriously compromised. Fortunately, Alice's implementation can easily be modified to avoid the large pulse attack. A setup with a coherent laser source contains an attenuator, and moving this to the end of the apparatus, as well as introducing an optical isolator, will put impossible requirements on Eve's laser [22]. In "plug-and-play" systems Alice already uses a detector to monitor the input of her setup. Therefore a large pulse attack can easily be revealed by monitoring the intensity of the input.

In a straightforward implementation of BB84, the phase modulator setting in Bob's setup only contains basis information. It usually poses no security threat if Eve reads the basis, as she will get it during the public discussion anyway. One only has to avoid that Eve receives the basis information before the pulse enters Bob's apparatus. This can be taken care of by placing a properly long coil of optical fiber at the entrance of Bob's setup.

However, if the DEM loophole is patched with four-state Bob, the large pulse attack is dangerous, because it may give Eve information about the detector assignments. Modifying Bob's setup to avoid large pulse attacks is not an easy task. The most practical solution seems to be a beam splitter or an optical circulator combined with an intensity detector [22]. Note that the key rate will suffer; the the input of Bob's setup is precious single photons. Also the setup gets more complex, which should be avoided as far as possible, to limit the number of "hidden surprises". It is therefore not obvious whether such modifications should be implemented, or whether the security should be regained with extra privacy amplification. Even though some systems implement four-state Bob, several of them lack countermeasures for a strong pulse attack on Bob's side. Therefore we will pursue the latter solution, i.e., we assume that Eve is able to read Bob's phase modulator setting after Bob's detection.

Security bounds state a unconditionally secure key rate, positive a range in some parameter(s). Ideally one should be able to prove the converse, namely that with the parameter(s) outside this range the QKD-system is provable insecure. Unfortunately this is not always simple. Usually there is a third range of the parameter(s) where it is not known whether the QKD-protocol is secure. For instance with perfect devices and one-way classical communication, the QKD-system is unconditionally secure for QBER < 11 % [8], and provable insecure for QBER > 14.6 % [24]. Until the gap is closed the security bounds represent a lower bound on the secure key rate, and the best known attacks represent an upper bound.

Fung et al. found a security bound for QKD systems with DEM [14]. QKD systems with four-state Bob is proved to be secure, provided Eve cannot read Bob's phase settings with a large pulse attack. The security proof assumes the so-called squashing model [11].

In this paper we first establish an upper bound for the secure key rate of QKD-system with DEM by presenting two powerful attacks, one of which even applies to implementations with four-state Bob (Section II). Then we will establish a lower bound for the secure key rate by providing a simple security proof of QKD systems with general, basis and bit dependent detector flaws (Section III), generalizing the proof by Fung et al. More precisely, any basis dependent, possibly lossy, linear optical imperfections in the channel and receiver are covered by the proof. For example, the proof covers mixing between all available optical modes, misalignments, mode-dependent losses, DEM, and any basis dependence of those effects. The proof is formulated for a decoy-state BB84 protocol and does not assume a squashing model. Finally, in Section IV we will examine some examples, including DEM, DEM with mode mixing, and DEM with misalignment.

2 Security analysis: upper bound

In this section we analyse two powerful attacks on systems with DEM. Such attacks are important because they establish a regime where QKD-systems with DEM is provable insecure. To analyze the attacks, for the moment we define $\eta = \max\{\min_t \eta_1(t)/\eta_0(t), \min_t \eta_0(t)/\eta_1(t)\} \in [0,1]$, representing the smallest efficiency ratio available for both bit values. For individual attacks the secret key rate is given by [12, 25] (given one-way classical communication)

$$R = I(\alpha:\beta) - I(\alpha:\epsilon), \tag{1}$$

where $I(\cdot:\cdot)$ denotes mutual information and α, β, and ϵ represent Alice's, Bob's and Eve's bits.

In the previous analysis of the faked-states attack [13], the attack was limited by the introduced QBER rather than Eve's insufficient knowledge about the key. By attacking only a fraction of the bits with the faked-states attack one can compromise the security for even higher values of η. The other fraction could be attacked with the time-shift attack [16] which introduces no QBER.

To tailor E, the QBER measured by Alice and Bob, the fraction r attacked by the faked-states attack is given by

$$r = \frac{E}{E_{\text{fs}}} = E\frac{1+3\eta}{2\eta}, \tag{2}$$

where $E_{\text{fs}} = 2\eta/(1+3\eta)$ is the QBER introduced by the faked-states attack. The mutual information between Alice and Eve is given by

$$\begin{aligned} I(\alpha:\epsilon) &= rI(\alpha:\epsilon)_{\text{fs}} + (1-r)I(\alpha:\epsilon)_{\text{ts}} \\ &= 1 - E - h(\frac{\eta}{1+\eta})\left(1 - \frac{1+3\eta}{2\eta}E\right), \end{aligned} \tag{3}$$

where r is given in (2) and $I(\alpha:\epsilon)_{\text{fs}} = 1-E$ and $I(\alpha:\epsilon)_{\text{ts}} = 1 - h(\eta/(1+\eta))$ denote the mutual information in the faked-states and the time-shift attack, respectively, as given in Refs [13, 16]. $h(\cdot)$ is the binary entropy function. Since Alice and Bob does not know how each bit is attacked, $I(\alpha:\beta)$ is simply given by $1-h(E)$. The key rate (1) thus becomes

$$R = E + h(\frac{\eta}{1+\eta})\left(1 - \frac{1+3\eta}{2\eta}E\right) - h(E). \tag{4}$$

Without considering DEM, Alice and Bob think that the key is secure when QBER $< 11\%$ (symmetric protocols with one-way classical communication [8]). Solving the equality $R=0$, where R is given by (4), and setting $E = 0.11$ gives $\eta = 0.215$.

The above combined attack is implementable with current technology. Up to $\eta = 0.160$ it represent an upper bound on the secure key rate (see Fig. 3). However with four-state Bob, the attack is impossible since the faked-states attack requires knowledge of the bit-detector mapping before Bob receives the pulse.

For higher values of η there exists an even more efficient attack. The optimal individual attack in the absence of imperfections is known [24]. Here Eve lets the qubit from Alice interact with a probe. After the basis is revealed, Eve's probe is in one of two non-orthogonal states [24]

$$|\xi_0\rangle = |0\rangle \tag{5a}$$

$$|\xi_1\rangle = \cos\varphi|0\rangle + \sin\varphi|1\rangle, \tag{5b}$$

where φ is related to the QBER by

$$\cos\varphi = 1 - 2E. \tag{6}$$

Eve has to separate between $|\xi_0\rangle$, corresponding to the bit value 0 at Alice, and $|\xi_1\rangle$, corresponding to the bit value 1. The two states occur with an *a priori* probability 1/2.

In the presence of DEM, we improve the attack as follows: In addition to using a probe, Eve launches a time-shift attack. If Bob announces receipt, the probabilities of the two bit values is now $\{1/\left(1+\eta\right), \eta/\left(1+\eta\right)\}$ according to the time-shift attack [16]. Then after the public discussion, Eve has to separate between the states (5) with the *a priori* probabilities $\{1/\left(1+\eta\right), \eta/\left(1+\eta\right)\}$. The optimal measurement is projective [26], and the probability p of Eve measuring the correct bit value is found to be

$$\begin{aligned} p = &\left(\frac{1}{1+\eta}\right)\cos^2\left[\frac{1}{2}\arctan\left(\frac{\sin 2\varphi}{\frac{1}{\eta}-\cos 2\varphi}\right)\right] \\ &+\left(\frac{\eta}{1+\eta}\right)\sin^2\left[\varphi+\frac{1}{2}\arctan\left(\frac{\sin 2\varphi}{\frac{1}{\eta}-\cos 2\varphi}\right)\right], \end{aligned} \tag{7}$$

where φ is related to the QBER as in Eq. (6).

Since Eve has probability p to have the same bit value as Alice, $I(\alpha:\epsilon)$ is simply $1-h(p)$. $I(\alpha:\beta)$ is given by $1-h(E)$. The key rate (1) for this improved optimal individual attack is thus

$$R = h(p) - h(E), \tag{8}$$

where p is given by (7).

Without considering DEM, Alice and Bob think that the key is secure when QBER $< 11\%$. Solving the equality $R = 0$, where R is given by (8), and setting $E = 0.11$ gives $\eta = 0.252$. In a commercial QKD system η was found to be approximately 0.25 (see Fig. 3 in [17]) [b] Therefore, this attack could be used to compromise the security of such QKD systems. Note that the attack does not require the bit-detector mapping until the post-processing step. Therefore systems patched with four-state Bob are vulnerable to the attack combined with a large pulse attack.

Note that the both attacks represent a substantial improvement compared to the previously published attacks which require $\eta < 0.066$ [13]. Fig. 3 shows the range of E, η which compromises security, and compares the two attacks.

[b] Also note that the DEM found in this system is heavily asymmetric, and the attacks might be more powerful if optimized for asymmetric DEM.

3 Security analysis: lower bound

In this section we will prove the security of the BB84 protocol in the presence of bit and basis dependent detector flaws, and establish the secure key generation rate. We will prove the security in a general setting, lifting the so-called squashing model assumption. That is, Eve may send any multimode, photonic state, and Bob uses practical threshold detectors. Alice may use a single-photon source or phase-randomized faint laser pulses; in the latter case, Alice may use decoy states [27, 28, 29] to estimate photon-number dependent parameters. Alice's source is otherwise assumed perfect: It emits an incoherent mixture of photonic number states, randomly in logical modes "0" or "1", randomly in the X or Z bases, with no correlation between the bits, bases, and photon number statistics [30].

The state space accessible to Eve consists of the Fock space associated with all photonic modes supported by the channel. The channel and receiver is modeled as a basis-dependent quantum operation, $\mathcal{C}_Z$ and $\mathcal{C}_X$, in front of two threshold detectors. Here Z and X denote the bases chosen by Bob. Since reduced detector efficiencies can be absorbed into the quantum operations, we can let Bob's threshold detectors have perfect efficiency. Dark counts are attributed to Eve, and for double click events, Bob assigns a random value to his bit [9, 11].

In our security proof, the key condition of $\mathcal{C}_Z$ and $\mathcal{C}_X$ is that they are passive, in the sense of

$$|0\rangle \to |0\rangle, \tag{9}$$

where $|0\rangle$ denotes the vacuum state of all modes. In other words, vacuum incident to all modes gives vacuum out. This condition is rather general; it includes all linear and nonlinear optical transformations of the modes supported by the channel.

For simplicity, however, we will restrict ourselves to linear optical imperfections. Bob's two detectors may still have different efficiencies, depending on the time, frequency, and/or polarization of the incoming states. Moreover, there may be imperfections in the channel and Bob's receiver. This can be described as arbitrary, square matrices C_Z and C_X, acting on the *channel modes* after Eve's intervention. The linear-optical property of C_Z and C_X is ensured from the fact that they are classical transformations (or transfer matrices) operating on the physical, photonic modes (e.g. temporal modes and polarization modes) rather than the total Fock space of the modes. Each mode can contain any photonic state such as number states or coherent states. Although C_Z and C_X have finite dimension, the associated, induced quantum operations $\mathcal{C}_Z$ and $\mathcal{C}_X$ operate on an infinite dimensional Fock space. We use the convention that Bob's basis selector is included in C_X (see Subsection 4.1).

With singular value decomposition, we can write

$$C_Z = U_Z F_Z V_Z C, \tag{10}$$

where U_Z and V_Z are unitary operators, and F_Z is a diagonal, positive matrix. In addition to the usual singular value decomposition, we have included an extra matrix factor C, governing losses and imperfections in the channel and/or receiver, independent of the basis chosen by Bob. The matrix C may for example describe loss of the channel and time-dependent detector efficiencies common for the two detectors. The operator C can be absorbed into Eve's attack, thus it never appears in the following analysis. The unitary operators U_Z and V_Z mix the modes together. For example, V_Z is the result of sending the modes through a network isomorphic to the type in [31]. The diagonal matrix F_Z represents the different efficiencies of the two detectors (in addition to basis-dependent absorptions in the receiver), and satisfies

$$|F_Z|^2 = \mathrm{diag}\left[\eta_{Z0}(t_1) \quad \eta_{Z1}(t_1) \quad \eta_{Z0}(t_2) \quad \eta_{Z1}(t_2)\ldots\right]. \tag{11}$$

The parameters $t_j, j = 1, 2, \ldots$ label different modes. For example, t_j may correspond to different temporal modes. In the absence of U_Z and V_Z, $\eta_{Z0}(t_j)$ and $\eta_{Z1}(t_j)$ can be viewed as the efficiencies of detector 0 and 1 in the Z-basis. Otherwise the efficiencies $\eta_{Z0}(t_j)$ and $\eta_{Z1}(t_j)$ do not necessarily correspond to the detectors 0 and 1, respectively, nor to detection time t_j. However, the notation is selected as in the special case for intuition. Note that F_Z may be represented as a collection of beam splitters with transmittivities $\eta_{Z0}(t_1)$, $\eta_{Z1}(t_1)$, and so forth. Then each mode is incident to its own beam splitter, and the vacuum state is sent into the other input.

The resulting model is shown in Fig. 2a. In the model we have included an extra measurement, giving information to Eve whether the total state is equal to the vacuum $|0\rangle$. While this information actually comes from Bob, it is convenient to let Eve obtain this information from a separate measurement. Note that this extra vacuum measurement does not disturb Bob's measurement statistics for any basis choice.

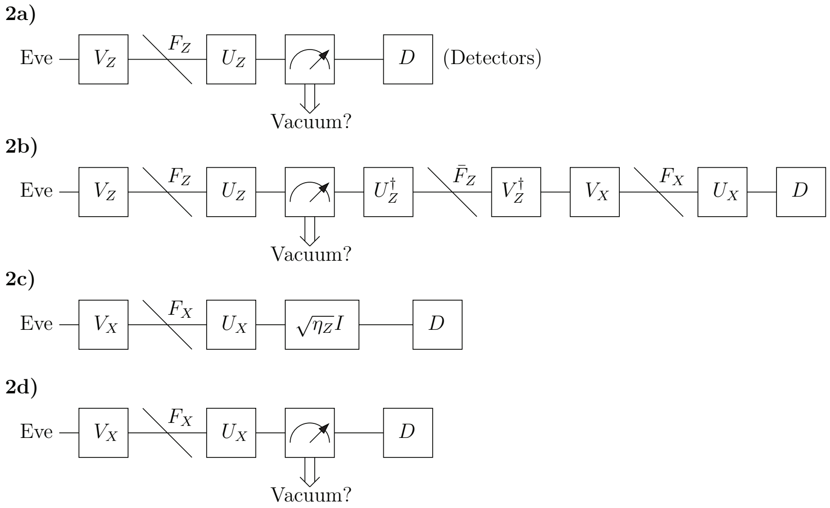


Fig. 2. a) Actual protocol. b) Estimation of Alice's virtual X-basis measurement. c) Simplification of Fig. 2b from Bob's point of view. d) Actual parameter estimation in the X-basis.

We will prove security using Koashi's argument [32, 33, 30] which we briefly summarize here. In the BB84-like actual protocol Alice generates a large number of bipartite states, where her part consists of a qubit which she measures randomly in the X- or Z-basis. The other part of the pairs is sent to Bob via Eve. Bob measures what he receives from Eve randomly in two different bases, which we will refer to as the "X-basis" or the "Z-basis". For example, for polarization encoding Bob's two measurements should ideally correspond to threshold detectors in horizontal/vertical or ±45° polarization bases, with double clicks as random assignment. Alice and Bob discard all events where they used incompatible basis. Further he publicly announces receipt if he receives something different from vacuum. Let Q_X and Q_Z be the fractions of non-vacuum results in each basis. Alice and Bob compare their X-basis measurement results to estimate Q_X and the error rate E_X. The N states measured in the Z-basis yield NQ_Z non-vacuum results. For these NQ_Z events Alice's measurement result is the raw key.

The required amount of privacy amplification can be found as follows: imagine a virtual experiment where Alice measures the qubits for the raw key in the X-basis instead of the Z-basis. Bob tries to predict the result of Alice's virtual X-basis measurement. Bob does not perform such a prediction in practice; thus in this prediction we may let Bob do everything permitted by quantum mechanics, as long as he does not alter the information given to Eve. Let $H_{\mathrm{virt}X}(A|B = \mu)$ denote the entropy of Alice's virtual X-basis measurement result, given measurement result μ in Bob's prediction. It turns out that $H_{\mathrm{virt}X}(A|B = \mu)$ can be bounded using E_X and Q_X, so assume that $H_{\mathrm{virt}X}(A|B = \mu) \leq H$. Since the uncertainty about Alice X-measurement is less than H, the entropic uncertainty relation [34] suggests that any prediction (including Eves prediction) of the measurement result of Alice Z-basis measurement will have at least $NQ_Z - H$ entropy. Thus Alice can extract $NQ_Z - H$ bits of secret key. Rigorously, this rate is found by concertizing the privacy amplification procedure by universal hashing. Although Koashi's original proof is formulated with an obsolete security definition based on accessible information, the proof can easily be adapted to a composable security definition [35, 36, 37].

Bob must ensure that he has an identical raw key. Since it does not matter to Eve what Bob does (as long as he gives Eve the same information), he measures the bits for the raw key in the Z-basis. Alice and Bob compares a subset of the raw key to find the error rate E_Z (consuming some of the raw key, but negliable in the asymptotic limit), and Alice sends Bob $NQ_Zh(E_Z)$ bits of error correcting information consuming $NQ_Zh(E_Z)$ bits of previously established secret key. In the asymptotic limit $N \to \infty$ the net secure key generation rate becomes

$$R_Z \geq 1 - \frac{H}{NQ_Z} - h(E_Z). \tag{12}$$

Note that H is needed to ensure that Alice's key is secret, and this only requires X-basis parameters to be estimated by Alice and Bob. Thus there is no need to invoke the classicalization argument [7] regarding statistics of measurements involved in the simultaneous estimation of E_X and E_Z.

For his prediction, Bob will use the virtual measurement in Fig. 2b. Bob first applies the unitary operator $U_Z^\dagger$, followed by the filter $\bar{F}_Z$, and the unitary operator $V_Z^\dagger$. Then he applies the operator $C_X = U_XF_XV_X$. Finally he performs an X-basis measurement. Note that we retain Eve's vacuum measurement and all components preceding it, so Eve obtains the identical information as in Fig. 2a. The matrix $\bar{F}_Z$ is diagonal, and is given by

$$\bar{F}_Z F_Z = \sqrt{\eta_Z} I, \tag{13}$$

where

$$\eta_Z = \min_{ij}\{\eta_{Zi}(t_j)\}. \tag{14}$$

Similarly to F_Z, the filter $\bar{F}_Z$ is implementable by beam splitters acting separately on each mode. The largest element of $|\bar{F}_Z|^2$ is 1, while the smallest element is $\eta_Z/\max_{ij}\{\eta_{Zi}(t_j)\}$.

To analyze how well Bob performs in his prediction, we will now simplify the system in Fig. 2b to determine Bob's measurement statistics. To do this, we introduce an extra vacuum measurement right before Bob's detectors, assuming nobody records the outcome. Clearly, Bob's measurement statistics are not altered by the presence of this extra measurement. The filter $U_X F_X V_X V_Z^\dagger \bar{F}_Z U_Z^\dagger$ obeys (9), being a linear optical transformation. As a result, we show in the appendix that the output state, after the extra vacuum measurement, is independent of the presence of Eve's vacuum measurement (i.e., the first vacuum measurement, after U_Z in Fig. 2b). Thus, to estimate Bob's measurement statistics, we can remove Eve's vacuum measurement. We end up with the simplified system shown in Fig. 2c. Note that the simplified system is identical to the system in Fig. 2d, the actual protocol when Bob has chosen the X-basis, except for one thing: There is an extra, mode-independent absorption η_Z in the channel. This fact will be used for estimating the performance of Bob's prediction.

To prove the security also for the multiphotonic case, we use the parameters $q_X^{(1)}$ and $e_X^{(1)}$ assumed known from the decoy state protocol. $q_X^{(1)}$ is the fraction of Bob's X-basis non-vacuum events that originate from single photons at Alice. $e_X^{(1)}$ is the QBER for single photon events in the X-basis (only single photons generate secure key). Consider the prediction in Fig. 2b-c. Let NQ_Z be the number of states in the raw key. In a worst case, the number of detection events that originate from single photons at Alice, will be only $\eta_Z q_X^{(1)} Q_X N$, due to the filter $\sqrt{\eta}_Z I$ (note that $\eta_Z Q_X < Q_Z$). For each of these events Bob's entropic uncertainty about Alice's bit is (asymptotically) $h(e_X^{(1)*})$, where $e_X^{(1)*}$ is the associated error rate. We note that $e_X^{(1)*}$ is not measured in the actual protocol; it will rather be estimated below. For the events lost in the filter $\sqrt{\eta}_Z I$, Bob's entropic uncertainty about Alice's bit is 1, since he has no detection result. Summarizing, Bob's entropic uncertainty about Alice's $Q_Z N$ bits (corresponding to the number of detection events in Fig. 2a) is at most $H = Q_Z N - \eta_Z q_X^{(1)} Q_X N[1 - h(e_X^{(1)*})]$. In our analysis we have ignored the events associated with Alice sending the vacuum state [30]; their contribution will only give a marginally larger rate. From (12) the secure key rate becomes

$$R_Z = -h(E_Z) + \eta_Z q_X^{(1)} Q_X/Q_Z \left[1 - h(e_X^{(1)*})\right]. \tag{15}$$

It remains to bound the parameter $e_X^{(1)*}$, which is the QBER for single photon events in the estimation Fig. 2b-c. Recall that $e_X^{(1)}$ is the estimated QBER for single photon events in the X-basis, Fig. 2d. The only difference between the setup in Fig. 2c and Fig. 2d is the filter $\sqrt{\eta}_Z I$, which represent identical absorption in all modes. However, the removal of detection events by this filter is dependent on the photon number, so $e_X^{(1)*} \neq e_X^{(1)}$ in general.[c] To bound $e_X^{(1)*}$ we use the fact that the filter only alter the detection statistics by removing detection events. (An exception occurs for the few coincidence counts; these can be taken into account easily.) In a worst case,

$$e_X^{(1)*} \leq \frac{e_X^{(1)}}{\eta_Z(1 - e_X^{(1)}) + e_X^{(1)}} \leq e_X^{(1)}/\eta_Z. \tag{16}$$

[c] Note that although Alice send a single photon for a particular event, Eve may send any state.

Putting these results together, we obtain the secure key generation rate

$$R_Z \geq -h(E_Z) + \eta_Z q_X^{(1)} Q_X/Q_Z \left[1 - h(e_X^{(1)}/\eta_Z)\right]. \tag{17}$$

A similar result holds when Alice and Bob have chosen the X-basis in the actual protocol:

$$R_X \geq -h(E_X) + \eta_X q_Z^{(1)} Q_Z/Q_X \left[1 - h(e_Z^{(1)}/\eta_X)\right]. \tag{18}$$

Ineqs. (17) and (18) are valid for any basis and bit dependence of the channel and receiver/detectors, as long as the imperfections (C_Z and C_X) can be described as possibly lossy, linear optical operators acting on the photonic modes.

To compare our result (17) to that of Ref. [14], we let Alice only send single photons. The rate then becomes

$$R \geq -h(E) + \eta[1 - h(E/\eta)], \tag{19}$$

where we have assumed symmetry between the bases, and therefore omitted the Z and X subscripts. The rate (19) coincides with the rate found in [14] (see Subsection 4.2 for a discussion on how to identify η). Note, however, that (19) is a stronger result in the sense that it applies to any basis-dependent linear optical imperfections, not only the case where $U_{Z,X} = I$, and $V_{Z,X}$ do not mix modes associated with different logical bits. Also it does not require the squashing model assumption.

Under the assumption that Eve only sends single photons, it is easy to realize that (16) can be replaced by $e_X^{(1)*} = e_X^{(1)}$. Then (19) is improved to

$$R \geq -h(E) + \eta[1 - h(E)]. \tag{20}$$

Fig. 3 shows the security bounds resulting from (19) and (20) when the right-hand side is set equal to zero.

4 Examples

4.1 DEM in the time-domain

Consider the case where Bob's detectors have time-dependent efficiencies, as indicated in Fig. 1. We assume that the efficiencies are independent of the basis chosen by Bob ($F_X = F_Z$). The channel and receiver are otherwise assumed perfect, except for a background loss C. The background loss may be mode dependent, but independent of the basis chosen by Bob.

With these assumptions, we may take $C_Z = F_Z C$ and $C_X = F_X HC = F_Z HC$, where H is a block-diagonal matrix consisting of 2×2 Hadamard matrices $H^{(2)}$, interchanging the bases Z and X for each time:

$$H = \mathrm{diag}\left[H^{(2)} \quad H^{(2)} \quad H^{(2)} \quad \ldots\right]. \tag{21}$$

To maximize the secure key rate, as much as possible of the detector flaws should be absorbed into C. Therefore, we factorize

$$F_Z = FF', \tag{22}$$

where

$$F'^2 = \mathrm{diag}\left[\eta'(t_1) \quad \eta'(t_1) \quad \eta'(t_2) \quad \eta'(t_2)\ldots\right], \tag{23}$$

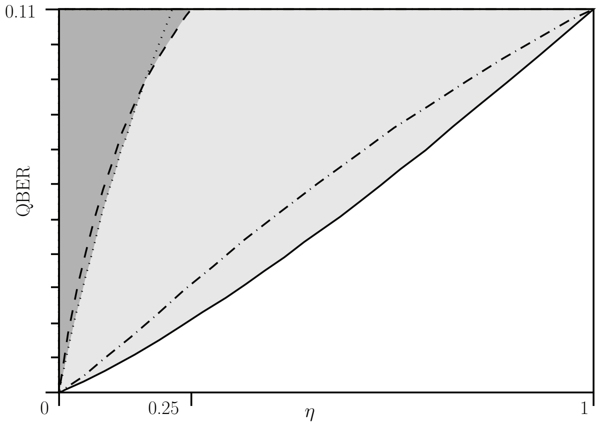


Fig. 3. Security bounds when Alice sends single photons ($q_Z^{(1)} = q_X^{(1)} = 1$), assuming symmetry between the bases. The bounds are found by setting the associated key generation rates equal to zero. Solid line: General security bound, as resulting from (19). Dash-dotted line: Security bound (20) assuming Eve sends single photons. Dashed line: The improvement of the optimal individual attack from Section 2, as resulting from (8). Dotted line: The combined attack from Section 2, as resulting from (4). For the attacks it is assumed that the DEM is equal for the two bit values. The dark grey region is proved to be insecure while the white region is proved to be secure with extra privacy amplification. The light grey region should be assumed insecure.

and $\eta'(t_j) = \max\{\eta_{Z0}(t_j), \eta_{Z1}(t_j)\}$. Noting that F' and H commute, we can absorb F' into C. The remaining diagonal matrix F then has the role of F_Z (and F_X) in the security proof. The parameter $\eta_Z = \eta_X$ to substitute into the secure key generation rate (17) is therefore the minimum diagonal element of $|F|^2$:

$$\eta_Z = \min_t \min\left\{\frac{\eta_{Z0}(t)}{\eta_{Z1}(t)}, \frac{\eta_{Z1}(t)}{\eta_{Z0}(t)}\right\}. \tag{24}$$

4.2 DEM and restricted mode mixing

Consider the case treated by Fung et al. [14], where there is no mixing between modes associated with different logical bits. Then C_Z can be written in block diagonal form

$$C_Z = \begin{bmatrix} C_0 & 0 \\ 0 & C_1 \end{bmatrix} C, \tag{25}$$

provided we reorder the modes as in

$$|F_Z|^2 = \mathrm{diag}\begin{bmatrix}\eta_{Z0}(t_1) & \eta_{Z0}(t_2) & \ldots & \eta_{Z1}(t_1) & \eta_{Z1}(t_2) & \ldots\end{bmatrix}, \tag{26}$$

to be compared to (11). As in Ref. [14] we assume basis independence in the sense

$$C_X = \begin{bmatrix} C_0 & 0 \\ 0 & C_1 \end{bmatrix} HC. \tag{27}$$

Here,

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} I & I \\ I & -I \end{bmatrix}, \tag{28}$$

with the present choice of mode order. We assume that C_Z is nonsingular. (Otherwise, the secure key generation rate would be zero.)

We should associate as much as possible of the imperfections to the common channel operator C. Let the singular-value decomposition of $C_0C_1^{-1}$ be usv, where u and v are unitary matrices, and s is diagonal and positive. Let λ^2 be the maximum of $\max s$ and $\max s^{-1}$. Factorize

$$C_Z = \lambda \begin{bmatrix} us^{1/2} & 0 \\ 0 & v^\dagger s^{-1/2} \end{bmatrix} \frac{1}{\lambda} \begin{bmatrix} s^{-1/2}u^\dagger C_0 & 0 \\ 0 & s^{1/2}vC_1 \end{bmatrix} C. \tag{29}$$

Defining

$$C' = \frac{1}{\lambda} \begin{bmatrix} s^{-1/2}u^\dagger C_0 & 0 \\ 0 & s^{1/2}vC_1 \end{bmatrix}, \tag{30}$$

and noting that $s^{-1/2}u^\dagger C_0 = s^{1/2}vC_1$, we have $C'H = HC'$. This gives

$$C_Z = \lambda \begin{bmatrix} us^{1/2} & 0 \\ 0 & v^\dagger s^{-1/2} \end{bmatrix} C'C, \tag{31a}$$

$$C_X = \lambda \begin{bmatrix} us^{1/2} & 0 \\ 0 & v^\dagger s^{-1/2} \end{bmatrix} HC'C. \tag{31b}$$

Similarly to the reasoning in Section III, Bob applies a virtual filter to transform C_Z into an operator proportional to C_X. Applying

$$\frac{1}{\lambda} \begin{bmatrix} us^{1/2} & 0 \\ 0 & v^\dagger s^{-1/2} \end{bmatrix} H \frac{1}{\lambda} \begin{bmatrix} s^{-1/2}u^\dagger & 0 \\ 0 & s^{1/2}v \end{bmatrix},$$

the operator C_Z is transformed into C_X/λ^2. Following Section III, $\sqrt{\eta} = 1/\lambda^2$. This gives

$$\sqrt{\eta} = \min(\min s, \min s^{-1}). \tag{32}$$

Equivalently, η is the minimum value of the eigenvalues and inverse eigenvalues of $C_0C_1^{-1}(C_0C_1^{-1})^\dagger = C_0(C_1^\dagger C_1)^{-1}C_0^\dagger$. This η should be substituted into (17) to find the secure key generation rate.

The parameter η can be measured as follows. For single photon input in a given superposition ψ of logical "0" modes, the probability of a click in detector 0 is given by $\psi^\dagger C_0^\dagger C_0\psi$. Similarly, we may use the identical superposition ψ of "1" modes to find the detection probability of detector 1. Note that ψ denotes a classical field vector, where each element corresponds to a separate mode. The parameter η turns out to be equal to the minimum detection probability ratio

$$\eta = \min\left(\min_\psi \frac{\psi^\dagger C_0^\dagger C_0\psi}{\psi^\dagger C_1^\dagger C_1\psi}, \min_\psi \frac{\psi^\dagger C_1^\dagger C_1\psi}{\psi^\dagger C_0^\dagger C_0\psi} \right). \tag{33}$$

In other words, η is given by the minimum efficiency mismatch ratio for all superpositions of input modes.

To see this, let $us^2u^\dagger$ be the spectral decomposition of $C_0(C_1^\dagger C_1)^{-1}C_0^\dagger$. Then we have

$C_0^{-1\dagger}(C_1^\dagger C_1)C_0^{-1} = us^{-2}u^\dagger$, and

$$\begin{aligned}\frac{\psi^\dagger C_1^\dagger C_1\psi}{\psi^\dagger C_0^\dagger C_0\psi} &= \frac{\psi'^\dagger C_0^{-1\dagger} C_1^\dagger C_1 C_0^{-1}\psi'}{\psi'^\dagger\psi'} \\ &= \frac{\psi'^\dagger u^\dagger s^{-2} u\psi'}{\psi'^\dagger\psi'} \\ &= s^{-2}.\end{aligned} \tag{34}$$

Combining (32) and (34) gives the desired result.

4.3 DEM and misalignments

In addition to the detector efficiency mismatch in Subsection 4.1, suppose that Bob's detectors are misaligned. The misalignments may be dependent on Bob's choice of basis, and are described by unitary matrices V_Z and V_X. This gives the channel operators $C_Z = F_Z V_Z C$ and $C_X = F_X V_X HC$. Assuming no coupling between different temporal modes (no multiple reflections), V_Z and V_X are block-diagonal matrices. For example,

$$V_Z = \operatorname{diag}\left[V_1^{(2)} \quad V_2^{(2)} \quad V_3^{(2)} \quad \ldots\right], \tag{35}$$

where $V_j^{(2)}$ are unitary 2×2 matrices. Here we have used the same order of modes as in the original definition (11). Taking $F_X = F_Z$ and factorizing as in Subsection 4.1, we find that the parameter $\eta_Z = \eta_X$ again is given by (24). The secure key generation rate is then found from (17).

If there is coupling between modes associated with different t's (in addition to the misalignment), we must retain the general definition of η_Z in (14). For unnormalized detection efficiencies, this definition can be rewritten

$$\eta_Z = \frac{\min_{i,t}\{\eta_{Zi}(t)\}}{\max_{i,t}\{\eta_{Zi}(t)\}}. \tag{36}$$

Eq. (36) is obtained by absorbing the maximum detector efficiency $\max_{i,t}\{\eta_{Zi}(t)\}$ into C. Omitting the requirement $F_X = F_Z$, (36) must be rewritten as

$$\eta_Z = \frac{\min_{i,t}\{\eta_{Zi}(t)\}}{\max\left(\max_{i,t}\{\eta_{Zi}(t)\}, \max_{i,t}\{\eta_{Xi}(t)\}\right)}. \tag{37}$$

4.4 Characterizing DEM of Bob's receiver

To estimate the secure key generation rate, Bob must characterize his receiver to find η_Z and η_X (or $\eta \equiv \min\{\eta_Z, \eta_X\}$). We note that rather different results are obtained dependent on whether or not there are coupling between different modes. For the case of DEM in the time-domain, since it is difficult to eliminate multiple reflections in Bob's receiver, a conservative approach is to use (37).

For the case with gated detectors, the efficiencies approach zero at the edges of the detection window. When there are coupling between different temporal modes, the resulting key generation rate will therefore be close to zero. Even if no such coupling is present, the key generation rate may approach zero, since at the edges of the detection window the efficiency ratio may be very small. (Although the average detection probability at the edges may be small, Eve may compensate this by replacing the channel by a more transparent one, or by increasing the power of her pulses [13].) A possible solution may be that Bob monitors his input signal at all times, to ensure that Eve does not send photons outside the central part of the window. Then η can be obtained by measuring the minimum and maximum detection efficiency for (superpositions of) modes with times inside this central part.

Such a measurement may be cumbersome due to many degrees of freedom of the possible inputs. Alternatively, one could specify the maximum possible amount of mode coupling in the system, and use this information to lower bound η. Suppose that the maximum (power) coupling from one mode j to all other modes is δ. Then the unitary matrix V_Z satisfies $\sum_{i,i\neq j} |V_{ij}|^2 < \delta$ in addition to $\sum_i |V_{ij}|^2 = 1$, omitting the subscript Z for clarity. Let $|f_j|^2$ be the jth diagonal element of F_Z. By measuring the detection efficiency when photons are incident to the jth mode, we obtain $\sum_i |V_{ij}|^2|f_i|^2 = |f_j|^2 + \sum_{i,i\neq j} |V_{ij}|^2 \left(|f_i|^2 - |f_j|^2\right)$. Hence, the elements $|f_j|^2$ can be found from the detection efficiency as a function of j of the incident mode, up to an error $\left|\sum_{i,i\neq j} |V_{ij}|^2 \left(|f_i|^2 - |f_j|^2\right)\right| < \delta$. A lower bound of η is therefore

$$\eta > \frac{\min_{t,\mathrm{basis},\mathrm{bit}}(\text{detection efficiency}) - \delta}{\max_{t,\mathrm{basis},\mathrm{bit}}(\text{detection efficiency}) + \delta}. \tag{38}$$

The required measurement is to obtain the detection efficiency as a function of t and logical bit value for both bases. For detection efficiency mismatch in the time-domain the test pulses should be sufficiently short, in order to capture all details. An upper bound of the parameter δ may be estimated from the (worst case) multiple reflections and misalignment's that may happen in the system.

5 Discussion and conclusion

In this work we have proved the security of BB84 in the presence of any basis dependent, possibly lossy, linear optical imperfections in the channel and receiver/detectors. The security proof thus covers a combination of several imperfections: Detection efficiency mismatch, misalignments, mixing between the modes, multiple reflections, and any basis dependence of those effects. Contrary to most previous security proofs, this proof does not require a squashing detector model.

A specific implementation of a QKD system may have several different imperfections. Ideally there should be a universal security proof with a set of parameters that cover all (worst case) imperfections and tolerances of the equipment. We have made a step towards this goal by describing generic imperfections at the detector, and by providing a compact proof, which may hopefully prove useful for an even more general description.

We have established an upper bound for the secure key rate by providing two powerful attacks. One of the attacks may be applied to systems even with the four-state Bob patch, and this demonstrates the seriousness of the detection efficiency loophole. This attack is based on a combination of an optimal individual attack, a time shift attack, and a large pulse attack. As a consequence of such types of attacks, the key generation rate may not increase substantially as a result of the four-state Bob patch. A possible countermeasure is to use the general bounds (17) and (18) for estimating the required amount of privacy amplification.

Acknowledgements

We would like to thank Vadim Makarov for comments and discussions. Financial support from NTNU and the Research Council of Norway (grant no. 180439/V30) is acknowledged.

References

1. C. H. Bennett and G. Brassard (1984), *Quantum cryptography: Public key distribution and coin tossing* in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE Press, New York, Bangalore, India, pp. 175–179.
2. A. K. Ekert (1991), *Quantum cryptography based on bell theorem*, Phys. Rev. Lett., Vol. 67, pp. 661–663.
3. C. H. Bennett (1992), *Quantum cryptography using any 2 nonorthogonal states*, Phys. Rev. Lett., Vol. 68, pp. 3121–3124.
4. N. Gisin, G. G. Ribordy, W. Tittel and H. Zbinden (2002), *Quantum cryptography*, Rev. Mod. Phys., Vol. 74, pp. 145–195.
5. D. Mayers (1996), *Advances in cryptology* in N. Koblitz, editor, *Proceedings of Crypto'96*, Vol. 1109, Springer, New York, pp. 343–357.
6. D. Mayers (2001), *Unconditional security in quantum cryptography*, J. Assoc. Comp. Mach., Vol. 48, pp. 351–406.
7. H.-K. Lo and H. F. Chau (1999), *Unconditional security of quantum key distribution over arbitrarily long distances*, Science, Vol. 283, pp. 2050–2056.
8. P. W. Shor and J. Preskill (2000), *Simple proof of security of the BB84 quantum key distribution protocol*, Phys. Rev. Lett., Vol. 85, pp. 441–444.
9. H. Inamori, N. Lütkenhaus and D. Mayers (2001), *Unconditional security of practical quantum key distribution*, e-print quant-ph/0107017.
10. M. Koashi and J. Preskill (2003), *Secure quantum key distribution with an uncharacterized source*, Phys. Rev. Lett., Vol. 90, 057902.
11. D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill (2004), *Security of quantum key distribution with imperfect devices*, Quant. Inf. Comp., Vol. 4, pp. 325–360.
12. I. Csiszàr and J. Körner (1978), *Broadcast channels with confidential messages*, IEEE Trans. Inf. Theory, Vol. 24, pp. 339–348.
13. V. Makarov, A. Anisimov and J. Skaar (2006), *Effects of detector efficiency mismatch on security of quantum cryptosystems*, Phys. Rev. A, Vol. 74, 022313; Ibid. **78**, 019905 (2008).
14. C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo and X. Ma (2009), *Security proof of quantum key distribution with detection efficiency mismatch*, Quant. Inf. Comp., Vol. 9, pp. 131–165.
15. V. Makarov and J. Skaar (2008), *Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols*, Quant. Inf. Comp., Vol. 8, 0622.
16. B. Qi, C. H. F. Fung, H.-K. Lo and X. F. Ma (2007), *Time-shift attack in practical quantum cryptosystems*, Quant. Inf. Comp., Vol. 7, pp. 73–82.
17. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen and H.-K. Lo (2008), *Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems*, Phys. Rev. A, Vol. 78, 042333.
18. P. M. Nielsen, C. Schori, J. L. Sørensen, L. Salvail, I. Damgård and E. Polzik (2001), *Experimental quantum key distribution with proven security against realistic attacks*, J. Mod. Opt., Vol. 48, pp. 1921–1942.
19. M. LaGasse (2005), *Secure use of a single single-photon detector in a qkd system*, US patent application 20050190922.
20. G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard and H. Zbinden (2000), *Fast and user-friendly quantum key distribution*, J. Mod. Opt., Vol. 47, pp. 517–531.
21. D. S. Bethune and W. P. Risk (2000), *An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light*, IEEE J. Quantum Electron., Vol. 36, pp. 340–347.

22. A. Vakhitov, V. Makarov and D. R. Hjelme (2001), *Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography*, J. Mod. Opt., Vol. 48, pp. 2023–2038.
23. N. Gisin, S. Fasel, B. Kraus, H. Zbinden and G. Ribordy (2006), *Trojan-horse attacks on quantum-key-distribution systems*, Phys. Rev. A, Vol. 73, 022320.
24. C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu and A. Peres (1997), *Optimal eavesdropping in quantum cryptography .1. information bound and optimal strategy*, Phys. Rev. A, Vol. 56, pp. 1163–1172.
25. U. M. Maurer (1993), *Secret key agreement by public discussion from common information*, IEEE Trans. Inf. Theory, Vol. 39, pp. 733–742.
26. L. B. Levitin (1995), *Optimal quantum measurements for two pure and mixed states* in V. P. Belavkin,O. Hirota and R. L. Hudson, editors, *Quantum Communications and Measurement*, Plenum Press, New York, pp. 439–448.
27. W. Y. Hwang (2003), *Quantum key distribution with high loss: Toward global secure communication*, Phys. Rev. Lett., Vol. 91, 057901.
28. X.-B. Wang (2005), *Beating the photon-number-splitting attack in practical quantum cryptography*, Phys. Rev. Lett., Vol. 94, 230503.
29. H.-K. Lo, X. F. Ma and K. Chen (2005), *Decoy state quantum key distribution*, Phys. Rev. Lett., Vol. 94, 230504.
30. M. Koashi (2006), *Efficient quantum key distribution with practical sources and detectors*, e-print quant-ph/0609180v1.
31. M. Reck, A. Zeilinger, H. J. Bernstein and P. Bertani (1994), *Experimental realization of any discrete unitary operator*, Phys. Rev. Lett., Vol. 73, pp. 58–61.
32. M. Koashi (2005), *Simple security proof of quantum key distribution via uncertainty principle*, e-print quant-ph/05051080v1.
33. M. Koashi (2006), *Simple security proof of quantum key distribution via uncertainty principle*, J. of Phys. Conference Series, Vol. 36, 98.
34. H. Maassen and J. B. M. Uffink (1988), *Generalized entropic uncertainty relations*, Phys. Rev. Lett., Vol. 60, pp. 1103–1106.
35. R. Renner and R. Koenig (2005), *Universally composable privacy amplification against quantum adversaries* in J. Kilian, editor, *Second Theory of Cryptography Conference, TCC 2005*, Vol. 3378 of *LNCS*, Springer Verlag, Berlin, pp. 407–425, also available at http://arxiv.org/abs/quant-ph/0403133.
36. M. Ben-Or, M. Horodecki, D. Leung, D. Mayers and J. Oppenheim (2005), *The universal composable security of quantum key distribution* in *Second Theory of Cryptography Conference*, Vol. 3378 of *Lecture Notes in Computer Science*, Springer, New York, pp. 386–406.
37. H.-K. Lo and J. Preskill (2007), *Security of quantum key distribution using weak coherent states with nonrandom phases*, Quant. Inf. Comp., Vol. 7, pp. 431–458.

Appendix A Properties of vacuum measurement

Let $\{|n\rangle\}$ be an orthonormal basis for a state space of interest. We refer to the state $|0\rangle$ as the "vacuum state of all modes", although it could in principle be any fixed, pure state. A vacuum measurement is a projective measurement with projectors $P = |0\rangle\langle 0|$ and $I - P$. We claim that if $\mathcal{F}$ is any quantum operation satisfying (9), i.e.,

$$\mathcal{F}(|0\rangle\langle 0|) = |0\rangle\langle 0|, \tag{A.1}$$

the presence of a vacuum measurement before $\mathcal{F}$ does not change the statistics and output state of a vacuum measurement after $\mathcal{F}$, see Fig. A.1.

This result can be proved by using the fact that any quantum operation can be viewed as a unitary transformation on an extended state space, with a standard state $|0\rangle_{\text{aux}}$ as auxiliary

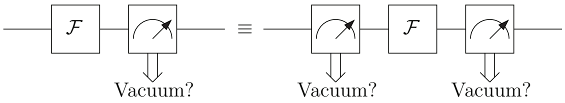


Fig. A.1. The statistics and output state of the vacuum measurement after $\mathcal{F}$ is not changed by the introduction of a vacuum measurement before $\mathcal{F}$.

input. Due to (A.1), we can assume that the unitary transformation transforms

$$|0\rangle \otimes |0\rangle_{\text{aux}} \to |0\rangle \otimes |0\rangle_{\text{aux}}, \tag{A.2}$$

with no loss of generality.

Consider the right-hand side of the identity (Fig. A.1). Let $P_{\text{aux}} = |0\rangle_{\text{aux}}\langle 0|_{\text{aux}}$. A vacuum measurement at the input can now be described as a projective measurement with $P \otimes P_{\text{aux}}$ and $I - P \otimes P_{\text{aux}}$, since the auxiliary input is fixed at $|0\rangle_{\text{aux}}$. Clearly, it does not matter if we measure the auxiliary output with projectors P_{aux} and $I - P_{\text{aux}}$. In total, the extended measurement at the output is described by projectors $P \otimes P_{\text{aux}}$, $P \otimes (I - P_{\text{aux}})$, $(I - P) \otimes P_{\text{aux}}$, and $(I - P) \otimes (I - P_{\text{aux}})$. Transforming the projector $P \otimes P_{\text{aux}}$ backwards, we find that the corresponding projector at the input is $P \otimes P_{\text{aux}}$. In other words, the extended vacuum measurement at the output contains the vacuum measurement at the input, so the latter is redundant.

Paper B

Security of quantum key distribution with arbitrary individual imperfections

Published in Physical Review A.

Physical Review A **82**, 032337 (2010)

arXiv: 0903.3525 [quant-ph]

Security of quantum key distribution with arbitrary individual imperfections

Øystein Marøy,* Lars Lydersen, and Johannes Skaar
Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway and University Graduate Center, NO-2027 Kjeller, Norway

(Received 23 March 2009; revised manuscript received 2 June 2010; published 30 September 2010)

We consider the security of the Bennett-Brassard 1984 protocol for quantum key distribution, with arbitrary individual imperfections simultaneously in the source and detectors. We provide the secure key generation rate and show that three parameters must be bounded to ensure security; the basis dependence of the source, a detector-blinding parameter, and a detector leakage parameter. The system may otherwise be completely uncharacterized and contain large losses.

DOI: 10.1103/PhysRevA.82.032337 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) is a method for distributing a secure key to two communicating parties, Alice and Bob. The most common QKD protocol, Bennett-Brassard 1984 (BB84) [1], has been proved secure by a number of approaches, some of which include different kinds of imperfections in the equipment [2–7]. The ultimate goal of QKD security analysis is to take all kinds of imperfections into account, at least those that cannot be eliminated completely by a suitable design of the setup. So far, most of the available security proofs for BB84 consider imperfections at the source or detector separately. An exception is the work by Gottesman *et al.* [5], which treats the security in the presence of source flaws and a squashing detector with certain limited imperfections. Also of interest is the article by Hayashi [8], which combines finite-length key analysis with photon number imperfections at the source. Proving security for a realistic system with arbitrary imperfections simultaneously in the source, channel, and detectors has so far been an open problem.

A particularly suitable approach for practical QKD is to limit the assumptions about the equipment. By considering entanglement-based protocols with detectors in both ends of the system [9], one can prove security in a rather general setting [10], assuming collective attacks and individual imperfections [11]. While these protocols and security proofs are promising, they do not necessarily provide security for realistic devices. All realistic systems have large losses due to the channel and limited detector efficiencies. An eavesdropper Eve may use imperfect detection efficiencies to effectively control Bob's basis choice [12,13]. Using this detection loophole, she may perform the identical measurement as Bob to obtain a perfect copy of the key.[1]

In this work we prove security for BB84 with any combination of individual imperfections, as well as channel losses. By individual imperfections we mean that the operation of the devices for a particular signal is independent of earlier signals. To obtain such generality, we describe the actual physics in the protocol rather than using, for example, squashing models with "tagging." Thus, the detectors are described as a basis-dependent quantum operation on the actual state space in front of a three-outcome measurement ("0", "1", and "vacuum"). Describing the detector in this way also enables an elegant solution to the problem of combining errors in the detectors and errors in the source.

To get around the detection loophole, we anticipate that at least two parameters must be known or bounded about the system; one for the source and one for the detectors. Our proof is formulated with two such parameters; the basis dependence of the source and a detector-blinding parameter. In addition to these parameters, we include a third parameter quantifying leakage from Bob's detectors. Once these parameters are bounded, the system may contain bit and basis leakage from Alice, multimode behavior, basis-dependent misalignments, losses, nonlinearities, basis-dependent threshold detectors with detector efficiency mismatch and information leakage, dark counts, etc. In that sense, our proof offers the generality of the entanglement-based scenarios [11], applies to realistic scenarios with loss, and provides universal composable security against the most general attacks.

II. PROTOCOL

Consider the following BB84-like protocol as the actual protocol. Alice chooses basis $a = Z$ or $a = X$ randomly according to some probability distribution and prepares the state $|\chi_a\rangle$, where

$$|\chi_Z\rangle = \sqrt{p_Z}|0\rangle|\beta_0\rangle + \sqrt{1-p_Z}|1\rangle|\beta_1\rangle, \tag{1a}$$

$$|\chi_X\rangle = \sqrt{p_X}|+\rangle|\beta_+\rangle + \sqrt{1-p_X}|-\rangle|\beta_-\rangle. \tag{1b}$$

Here p_Z and p_X are probabilities, $|0\rangle,|1\rangle$ are some orthonormal qubit basis states, and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Alice measures the qubit in the a basis (this measurement can be delayed to the end of the protocol). She repeats the procedure to obtain a large number of "β states," which are sent via Eve to Bob. These β states include any system that is correlated to Alice's system and to which Eve has access. Note that Eve is free to send anything to Bob, including parts of β and/or any state of her own choice. Depending on Alice's source, the four different β states will differ in photon number statistics, polarization, wavelength, etc. Any

*oystein.maroy@iet.ntnu.no

[1] For any protocol, Bob's basis choice (or more generally, measurement setting) must be random and come from a trusted random-number generator; otherwise, Eve could perform the same measurement as Bob to obtain a perfect copy of his result.

leakage in nonphotonic side channels will also be included in these states. With no loss of generality, the β states are assumed to be pure; if they were mixed, we could simply purify them, sending the auxiliary, purifying system to Eve.

For each state received by Bob, he chooses a "basis" variable b according to some probability distribution and conducts measurements M_b. The measurements M_b have three outcomes: "0", "1", and "vacuum." When he obtains "0" or "1", he publicly acknowledges receipt. After transmission, Alice and Bob broadcast a and b. When $b = X$, they openly compare their measurement results to estimate the fraction q_X of nonvacuum events at Bob when $a = X$, the corresponding error rate δ_X, and the fraction q_{ph} of nonvacuum events when $a = Z$. After this estimation only the n states for which $a = b = Z$ are kept. Discarding all events where Bob detected "vacuum," Alice and Bob each end up with nq_Z bits. Alice's bits are the raw key.

We now summarize Koashi's generic framework for security proofs [14,15]. Imagine a virtual experiment where Alice measures her final nq_Z qubits (corresponding to the raw key) in the X basis instead of Z basis. In this virtual experiment, instead of measuring M_Z, Bob now tries to predict the outcome of Alice's measurement. To do this, he may do whatever is permitted by quantum mechanics, as long as he does not alter the information given to Eve. Let $H_{\mathrm{virt}X}(A|B = \mu)$ denote the entropy of Alice's result, given measurement result μ in Bob's prediction. Let $H_{\mathrm{virt}X}(A|B = \mu) \leqslant H$ for some constant H. Since the uncertainty after Bob's prediction is less than H, the entropic uncertainty relation [16] suggests that anyone (including Eve) cannot predict the outcome of a Z-basis measurement by Alice with less entropy than $nq_Z - H$. This indicates that Alice can extract $nq_Z - H$ bits of secret key. The quantity H is to be found from the estimated parameters q_X, δ_X, and q_{ph}.[2] The detailed proof [14] of the fact that Alice can extract $nq_Z - H$ bits of secret key is based upon the universal, composable security definition and considers the actual privacy amplification protocol by universal hashing.

To ensure that Bob has the identical key, we note that it does not matter to Eve what Bob does (as long as he gives the same receipt acknowledgment information); he can as well measure M_Z. Then Bob obtains the identical raw key from his measurement result and $nq_Z h(\delta_Z)$ extra bits of error correction information from Alice, consuming $nq_Z h(\delta_Z)$ of previous established secure key. Here $h(\cdot)$ is the binary Shannon entropy function, and the error rate δ_Z can be estimated by sacrificing a subset of the raw key (whose size we can neglect in the asymptotic limit $n \to \infty$). We therefore obtain the asymptotic net secure key generation rate

$$R_Z \geqslant 1 - H/nq_Z - h(\delta_Z). \tag{2}$$

III. INDIVIDUAL IMPERFECTIONS IN THE DETECTORS

We first consider the situation where Alice's source is perfect ($|\chi_X\rangle = |\chi_Z\rangle$) and Bob's detectors can be subject to any kind of individual imperfections. With the understanding that Bob chooses his bit randomly for coincidence counts [3,5], his detectors can be modeled by a basis-dependent quantum operation ($\mathcal{E}_Z$ and $\mathcal{E}_X$) in front of a measurement with three possible outcomes: "0", "1", and "vacuum." Note that there is no need to require a squash model [5,18,19] in our proof as Bob's basis selector is included into the basis-dependent quantum operation.

In addition to the optical modes, there may also be other relevant degrees of freedom in the detector. For example, dark counts are caused by physical processes internally in the detector. Thus, we consider an extended state space consisting of the Fock space of all optical modes in addition to the state space associated with "electronic" degrees of freedom inside the detectors. Pessimistically, we let Eve control all degrees of freedom.

The quantum operations $\mathcal{E}_Z$ and $\mathcal{E}_X$ are decomposed as follows: First there is a basis-dependent quantum operation ($\mathcal{F}_Z$ and $\mathcal{F}_X$) acting on the Fock space associated with all optical modes. This operation contains Bob's basis selector. The operations $\mathcal{F}_Z$ and $\mathcal{F}_X$ are assumed to be passive in the sense that if vacuum is incident to all modes, there will also be vacuum at the output. Then there is another quantum operation $\mathcal{F}$ describing interaction between the photonic state and the internal degrees of freedom in the detectors (see Fig. 1). The quantum operation $\mathcal{F}$ may be active in the sense that even though vacuum is incident to all optical modes, there may be nonvacuum detections. When the optical modes contain the vacuum state, we can (pessimistically) assume that Eve has full control over Bob's detectors through $\mathcal{F}$; in other words, she controls the dark counts directly with the "electronic" modes. The quantum operation $\mathcal{F}$ is assumed to be independent of

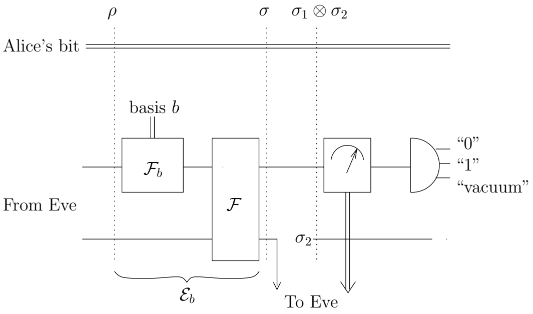


FIG. 1. Bob's detectors consist of a basis-dependent quantum operation ($\mathcal{E}_Z = \mathcal{F} \circ \mathcal{F}_Z$ and $\mathcal{E}_X = \mathcal{F} \circ \mathcal{F}_X$) in front of a three-outcome measurement. The fact that Eve gets arrival information from Bob is included through a dedicated vacuum measurement preceding Bob's three-outcome measurement. On the input side of $\mathcal{F}$, the lower line contains the electronic modes of the detector, while on the output side of $\mathcal{F}$, the lower line indicates the part of the Hilbert space leaked to Eve. Alice's classical bit, indicated in the upper part of the figure, is included in the state σ.

[2] The Z-basis error rate δ_Z is not needed to ensure that Alice's key is secret; thus, there is no need to invoke the classicalization argument [17] regarding statistics of measurements involved in the simultaneous estimation of δ_X and δ_Z.

Bob's basis choice. This assumption is natural as Bob's basis choice does not influence internal degrees of freedom in the detector. In other words, when Eve emits the vacuum in all optical modes, Bob's basis choice will not affect the detection statistics.

To achieve a completely general detector model, we should not only let Eve control the detectors; in addition, we must let information return to Eve. Consider the case where Bob has chosen the Z basis. In the most general case, the information leakage is quantum; that is, a part of the total Hilbert space is given directly to Eve. Replacing this part of the Hilbert space with some standard state σ_2, we can quantify the leakage ϵ_Z by the trace distance $D(\cdot,\cdot)$ as follows:

$$\epsilon_Z = \min_{\sigma_2} \max_{\rho} D(\sigma,\sigma_1 \otimes \sigma_2). \tag{3}$$

Here ρ is any state at Bob's input (including Alice's part of the system; see Fig. 1), σ is the state of Alice and Bob before leakage, and $\sigma_1 = \mathrm{Tr}_2(\sigma)$ is the state of the remaining Hilbert space after leakage. Note that these density operators refer to a single signal, not the entire block of n signals. The parameter ϵ_Z measures the correlation between the leaked quantum state and the state of Alice and Bob, maximized over states sent by Eve. More precisely, ϵ_Z is the maximum probability that the actual state before leakage can be distinguished from the state where the leaked part is replaced by the standard state σ_2 [20]. Equation (3) has another very useful physical interpretation: Choose a fixed σ_2, dependent on $\mathcal{E}_Z$, but independent of the state coming from Eve. For any σ, the probability of a measurement result of $\sigma_1 \otimes \sigma_2$ deviates no more than ϵ_Z from the corresponding probability when measuring σ [20].

Although we now have a general detector model, we add one little feature. In the actual protocol, Eve gets to know whether a particular signal was detected. This can be included as an extra projective measurement with projectors P and $I - P$, where $I - P$ is a projector onto the subspace corresponding to detection result "vacuum" in Bob's measurement. Clearly, this addition does not disturb Bob's measurement statistics. The composed measurement consisting of $\mathcal{E}_Z$ followed by this projective measurement will be referred to as Eve's vacuum measurement. It can be described by some positive operator-valued measure (POVM) elements E and $I - E$, where $I - E$ corresponds to detection result "vacuum" at Bob. Including Eve's vacuum measurement separately, rather than absorbing it into the quantum leakage (3), leads to a better rate. The reason is that the information from the vacuum measurement is classical and available to Bob, as opposed to general, leaked quantum information.

Having described the model, we now turn to the security analysis. As before, Alice extracts the key in the Z basis. In Koashi's security proof, Bob wants to predict the outcome of a virtual X-basis measurement by Alice. In this virtual prediction there is only one important restriction: Bob is not allowed to alter the information going to Eve. Thus, Eve's vacuum measurement must be retained.

The setup used by Bob to perform the virtual X-basis prediction is depicted in Fig. 2. The state from Eve is incident to a first vacuum measurement, Bob's vacuum measurement, a projective measurement with certain projectors Q and $I - Q$, corresponding to results "nonvacuum" and "vacuum," respectively. Then it goes through the quantum operation $\mathcal{E}_Z$ and leaks partially back to Eve. The remaining part is measured by Eve's vacuum measurement and sent through a reversal operation. The goal of the reversal operation is to reverse the effect of the vacuum measurement so that the combined operation consisting of Eve's vacuum measurement and the reversal operation is identity, with a certain probability. Finally, the quantum operation $\mathcal{E}_X$ and Bob's three-outcome measurement are applied.

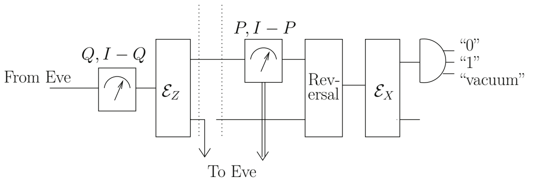


FIG. 2. Bob's setup for virtual X-basis prediction. The optical and electronic modes are denoted by a single line in this figure.

To analyze Bob's virtual prediction, we note the following observations. The quantum operation $\mathcal{E}_Z$ can be viewed as a unitary operation on an extended state space. Moreover, since Bob's reversal operation does not have to be realizable in practice (only in principle), we may assume that Bob has access to any extra degrees of freedom used to "unitarize" $\mathcal{E}_Z$. He does not have access to the quantum state leaked to Eve; however, the leakage disturbs the probabilities of Bob's prediction by no more than ϵ_Z. Therefore, for the moment we can ignore the leakage, taking it into account in the final expression for the key rate.

To proceed, we need the following results.

Lemma 1 (Koashi and Ueda [21]). Let E, acting on a Hilbert space $\mathcal{H}$, be a POVM element associated with some measurement M. If any state in some subspace $\mathcal{Q} \subseteq \mathcal{H}$ is measured with M, the measured state can be reversed to the original state, with maximum joint probability of outcome E and successful reversal $\inf_{|\Phi\rangle\in\mathcal{Q},\langle\Phi|\Phi\rangle=1}\langle\Phi|E|\Phi\rangle$. It is possible to know when the reversal is successful or not.

Lemma 2. The output of a quantum operation $\mathcal{E}_b$ is measured with projectors P_0, P_1, and $I - P_0 - P_1$, corresponding to detection results "0", "1", and "vacuum," respectively, or alternatively, with $P \equiv P_0 + P_1$ and $I - P$. Let $I - Q$ be a projector onto an input subspace of $\mathcal{E}_b$ that leads to detection result "vacuum" with certainty. The measurement statistics are not changed by the presence of a projective measurement $\{Q, I - Q\}$ before $\mathcal{E}_b$.

Proof. Lemma 2 is not as trivial as it may appear at first sight since states in the support of Q may also lead to detection result "vacuum." Thus, the measurement before $\mathcal{E}_b$ gives extra information. Nevertheless, the quantum operation $\mathcal{E}_b$ can be viewed as a unitary transformation on an extended Hilbert space, with a standard state as auxiliary input. Clearly, it does not matter if we measure the extra degrees of freedom at the output. This measurement can be constructed so that the total output measurement distinguishes between input states in the support of Q or $I-Q$. Then, an input measurement $\{Q, I-Q\}$ is redundant.

More precisely, the unitary operator can be chosen such that the projective measurement at the output is implemented as a measurement of a single qutrit in the computational basis. Thus, it transforms

$$|0_1\rangle|0\rangle_{\text{aux}} \to |v\rangle|\psi_1\rangle, \tag{4a}$$

$$|0_2\rangle|0\rangle_{\text{aux}} \to |v\rangle|\psi_2\rangle, \tag{4b}$$

and

$$|1_1\rangle|0\rangle_{\text{aux}} \to |v\rangle\left|\phi_1^v\right\rangle + |0\rangle\left|\phi_1^0\right\rangle + |1\rangle\left|\phi_1^1\right\rangle, \tag{5a}$$

$$|1_2\rangle|0\rangle_{\text{aux}} \to |v\rangle\left|\phi_2^v\right\rangle + |0\rangle\left|\phi_2^0\right\rangle + |1\rangle\left|\phi_2^1\right\rangle, \tag{5b}$$

etc. Here $|0_i\rangle$ and $|1_i\rangle$ are bases for the support of $I-Q$ and Q, respectively; $|0\rangle_{\text{aux}}$ is the auxiliary standard state; and $|0\rangle\langle 0| = P_0$, $|1\rangle\langle 1| = P_1$, and $|v\rangle\langle v| = I - P_0 - P_1$. The ψ and ϕ vectors are (not necessarily normalized) states of the remaining part of the output state space. Since $\langle 1_i|0_j\rangle = 0$, we have $\langle \phi_i^v|\psi_j\rangle = 0$ for any i,j. Thus, by a measurement of the ψ or ϕ part of the output state space in addition to the qutrit, we can distinguish between the $|0_i\rangle$ states and $|1_i\rangle$ states. ■

We define the projector $I-Q$ so as to project onto vacuum in all photonic modes and onto the biggest subspace of the "electronic" modes that gives detection result "vacuum" in Eve's vacuum measurement. The orthogonal subspace, which is the support of Q, is denoted $\mathcal{Q}$. Lemma 2 ensures that Bob's vacuum measurement does not change the statistics of Eve's vacuum measurement. When Eve's vacuum measurement gives result "vacuum," or the reversal operation is not successful, the reversal operation is assumed to output a state in the support of $I-Q$. Thus, in these cases the output of Bob's virtual prediction is "vacuum" with certainty.

If the outcome of Bob's vacuum measurement is "vacuum," the outcome of Eve's vacuum measurement is "vacuum," and the reversal operation is successful with certainty. Suppose the outcome of Bob's vacuum measurement is "nonvacuum." According to Lemma 1, the maximum joint probability of result E in Eve's vacuum measurement and successful reversal is $\eta_Z = \inf_{|\Phi\rangle\in\mathcal{Q},\langle\Phi|\Phi\rangle=1}\langle\Phi|E|\Phi\rangle$. When result E and the reversal is successful (and Bob knows when it is), the statistics of Bob's measurement compared to Alice's virtual X-basis measurement will be identical to that of Alice's and Bob's ordinary parameter estimation in the X basis, except for any disturbance by Bob's vacuum measurement. According to Lemma 2 such disturbance does not exist. The number of detection events E in Eve's vacuum measurement is nq_Z; of these $nq_X\eta_Z$ is successfully reversed *and* detected as "0" or "1" in Bob's virtual prediction. Thus, we obtain $H \leqslant (nq_Z - nq_X\eta_Z) + nq_X\eta_Z h(\delta_X)$, which gives us the rate

$$R_Z \geqslant \eta_Z q_X/q_Z[1-h(\delta_X)] - h(\delta_Z). \tag{6}$$

The parameter $\eta_Z = \inf_{|\Phi\rangle\in\mathcal{Q},\langle\Phi|\Phi\rangle=1}\langle\Phi|E|\Phi\rangle$ is the minimum probability that a state in $\mathcal{Q}$ gives result E by Eve. This parameter has a clear physical interpretation. When vacuum is incident to the optical modes, recall that with no loss of generality we may assume that Eve has full control of the detectors through the "electronic" modes. Then there are no losses of her excitation in the "electronic" modes through the quantum operation $\mathcal{F}$. Thus, we identify η_Z as the minimum probability that a nonvacuum photonic state is detected by Bob. In other words, $1-\eta_Z$ is the maximum probability that a nonvacuum photonic state is absorbed in the detectors and detected as vacuum in the actual setup (Fig. 1).

So far we have ignored the effect of any quantum leakage from the detectors. Parametrizing the leakage by (3), ϵ_Z quantifies the maximum deviation of any measurement probabilities. In the absence of leakage, the probabilities of correct and incorrect predictions are $q_X\eta_Z(1-\delta_X)$ and $q_X\eta_Z\delta_X$, respectively, while the probability of vacuum result is $1-q_X\eta_Z$. When there is leakage, in the worst case these probabilities are changed to $q_X\eta_Z(1-\delta_X)-\epsilon_Z$, $q_X\eta_Z\delta_X+\epsilon_Z-\xi$, and $1-q_X\eta_Z+\xi$, respectively. Here ξ is an unknown parameter satisfying $0\leqslant\xi\leqslant\epsilon_Z$. Of the nq_Z nonvacuum results in Eve's vacuum measurement, there are $n(q_X\eta_Z-\xi)$ nonvacuum results in Bob's virtual prediction. This leads to

$$\begin{aligned} H &\leqslant nq_Z - n(q_X\eta_Z-\xi) \\ &\quad + n(q_X\eta_Z-\xi)h\left(\frac{q_X\eta_Z\delta_X+\epsilon_Z-\xi}{q_X\eta_Z-\xi}\right) \\ &\leqslant nq_Z - nq_X\eta_Z + nq_X\eta_Z h\left(\delta_X + \frac{\epsilon_Z}{q_X\eta_Z}\right). \end{aligned} \tag{7}$$

The last inequality in (7) can be found after some algebra using the facts that $h(u)-h(u-\Delta)\geqslant h'(u)\Delta$ for $\Delta\geqslant 0$ and $u\leqslant 1/2$, and $h'(u)(1-u)\geqslant 1$ for $u\leqslant 0.277$. Here we have set $u=\delta_X+\frac{\epsilon_Z}{q_X\eta_Z}$.

This gives the rate

$$R_Z \geqslant \eta_Z\frac{q_X}{q_Z}\left[1-h\left(\delta_X+\frac{\epsilon_Z}{q_X\eta_Z}\right)\right] - h(\delta_Z) \tag{8}$$

for $\delta_X+\frac{\epsilon_Z}{q_X\eta_Z}\leqslant 0.277$. An expression for the rate, also valid for $0.277\leqslant\delta_X+\frac{\epsilon_Z}{q_X\eta_Z}\leqslant 0.5$, can be derived straightforwardly; however, this regime is only relevant for very small δ_Z and large δ_X and/or $\frac{\epsilon_Z}{q_X\eta_Z}$.

IV. INDIVIDUAL IMPERFECTIONS IN THE ENTIRE SYSTEM

From the previous section we note that when the reversal operation is successful (and Bob knows when it is), the measurement statistics in the prediction becomes identical to the statistics if Bob measured in the X basis. This makes it possible to consider simultaneous imperfections at the source and detector. We may then consider the case where Alice creates a general state ρ_a depending on the basis choice a. The basis dependence of the source is characterized by the fidelity $F(\rho_Z,\rho_X)\equiv\text{Tr}(\sqrt{\rho_Z}\rho_X\sqrt{\rho_Z})^{\frac{1}{2}}$. We let this dependence be bounded by a parameter Δ defined by $F\geqslant 1-2\Delta$. By Uhlmann's theorem there exist purifications, $|\chi_a\rangle$ of ρ_a, such that $\langle\chi_Z \mid \chi_X\rangle = 1-2\Delta$. We note that $|\chi_a\rangle$ can be expressed as in Eq. (1).

Again, we first ignore the detector leakage, taking it into account in the final expression for the rate. Since Bob wants to predict Alice's virtual X-basis measurement on $|\chi_Z\rangle$, the error rate δ_X and the transmission rate q_X in (6) must be replaced with δ_{ph} and q_{ph}, respectively. Here δ_{ph} is the error rate when Alice measures her part of $|\chi_Z\rangle$ in the X basis and Bob measures his part using M_X.

In BB84 such a measurement is not actually performed, but δ_{ph} can be bounded from the measured error and transmission rates. We expand the statistical argument from [14] to include "vacuum" as a possible measurement result. Assume that for the systems used in the random sampling Alice chooses her basis by measuring a quantum coin in the Z basis. Then these systems can be described by state $|\Psi\rangle = (|\chi_Z\rangle|0\rangle + |\chi_X\rangle|1\rangle)/\sqrt{2}$, with the last system being that of the quantum coin.

We then consider the situations where Alice and Bob both conduct X-basis measurements. For each measurement a variable t is assigned the value $t = 0$ if their results are the same, $t = 1$ if there is an error, and $t = 2$ if Bob gets no result. Alice then measures her quantum coin in the Z basis, getting the result c. We obtain the following conditional probabilities.

$$p(t = 0|c = 1) = q_X(1 - \delta_X), \tag{9a}$$

$$p(t = 0|c = 0) = q_{\text{ph}}(1 - \delta_{\text{ph}}), \tag{9b}$$

$$p(t = 1|c = 1) = q_X\delta_X, \tag{9c}$$

$$p(t = 1|c = 0) = q_{\text{ph}}\delta_{\text{ph}}, \tag{9d}$$

$$p(t = 2|c = 1) = 1 - q_X, \tag{9e}$$

$$p(t = 2|c = 0) = 1 - q_{\text{ph}}. \tag{9f}$$

Assuming that the systems used to estimate error and transmission rates are randomly chosen, the probabilities given $c = 0$ are also valid for the systems used to extract the raw key.

Now assume that for some states Alice measures the coin in the X basis, getting measurement result $\bar{c}$. Note that

$$\sum_j p(t = j)p(\bar{c} = 1|t = j) = \Delta. \tag{10}$$

Using (9), (10), and the bound [22],

$$[1 - 2p(\bar{c} = 1|t = j)]^2 + [1 - 2p(c = 0|t = j)]^2 \leqslant 1,$$

we find

$$\begin{aligned} 1 - 2\Delta &\leqslant \sum_j \sqrt{p(t = j|a = Z)p(t = j|a = X)} \\ &= \sqrt{q_X(1 - \delta_X)q_{\text{ph}}(1 - \delta_{\text{ph}})} + \sqrt{q_X\delta_X q_{\text{ph}}\delta_{\text{ph}}} \\ &\quad + \sqrt{(1 - q_X)(1 - q_{\text{ph}})}. \end{aligned} \tag{11}$$

δ_{ph} can now be taken to be the maximal value for which the inequality is obeyed.

Similarly to the analysis in the previous section, we can include detector leakage by modifying the detection probabilities. As in (8), the leakage is accounted for by adding a term proportional to the leakage parameter ϵ_Z,

$$\tilde{\delta}_{\text{ph}} \leqslant \delta_{\text{ph}} + \frac{\epsilon_Z}{q_{\text{ph}}\eta_Z}. \tag{12}$$

We have arrived at our main result.

Theorem 1. In BB84 the basis dependence of Alice's source is bounded by $F(\rho_X,\rho_Z) \geqslant 1 - 2\Delta$. Bob's detectors are modeled by a passive, basis-dependent quantum operation ($\mathcal{F}_Z$ and $\mathcal{F}_X$) acting on the multimode photonic state, followed by a basis-independent quantum operation ($\mathcal{F}$) describing interaction with internal degrees of freedom in the physical detector, followed by a measurement with three outcomes: "0", "1", and "vacuum." Suppose Eve controls the photonic modes and the internal degrees of freedom in the detectors and that a quantum state leaks back to Eve from the detectors. Then the asymptotic secure key generation rate for key extraction in the Z basis satisfies

$$R_Z \geqslant \eta_Z q_{\text{ph}}/q_Z[1 - h(\tilde{\delta}_{\text{ph}})] - h(\delta_Z), \tag{13}$$

provided $\tilde{\delta}_{\text{ph}} \leqslant 0.277$. Here δ_Z is the estimated error rate in the Z basis, $\tilde{\delta}_{\text{ph}}$ is given by (11) and (12), $1 - \eta_Z$ is the maximum probability that a nonvacuum photonic state is detected as "vacuum," and q_{ph}/q_Z is the ratio between the transmission rates for Bobs measurements M_X and M_Z given that Alice sends in the Z basis.

The rate (13) is valid for any kind of individual imperfection and loss. The parameters q_X, q_Z, q_{ph}, δ_X, and δ_Z are estimated directly in the protocol, while Δ, η_Z, and ϵ_Z characterize the practical setup.

V. DISCUSSION OF RESULTS

In this discussion we assume that the quantum channel is symmetric with respect to loss; that is, $q_X = q_{\text{ph}} = q_Z \equiv q$. This will be approximately true for most setups. We also assume no information returned to Eve from the detectors, $\epsilon_Z = 0$, anticipating that such errors could be avoided by modifying the setup.

In this case (11) reduces to

$$\frac{2\Delta}{q} \geqslant 1 - \sqrt{(1 - \delta_X)(1 - \delta_{\text{ph}})} - \sqrt{\delta_X\delta_{\text{ph}}} \tag{14}$$

and the estimated worst possible error rate is

$$\begin{aligned} \delta_{\text{ph}} = \min\Bigg\{\frac{1}{2}, \delta_X + 8\frac{\Delta}{q}\Bigg[\left(1 - \frac{\Delta}{q}\right)(1 - 2\delta_X) \\ + \sqrt{\frac{\Delta}{q}\left(1 - \frac{\Delta}{q}\right)\delta_X(1 - \delta_X)}\Bigg]\Bigg\}. \end{aligned} \tag{15}$$

We see that errors in the source are more critical when the transmission is low. In fact, both the basis dependence of the source, Δ, and transmission rate, q, only appears in the equation in the form $\frac{\Delta}{q}$. If the source is perfect, $\Delta = 0$, loss in the channel does not affect the secret key rate. This relationship between the source error and the transmission rates is due to Eve's control of the channel, which let her pass to Bob only the systems where her operation has given her the most information for the least disturbance. The upper limit on the source error for which key gain is possible is $\frac{\Delta}{q} \leqslant \frac{\sqrt{2}-1}{2\sqrt{2}} \approx 0.146$. This is independent of the blinding parameter η_Z, as long as it is nonzero, but demands error rates equal to zero. For larger error rates the limit depends heavily on η_Z (Fig. 3).

Channel loss and imperfect sources only contributes to an increase in δ_{ph}. A better estimate of δ_{ph} would increase the rate. This is related to the method of decoy states [23–25], where Alice instead of producing ρ_Z, sometimes produces a decoy state with a different mean photon number. From the

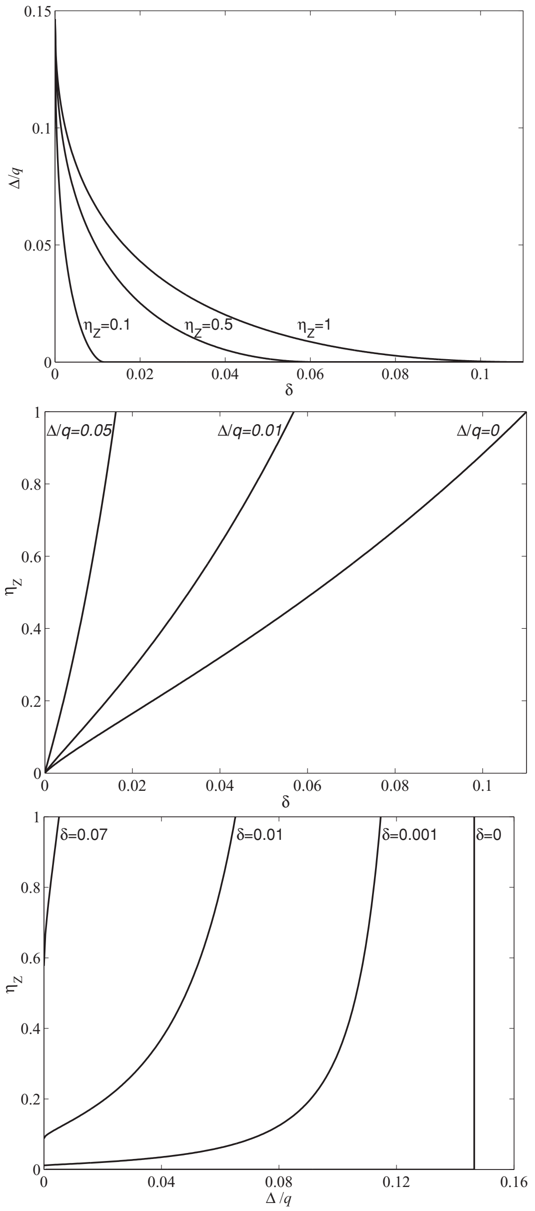


FIG. 3. Plots showing the security bounds $R_Z = 0$ for different values of the blinding parameter η_Z, the basis dependence of the source Δ, and the error and transmission rates δ and q. The security bound is found by setting $R_Z = 0$ in (13). Positive key gain is possible for parameter values to the left of the curves. We have assumed $\epsilon_Z = 0$, $\delta_X = \delta_Z = \delta$, and $q_X = q_{\text{ph}} = q_Z = q$.

transmission and error rates for this state, Alice and Bob are able to derive a stricter bound on δ_{ph}, effectively reducing R_Z's dependence of channel loss. To generalize this method, using decoy states where other properties of the signal state are varied might prove useful when operating with an imperfect source. However, creating such states may require the detailed output statistics of the source and might be experimentally difficult in general.

Considering the special case of a perfect source, our rate is larger than the rate proved for restricted detector flaws in previous literature [6,7]. Key gain is possible for $\eta_Z \leqslant \frac{h(\delta_Z)}{1-h(\delta_X)}$. Unlike previous results, our rate applies to all relevant, individual imperfections at the detectors, for example, mode coupling including misalignments and multiple reflections, nonlinearities, mode-dependent losses and detector efficiency mismatch, and any basis dependence of those effects. Moreover, it applies to threshold detectors with dark counts.

Note that the detector-blinding parameter η_Z is not supposed to contain the transmission efficiency of the channel. Generally, one should factorize $\mathcal{E}_Z = \tilde{\mathcal{E}}_Z \circ \mathcal{E}$ and $\mathcal{E}_X = \tilde{\mathcal{E}}_X \circ \mathcal{E}$ to put as much as possible of the imperfections into the basis-independent operation $\mathcal{E}$. By absorbing $\mathcal{E}$ into Eve and treating $\tilde{\mathcal{E}}_Z$ and $\tilde{\mathcal{E}}_X$ as the new imperfections, η_Z will be maximal. For example, for the case where reduced detector efficiencies can be described as beam splitters in front of ideal detectors, and if there is no coupling between modes associated with different logical bits, η_Z is the minimum ratio between the two detection efficiencies [7]. For detectors that cannot be modeled by beam splitters in front of ideal detectors, our security proof clearly shows the danger associated with the possibility of detector blinding [13]: If the detection probability of a nonvacuum state is zero, our proof predicts zero key rate. For the case where the detectors can only be partially blinded, our proof can predict positive rate.

Returning to the general case, the rate (13) is dependent on Δ, η_Z, and ϵ_Z, in addition to estimated parameters. For a specific QKD setup, Δ and ϵ_Z must be upper bounded, and η_Z must be lower bounded. How to deal with this in practice is an interesting question for future research.

VI. CONCLUSION

We have proved security for arbitrary, individual imperfections in a BB84 system. The detector model includes a basis-dependent quantum operation, possibly with quantum leakage back to Eve, followed by a three-outcome measurement with outcomes "0", "1", and "vacuum." Such a general detector model can describe detector efficiency mismatch, nonlinear blindable behavior, response to multiple modes, mode coupling and multiple reflections, misalignments, back-reflection leakage, nonoptical leakage, etc. By reversing the measurement which gives Eve information about whether a particular signal was detected (Eve's vacuum measurement), we show how to treat the general case with a lossy channel and general, individual imperfections at the source, combined with the flawed detector. The final rate is dependent on three parameters which describe the equipment, in addition to error and transmission rates. These parameters are the basis dependence of the source and a blinding parameter and a leakage parameter characterizing the detector.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, Bangalore, India, 1984), p. 175.

[2] D. Mayers, in *Proceedings of Crypto '96*, edited by N. Koblitz (Springer, New York, 1996), Vol. 1109, p. 343.

[3] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[4] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[5] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[6] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **9**, 131 (2009).

[7] L. Lydersen and J. Skaar, Quantum Inf. Comput. **10**, 60 (2010).

[8] M. Hayashi, Phys. Rev. A **76**, 012329 (2007).

[9] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[10] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[11] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[12] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006); **78**, 019905 (2008).

[13] V. Makarov, New J. Phys. **11**, 065003 (2009).

[14] M. Koashi, New J. Phys. **11**, 045018 (2009); e-print quant-ph/0505108v1.

[15] M. Koashi, e-print quant-ph/0609180.

[16] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

[17] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[18] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).

[19] T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008).

[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[21] M. Koashi and M. Ueda, Phys. Rev. Lett. **82**, 2598 (1999).

[22] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).

[23] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[24] H.-K. Lo, X. F. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[25] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

C

Paper C

Hacking commercial quantum cryptography systems by tailored bright illumination

Published in Nature Photonics.

DOI: 10.1038/nphoton.2010.214

arXiv: 1008.4593 [quant-ph]

Paper D

Avoiding the blinding attack in QKD

Published in Nature Photonics.

DOI: 10.1038/nphoton.2010.278

arXiv: 1012.0476 [quant-ph]

Is not included due to copyright

Paper E

Thermal blinding of gated detectors in quantum cryptography

E

Published in Optics Express.

DOI: 10.1364/oe.18.027938

arXiv: 1009.2663 [quant-ph]

Thermal blinding of gated detectors in quantum cryptography

Lars Lydersen,[1,2,*] **Carlos Wiechers,**[3,4,5] **Christoffer Wittmann,**[3,4] **Dominique Elser,**[3,4] **Johannes Skaar,**[1,2] **and Vadim Makarov**[1]

[1] *Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway*
[2] *University Graduate Center, NO-2027 Kjeller, Norway*
[3] *Max Planck Institute for the Science of Light, Günther-Scharowsky-Str. 1/Bau 24, 91058 Erlangen, Germany*
[4] *Institut für Optik, Information und Photonik, University of Erlangen-Nuremberg, Staudtstraße 7/B2, 91058 Erlangen, Germany*
[5] *Departamento de Física, Universidad de Guanajuato, Lomas del Bosque 103, Fraccionamiento Lomas del Campestre, 37150, León, Guanajuato, México*

[*] *lars.lydersen@iet.ntnu.no*

Abstract: It has previously been shown that the gated detectors of two commercially available quantum key distribution (QKD) systems are blindable and controllable by an eavesdropper using continuous-wave illumination and short bright trigger pulses, manipulating voltages in the circuit [Nat. Photonics **4**, 686 (2010)]. This allows for an attack eavesdropping the full raw and secret key without increasing the quantum bit error rate (QBER). Here we show how thermal effects in detectors under bright illumination can lead to the same outcome. We demonstrate that the detectors in a commercial QKD system Clavis2 can be blinded by heating the avalanche photo diodes (APDs) using bright illumination, so-called *thermal blinding*. Further, the detectors can be triggered using short bright pulses once they are blind. For systems with pauses between packet transmission such as the plug-and-play systems, thermal inertia enables Eve to apply the bright blinding illumination *before* eavesdropping, making her more difficult to catch.

OCIS codes: (040.1345) Avalanche photodiodes (APDs); (040.5570) Quantum detectors; (270.5568) Quantum cryptography; (270.5570) Quantum detectors.

References and links

1. C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in “Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing,” (IEEE Press, New York, Bangalore, India, 1984), pp. 175–179.
2. A. K. Ekert, “Quantum cryptography based on bell theorem,” Phys. Rev. Lett. **67**, 661–663 (1991).
3. H.-K. Lo and H. F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances,” Science **283**, 2050–2056 (1999).
4. P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol,” Phys. Rev. Lett. **85**, 441–444 (2000).
5. D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,” N. J. Phys. **11**, 075003 (2009).
6. Commercial QKD systems are available from at least two companies: ID Quantique (Switzerland), `http://www.idquantique.com`; MagiQ Technologies (USA), `http://www.magiqtech.com`.

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

7. D. Mayers, "Advances in cryptology," in "Proceedings of Crypto'96," , vol. 1109, N. Koblitz, ed. (Springer, New York, 1996), vol. 1109, pp. 343–357.
8. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput. **4**, 325–360 (2004).
9. H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," Eur. Phys. J. D **41**, 599–627 (2007).
10. C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, "Security proof of quantum key distribution with detection efficiency mismatch," Quantum Inf. Comput. **9**, 131–165 (2009).
11. L. Lydersen and J. Skaar, "Security of quantum key distribution with bit and basis dependent detector flaws," Quantum Inf. Comput. **10**, 0060 (2010).
12. Ø. Marøy, L. Lydersen, and J. Skaar, "Security of quantum key distribution with arbitrary individual imperfections," Phys. Rev. A **82**, 032337 (2010).
13. A. Vakhitov, V. Makarov, and D. R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," J. Mod. Opt. **48**, 2023–2038 (2001).
14. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," Phys. Rev. A **73**, 022320 (2006).
15. V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," Phys. Rev. A **74**, 022313 (2006).
16. V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems: erratum," **78**, 019905 (2008).
17. V. Makarov and J. Skaar, "Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols," Quantum Inf. Comput. **8**, 0622 (2008).
18. B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, "Time-shift attack in practical quantum cryptosystems," Quantum Inf. Comput. **7**, 73–82 (2007).
19. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," Phys. Rev. A **78**, 042333 (2008).
20. A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," Opt. Express **15**, 9388–9393 (2007).
21. S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, "Information leakage via side channels in freespace BB84 quantum cryptography," N. J. Phys. **11**, 065001 (2009).
22. C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," Phys. Rev. A **75**, 032314 (2007).
23. F. Xu, B. Qi, and H.-K. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," N. J. Phys. **12**, 113026 (2010).
24. Precisely, the quantum bit error rate (QBER) is the fraction given by the number of bits which differ in Alice's and Bob's raw key, divided by the length of the raw key.
25. H. F. Chau, "Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate," Phys. Rev. A **66**, 060302 (2002).
26. D. Gottesman and H.-K. Lo, "Proof of security of quantum key distribution with two-way classical communications," IEEE Trans. Inf. Theory **49**, 457–475 (2003).
27. V. Makarov, "Controlling passively quenched single photon detectors by bright light," N. J. Phys. **11**, 065003 (2009).
28. V. Makarov, A. Anisimov, and S. Sauge, "Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by Eve," e-print arXiv:0809.3408v2 [quant-ph] .
29. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nat. Photonics **4**, 686–689 (2010).
30. C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem," e-print arXiv:1009.2683 [quant-ph] .
31. I. Gerhardt, Q. Liu, J. Skaar, A. Lamas-Linares, C. Kurtsiefer, and V. Makarov, "Perfect eavesdropping on a quantum cryptography system," e-print arXiv:1011.0105 [quant-ph] .
32. I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Free-space quantum key distribution with entangled photons," Appl. Phys. Lett. **89**, 101122 (2006).
33. M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, "Daylight operation of a free space, entanglement-based quantum key distribution system," N. J. Phys. **11**, 045007 (2009).
34. Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Avoiding the detector blinding attack on quantum cryptography," Nat. Photonics **4**, 800–801 (2010).
35. S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, "Evolution and prospects for single-photon avalanche diodes and quenching circuits," J. Mod. Opt. **51**, 1267–1288 (2004).
36. All references to the APD bias voltage are absolute valued, thus an APD biased "above" the breakdown voltage is in the Geiger mode. In practice the APDs are always reverse-biased.
37. V. Makarov and D. R. Hjelme, "Faked states attack on quantum cryptosystems," J. Mod. Opt. **52**, 691–705 (2005).
38. V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

splitting attacks for weak laser pulse implementations," Phys. Rev. Lett. **92**, 057901 (2004).
39. W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
40. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
41. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
42. S. Cova, A. Longoni, and A. Andreoni, "Towards picosecond resolution with single-photon avalanche diodes," Rev. Sci. Instrum. **52**, 408–412 (1981).
43. D. S. Bethune and W. P. Risk, "An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light," IEEE J. Quantum Electron. **36**, 340–347 (2000).
44. A. Tomita and K. Nakamura, "Balanced, gated-mode photon detector for quantum-bit discrimination at 1550 nm," Opt. Lett. **27**, 1827–1829 (2002).
45. Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, "High speed single photon detection in the near infrared," Appl. Phys. Lett. **91**, 041114 (2007).
46. Osterm, PE4-115-14-15, `http://osterm.ru/PAGE/MULTISTAGE.HTM`, visited 3. August 2010.
47. When the temperature increases, the lattice vibrations in the APD increase. This increases the probability that the electron collides with the lattice, and therefore reduces the probability that the electron gains enough energy to trigger ionization of a new electron-hole pair. Therefore, to ensure that the electron gains ionization energy, the electric field must be larger, and thus the breakdown voltage is increased.
48. S. M. Sze and K. K. Ng, *Physics of semiconductor devices* (Wiley-Interscience, 2007).
49. Marlow, NL4012, `http://www.marlow.com/media/marlow/product/downloads/nl4012t/NL4012.pdf`, visited 3. August 2010.
50. The detectors do not have any dark counts and are assumed blind at a temperature of about $-40\,^{\circ}\mathrm{C}$ at the cold plate, or when the bias voltage is decreased by $0.97\,\mathrm{V}$. If one assumes that the APD temperature is equal to the cold plate temperature, this means that heating the detectors by $10\,\mathrm{K}$ is equivalent to decreasing the bias voltage by about $1\,\mathrm{V}$.
51. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Automated 'plug & play' quantum key distribution," Electron. Lett. **34**, 2116–2117 (1998).
52. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," N. J. Phys. **4**, 41 (2002).
53. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
54. S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov. in preparation.
55. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Fast and user-friendly quantum key distribution," J. Mod. Opt. **47**, 517–531 (2000).
56. The system actually sends the qubits in frames of 1075 qubits each. We initially made a mistake when counting them and used 1072 qubits, which is very close and does not affect the results.
57. We picked the second bit to simplify synchronization in our measurement setup. The results for the first bit should be very similar to the results for the second bit.
58. S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," Rev. Mod. Phys. **77**, 513–577 (2005).
59. U. L. Andersen, G. Leuchs, and C. Silberhorn, "Continuous-variable quantum information processing," Laser Photon. Rev. **4**, 337 (2010), ArXiv:1008.3468v1 [quant-ph].

1. Introduction

In theory quantum mechanics allows two parties, Alice and Bob, to grow a private, secret key, even if the eavesdropper Eve can do anything permitted by the laws of nature [1–4]. The field of quantum key distribution (QKD) has evolved rapidly in the last two decades, with transmission distance increasing from a table top demonstration to over 250 km in the laboratory [5], and commercial QKD systems available from several vendors [6].

However the components used for the experimental realizations of QKD have imperfections. As for any security technology, it is crucial to scrutinize the implementations in order to obtain a high level of practical security. The discovery of security loopholes does not prove that QKD is insecure, but rather that principles of QKD are not sufficiently well implemented.

Numerous imperfections have been addressed in security proofs [7–12]. For some loopholes it took several years from their discovery until they were covered by security proofs, for instance the Trojan-horse [13, 14] loophole and detector efficiency mismatch [15–17]. The latter was exploited in the time-shift attack [18] on a commercial QKD system [19]. Other loopholes

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

include a variety of side-channels [20–23].

Common to the loopholes mentioned so far is that the corresponding attacks are not implementable in practice, leave Eve with a probabilistic advantage, or introduce a QBER close to the tolerable limit. For instance, the implementation of the time-shift attack [19] gave Eve a probabilistic, information-theoretic advantage. With probability 0.04 the unconditional security is broken; however, extra information is needed and a nontrivial computational task remains to obtain the secret key. In the practical phase-remapping attack [23], Eve caused 19.7% QBER [24] compromising the rarely used two-way post-processing protocol which produces secure key at QBER up to 20% [25, 26].

There is however one class of attacks which stands out in terms of implementability, Eve's information and QBER: The *blinding attacks* [27–29] are fully implementable with current technology, and give Eve the whole raw key while causing zero additional QBER. The latter is essential as the QBER is measured to reveal Eve's presence. In these attacks, the APDs are tricked to exit the single-photon sensitive Geiger mode, and are so-called *blind*. Eve uses a copy of Bob's apparatus to detect Alice's signals, but resends bright trigger pulses instead of single photons, as in the after-gate attack [30]. When the detectors are blind, Bob will only detect the bright trigger pulses if he uses the same basis as Eve. Otherwise his detectors remain silent. Hence Eve gets a full copy of the raw key while causing no additional QBER. Both passively quenched detectors [27], actively quenched detectors [28] and the gated detectors of two commercially available QKD systems [29] have been shown to be vulnerable to blinding. In the case of the passively-quenched detectors, this loophole has been exploited in the first full-scale implementation of an eavesdropper [31], which was inserted in the middle of the 290 m transmission line in an experimental entanglement-based QKD system [32, 33], and recovered 100% of the raw key.

Previously the gated detectors in the commercially available system Clavis2 from manufacturer ID Quantique were subject to continuous-wave (CW) blinding [29]. The blinding illumination caused the bias voltage at the APDs to drop due to the presence of DC impedance of the bias voltage supply, and therefore the APDs were never in Geiger mode. Shortly after the result was published, Yuan *et al.* proposed that removing the bias voltage impedance or lowering the comparator threshold in the detectors would hinder blinding in gated detectors [34]. However, in this paper we show how the same detectors, regardless of the impedance of the bias voltage supply, can be blinded by heating the APD, so-called *thermal blinding*. Furthermore we show how the AC-coupling of the detectors allows a blinding technique which may blind the detectors even if the comparator threshold is lowered. We show that thermal blinding is more sophisticated form of attack than previously reported CW-blinding [29] because the APD can be heated well in advance of the detection times, and is as such harder to catch. Especially for Clavis2, all the detector parameters such as temperature of the cold plate, bias voltage and APD current indicate single photon sensitivity while the detectors are in fact blind.

In this paper we first briefly review how APDs in the linear mode can be exploited to eavesdrop on QKD systems (Section 2). Then the detector design in Clavis2 is discussed (Section 3) before we show how it is possible to thermally blind and trigger the detectors (Section 4). Finally we briefly discuss countermeasures in Section 5 and conclude in Section 6.

2. Eavesdropping exploiting APDs in linear mode

In this section we briefly review how APDs in the linear mode can be exploited to eavesdrop on QKD systems [28, 29].

In Geiger mode operation, an electron-hole pair produced by an absorbed single photon is amplified to a large current in the APD, which exceeds a current comparator threshold and reveals the photon's presence. This is referred to as a *click* [35].

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

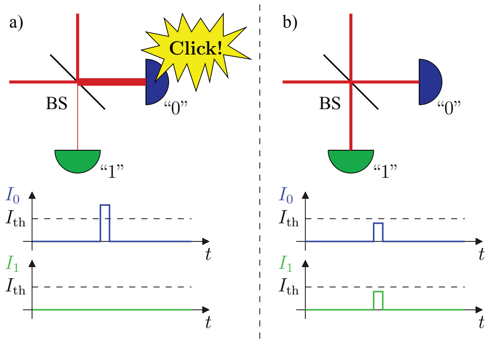


Fig. 1. The last beam splitter (BS) as well as the detectors in a phase-encoded QKD system. I_0 and I_1 is the current running through APD 0/1, and I_{th} is the comparator threshold current above which the detector registers a click. Here we assume that the APDs are in the linear mode, and that Eve sends a bright pulse slightly above the optical power thresholds. a) Eve and Bob have selected matching bases. Therefore the full intensity in the pulse from Eve hits detector 0. The current caused by Eve's pulse crosses the threshold current and causes a click. b) Eve and Bob have selected opposite bases. Therefore half the intensity of Eve's pulse hits each detector (corresponding to 50% detection probability in either detector for single photons). This causes no click as the current is below the threshold for each detector.

In the linear mode however, when an APD is reverse-biased at a constant voltage below the breakdown voltage [36], the current through the APD is proportional to the incident optical power. Usually the APD is placed in a resistive network, and also has an internal resistance. Hence, the current through the APD lowers the bias voltage, and the current through the APD is monotonically increasing with the incident optical power. In this regime, the comparator current threshold translates to a classical optical power threshold [29].

If APDs are used as detectors in a QKD system, and they are optically accessible to Eve when biased under the breakdown voltage, Eve may eavesdrop on the QKD system with an intercept-resend (faked-state [37]) attack. Eve uses a copy of Bob to detect the qubits from Alice in a random basis. Eve resends her detection results, but instead of sending single photons she sends bright pulses, just above the classical optical power threshold. Bob will only have a detection event if his basis choice coincides with Eve's basis choice (see Fig. 1), otherwise no detector clicks.

After the raw key exchange, Bob and Eve are identical both in bit values and basis choices. Since Eve uses a copy of Bob's detectors, Bob's photon-number detection statistics is equal with or without Eve. Therefore the attack works equally well on the BB84 protocol [1], the Scarani-Acin-Ribordy-Gisin 2004 (SARG04) [38] and decoy-state BB84 protocols [39–41]. In addition to attacking the quantum channel, Eve listens on the classical channel between Alice and Bob. Afterwards Eve performs the same classical post-processing as Bob to obtain the identical secret key.

Note that the classical optical power threshold has to be sufficiently well defined for successful perfect eavesdropping. To be precise, let an optical power of $P_{100\%,i}$ or greater always cause a click when applied to detector i. Likewise, let an optical power of $P_{0\%,i}$ or less never cause a click when applied to detector i. The sufficient condition for Eve to be able to make any single

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

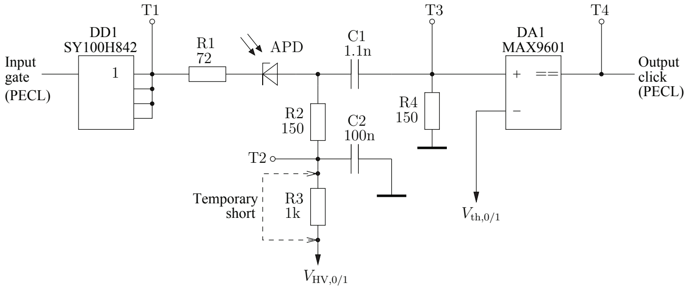


Fig. 2. Equivalent detector bias and comparator circuit. Taps T1-T3 are analog taps of the APD gates ($V_{\mathrm{gate},0/1}$), the APD bias ($V_{\mathrm{bias},0/1}$) and the comparator input ($V_{\mathrm{comp},0/1}$). The digital tap T4 of the detector output ($V_{\mathrm{click},0/1}$) has been converted to logic levels in all oscillograms. For the experiments presented in section 4, the resistor R3 has been shorted.

detector click while none of the other detectors click, can be expressed as

$$\max_i \{P_{100\%,i}\} < 2\left(\min_i \{P_{0\%,i}\}\right). \tag{1}$$

Note that since Alice and Bob openly report the failure due to too high QBER, it is unnecessary for Eve to know the classical optical thresholds $P_{0\%,i}, P_{100\%,i}$ beforehand. In particular, she could start with a high optical power, lowering it each time the protocol fails until it succeeds. Then she knows that she has found the proper trigger pulse power. Note that to avoid causing the protocol to fail, she could probe just a part of the transmission [37].

3. Detector design

3.1. *Detector circuit*

Figure 2 shows an equivalent detector bias and comparator circuit diagram for the detectors in Clavis2, based on reverse engineering. The system ships with factory settings for the detectors, ready for QKD, which we used. The APD is biased just above its breakdown voltage by the high voltage supply $V_{\mathrm{HV},0} = -42.89\,\mathrm{V}$, $V_{\mathrm{HV},1} = -43.08\,\mathrm{V}$. On top of this bias the APD is gated with 2.8 ns TTL pulses every 200 ns from DD1 to create Geiger mode gates. The gates are applied as PECL signals from the mainboard, and the buffer converts them to TTL levels, 0 V and approximately 3 V. The anode of the APD is AC-coupled to a fast comparator DA1 with the thresholds $V_{\mathrm{th},0} = 78\,\mathrm{mV}$ and $V_{\mathrm{th},1} = 82\,\mathrm{mV}$.

The normal operation of the detector circuit can be seen in Fig. 3. A number of techniques have been developed for compensating the capacitive pulse through APDs in the absence of an avalanche [42–45], but this particular detector simply sets the comparator thresholds above the amplitude of the capacitive pulse.

As a side note, applying CW illumination to the APD allowed us to measure the timing of the quantum efficiency curve within the gate quite precisely, see Appendix B.

3.2. *Detector cooling*

To reduce the probability of dark counts, APDs are usually cooled to a low temperature. The two APDs in this QKD system are cooled together by one 4-stage thermoelectric cooler (TEC) (Osterm PE4-115-14-15 [46]). The system software reports the temperature measured by a

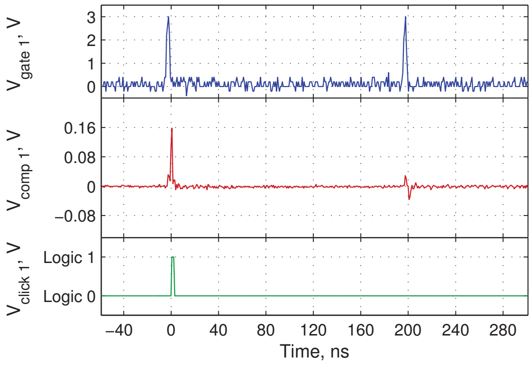


Fig. 3. An example of electrical signals during two gates in detector 1 without any illumination. In the first gate thermal fluctuations or trapped carriers have caused an avalanche, and a click at the comparator output (dark count). A typical amplitude of the avalanche peak is 200 mV for detector 0 and 300 mV for detector 1. Normally the system removes 50 gates after a detection event, but for this oscillogram this feature has been disabled. In the second gate there is no detection event. When no current runs through the APD, it is equivalent to a capacitor, and thus approximately the derivative of the gate pulse shape propagates to the comparator input, with peak positive amplitude ≈ 35 mV.

thermistor mounted on the cold side of the top stage (cold plate), and close to where the APDs are mounted. Note that the cold plate temperature is not always the same as the APD chip temperature, as there is actually a quite substantial thermal resistance between the two. This will become an important point in section 4.2. The hot side of the TEC is mounted on a large heatsink with a fan, such that it stays at approximately room temperature.

The temperature of the cold plate is maintained at a pre-set value by a closed-loop controller that adjusts the TEC current. When the system is switched on, the cold plate (and thus the APDs) is first cooled to the target temperature, $-50\,^{\circ}$C. The system will not start operation unless the cold plate settles at a temperature below $-49.8\,^{\circ}$C. After this the temperature controller always tries to maintain the target temperature. However, there seems to be no alarm: QKD proceeds even if the cold plate temperature is several tens of degrees different from the target temperature.

4. Blinding and control

Blinding is achieved when the system is insensitive to single photons. This can be achieved by ensuring that the APD bias voltage is below the breakdown voltage, or by lowering the voltage in front of the comparator such that the avalanche current does not cross the comparator threshold. The detectors are controllable if they are accessible to Eve in the linear mode with a sufficiently well defined classical optical power click threshold, as in Eq. (1).

We have previously reported that blinding Clavis2 can be achieved by CW illumination due to the bias voltage supply impedance $R3 = 1\,\mathrm{k}\Omega$, which makes the bias voltage drop to a level where the APD is never in Geiger mode [29], even inside the gate.

One fast and easy countermeasure could be to use a low-impedance bias voltage source in the detectors. Therefore, in this paper we consider a modified version of the detectors with R3 shorted (see Fig. 2). We present three different blinding techniques which may be used

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

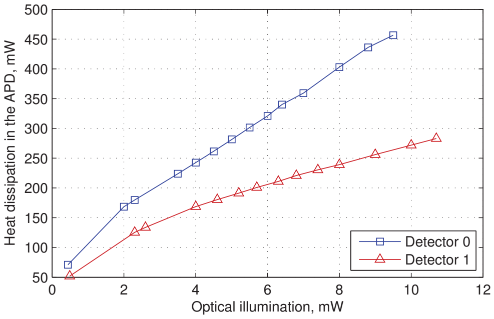


Fig. 4. Calculated heat dissipation (based on measured APD current and voltage) versus the optical illumination for each of the two detectors.

against detectors with a low-impedance bias voltage source, and show that the detectors can be controlled by trigger pulses in the blind state. The technique in section 4.1 clearly works against high-impedance biased detectors as well as against low-impedance biased detectors since it has been demonstrated [29]. The difference is that with a low-impedance bias voltage source, the blinding originates from thermal effects instead of bias voltage drop. The technique in section 4.2 has been used on low-impedance biased detectors, but we see no reason why it should not work similarly well against the unmodified high-impedance biased detectors. The technique in section 4.3 has been used on both high- and low-impedance biased detectors, but we only present the results for the low-impedance biased detectors in this paper.

4.1. Thermal CW-blinding

It turns out that it is possible to blind also low-impedance biased detectors (R3 = 0) by CW illumination. When an APD is illuminated, the power dissipated in the APD is transformed to heat, which may increase the APD temperature. The breakdown voltage is temperature dependent: increasing the temperature increases the breakdown voltage [47, 48]. Since the bias voltage is constant, this makes the APD leave the Geiger mode. Two effects contribute to the power dissipation: electrical heating ($V_{\mathrm{APD}} \cdot I_{\mathrm{APD}}$) and the small contribution by the absorption of the optical power. For the heat dissipation calculations, we simply assume that all the optical power is absorbed and transformed to heat. Figure 4 shows how the heat dissipation increases with the optical illumination.

When the sum of the heat dissipations of the two detectors is approximately 300 mW, the cooling system is running at its maximum capacity with a TEC current of about $I_{\mathrm{TEC}} = 2.37\,\mathrm{A}$ (the air temperature at the heatsink fan intake at this time was 23.6 °C). When the optical illumination is increased beyond this point, the cold plate (and thus APD) temperature starts to increase. Figure 5 shows how the temperature of the cold plate increases with the total amount of heat dissipated in the APDs. When the optical illumination, and thus the load is increased beyond the maximum capacity of the TEC, the cold plate temperature increases approximately linearly with the heat dissipated by the APD. While not in the specifications of this specific TEC [46], other data sheets of similar TECs [49] show that the temperature difference between the hot and cold plate decreases linearly with respect to the load, given a constant TEC current.

When the temperature of the APDs increases, the breakdown voltage also increases with the coefficient of about 0.1 V/K [50]. In this experiment we illuminated both detectors simultaneously, to get sufficient temperature increase without risking a permanent damage to the APDs.

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

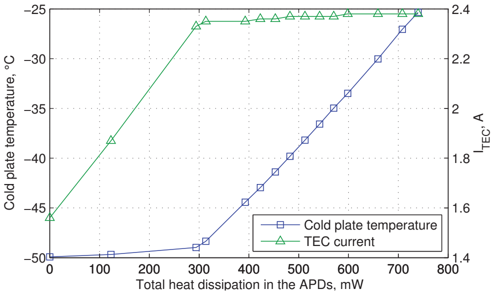


Fig. 5. The temperature of the cold plate and TEC current reported by the software, versus the total amount of heat dissipated in the APDs. It takes several minutes for the cold plate temperature to stabilize at a new value (hotter than −50 °C) after the power dissipation in the APDs is changed.

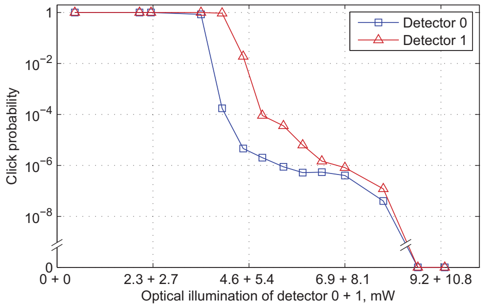


Fig. 6. Click probability versus power of CW illumination applied to both detectors simultaneously.

We used a fibre-optic coupler (see appendix A for the experimental setup) to illuminate both detectors, with 46.75%/53.25% of the optical power going to detector 0/1. This is approximately equal to the measured splitting ratio for the beam splitter in front of the detectors in the system, when illuminated through the short arm of the interferometer [51–53].

Figure 6 shows the click probability versus the CW illumination of the two detectors. The click probability drops below the normal dark count probability (about 10^{-4}), before it becomes *exactly zero* when the illumination exceeds 8.8 mW and 10 mW at the detectors. In the experiment the blinding caused clicks for several minutes before the APDs were properly heated. However, the blinding only needs to be turned on once, afterwards Eve remains undetected.

After the cold plate has been heated by APD illumination, it takes several tens of seconds before it cools to the target temperature of −50 °C. Therefore, the detectors stay blind for some time after the CW blinding illumination is turned off. Detectors 0 and 1 regain dark counts when the cold plate (and thus the APDs) becomes colder than −39.8 °C and −40.1 °C, respectively.

To verify that the detectors could be controlled, the detectors were blinded with 9.5 mW at detector 0 and 10.7 mW at detector 1, and controlled by superimposing a 3 ns long laser pulse slightly after the gate. The click probability thresholds are listed in Table 1. The thresholds

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

Table 1. Control pulse peak power at 0 % and 100 % click probability thresholds, in CW thermal blinding mode

Detector	Click probabilities	
	0 %	100 %
0	1.12 mW	1.31 mW
1	1.71 mW	2.02 mW

satisfy Eq. (1), and thus the eavesdropping method described in Section 2 should be possible when the detectors are thermally blinded by CW illumination.

After observing thermal blinding in this experiment, we realized that this could be the reason why the PerkinElmer SPCM-AQR actively-quenched detector module remained blind at bright pulse frequencies above 400 kHz, despite no substantial bias voltage drop [28]. Therefore we did more precise measurements which confirm that PerkinElmer SPCM-AQR can be thermally blinded [54].

4.2. *Thermal blinding of frames*

As this QKD system is of plug-and-play type, it sends the qubits in packets called *frames* to avoid Rayleigh back-scattered photons to arrive during the gates and increase the QBER [51, 55]. For our experiment we used 1072 qubits per frame [56]. With a 200 ns bit period this makes the frame length 214.4 µs. The break in between the frames varies with the fibre length between Alice and Bob, but is always longer than the frame itself. In our experiment we simply used a 250 µs frame break, which makes a total frame + break period of 464.4 µs.

It turns out that the APD chip and the inner parts immediately touching it (*not* the APD package and not the cold plate) act as a thermal reservoir on the frame period time scale. Therefore bright illumination between the frames heats the APD sufficiently that it stays blind throughout the whole frame. Based on the optical power where the frames went blind, and the average current through the APDs, the thermal resistance between each APD chip and the cold plate is estimated to be at least $190\,\mathrm{K/W}$.

To heat the APDs we used 225 µs long pulses timed in between the frames and fired at both APDs simultaneously. The whole frame went blind at approximately 1.5 mW and 1.7 mW pulse power at detector 0 and 1 respectively. The oscillograms in Fig. 7 show the electrical and optical signals in detector 1 when frames of 1072 gates are thermally blinded by the 225 µs long pulses with 3.5 mW in-pulse power at detector 0, and 4 mW in-pulse power at detector 1. While the system was blind, the cold plate temperature reading was $-49.5\,^{\circ}\mathrm{C}$, and the TEC was running well below its maximum capacity at $I_{\mathrm{TEC}} = 2.006\,\mathrm{A}$. Therefore it seems that even though this system does not check the cold plate temperature after the initial check, further checks of the cold plate temperature would probably not reveal that the detectors are in fact blind.

To verify that the detectors could be controlled, we checked the response to a 4 ns long control pulse timed slightly after the gate of one of the first bits of the frame, and the last bit of the frame. The detection probability thresholds for the second [57] and the last bit are given in Tables 2 and 3. Figure 8 shows oscillograms from detector 1 when it is blinded and controlled in the second bit of the frame.

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

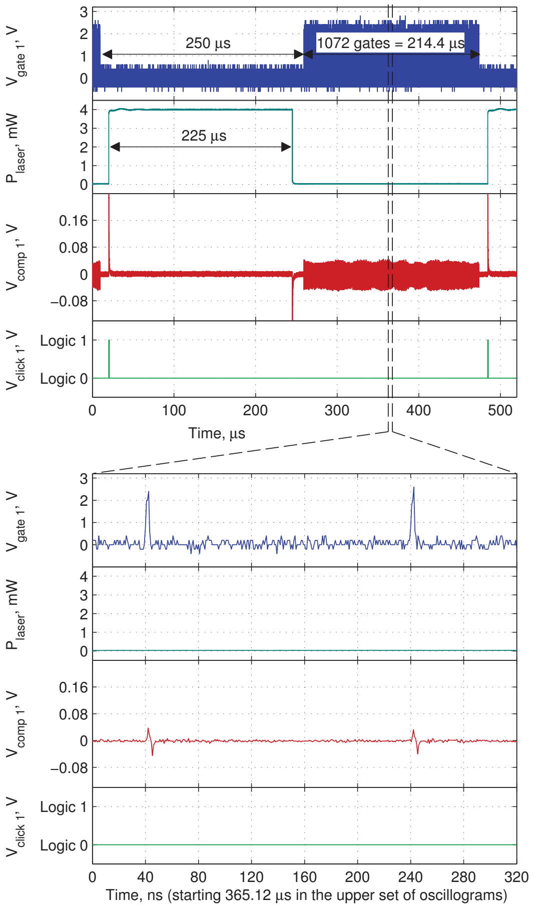


Fig. 7. Thermal blinding of frames. The oscillograms show electrical and optical signals when frames of 1072 gates in detector 1 are thermally blinded by a 225 μs blinding pulse, with 3.5 mW pulse power at detector 0, and 4 mW pulse power at detector 1. The blinding pulse causes a detection event outside the frame, where the system probably does not register clicks (If the click is registered, it could easily be avoided by increasing the power of the blinding pulse gradually, such that the comparator input AC-coupling keeps the voltage below the comparator threshold).

#135153 - $15.00 USD   Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

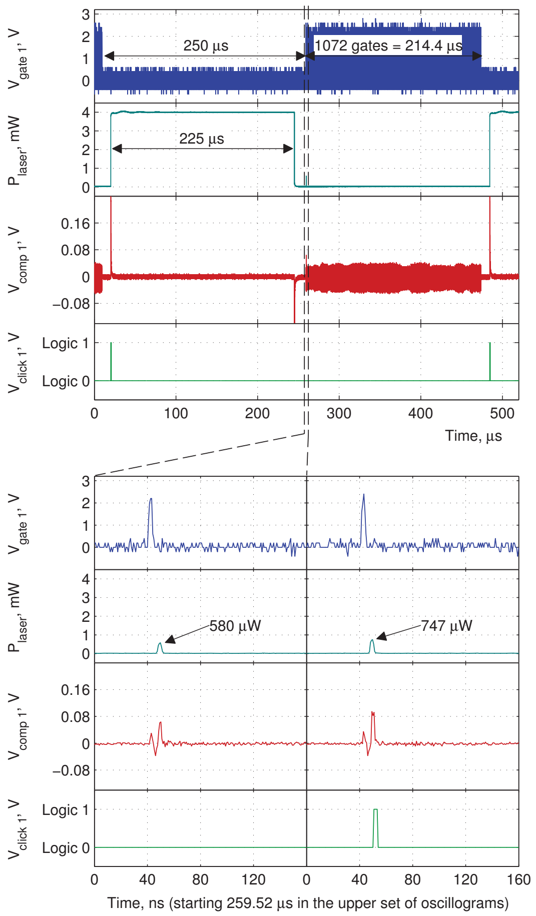


Fig. 8. Detector control during thermal blinding of frames. The oscillograms show electrical and optical signals when frames of 1072 gates in detector 1 are thermally blinded by a 225 µs blinding pulse, with 3.5 mW pulse power at detector 0, and 4 mW pulse power at detector 1, and the detector is controlled by a 4 ns long control pulse timed slightly after the second gate in the frame. In the upper and lower left sets of oscillograms, the 580 µW control pulse never causes any click. In the lower right set, the control pulse is applied after the same gate in the frame, but now its increased 747 µW peak power always causes a click.

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

Table 2. Control pulse peak power at 0 % and 100 % click probability thresholds for the second bit in the frame, when the frame is thermally blinded

Detector	Click probabilities	
	0 %	100 %
0	401 μW	533 μW
1	580 μW	747 μW

Table 3. Control pulse peak power at 0 % and 100 % click probability thresholds for the last bit in the frame, when the frame is thermally blinded

Detector	Click probabilities	
	0 %	100 %
0	305 μW	420 μW
1	340 μW	532 μW

The click probability thresholds in Tables 2 and 3 each satisfy Eq. (1) individually. However, $P_{0\%,0}$ in the last bit of the frame is less than $1/2$ of $P_{100\%,1}$ in the second bit of the frame. This means that the control pulse power would have to be decreased throughout the frame. Since the second and the last bit of the frame can be controlled, it is plausible that the eavesdropping method described in Section 2 could be applied to any bit of the frame.

What is remarkable about this blinding method is that due to the low thermal conductivity between the APD chip and the cold plate, as well as the thermal inertia of the nearby parts, the cold plate thermistor reports a value very close to the normal value. Therefore monitoring the cold plate temperature would not suffice to prevent thermal blinding.

In fact the system needs not to be operating in frames for such blinding to take place: Eve may heat the detectors accepting a 50% QBER for some sessions, eavesdropping on the next sessions.

4.3. *Sinkhole blinding*

It is natural to ask whether the framed blinding technique can be applied at the single gate level, i.e. what happens if bright illumination is applied between adjacent gates? It turns out that this also leads to blinding, but not primarily due to thermal effects. Since the comparator input is AC-coupled (see Fig. 2), the signal at the input of the comparator has the same area over and under 0 V level when averaged over time much longer than R4·C1 = 165 ns. Thus by sending long bright pulses between the gates and no illumination near the gate, it is possible to superimpose a negative-voltage pulse at the comparator input at the gate time. We call this negative pulse a *sinkhole*. An avalanche that occurs within it can have a normal amplitude yet remain below the comparator threshold level.

Using a 140 ns long pulse beginning about 25 ns after the gate, detector 0 becomes completely blind when $P_{\text{laser}} > 205\,\mu\text{W}$, and detector 1 becomes blind when $P_{\text{laser}} > 400\,\mu\text{W}$. To keep both detectors blind, $P_{\text{laser}} = 500\,\mu\text{W}$ is used subsequently. When a large pulse is applied between the gates, the detector will always experience a dark count in the gate due to trapped carriers. Figure 9 shows detector 1 blinded by a 140 ns long, 500 μW bright pulse, starting about 25 ns after the gate.

Initially when the blinding pulses are turned on, there is a transient with about 20-100 clicks, which would be easily detectable in post-processing. Note again that the blinding only needs to be turned on once, and that the blinding can be turned on before the raw key exchange to avoid the clicks being registered.

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

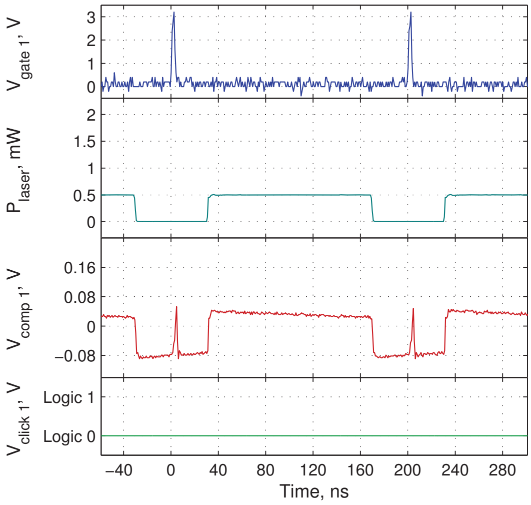


Fig. 9. Sinkhole blinding. The oscillograms show electrical and optical signals when detector 1 is blinded by a 500 µW, 140 ns long laser pulse in between the gates. The avalanche amplitude is about 130 mV and would cause a click if it were not sitting in the negative-voltage pulse. It seems that the reduction in avalanche amplitude (compare to Fig. 3) is caused by heating of the APD, which effectively rises the breakdown voltage.

Table 4. Control pulse peak power at 0 % and 100 % click probability thresholds, during sinkhole blinding

Detector	Click probabilities	
	0 %	100 %
0	655 µW	751 µW
1	773 µW	908 µW

Detector control is obtained by a 3.2 ns long laser pulse timed shortly after the gate. The click probability thresholds found are listed in Table 4. Figure 10 shows oscillograms from detector 1 when it is blind and controlled. Once again, the thresholds in Table 4 satisfy Eq. (1), and thus the eavesdropping method described in Section 2 should be possible when the detectors are sinkhole blinded.

5. Discussion and countermeasures

First of all, the numerous detectors proved blindable and controllable [27–29, 31, 54], and the large number of independent blinding methods available show that avoiding this loophole is non-trivial. Further the results presented in this paper clearly show that removing the impedance of the bias voltage supply is far from being a sufficient countermeasure for this detector design. Yuan *et al.* proposed to lower the comparator threshold, but as seen from the oscillograms in Fig. 9 sinkhole blinding can produce a very low amplitude on the comparator input by choosing an appropriate duty cycle of the blinding illumination. Therefore, lowering the comparator threshold also seems to be an insufficient countermeasure.

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

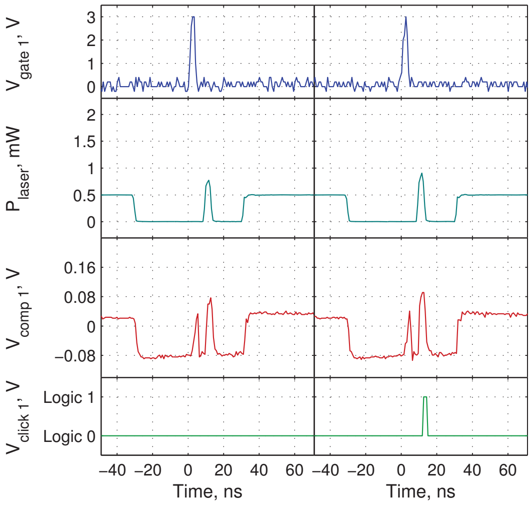


Fig. 10. Detector control during sinkhole blinding. The oscillograms show electrical and optical signals when detector 1 is blinded with a 500 μW, 140 ns long laser pulse in between the gates, and controlled with a 3.2 ns long laser pulse timed shortly after the gate. To the left, the 773 μW control pulse never causes any click. To the right, the 908 μW control pulse always causes a click.

At this point it is not clear to us how to design hack-proof detectors. As we pointed out previously, the most obvious countermeasure is to monitor the optical power at Bob's entrance with an additional detector. However as we also pointed out it is not obvious that this actually closes the loophole; the click threshold close to the gate may be very low, allowing for practically non-detectable control pulses [29]. Thus it is not clear how to set the threshold value for the entrance monitor; in any case the threshold should be derived from and incorporated into a security proof. It would also be crucial that this monitoring detector is not blindable, while being extremely sensitive. Until a detection scheme with a monitoring detector is proven secure, we believe that it cannot be considered as a sufficient countermeasure.

For the passively quenched scheme it has been proposed previously to monitor APD parameters such as APD bias voltage, current and temperature [27]. However, the results in Section 4.2 show that normal APD parameters do not necessarily guarantee single photon sensitivity: for thermal blinding of frames all the APD parameters report normal values during the frames while the detectors are in fact blind.

It is worth emphasizing that the loophole opens when Eve drives the detectors into an abnormal operating regime, namely the linear mode. However, there are also quantum detectors which are actually designed to operate in linear mode. For example, homodyne detectors used in continuous-variable QKD [58, 59] are probably not susceptible to the described attack.

6. Conclusion

The detectors in the Clavis2 QKD system have proved to be blindable by a variety of methods, even with a low-impedance bias voltage supply. Further, the detectors can always be controlled in the blind state. This allows eavesdropping on the QKD system, using the method described in

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

Section 2. Since Eve may use an exact copy of Bob's system, no parameters currently available to Bob reveal Eve's presence. In practice, this should allow for perfect eavesdropping where Eve has an exact copy of Bob's raw key, and thus can extract the full secret key. The eavesdropping strategy described in Section 2 has been implemented and used to capture 100% of the raw key in a 290 m experimental entanglement-based QKD system [31]. We see no practical difficulties implementing the same eavesdropper for this commercial QKD system, using off-the-shelf components. Actually we have proposed a plug-and-play eavesdropper scheme [29] for easy deployment.

Many detectors have already been proved blindable and controllable by Eve [27–29], and the large variety of blinding methods available for the system tested could probably be used on other detector designs as well. While it is relatively easy to design a countermeasure that prevents blinding attacks with the specific parameters chosen in the present work, it is unclear to us how to build generic secure detectors.

This work further emphasizes the importance of thoroughly investigating the non-idealities of each component in a QKD system, as well as battle-testing the system as a whole. This has been a necessary step for any security technology, and will surely be a crucial step for QKD as well. QKD cannot be cracked nor broken, since the principles have been proven secure once and for all. Now the challenge is to make a truly secure implementation of QKD where the components behave within the assumptions of the security proofs.

ID Quantique has been notified about the loophole prior to this publication, and has implemented countermeasures.

A. Measurement setup

Figure 11 shows the measurement setup used for this experiment. The trigger signal is tapped directly from the PECL gate signal (before DD1 in Fig. 2).

When pump current is used to control the power of the laser, the pulse width will vary slightly with the peak power. In our experiment, the observed change in pulse width is less than 10 % after doubling the laser power. Also, the comparator threshold does not seem to be significantly dependent on the pulse width, thus we consider our results valid despite this small change in the laser pulse width.

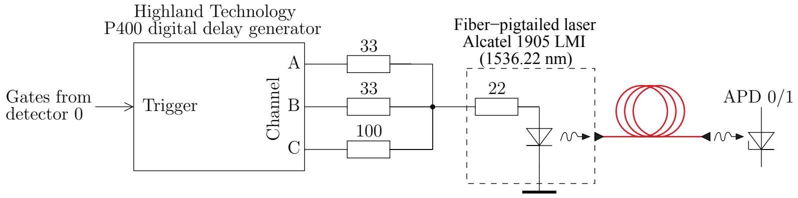


Fig. 11. The setup used in the experiment. Both detectors were illuminated simultaneously by inserting a 50/50 fibre-optic coupler (not shown in the diagram) before the APDs.

B. Direct measurement of quantum efficiency

When CW illumination is applied to the APD, the applied electrical gate "propagates" to the comparator input. This might be caused by a change in linear multiplication coefficient caused by the electrical gate. This allowed us to measure the quantum efficiency mapped inside the "propagated" gate with about 200 ps precision.

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

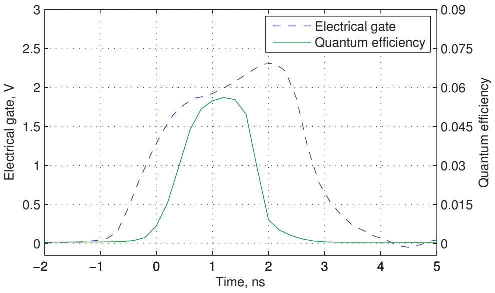


Fig. 12. Quantum efficiency measured directly within the electrical gate for detector 1. The photon sensitivity drops about 1 ns before the falling edge of the gate, because avalanches that start late do not have time to develop a large enough current to cross the comparator threshold.

The single photon sensitivity was measured using a id300 short-pulsed laser attenuated to a mean photon number of 1 per pulse. The quantum efficiency η was derived from the data assuming that the detector is linear (i.e. that an n-photon state is detected with probability $1-(1-\eta)^n$). The timing of the photon arrival at the APD relative to the applied gate was aligned by observing a response to unattenuated laser pulse on top of the 2.1 mW CW illumination. Figure 12 shows the result of the measurement on detector 1.

Acknowledgments

We acknowledge discussions with Sergio Cova. This work was supported by the Research Council of Norway (grant no. 180439/V30) and DAADppp mobility program financed by NFR (project no. 199854) and DAAD (project no. 50727598).

#135153 - $15.00 USD Received 14 Sep 2010; revised 17 Nov 2010; accepted 13 Dec 2010; published 17 Dec 2010

Paper F

After-gate attack on a quantum cryptosystem

F

Published in New Journal of Physics.

DOI: 10.1088/1367-2630/13/1/013043

arXiv: 1009.2683 [quant-ph]

New Journal of Physics
The open-access journal for physics

After-gate attack on a quantum cryptosystem

C Wiechers^{1,2,3,6}, L Lydersen^{4,5,6}, C Wittmann^{1,2,7}, D Elser^{1,2}, J Skaar^{4,5}, Ch Marquardt^{1,2}, V Makarov^{4} and G Leuchs^{1,2}

[1] Max Planck Institute for the Science of Light, Günther-Scharowsky-Straße 1, Bau 24, 91058 Erlangen, Germany
[2] Universität Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany
[3] Departamento de Física, Campus Leon, Universidad de Guanajuato, Loma del Bosque 103, Fracc. Lomas del Campestre, 37150 Leon, Gto, Mexico
[4] Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway
[5] University Graduate Center, NO-2027 Kjeller, Norway
E-mail: Christoffer.Wittmann@mpl.mpg.de

New Journal of Physics **13** (2011) 013043 (14pp)
Received 14 September 2010
Published 26 January 2011
Online at http://www.njp.org/
doi:10.1088/1367-2630/13/1/013043

Abstract. We present a method to control the detection events in quantum key distribution systems that use gated single-photon detectors. We employ bright pulses as faked states, timed to arrive at the avalanche photodiodes outside the activation time. The attack can remain unnoticed, since the faked states do not increase the error rate *per se*. This allows for an intercept–resend attack, where an eavesdropper transfers her detection events to the legitimate receiver without causing any errors. As a side effect, afterpulses, originating from accumulated charge carriers in the detectors, increase the error rate. We have experimentally tested detectors of the system id3110 (Clavis2) from ID Quantique. We identify the parameter regime in which the attack is feasible despite the side effect. Furthermore, we outline how simple modifications in the implementation can make the device immune to this attack.

[6] These authors contributed equally to this work.
[7] Author to whom any correspondence should be addressed.

1367-2630/11/013043+14$33.00

Contents

1. Introduction 2
2. Intercept–resend attack using faked states 3
3. Detectors in Clavis2 4
4. Description of loopholes in the system 5
   4.1. Linear mode avalanche photodiodes 5
   4.2. Faked states applied during the dead time 7
5. Characterization of afterpulsing side effect 7
6. Simulations of after-gate attack and quantum bit error rate estimation 9
   6.1. Strategy of Eve with dead time 10
   6.2. Strategy of Eve without dead time 11
7. Countermeasures 12
8. Conclusions 12

Acknowledgments 13

References 13

1. Introduction

An intriguing feature of quantum optics is that it enables communication protocols that are impossible to achieve by classical means. One prominent example is quantum key distribution (QKD) [1, 2], which in principle allows two parties (Alice and Bob) to communicate with unconditional security. It is thus impossible for an arbitrarily powerful eavesdropper (Eve) to obtain knowledge of the transmitted information.

In the well-known Bennett–Brassard 1984 (BB84) protocol in its original form [3], Alice sends single photons of different polarizations to Bob. Under ideal conditions, the security of this protocol can be rigorously proved [4]. Furthermore, practically feasible procedures for distilling a secret key from the exchanged quantum states are known [5]. During the distillation, Alice and Bob generate a key sequence out of their raw data stemming from the quantum state exchange. Eve's attempt to gain knowledge results in a perturbation of the quantum states, such that her information about the raw key can be upper bounded. Alice and Bob can thus shrink their raw data such that Eve's knowledge of the resulting key sequence becomes negligible.

Rigorous security proofs show that Eve cannot successfully attack an ideal implementation of BB84. However, real implementations always exhibit deviations from the ideal model. In order to guarantee secure communication, such deviations must be included into the security proofs. One example is the use of weak coherent states instead of single photons, which is considered in the Gottesman–Lo–Lütkenhaus–Preskill security proof [6]. The resulting reduction of the key rate can be mitigated by modifications to the protocol, such as in the decoy state method [7]–[9] or in the Scarani–Acin–Ribordy–Gisin 2004 (SARG04) protocol [10]. More subtle deviations can result in side channels through which information can unnoticeably leak to Eve. For example, photons might carry information in unwanted degrees of freedom [11]. Once such side channels are known, they need to be considered in a more general security proof.

Nowadays, quantum cryptography has matured to the point where several commercial products are available[8,9]. Each system might have loopholes that are particular to its implementation. Some implementations are, for example, susceptible to non-conforming light pulses that Eve sends into Alice's or Bob's devices. Eve could use reflectometry to read modulator states [12] or take control of the detectors by sending faked states [13, 14], time-shifted pulses [15] or by detector blinding combined with faked states [16]. The impact of such interventions strongly depends on the particular implementation. It is thus difficult to include them in general security proofs. Alternatively, specific countermeasures could be devised by adapting hardware or software of the systems, such that all assumptions in the security proof about the QKD module are again valid.

In this paper, we investigate a particular attack on the QKD device id3110 Clavis2 from ID Quantique. The fiber-based system utilizes the plug&play principle [17], where the quantum states are encoded as the relative phase of two pulses. In our experiment, we send irregular, bright light pulses (faked states) outside the activation time of the gated detectors. We show that we can generate measurement results in the Bob module with only a slight increase in the quantum bit error rate (QBER), if the side effects of the attack are considered properly.

The paper is organized as follows. Section 2 describes the basic principles of our attack. In section 3, we elaborate on the particular implementation of the detectors in the Clavis2 system. In section 4, we present the imperfections found in the system. Section 5 discusses the side effect of the faked-state attack, which actually partly protects the security of the system. Section 6 presents all of the necessary elements for simulations and shows the parameters for which the Clavis2 system is *not* secure. In section 7, we discuss possible countermeasures against the proposed attack before concluding in section 8.

2. Intercept–resend attack using faked states

In the BB84 protocol [3], Alice randomly chooses one of two non-orthogonal bases to encode her quantum bit. Bob independently chooses his measurement basis at random. If his basis matches Alice's, he will measure the quantum state correctly. In half of the cases, however, Bob chooses the wrong basis. Alice and Bob compare the encoding and measurement basis via a classical authenticated channel and remove all events with basis mismatch from their raw data.

In an intercept–resend attack, Eve places a copy of Bob's apparatus into the quantum channel. Then she performs the same kind of measurement as Bob, tries to reproduce the original quantum state and sends it to Bob. Since Eve is unaware of Alice's basis choice, she will inevitably introduce errors in case of a basis mismatch between her basis and the one used by Alice and Bob. Eve will thus always be detected in a perfect implementation of a QKD system [5, 6].

In case of an imperfect implementation, however, Eve may attack the QKD system by sending faked states instead of quantum states [13]. Her aim is to generate faked states that only produce a detection event in the Bob module if Eve's basis matches Bob's basis. In this case, after Alice and Bob discard their non-matching bases, all that remains in the key are bits for which Alice, Eve and Bob had the same basis. Thus, Eve generates no errors.

[8] ID Quantique, URL: http://www.idquantique.com.

[9] MagiQ Technologies, URL: http://www.magiqtech.com.

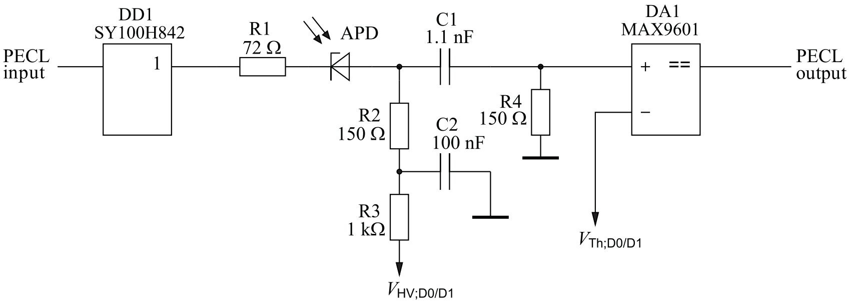


Figure 1. Equivalent circuit diagram of Bob's detectors in Clavis2. See text for description.

After the attack, Bob and Eve share identical bit values and basis choices. The attack works on widely used QKD protocols, namely BB84, SARG04 and the decoy method. The attack exhibits an extra 3 dB loss because of the possible basis mismatch of Eve and Bob. This is easily compensated in a practical Eve, since she may use better detector efficiencies and exclude loss in the line [13].

3. Detectors in Clavis2

The impact of faked states strongly depends on the implementation of the detection scheme in a QKD system. We will focus on systems employing avalanche photodiodes (APDs) in the Geiger mode, as is the case in many QKD systems [18, 19], and all commercially available realizations (see footnotes 8 and 9). Furthermore, we assume that the APDs are gated, i.e. activated only in time intervals when signal states are expected to arrive. During the activation time, a large reverse voltage is applied to the APDs such that the APDs are biased above the breakdown voltage. Then a single photon can trigger a carrier avalanche that results in a macroscopic current. If the generated current exceeds a certain threshold, a detection event (click) is registered.

As an example, we consider the behavior of the gated detectors in ID Quantique's Clavis2 QKD system. A detector circuitry reverse-engineered by us is shown in figure 1. In the following, we explain the circuitry and mention the detector parameters that were preset by the manufacturer. The APDs are biased by the high-voltage supply with $V_{\mathrm{HV;D0/D1}}$ almost as large as the breakdown voltage ($V_{\mathrm{HV;D0}} = -42.89\,\mathrm{V}$ and $V_{\mathrm{HV;D1}} = -43.08\,\mathrm{V}$). The detectors are gated in the Geiger mode by means of TTL signals, which are applied on top of the bias voltage with a period of 200 ns. The gates are supplied as PECL logic-level signals from the main board and converted to TTL signals by the buffer DD1. The comparator DA1 monitors the APD current and registers a click in the detector when the current peak passes a threshold ($V_{\mathrm{Th;D0}} = 77\,\mathrm{mV}$, $V_{\mathrm{Th;D1}} = 84\,\mathrm{mV}$). The comparator produces a PECL output pulse for each detection event.

During all of the time not covered by the gate, each APD is biased at a constant value $V_{\mathrm{HV;D0/D1}}$ below the breakdown voltage. The current through the APD is then approximately proportional to the incident optical power. The circuit behaves similarly to a linear photodiode followed by a comparator.

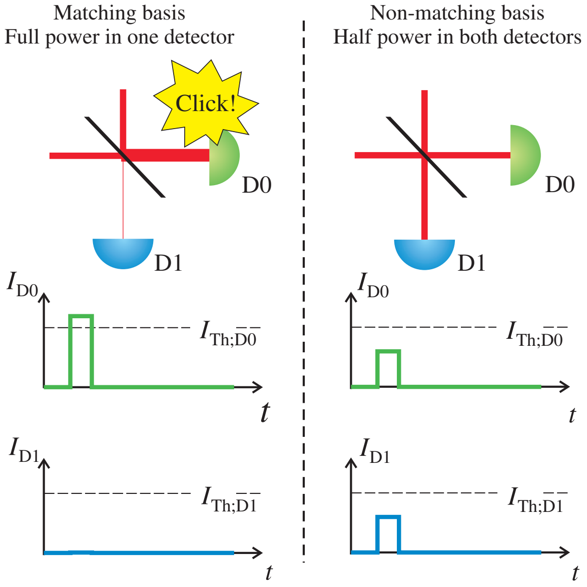


Figure 2. Principle of detector control. In the detection part of a phase-encoded QKD, the two pulses that could be generated by Eve as a faked state interfere at a 50 : 50 beamsplitter. (a) For Bob's basis choice matching Eve's, the signals interfere such that detector D0 clicks deterministically, because the photocurrent surpasses the detection threshold $I_{\mathrm{Th;D0}}$. (b) For Bob's basis choice not matching Eve's, the power is split 50 : 50 to both detectors. The photocurrent does not surpass the threshold. Therefore, the faked state is not detected.

4. Description of loopholes in the system

In the following subsections, we describe two unexpected deviations of the detection system from the idealized behavior implicitly assumed by the designers of the QKD system. We start by explaining the detection process in detail. In an ideal plug&play system, the relative phase between the signal states and reference pulses in the receiver module (0, $\pi/2$, π, $3\pi/2$) is determined by a combined phase modulation of Alice and Bob, i.e. by a combination of Alice's bit and basis (0, $\pi/2$, π, $3\pi/2$) and Bob's measurement basis (0, $\pi/2$).

Let us consider a standard intercept–resend attack. For a matching basis choice of Alice, Eve and Bob, the phase difference is 0 or π. This restricts the possible outcome of the measurement to a single detector and results in a conclusive outcome for Bob. For a mismatched basis choice, the phase difference is $\pi/2$ or $3\pi/2$. In this case, either of their detectors will click randomly. This clearly causes a QBER of 25%.

4.1. Linear mode avalanche photodiodes

In the linear regime of the APDs, Eve can substitute the quantum states with bright coherent states [16]. Figure 2 shows examples of pulses that generate a click only if Bob's and Eve's bases match, since the comparator following the APD will only click if the input optical power

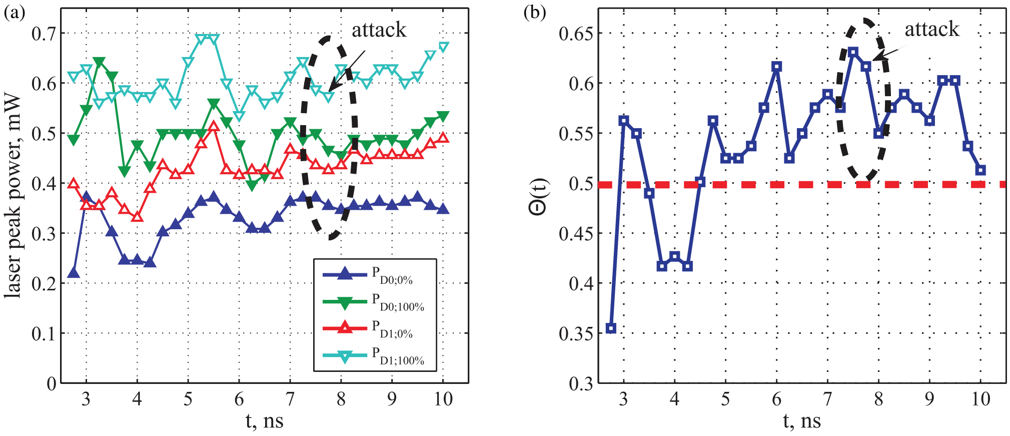


Figure 3. Detection click thresholds in Clavis2 for a pulse duration of 0.12 ns. (a) Power thresholds $P_{\mathrm{D0,D1;0\%,100\%}}$ for 0 and 100% probability of a bright pulse detection in detectors D0 and D1. The fluctuations are reproducible and are probably caused by the fluctuating bias voltage after the gate. (b) Calculated $\Theta(t)$ (see equation (1)), which shows that an atttack is possible for delays of 4.5–10 ns with an optimal and comfortable margin of Θ at 7.5 ns.

surpasses a critical power threshold. In case of a basis mismatch, the optical power is distributed equally among the detectors and no detection click is generated.

To exploit the loophole experimentally, we look closer at the detector characteristics. As mentioned, the APDs are biased below the breakdown voltage before and after the gate. Optically, Bob's phase modulation extends temporally on either side of the gate pulse by approximately 10 ns. We have verified that the system accepts clicks at least 10.5 ns after the gate, still assigning the click to the bit slot associated with the gate.

We send bright laser pulses to both detectors before and after they are gated, in order to find the click thresholds of each detector. A perfect control of Bob is possible if the maximum power at which the detectors do not produce clicks is higher than half the power at which they always produce a click. This can be written as

$$\Theta(t) = \frac{\min\left\{P_{\mathrm{D0;0\%}}(t)\,,\,P_{\mathrm{D1;0\%}}(t)\right\}}{\max\left\{P_{\mathrm{D0;100\%}}(t)\,,\,P_{\mathrm{D1;100\%}}(t)\right\}} > 0.5, \tag{1}$$

where t is the time between the leading edge of the gate and the bright pulse, $P_{\mathrm{D0;0\%}}(t)$ is the maximum power that does not generate a click in D0 and $P_{\mathrm{D0;100\%}}(t)$ is the minimum power that certainly generates a click in D0 (analogously for D1).

We have found that the linear behavior prior to the gate cannot be exploited, since charge carrier generation results in a large afterpulse effect during the gate. For an attack after the gate, figure 3 shows the experimentally measured power thresholds and the corresponding values of $\Theta(t)$ for 0.12 ns long 1550 nm laser pulses. The figure shows that an attack is feasible in a wide time window with the maximum value of $\Theta(t)$ at 7.5 ns after the gate. At this time, a 587 μW laser pulse can cause a click in both detectors, while a 293.5 μW laser pulse will never cause a click in any detector. This result reveals a weak spot in the system. We have found, however,

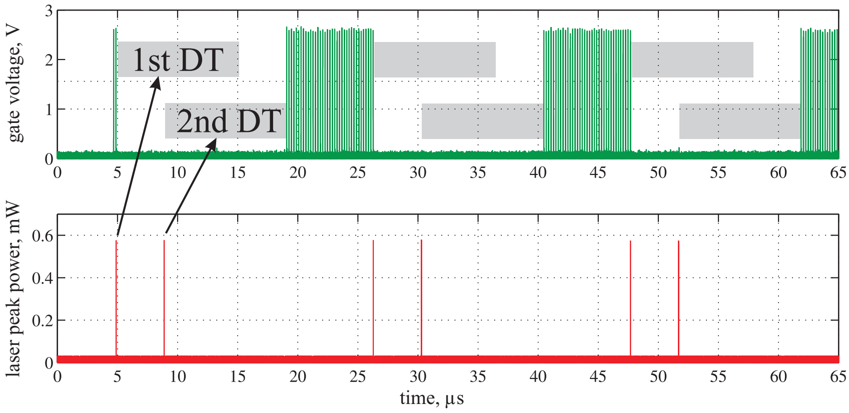


Figure 4. Dead time extension behavior. The figure shows that if a bright pulse (or avalanche) causes a dead time (1st DT), any bright pulse during the dead time will be a valid detection and causes an extra dead time (2nd DT). Therefore, it extends the effective dead time. (upper oscillogram) The gate pattern applied to the detector. (lower oscillogram) Optical power of successive bright pulses impinging on the detector with a delay of 4 μs.

that the attack cannot be applied straightforwardly, because of an afterpulsing side effect, which is discussed in section 5. Therefore, we attacked at the point 7.75 ns after the gate to slightly reduce the maximum laser power applied to the system. At 7.75 ns after the gate, a 575 μW laser pulse can cause a click in both detectors, while a 287.5 μW laser pulse will never cause a click in any detector.

4.2. Faked states applied during the dead time

As a second loophole in the system, we have found that the system registers detection events from bright faked states at any time. Typically, the device applies a dead time of 10 μs whenever the system registers a click at any of the detectors, not gating both APDs for the duration of the dead time [22]. However, we have found that the time between the detection events originating from our faked states can be as short as 30 ns.

Figure 4 shows the effect of a bright pulse arriving during the dead time. The electronic logic registers a valid click and subsequently resets the dead time to another 10 μs after the second bright pulse. We found experimentally that in the dead time all faked states with a laser peak power of 575 μW were detected by detector D0 while the detection probability of Bob's D1 was $\eta_B > 0.99985$. In section 6.2, we will show how this loophole can be exploited in order to overcome the negative side effect of afterpulses, which is described in the next section.

5. Characterization of afterpulsing side effect

Once a detection is registered in a gated APD, a long dead time is typically applied to reduce afterpulsing. This dead time is considerably longer than the inverse of the gating frequency and is typically of the order of several microseconds.

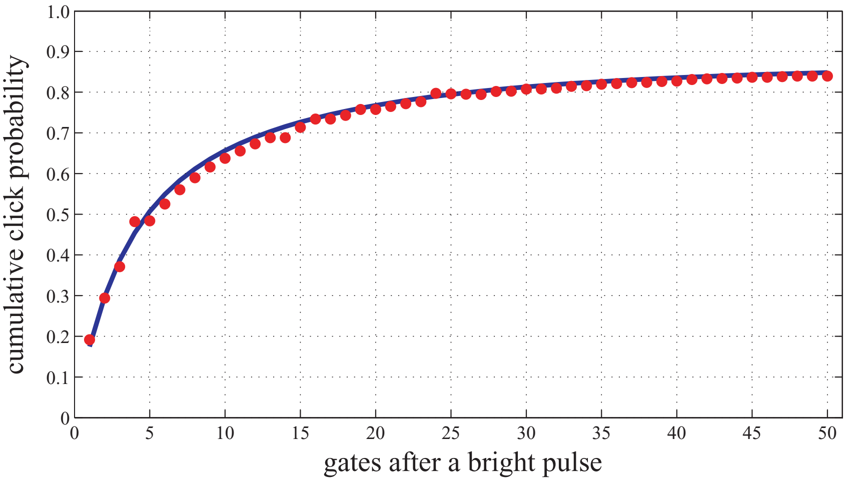


Figure 5. Afterpulses caused by the after-gate attack. The chart shows the experimentally measured cumulative probability to obtain at least one dark count after a 287.5 μW pulse applied to both detectors (red dots), and a Monte Carlo simulation of the same process using the parameters from table 1 (solid line).

The afterpulse effect is due to carrier traps, which are populated by avalanche current in the detection process [19, 23]. We have found that bright pulses also populate the carrier traps, irrespective of whether they generate detection events or not. Without a registered detection, a dead time is not applied by the detector's circuitry. The carriers released from traps can therefore cause afterpulsing in the detector. These uncontrollable clicks will contribute to the QBER.

We have characterized this side effect of the after-gate attack in the successive gates by plugging a laser directly to one of the fiber inputs of the 50 : 50 beamsplitter of figure 2. The laser pulses have a peak power of 287.5 μW for each detector. As expected, the pulse never causes a click immediately. However, very often it causes an afterpulse within the following gates. Figure 5 shows the cumulative probability to obtain a click in any of the two detectors in the next gates. After 50 gates, the cumulative probability to obtain a random click has reached 84%, which could jeopardize Eve's attack by causing a too high QBER.

Note that the system sends frames of 1075 pulses as dictated by the send–return configuration [17]. Therefore, the attack can always be applied in the end of the frame with a reduced risk of a random afterpulse. If the system requires on average only one detection per two frames, then the security is completely compromised. Additionally, the attack may be applicable for a different set of system parameters, e.g. different operation frequencies of Bob.

We have modeled the afterpulse effects of carrier traps. We have found that the probabilities $P_{\mathrm{ap;D0/D1}}(t_j)$ of a detection event after a faked-state attack can be modeled using a double exponential decay for the detectors,

$$P_{\mathrm{ap;D0/D1}}(t_j) = P_{\mathrm{dark;D0/D1}} + (1 - P_{\mathrm{dark;D0/D1}}) \sum_{i=1}^{2} A_{i;\mathrm{D0/D1}} \mathrm{e}^{-t_j/\tau_{i;\mathrm{D0/D1}}}, \tag{2}$$

where $P_{\mathrm{dark;D0/D1}}$ is the dark count probability, $A_{i;\mathrm{D0/D1}}$ are probability amplitudes that depend on the number of carriers that are generated in the detector, and $\tau_{i;\mathrm{D0/D1}}$ are the associated

Table 1. Decay parameters of trap levels in both detectors. These parameters were used for the Monte Carlo simulation shown in figure 5.

Detector 0		Detector 1	
Parameter	Value	Parameter	Value
$P_{\mathrm{dark;D0}}$	1.158×10^{-4}	$P_{\mathrm{dark;D1}}$	3.812×10^{-4}
$A_{1;\mathrm{D0}}$	3.572×10^{-2}	$A_{1;\mathrm{D1}}$	1.068×10^{-1}
$A_{2;\mathrm{D0}}$	2.283×10^{-2}	$A_{2;\mathrm{D1}}$	5.054×10^{-2}
$\tau_{1;\mathrm{D0}}$	$1.159\,\mu\mathrm{s}$	$\tau_{1;\mathrm{D1}}$	$0.705\,\mu\mathrm{s}$
$\tau_{2;\mathrm{D0}}$	$4.277\,\mu\mathrm{s}$	$\tau_{2;\mathrm{D1}}$	$3.866\,\mu\mathrm{s}$

decay constants. The afterpulse probabilities in figure 5 were reproduced by a Monte Carlo simulation using the double exponential decay model given by equation (2). By iterating the Monte Carlo simulation, the decay parameters were found by minimizing the squared distance between the measurement data and the simulation data, equivalent to the method of least squares in regression analysis. Table 1 shows the resulting decay parameters, and the final Monte Carlo simulation is shown in figure 5. The decay parameters are in agreement with earlier published data on APDs [19, 23].

6. Simulations of after-gate attack and quantum bit error rate estimation

We estimate the QBER for different attack scenarios using a Monte Carlo simulation. In our simulation, Alice and Bob use the BB84 protocol. Eve performs a faked-state attack by putting her modified Bob and Alice modules in the channel. Eve places her Bob module in the beginning of the line next to Alice. We assume that Alice sends an optimized signal amplitude [20] where the sent mean photon number μ is equal to the channel transmittance T. Unless otherwise noted, Eve measures this signal with perfect detectors (100% efficiency and noiseless) and a lossless apparatus. Then she reproduces a bright faked state with the corresponding bit value for Bob.

Bob's module is simulated, including realistic parameters that were determined experimentally for our device. Besides the parameters for the afterpulsing and dark count effects (see table 1), there are the optical transmittance of Bob's setup ($T_{\mathrm{B}} = 0.412$), the quantum efficiency of the detectors ($\eta_{\mathrm{B}} = 0.1$) and the detector dead time ($\tau_{\mathrm{dead}} = 10\,\mu\mathrm{s}$).

In the simulation, we process the consecutive gates of a frame separately. We incorporate the side effect by increasing the afterpulse probability of a detector, if carriers were generated either by a regular avalanche or by bright pulses with full or half power[10]. We have experimentally verified that for the operation frequency and used optical powers, the carrier traps in the detectors are not saturated by our attack and that the afterpulses of the two carrier-generating processes with different lifetimes occur independently and with Poissonian statistics [21]. The afterpulse probability of a gate at time t_j is then increased by a previous gate

[10] Carrier generation by the half-power pulses is the most important effect, because the system does not apply the dead time after them.

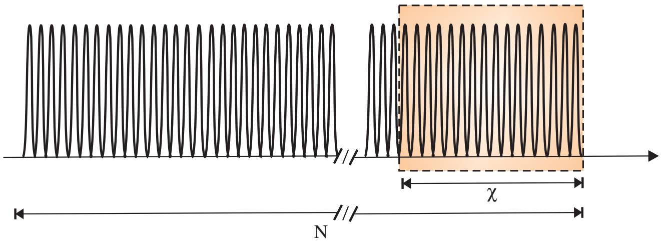


Figure 6. We attack only the last χ gates of the total number of gates $N = 1075$ in the frame, such that the raw key rate generated by the attack on each frame is equal to the rate without eavesdropping.

with carrier generation at time t_k as

$$P^{\text{new}}_{\text{ap;D0/D1}}(t_j) = P^{\text{old}}_{\text{ap;D0/D1}}(t_j) + (1 - P^{\text{old}}_{\text{ap;D0/D1}}(t_j)) \sum_{i=1}^{2} \gamma_{i;\text{D0/D1}} A_{i;\text{D0/D1}} \mathbf{e}^{-(t_j - t_k)/\tau_{i;\text{D0/D1}}}, \tag{3}$$

where $\gamma_{i;\text{D0/D1}}$ is a correction of the probability amplitude $A_{i;\text{D0/D1}}$. In case of a bright pulse attack with 287.5 μW pulses, $\gamma_{i;\text{D0/D1}} = 1$. For a bright pulse attack with full 575 μW power to one detector (successful attack), we increase the afterpulse probability by applying equation (3) twice. We have measured that a regular avalanche in D0 and D1 has $\{\gamma_{i;\text{D0}}, \gamma_{i;\text{D1}}\} = \{1.836, 3.673\}$.

6.1. Strategy of Eve with dead time

We first simulated the QBER without the dead-time loophole described in section 4.2, i.e. assuming that Bob rejects detection events during the detector dead time. To increase the performance of Eve's attack, she adopts the following strategy. (i) Attack only the last χ gates of the total of N gates of a frame, as shown in figure 6. This will lead to a larger trapped carrier density at the end of the frame, which, when gates are absent, is ignored by the detectors. (ii) Use a small classical memory (up to three consecutive gates), which allows for checking whether she received several consecutive clicks. These are then sent to Bob as a *burst attack*. This will lead to a decreased time between failed attacks and following attacks, which suppresses the afterpulsing by forcing earlier dead time. (iii) After the burst attack, wait as long as the dead time of Bob's detectors, in order to avoid carrier generation and afterpulsing directly after the dead time.

We perform a simulation of the QBER induced by the attack for varying repetition rate and channel transmittance. Repetition rates between 100 kHz and 10 MHz are simulated, because the maximal gate frequency of 8 MHz specified for stand-alone single-photon counters id201 from ID Quantique[11] suggests that gate frequencies in this range are feasible. The simulation consists of two major steps. Firstly, Eve adjusts the number of attacked gates χ in order to adjust the channel transmittance T to the one anticipated by Alice and Bob. Eve tries to maximize the burst length in her attack. For a decreasing channel transmittance, Eve, however, receives fewer photons from Alice. Therefore, the maximal burst length decreases for decreasing transmittance

[11] Datasheet id201, ID Quantique.

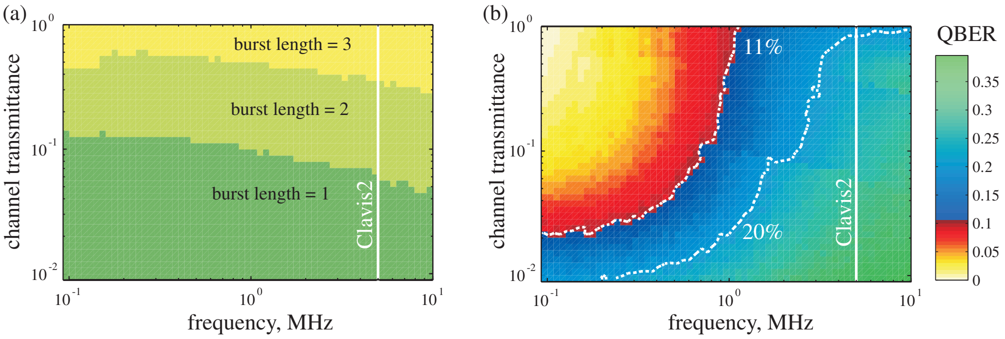


Figure 7. Simulated attack performance for the case when Bob discards clicks during the detector dead time. (a) Burst length for different channel transmittances and gate frequencies. (b) QBER generated by the attack. We show contour lines for QKD security proofs that are more [24] or less [5] tolerant to errors, allowing for a QBER of 20 or 11%, respectively.

(see figure 7(a)). Secondly, the QBER is simulated for 10^4 frames. The average QBER is shown in figure 7(b) and compared to upper bounds of two different security proofs [5, 24]. The protocol in [24] would require a single photon source and is therefore not directly applicable in Clavis2. Therefore, we find that the attack cannot compromise the security of Clavis2 due to increased afterpulse probability at the gate repetition rate of 5 MHz. However, the security would be compromised for a more advanced system using single photons and the protocol in [24], or for gate frequencies below about 1 MHz. We note that there are numerous experimental setups and a commercial QKD system (see footnote 9) working below the critical operation frequency of about 1 MHz. Additionally, technological improvements in the detectors could reduce the afterpulse effects and thereby enable the attack for high frequencies.

6.2. *Strategy of Eve without dead time*

Eve can adapt her attack strategy if she has access to both the after-gate and the dead-time loopholes. In the following, we show a strategy that is not an optimized one, but a rather intuitive and (as it turns out) successful approach. Eve again attacks the end of the frame, as shown in figure 6. Her strategy is to attack as frequently as possible. Thereby, she quickly enters a dead time of Bob's detectors. She will generate detection events during the dead time and, thereby, can prolong the detector dead time, as shown in section 4.2. Ideally, a major part of the attack happens during the dead state, which would completely remove the effect of afterpulses and result in negligible QBER for this part of the attack.

In the simulation, we again adjust the number of attacked gates χ and simulate the QBER for 10^4 frames. Figure 8 shows that for high transmittance, the QKD system is vulnerable against the advanced attack, including for an eavesdropper with detection efficiency implementable today. The photon statistics are maintained during the attack. It is therefore also applicable to decoy state protocols [7]–[9].

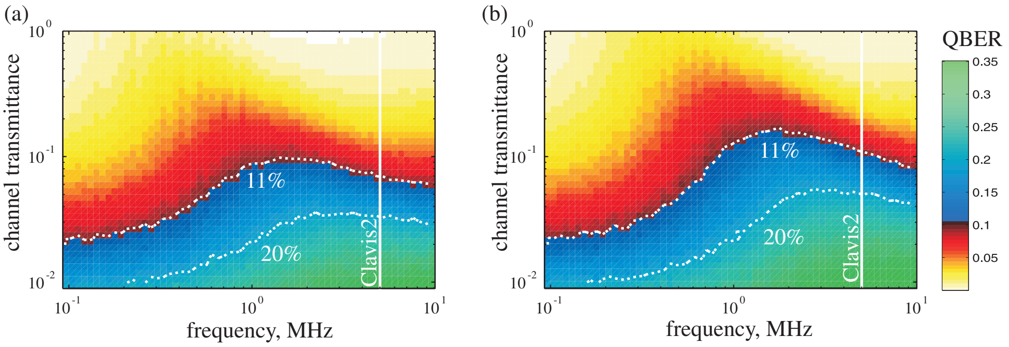


Figure 8. Simulated attack performance without dead time. The figures show the QBER generated by the attack, taking advantage of the sensitivity of the detectors during the dead time together with the elongation of the dead time. (a) QBER with a perfect Eve. The attack is feasible for all repetition rates and a wide range of channel transmittances. (b) QBER with a realistic Eve with a detection efficiency $T_B\eta_B = 0.5$ and a dark count probability $P_{\text{dark}} = 10^{-5}$, corresponding to a technically advanced but feasible eavesdropper.

7. Countermeasures

Note that both eavesdropping strategies (especially the latter one) leave strong fingerprints. In the latter case, the distance between two valid detection events can be smaller than the dead time of 10 μs. Therefore, one countermeasure is to search for too closely timed detection events. Furthermore, rejecting detections during the dead time would restrict eavesdropping to lower frequencies, as shown by our first simulation (see figure 7). A complete protection against the presented attacks is guaranteed if the detection times are resolved, such that Bob can discriminate between detections inside and outside the single-photon-sensitive part of the gate. Note, however, that this is highly non-trivial since the intrinsic jitter caused by the avalanche build-up is about equal to the length of the gate itself. Alternatively, a watchdog detector can be placed at Bob's input in order to detect bright faked states. Since such a detector cannot be an avalanche detector (this can be hacked), the countermeasure is only effective against bright faked states.

8. Conclusions

We have demonstrated that gated detectors in QKD systems can be controlled by an external eavesdropper using bright laser pulses during the linear mode operation. In particular, we have analyzed the attack parameters for the commercial QKD system Clavis2 from ID Quantique. In principle, the system is controllable by bright trigger pulses arriving after the gate time. Other present and future detector technologies will have to be tested for this vulnerability. However, we have found a side effect: afterpulse generation due to the faked states. The side effect generates high QBER, and therefore actually protects the system from a straightforward faked-state attack. Eve can, however, take advantage of a second imperfection, namely that the system accepts the bright pulses even in the dead time and, furthermore, resets the remaining dead time. In a simulation of the attack, we have found that the system is insecure if clicks are accepted during the dead time. The presented after-gate attack can be used independently or together with the blinding attack in [16]. Although the after-gate attack in contrast to the blinding increases the QBER, it has the advantage that the optical power sent into the Bob module is weaker. Therefore, the after-gate attack is harder to detect with a watchdog detector. Another advantage is that this attack can be applied to detectors that are not blindable.

ID Quantique has been notified about this loophole prior to the submission of the manuscript, and has implemented countermeasures. Part of their countermeasure is to remove gates at random times, and check whether detection events still occur without a gate[12]. This would likely reveal the after-gate attack, with the bright pulses placed well behind the gate. However, it is not obvious that this fully negates the after-gate attack, since it might be possible to shift the trigger pulse close to the gate, making it trigger only in the presence of a gate.

Acknowledgments

We acknowledge ID Quantique's valuable assistance in this project. We also thank Georgy Onishchukov and Nitin Jain for fruitful discussions. This work was supported by the Research Council of Norway (grant no. 180439/V30), DAADppp mobility program financed by NFR (project no. 199854) and DAAD (project no. 50727598). CW acknowledges support from FONCICYT project no. 94142.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[3] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing* (*Bangalore, India*) p 175

[4] Mayers D 1996 Quantum key distribution and string oblivious transfer in noisy channels *Advances in Cryptology-Proc. Crypto 96 (Lecture Notes Comp. Sci. 1109)* (Berlin: Springer) p 343

[5] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[6] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quant. Inf. Comp.* **4** 325

[7] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[8] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[9] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[10] Scarani V, Acín A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901

[11] Nauerth S, Fürst M, Schmitt-Manderbach T, Weier H and Weinfurter H 2009 *New J. Phys.* **11** 065001

[12] Vakhitov A, Makarov V and Hjelme D R 2001 *J. Mod. Opt.* **48** 2023
Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev.* A **73** 022320

[13] Makarov V and Hjelme D R 2005 *J. Mod. Opt.* **52** 691

[14] Makarov V 2009 *New J. Phys.* **11** 065003

[15] Zhao Y, Fung C H F, Qi B, Chen C and Lo H K 2008 *Phys. Rev.* A **78** 042333

[16] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photonics* **4** 686

[12] Private communication with ID Quantique SA, Chemin de la Marbrerie 3, 1227 Carouge, Geneva, Switzerland.

[17] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N 1997 *Appl. Phys. Lett.* **70** 793
Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New J. Phys.* **4** 41

[18] Ribordy G, Gisin N, Guinnard O, Stucki D, Wegmuller M and Zbinden H 2004 *J. Mod. Opt.* **51** 1381

[19] Trifonov A, Subacius D, Berzanskis A and Zavriyev A 2004 *J. Mod. Opt.* **51** 1399

[20] Branciard C, Gisin N, Kraus B and Scarani V 2005 *Phys. Rev.* A **72** 032301

[21] Goodman J W 1985 *Statistical Optics* (New York: Wiley)

[22] Makarov V, Brylevski A and Hjelme D R 2004 *Appl. Opt.* **43** 4385

[23] Cova S, Lacaita A and Ripamonti G 1991 *IEEE Electron. Dev. Lett.* **12** 685

[24] Chau H F 2002 *Phys. Rev.* A **66** 060302

Paper G

Secure gated detection scheme for quantum cryptography

Published in Physical Review A.

DOI: 10.1103/PhysRevA.83.032306

arXiv: 1101.5698 [quant-ph]

Secure gated detection scheme for quantum cryptography

Lars Lydersen,[1,2,*] Vadim Makarov,[1] and Johannes Skaar[1,2]

[1]*Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway*

[2]*University Graduate Center, NO-2027 Kjeller, Norway*

(Received 29 January 2011; published 11 March 2011)

Several attacks have been proposed on quantum key distribution systems with gated single-photon detectors. The attacks involve triggering the detectors outside the center of the detector gate, and/or using bright illumination to exploit classical photodiode mode of the detectors. Hence a secure detection scheme requires two features: The detection events must take place in the middle of the gate, and the detector must be single-photon sensitive. Here we present a technique called *bit-mapped gating,* which is an elegant way to force the detections in the middle of the detector gate by coupling detection time and quantum bit error rate. We also discuss how to guarantee single-photon sensitivity by directly measuring detector parameters. Bit-mapped gating also provides a simple way to measure the detector blinding parameter in security proofs for quantum key distribution systems with detector efficiency mismatch, which up until now has remained a theoretical, unmeasurable quantity. Thus if single-photon sensitivity can be guaranteed within the gates, a detection scheme with bit-mapped gating satisfies the assumptions of the current security proofs.

DOI: 10.1103/PhysRevA.83.032306 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum mechanics allows two parties, Alice and Bob, to grow a random, secret bit string at a distance [1–4]. In theory, the quantum key distribution (QKD) is secure, even if an eavesdropper Eve can do anything allowed by the currently known laws of nature [5–9].

In practical QKD systems there will always be imperfections. The security of QKD systems with a large variety of imperfections has been proved [5,10–17]. Device-independent QKD tries to minimize the number of assumptions on the system, but unfortunately the few assumptions [2,18,19] in the security proofs seem to be too strict to allow useful implementations [20] with current technology [21].

Several security loopholes caused by imperfections have been identified, and attacks have been proposed and in some cases implemented [15,22–34]. With notable exceptions [22,23,27,30,33], most of the loopholes are caused by an insufficient model of the detectors.

While several detection schemes exist, most implementations use avalanche photodiodes (APDs) gated in the time domain to avoid a high rate of dark counts. Gated means that the APD is single-photon sensitive only when a photon is expected to arrive in a time window called the detector gate. Attacks on these detection schemes are based on exploiting the classical photodiode mode of the APD, or the detector response at the beginning and/or end of the detector gate.

In the attacks based on the classical photodiode mode of the APD, the detectors are triggered by bright pulses [28,31]. If necessary, the APDs can be kept in the classical photodiode mode, in a so-called blind state, using additional bright background illumination [28,29,31,34,35]. When the detectors are blind, they are not single-photon sensitive any more, but only respond to bright optical trigger pulses. In most gated systems, blinding is not necessary because the APDs are in the classical photodiode mode outside the gates. Therefore, in the after-gate attack [36], the trigger pulses are simply placed after the gate.

Several attacks are based on detector efficiency mismatch (DEM) [24]. If Bob's apparatus has DEM, Eve can control the efficiencies of Bob's detectors individually, by choosing a parameter t in some external domain. Examples of such domains can be the timing, polarization, or frequency of the photons [14,24]. As an example, consider DEM in the time domain. Usually Bob's apparatus contains two single-photon detectors to detect the incoming photons, one for each bit value. Owing to different optical path lengths, inaccuracies in the electronics, and finite precision in detector manufacturing, the detection windows and hence the efficiency curves of the two detectors a and b are slightly shifted, as seen in Fig. 1(a). Several attacks exploit DEM [15,24,25] in various protocols [37], some of which are implementable with current technology. The time-shift attack [25] has been used to gain an information-theoretical advantage for Eve when applied to a commercially available QKD system [32]. In the experiment, Eve captured partial information about the key in 4% of her attempts, such that she could improve her search over possible keys.

After each loophole has been identified, effort has been made to restore the security of the detection schemes. DEM is now included in the receiver model of several security proofs [14,15,17] as an efficiency mismatch or blinding parameter η, defined differently according to the generality of the proof. For arbitrary systems that can be described with linear optics [15],

$$\eta = \frac{\min_t\{\eta_a(t),\eta_b(t)\}}{\max_t\{\eta_a(t),\eta_b(t)\}}, \tag{1}$$

where $\eta_a(t)$ and $\eta_b(t)$ are the detection efficiencies of the two detectors. Here t labels the different optical modes; in the special case without mode coupling it labels the different temporal modes. An example is given in Fig. 1(a). In the most general case η is given by the lowest probability that a nonvacuum state incident to Bob is detected [17]. For either definition of η, there is an infinite number of modes involved

[*] lars.lydersen@iet.ntnu.no

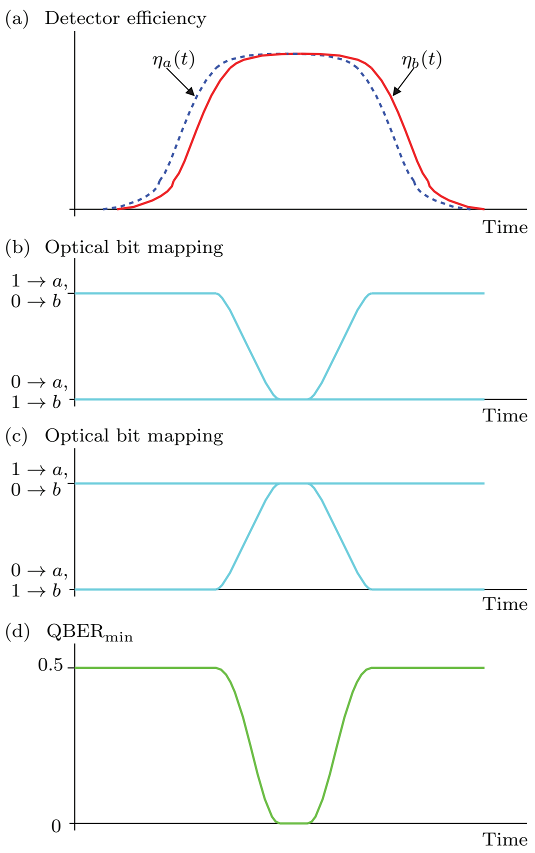


FIG. 1. (Color online) Bit-mapped gating. (a) Detector gates with DEM. $\eta_a(t)$ (blue, dashed) and $\eta_b(t)$ (red, solid) are the efficiencies of the two detectors a and b with respect to time t. (b),(c) Possible optical bit mapping (teal) when the software bit mapping is set to $a \to 0, b \to 1$ (b) and $a \to 1, b \to 0$ (c). In a phase-encoded system the two levels would correspond to 0 and π phase shift in one basis, and $\pi/2$ and $3\pi/2$ phase shift in the opposite basis. Note that software bit mapping and optical bit mapping coincide in the bit-mapped gate, which is well within the detector gates. (d) QBER$_{\mathrm{min}}(t)$ (green) as obtained from (8) with the bit-mapped gate shown in (b) and (c).

(all superpositions of temporal modes [15]), which makes the blinding parameter difficult to measure or bound in practice. For a given value of η, the secret key rate is given by [17]

$$R \geqslant -h(E) + \eta[1 - h(E)], \tag{2}$$

where E is the quantum bit error rate (QBER) measured by Alice and Bob, and $h(\cdot)$ is the binary Shannon entropy function. Here we have assumed symmetry between the bases in the protocol; in addition, we have ignored any basis leakage from Alice and back reflection from Bob (the most general expression is given in the original reference [17]). Unfortunately, in practical systems the rate (2) will usually be zero, because $\eta \to 0$ owing to the edges of the detector gates. For the commercial QKD system subject to the time-shift attack, $\eta < 0.01$ [estimated from the curves in Fig. 3 of Ref. [32] using Eq. (1)].

As noted in Ref. [15], one way of obtaining a better η would be to discard pulses near the edge of the detector gate. Then η could be calculated from (1) including only the modes t that are accepted as valid detections. However, this is highly nontrivial. The avalanche in an APD is a random process, and the jitter in the photon-timing resolution is of the same order of magnitude as the duration of the detector gate. A good photon-timing resolving detector still has 27-ps jitter [38]. Furthermore, the unavoidable difference in the acceptance windows for the different detectors will also contribute to DEM (one detector accepts clicks while the other discards them).

A frequently mentioned countermeasure for systems with DEM is called four-state Bob [24,25,39,40]. Then Bob uses a random detector–bit mapping, randomly assigning the bit values 0 and 1 to the detectors a,b for each gate. In a phase-encoded QKD system, this can be implemented by Bob choosing from four different phase settings $\{0,\pi/2,\pi,3\pi/2\}$ instead of only two $\{0,\pi/2\}$. Then Eve does not know which detector characteristics correspond to which bit value. However, as mentioned previously [15,24,25], this patch does not close the loophole. Eve may use a Trojan-horse attack [22,23,41,42] to read Bob's phase modulator settings. While Alice's system is usually secured against the Trojan-horse attack by the optical attenuator at her entrance, this solution will not work for Bob's system because the attenuator would also absorb nearly all the single photons from Alice. Note also that the four-state Bob patch does not secure against the after-gate attack [36] nor any of the detector control attacks [31,35].

Here we present a novel way of securing Bob's receiver called bit-mapped gating (Sec. II). It secures the system against all kinds of pulses outside the central part of the detector gate in the Bennett-Brassard 1984 (BB84) and related protocols [1,43–45]. The technique is compatible with the existing security proofs [14,15,17] and makes it simple to find η. In general, it represents a useful concept, where parameters from characteristics of the QKD system are coupled to the parameters estimated by the protocol. In this case η becomes coupled to the QBER. Subsequently we analyze the security of bit-mapped gating (Sec. III), discuss how to characterize detectors, and how to implement a guarantee of single-photon sensitivity (Sec. IV). Finally we conclude (Sec. V).

II. BIT-MAPPED GATING

Let us start with two definitions. Software bit mapping determines how the signals from detectors a and b are mapped into the logical bits 0, 1. Similarly, optical bit mapping, which can be implemented by generalizing the basis selector, maps quantum states with bit values 0,1 (for instance, $|0\rangle$,$|1\rangle$ in the Z basis) to the detectors a,b. Note that if software bit mapping and optical bit mapping do not coincide, the bit value 0 sent by Alice will be detected as the bit value 1 by Bob.

Bit-mapped gating works as follows:

(1) Somewhere in between the detector gates, Bob randomly selects software bit mapping, assigning detectors a,b to bit values 0,1.

(2) Likewise, the basis is selected randomly between the X and Z basis, along with random optical bit mapping. Because this happens between the detector gates, jitter is not critical.

(3) Inside the detector gate, optical bit mapping is matched to software bit mapping. The period with matching optical and software bit mapping is the bit-mapped gate.

Note that optical bit mapping can be equal on both sides of the bit-mapped gate to minimize the need for random numbers. Figure 1 shows a typical time diagram.

As an example, consider a phase-encoded implementation of the BB84 protocol, where the basis selector at Bob is usually a phase modulator. The zero-phase shift corresponds to the Z basis and the $\pi/2$ phase shift corresponds to the X basis. Optical bit mapping can be selected by adding either 0 or π to the phase shift. Hence in this implementation the bit-mapped gating patch could be implemented as follows: Bob randomly selects software bit mapping somewhere between the gates. Furthermore, Bob selects a random basis, i.e., 0 or $\pi/2$ phase shift between the gates, and adds either 0 or π to the phase shift to apply the random optical bit mapping. During the gate, the software and optical bit mapping coincide.

All states received and detected outside the bit-mapping gate cause random detection results (owing to the random optical and software bit mapping), and thus introduce a QBER of 50%. The measured QBER could be used to estimate the fraction of detections that must have occurred in the center of the gate (in Fig. 1: Close to zero QBER would mean that most detection events must have passed the basis selector, and thus hit the detector, in the middle of the gate). This can be used to limit the DEM, because considering only the modes in the center of the detector gate gives less DEM than considering all modes.

III. SECURITY ANALYSIS

The goal of this section is to derive an expression for the minimum QBER introduced by any state received by Bob, during the transition to and from the bit-mapped gate. Ideally, the minimum QBER is 0 inside the bit-mapped gate, and $1/2$ outside the bit-mapped gate.

The input of Bob's detection system consists of many optical modes t, for instance, corresponding to different arrival times at Bob's system. Each mode t may contain a mixture of different number states. Note that Bob could have measured the photon number in each mode without disturbing the later measurement; thus it suffices to address specific number states. We use the usual assumption that each photon in a n-photon state is detected individually. Under these assumptions, we first calculate the minimum QBER caused by a single photon arriving in a single mode at Bob. Then, in the Appendix, we show that multiple photons in this mode, or photons in other modes, can only increase the minimum QBER.

Consider a single photon arriving at Bob in a given mode t. Because the BB84 protocol is symmetric with respect to the bit values and the bases, we may assume without loss of generality that Alice sent $Z0$ and that Bob measures in the Z basis. Outside the bit-mapped gate, Bob performs four different measurements depending on the software and optical bit mapping. For each measurement, Bob will obtain one out of three measurement outcomes, bit 0, bit 1, or vacuum denoted by subscript v.

Let η_a,η_b be the efficiencies of the two detectors, $|\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$ and $|\theta^\perp\rangle = \sin\theta|0\rangle - \cos\theta|1\rangle$. During a bit-mapped gate, θ is varied from 0 to $\pi/2$. For each value of θ, Bob performs one out of the four measurements,

$$M_0 = \eta_a|0\rangle\langle 0|, \quad M_1 = \eta_b|1\rangle\langle 1|, \quad M_v = I - M_0 - M_1, \tag{3a}$$

$$M_0' = \eta_b|0\rangle\langle 0|, \quad M_1' = \eta_a|1\rangle\langle 1|, \quad M_v' = I - M_0' - M_1', \tag{3b}$$

$$M_0'' = \eta_a|\theta\rangle\langle\theta|, \quad M_1'' = \eta_b|\theta^\perp\rangle\langle\theta^\perp|, \quad M_v'' = I - M_0'' - M_1'', \tag{3c}$$

$$M_0''' = \eta_b|\theta\rangle\langle\theta|, \quad M_1''' = \eta_a|\theta^\perp\rangle\langle\theta^\perp|, \quad M_v''' = I - M_0''' - M_1'''. \tag{3d}$$

If Bob uses the four measurements with equal probabilities, the statistics will be given by using the measurement operators,

$$\begin{aligned} E_0 &= \tfrac{1}{4}(M_0 + M_0' + M_0'' + M_0''') \\ &= \tfrac{1}{4}(\eta_a + \eta_b)[(1+\cos^2\theta)|0\rangle\langle 0| + \sin^2\theta|1\rangle\langle 1| \\ &\quad + \sin\theta\cos\theta(|0\rangle\langle 1| + |1\rangle\langle 0|)], \end{aligned} \tag{4a}$$

$$\begin{aligned} E_1 &= \tfrac{1}{4}(M_1 + M_1' + M_1'' + M_1''') \\ &= \tfrac{1}{4}(\eta_a + \eta_b)[\sin^2\theta|0\rangle\langle 0| + (1+\cos^2\theta)|1\rangle\langle 1| \\ &\quad - \sin\theta\cos\theta(|0\rangle\langle 1| + |1\rangle\langle 0|)], \end{aligned} \tag{4b}$$

$$\begin{aligned} E_v &= \tfrac{1}{4}(M_v + M_v' + M_v'' + M_v''') \\ &= \left(1 - \frac{\eta_a + \eta_b}{2}\right) I. \end{aligned} \tag{4c}$$

Note that $E_v \propto I$, so the detection probability is independent of the photon state ρ:

$$p_{\text{det}} = 1 - \text{Tr}[\rho E_v] = \frac{\eta_a + \eta_b}{2}. \tag{5}$$

The eigenvalues of operators E_0 and E_1 are given by $p_{\text{det}}(1 \pm \cos\theta)/2$. Thus the minimum and maximum probability of detecting bit values 0 and 1 for any single photon sent by Eve is given by

$$p_{0,\,\text{min}} = p_{1,\,\text{min}} = \frac{p_{\text{det}}}{2}(1 - \cos\theta), \tag{6}$$

$$p_{0,\,\text{max}} = p_{1,\,\text{max}} = \frac{p_{\text{det}}}{2}(1 + \cos\theta). \tag{7}$$

Because Alice sent $Z0$, the minimum QBER introduced by a single photon is given by

$$\text{QBER}_{\text{min}} = \frac{p_{1,\,\text{min}}}{p_{\text{det}}} = \frac{1}{2}(1 - \cos\theta). \tag{8}$$

As expected, for $\theta = \pi/2$, $\text{QBER}_{\text{min}} = 1/2$. For multiphotons, a random bit value is assigned to double clicks [10,16]. The Appendix shows that sending multiple photons can only increase the QBER caused by detection events. Hence Eq. (8) gives the minimum QBER for any photonic state sent by Eve.

The security proofs in Refs. [14,15,17] involve Bob predicting the results of Alice's virtual X-basis measurement. Because the prediction is not carried out in practice, Bob can perform any operation permitted by quantum mechanics. In the proofs Bob's prediction consists of a filter followed by an "X-basis" measurement. When nothing is known about the distribution of the detection events within the gate, the worst-case assumption is that all the detection events occur with maximum DEM. Therefore, the best filter we can construct can only guarantee that a fraction η of the inputs can successfully pass the filter.

With our patch, we may use the QBER to determine a lower bound for the number of detection events which must have occurred in the central part of the detector gate. Assuming that t labels temporal modes, consider the number of detection events that occurred in the range where $\text{QBER}_{\text{min}} < E'$ (see Fig. 2). Here, E' is a threshold selected by Bob. Let η' be the blinding parameter for the modes for the range where $\text{QBER}_{\text{min}} < E'$. It can be calculated from Eq. (1), but where t only runs over this range. If the measured QBER is equal to E, a fraction

$$f = \frac{E' - E}{E'} \tag{9}$$

must have been detected in the modes where $\text{QBER}_{\text{min}} < E'$. Note that increasing E' increases f, and may decrease η' (see Fig. 2). As will become apparent below, E' should be selected to maximize $f\eta'$.

For decoy protocols [43–45], E should be replaced with the QBER estimated for single-photon states. This improves the estimate of the fraction f, especially for large distances where the dark counts become a major part of the total QBER.

In the worst case, a fraction f experienced a reduced DEM η'. Therefore, the filters in the security proofs can be replaced as follows: The new filter discards pulses in the modes for which $\text{QBER}_{\text{min}} > E'$. For the modes inside the bit-mapped gate, where $\text{QBER}_{\text{min}} < E'$, the new filter reverts the quantum operation from the receiver in the opposite basis in the same way that the old filter reverted it for all modes, but now having a success rate η'. Because we can guarantee that a fraction f of the photons are in the bit-mapped gate, at least $f\eta'$ pulses will successfully pass the new filter. Therefore the parameter η in all the proofs [14,15,17] can be replaced with $f\eta'$, and the rate (2) becomes

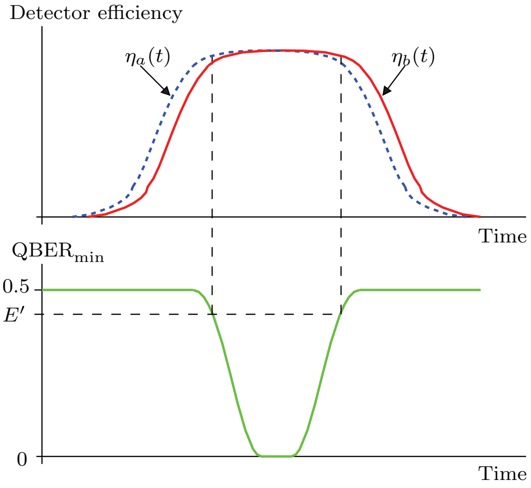


FIG. 2. (Color online) Curves (a) and (d) from Fig. 1. The dashed line shows how a threshold E' can be used to limit the range of modes t used to calculate or bound η'.

$$R \geqslant -h(E) + f\eta'[1 - h(E)], \tag{10}$$

when one assumes symmetry between the bases, and no source errors. Without symmetry between the bases, all parameters become basis dependent, and the rate is the sum of the rates in each basis.

Let us see how bit-mapped gating could improve the secure key rate for the commercial QKD system in Ref. [32]. For this system, $\eta < 0.01$. In the same experiment, the QBER is measured to be 5.68%. Assuming $E' = 0.45$ and $\eta' = 0.9$, $f\eta'$ becomes 0.79, thus a substantial improvement. In fact, the rate obtained from Eq. (2) without the patch is 0, while the rate obtained from Eq. (10) is 0.227, so clearly the patch can be used to resecure an insecure implementation.

IV. DETECTOR DESIGN AND CHARACTERIZATION

When designing Bob's system, one should ensure that the bit-mapped gate is well within the detector gate, i.e., that the detector efficiencies are approximately equal within the bit-mapped gate. Then, it should be possible to measure or bound the detector efficiencies and the basis selector response $\theta(t)$ in the temporal domain. In a phase-encoded system this would correspond to measuring the detector efficiencies and the phase modulation as a function of time [46], over the range of wavelengths and polarizations accepted by Bob. With this data, the minimum QBER as a function of time can be calculated from (8), and a diagram similar to Fig. 2 can be obtained. After selecting an appropriate limit E', η' can be calculated by (1) but where t runs only over the modes where $\text{QBER}_{\text{min}} < E'$, and not over all available modes.

In general, there might be coupling between the different temporal modes owing to misalignments and multiple reflections [14,15]. The bit-mapped gate ensures that the pulse passed the basis selector inside the temporal detector gate, but does not guarantee the actual detection time. For example, a pulse could pass in the center of the bit-mapped gate, but afterwards take a multiple reflection path such that it hits the detector outside the detector gate. This can be handled by characterizing the worst-case mode coupling as described previously [15]. Let δ be the worst-case (power) coupling of modes inside the bit-mapped gate to outside the gate. This will typically be the worst-case multiple-reflection path after the basis selector, and should be boundable from component characteristics. Then, the parameter δ can be interpreted as

$$\delta = \frac{\text{\# pulses that hits the detector outside the gate}}{\text{\# pulses sent into the gate}}. \tag{11}$$

In the worst case, δ of the f detection events might have happened outside the central part of the detector gate; thus one must let $f \to f(1-\delta)$.

Finally one must guarantee that the detectors are not blind within the gate [31], and fulfill the assumptions in Sec. III during the transition of the optical bit mapping. Note that the transition ends when there is no longer any correlation between software bit mapping and optical bit mapping. If a significant correlation exists also after the detector gate, it could be exploited in the after-gate attack [36].

Although it is tempting to place an optical watchdog detector at the entrance of Bob, the absence of bright illumination does not necessarily mean that the detectors are single-photon sensitive. For instance, owing to the thermal inertia of the APD, it can remain blind for a long time after the bright illumination is turned off [35].

A cheap way to guarantee single-photon sensitivity is to monitor all detector parameters [29], such as APD bias voltage, current, and temperature. It seems difficult to monitor the temperature of the APD chip [35], but monitoring the bias voltage and current should make it possible to predict the heat generated by the APD, and thus prevent thermal blinding [35].

The ultimate way of guaranteeing single-photon sensitivity is to measure it directly. This can be done by placing a calibrated light source inside Bob that emits faint pulses at random times [34] (see Fig. 3). Then the absence of detection events caused by this source would indicate that the detector is blind. Further, a calibrated light source inside Bob could be useful in more ways, for instance, to characterize and calibrate detector performance in deployed systems.

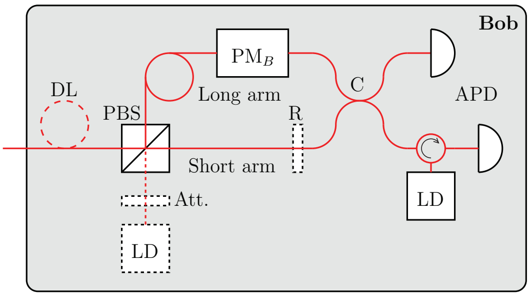


FIG. 3. (Color online) A calibrated light source inside Bob. The figure shows the Bob module in a plug-and-play system [4,47–49], which has two possible implementations of the calibrated light source: either a separate attenuated laser diode (LD) at a suitable place, or in the case of send-return systems where Bob already contains a laser diode, a weakly reflective element (R) to reflect some light back into the APDs. In one-way systems [3,50], Bob does not normally contain any light source, therefore a separate laser diode would be the only option. A short delay line (DL, delay > gate period/2) at Bob's input guarantees that Eve cannot interfere with the detector operation based on whether the source is activated or not. PBS: polarizing beam splitter; Att.: optical attenuator; PM: phase modulator; 50 : 50 fiber-optic coupler.

The patch could cause a minor reduction in QKD performance compared to running an (insecure) system without the patch. In particular, the detector gates might have to be longer to contain the basis-selector gate. This would increase the dark count rate, and thus limit the maximum transmission distance. A calibrated light source inside Bob would also cause a minor reduction in the performance because the gates used for testing the detector sensitivity likely cannot be used to extract the secret key. However, both these effects are minor, and are easily justified by the restoration of security.

V. DISCUSSION AND CONCLUSION

In this work, we have presented a technique called "bit-mapped gating" to secure gated single-photon detectors in QKD systems. It is based on a general concept where hardware imperfections are coupled to the parameters estimated by the protocol. Bit-mapped gating causes all detection events outside the central part of the detector gate to cause high QBER.

Bit-mapped gating is compatible with the current security proofs for QKD systems with detector efficiency mismatch [14,15,17]. In particular, it provides a simple way of measuring the detector blinding parameter. A secure gated detection scheme is obtained if bit-mapped gating is combined with detectors guaranteed to be single-photon sensitive.

ACKNOWLEDGMENT

Financial support is acknowledged from the Research Council of Norway (Grant No. 180439/V30).

APPENDIX: MINIMUM QBER FOR MULTIPHOTONS

Here we prove that the minimum QBER can only increase when the number of photons sent to Bob is increased. As noted previously, we use the usual assumption that each photon in a n-photon state is detected individually. This means that each photon hits a separate set of detectors, and then the detection results are merged to give the detection results of threshold detectors.

Let us first consider the case where Bob receives a large number of two-photon states. Let the two photons within the states be labeled 1 and 2. Individually, each of the two photons would have caused the minimum QBER Q_1 and Q_2 [as found from Eq. (8)]. Again we assume that Alice sends the bit value 0, without loss of generality. For two-photon states there will be three cases of detected events: either only photon 1 is detected, only photon 2 is detected, or both photons are detected (in our model, this latter possibility corresponds to the case where both sets of detectors register a click). Let there be n_1 events where only photon 1 was detected, n_2 events where only photon 2 was detected, and c events where both photons were detected. For photon i, out of the $n_i = n_{i,0} + n_{i,1}$ events, $n_{i,0}$ and $n_{i,1}$ were detected as the bit value 0 and 1, respectively. Likewise, out of the $c = c_{i,0} + c_{i,1}$ events where both photons are detected,

$c_{i,0}$ and $c_{i,1}$ were detected as the bit value 0 and 1 for photon i (remember that in the model each photon hits a separate set of detectors).

When only one of the photons is detected, the situation is identical to the single-photon case treated in Sec. III. Hence states such that $Q_i = n_{i,1}/n_i$ give the lowest possible QBER. For the events where both photons are detected, the detections can have any correlation, but for each photon $c_{i,1} \geqslant cQ_i$, because Q_i represents the lowest fraction of the bit value 1 possible, regardless of the correlation with any other photon. The total QBER Q can be found from merging the detections from the two sets of detectors. Double clicks are assigned a random bit value [10,16], therefore half of the double clicks get the bit value 1. This gives the total QBER,

$$\begin{aligned} Q &= \frac{n_{1,1} + n_{2,1} + \frac{1}{2}(c_{1,1} + c_{2,1})}{n_1 + n_2 + c} \\ &\geqslant \frac{Q_1\left(n_1 + \frac{c}{2}\right) + Q_2\left(n_2 + \frac{c}{2}\right)}{n_1 + n_2 + c} \\ &\geqslant \min(Q_1, Q_2). \end{aligned} \tag{A1}$$

By repeating the argument above, but replacing the detection of photon 1 with the detection of N photons, it is easy to see that $Q \geqslant \min(Q_N, Q_{N+1})$. Hence, by induction, any detection event caused by more than one photon can only cause a higher QBER than the single-photon case.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[5] D. Mayers, in *Proceedings of Crypto'96*, edited by N. Koblitz (Springer, New York, 1996), Vol. 1109, pp. 343–357.

[6] D. Mayers, J. ACM **48**, 351 (2001).

[7] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[8] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[9] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[10] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[11] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[12] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **7**, 431 (2007).

[13] Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A **77**, 052327 (2008).

[14] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **9**, 131 (2009).

[15] L. Lydersen and J. Skaar, Quantum Inf. Comput. **10**, 60 (2010).

[16] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[17] Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).

[18] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[19] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[20] There exists at least one proposal for implementing device-independent QKD [51]. The implementation looks challenging and leads to a much lower secret key rate than the rate in conventional systems.

[21] V. Scarani and C. Kurtsiefer, e-print arXiv:0906.4547v1.

[22] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).

[23] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).

[24] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006); **78**, 019905 (2008).

[25] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).

[26] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).

[27] Chi-Hang Fred Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).

[28] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, e-print arXiv:0809.3408.

[29] V. Makarov, New J. Phys. **11**, 065003 (2009).

[30] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, New J. Phys. **11**, 065001 (2009).

[31] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).

[32] Y. Zhao, Chi-Hang Fred Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).

[33] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[34] I. Gerhardt, Q. Liu, J. Skaar, A. Lamas-Linares, C. Kurtsiefer, and V. Makarov, e-print arXiv:1011.0105.

[35] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010).

[36] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).

[37] V. Makarov and J. Skaar, Quantum Inf. Comput. **8**, 622 (2008).

[38] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, J. Mod. Opt. **51**, 1267 (2004).

[39] P. M. Nielsen, C. Schori, J. L. Sørensen, L. Salvail, I. Damgård, and E. Polzik, J. Mod. Opt. **48**, 1921 (2001).

[40] M. J. LaGasse, US Patent application 20,050,190,922 (2005).

[41] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 517 (2000).

[42] D. S. Bethune and W. P. Risk, IEEE J. Quantum Electron. **36**, 340 (2000).

[43] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[44] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[45] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[46] If the phase modulator response differs depending on the software bit mapping and basis choice, it should simply be bounded.

[47] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).

[48] H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, Electron. Lett. **33**, 586 (1997).

[49] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electron. Lett. **34**, 2116 (1998).

[50] P. D. Townsend, J. G. Rarity, and P. R. Tapster, Electron. Lett. **29**, 634 (1993).

[51] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).

Paper H

Tailored bright illumination attack on distributed-phase-reference protocols

Published in Journal of Modern Optics.

DOI: 10.1080/09500340.2011.565889

arXiv: 1012.4366 [quant-ph]

Paper I

Device calibration impacts security of quantum key distribution

Accepted for publication in Physical Review Letters.

arXiv: 1103.2327 [quant-ph]

Device calibration impacts security of quantum key distribution

Nitin Jain,[1, 2, *] Christoffer Wittmann,[1, 2] Lars Lydersen,[3, 4] Carlos Wiechers,[1, 2, 5]
Dominique Elser,[1, 2] Christoph Marquardt,[1, 2] Vadim Makarov,[3, 4] and Gerd Leuchs[1, 2]

[1] *Max Planck Institute for the Science of Light, Günther-Scharowsky-Str. 1, Bau 24, 91058 Erlangen, Germany*
[2] *Institut für Optik, Information und Photonik, University of*
Erlangen-Nuremberg, Staudtstraße 7/B2, 91058 Erlangen, Germany
[3] *Department of Electronics and Telecommunications,*
Norwegian University of Science and Technology, NO-7491 Trondheim, Norway
[4] *University Graduate Center, NO-2027 Kjeller, Norway*
[5] *Departamento de Física, Campus León, Universidad de Guanajuato,*
Lomas del Bosque 103, Fracc. Lomas del Campestre, 37150, León, Gto, México

(Dated: August 18, 2011)

Characterizing the physical channel and calibrating the cryptosystem hardware are prerequisites for establishing a quantum channel for quantum key distribution (QKD). Moreover, an inappropriately implemented calibration routine can open a fatal security loophole. We propose and experimentally demonstrate a method to induce a large temporal detector efficiency mismatch in a commercial QKD system by deceiving a channel length calibration routine. We then devise an optimal and realistic strategy using faked states to break the security of the cryptosystem. A fix for this loophole is also suggested.

PACS numbers: 03.67.Hk, 03.67.Dd, 03.67.Ac, 42.50.Ex

Quantum key distribution (QKD) offers unconditionally secure communication as eavesdropping disturbs the transmitted quantum states, which in principle leads to the discovery of the eavesdropper Eve [1]. However, practical QKD implementations may suffer from technological and protocol-operational imperfections that Eve could exploit in order to remain concealed [2, 3].

Until now, a variety of eavesdropping strategies have utilized differences between the theoretical model and the practical implementation, arising from (technical) imperfections or deficiencies of the components. Ranging from photon number splitting and Trojan-horse, to leakage of information in a side channel, time-shifting and phase-remapping, several attacks have been proposed and experimentally demonstrated [4–8]. Recently, proof-of-principle attacks [9–11] based on the concept of faked states [12] have been presented. Eve targets imperfections of avalanche photodiode (APD) based single-photon detectors [13] that allow her to control them remotely.

Another important aspect of QKD security not yet investigated, however, is the calibration of the devices. A QKD protocol requires a classical and a quantum channel; while the former must be authenticated, the latter is merely required to preserve certain properties of the quantum signals [2, 14]. The establishment of the quantum channel remains an implicit assumption in security proofs: channel characterization (e.g. channel length) and calibration of the cryptosystem hardware, especially the steps involving two-party communication, haven't yet been taken into account. As we show, the calibration of the QKD devices must be carefully implemented, otherwise it is prone to hacks that may strengthen existing, or create new eavesdropping opportunities for Eve.

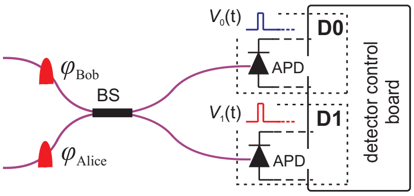


FIG. 1. Typical detection system in a Mach-Zehnder interferometer based QKD implementation: The bit and basis choices of Alice and Bob (phases φ_{Alice} and φ_{Bob}) determine the interference result at the 50:50 beam splitter (BS), or which of the two detectors D0 or D1 would click. It is thus crucial that D0 and D1 are indistinguishable to the outside world (i.e. Eve). If gated mode APDs are employed, the detector control board ensures that the activation of D0 and D1 (via voltage pulses $V_0(t)$ and $V_1(t)$) happens almost simultaneously, to nullify any existing temporal efficiency mismatch.

In this Letter, we propose and experimentally demonstrate the hacking of a vital calibration sequence during the establishment of the quantum channel in the commercial QKD system Clavis2 from ID Quantique [15]. Eve induces a parameter mismatch [16] between the detectors that can break the security of the QKD system. Specifically, she causes a temporal separation of the order of 450 ps of the detection efficiencies by deceiving the detection system, shown in Fig. 1. This allows her to control Bob's detection outcomes using time, a parameter already shown to be instrumental in applying a time-shift attack (TSA) [7]. Alternatively, she could launch a faked-state attack (FSA) [16] for which we calculate the quantum bit error rate (QBER) under realistic conditions. Since FSA is an intercept-resend attack, Eve has full information-theoretic knowledge about the key

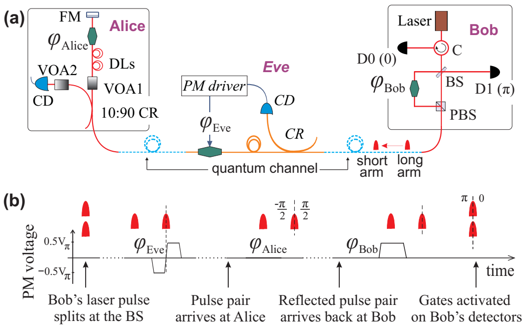


FIG. 2. Manipulation of the calibration routine: **(a)** Simplified version of Alice and Bob devices and Eve (in italic) gearing for the hack. FM: Faraday mirror, CD: classical photodiode, DLs: delay loops, VOA: variable optical attenuator, CR: coupler, BS: 50:50 beam splitter, PBS: polarizing beam splitter, C: optical circulator. The hexagonal-shaped objects are phase modulators (PMs); φ_{X}, where X is Bob, Alice or Eve, represents the applied modulation. **(b)** Timeline for a cycle of the hacked LLM. V_π: PM voltage for a π phase shift.

as long as Alice and Bob accept the QBER at the given channel transmission T, and do not abort key generation [17]. Constricting our FSA to match the raw key rate expected by Bob and Alice, i.e. maintaining T at nearly the exact pre-attack level, we find that the security of the system is fully compromised. Our hack has wide implications: most practical QKD schemes based on gated APDs, in both plug-and-play and one-way configurations [19–21], need to perform channel characterization and hardware calibration regularly. A careful implementation of these steps is required to avoid leaving inadvertent backdoors for Eve.

The optical setup of Clavis2 is based on the plug-and-play QKD scheme [15, 19]. An asymmetric Mach-Zehnder interferometer operates in a double pass over the quantum channel by using a Faraday mirror; see Fig. 2(a) without Eve. The interference of the paths taken by two pulses travelling from Bob to Alice and back is determined by their relative phase modulation ($\varphi_{\text{Bob}} - \varphi_{\text{Alice}}$), and forms the principle for encoding the key. Any birefringence effects of the quantum channel are passively compensated. As a prerequisite to the key exchange, Clavis2 calibrates its detectors in time via a sequence named Line Length Measurement (LLM). Bob emits a pair of *bright* pulses and applies a series of detector gates around an initial estimate of their return. The timing of the gates is electronically scanned (while monitoring detector clicks) to refine the estimation of the channel length and relative delay between the time of arrival of the pulses at D0 and D1. Alice keeps her phase modulator (PM) switched off, while Bob applies a uniform phase of $\pi/2$ to one of the incoming pulses. Therefore, both detectors are equally illuminated and their detection efficiencies, denoted by $\eta_0(t)$ and $\eta_1(t)$, can be resolved in time. Any existing mismatch can thus be minimized by changing the gate-activation times (see Fig. 1).

However, the calibration routine does not always succeed; as reported in [7], a high detector efficiency mismatch (DEM) is sometimes observed after a normal run of LLM. For example, we have noticed a temporal mismatch as high as 400 ps in Clavis2. This physical limitation of the system – arising due to fast and uncontrollable fluctuations in the quantum channel or electromagnetic interference in the detection circuits – is the vulnerability that the TSA exploits. However, the attack has some limitations: it is applicable only when the temporal mismatch happens to exceed a certain threshold value, which is merely 4% of all the instances [7]. Also, Eve can neither control the mismatch (as it occurs probabilistically), nor extract its value (as it is not revealed publicly).

We exploit a weakness of the calibration routine to induce a large and deterministic DEM without needing to extract any information from Bob. As depicted in Fig. 2(a), Eve installs her equipment in the quantum channel such that the laser pulse pair coming out of Bob's short and long arm passes through her PM. Eve's modulation pattern is such that a rising edge in the PM voltage flips the phase in the second (long arm) optical pulse from $-\pi/2$ to $\pi/2$, as shown in Fig. 2(b). As a result of this hack, when the pulse pair interferes at Bob's 50:50 beam splitter, the two temporal halves have a relative phase difference ($\varphi_{\text{Bob}} - \varphi_{\text{Eve}}$) of π and 0, respectively. This implies that photons from the first (second) half of the interfering pulses yield clicks in D1 (D0) deterministically. As the LLM localizes the detection efficiency peak corresponding to the optical power peak, an *artificial* temporal displacement in the detector efficiencies is induced. An inverse displacement can be obtained by simply inverting the polarity of Eve's phase modulation.

In the supplementary section [22], we describe a proof-of-principle experiment to deceive the calibration routine. With this setup, we record the temporal separation Δ_{01}, i.e. the difference between the delays for electronically gating D0 and D1, for several runs of LLM. Relative to the statistics from the normal runs (denoted by $\Delta_{01}^{\text{no Eve}}$), the hacked runs yield an average shift, $\Delta_{01}^{\text{Eve}} - \Delta_{01}^{\text{no Eve}} =$ 459 ps with a standard deviation of 105 ps. Figure 3 shows the detection efficiencies $\eta_0(t)$ and $\eta_1(t)$ (measurement method explained in [22]) for the normal and hacked cases. It also provides a quantitative comparison between the usual and induced mismatch. Note that a larger mismatch can be obtained by modifying the shape of laser pulses coming from Bob.

After inducing this substantial efficiency mismatch, Eve can use an intercept-resend strategy employing 'faked states' [12] to impose her will upon Bob (and Alice). Compared to her intercepted measurements, she prepares the opposite bit value in the opposite basis and sends it with such a timing that the detection of the op-

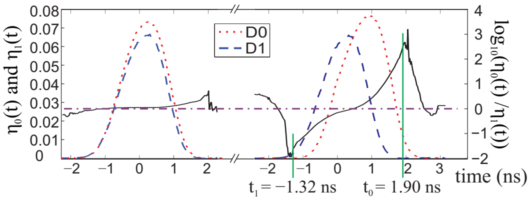


FIG. 3. Induced temporal mismatch: Efficiencies $\eta_0(t)$ (dotted) and $\eta_1(t)$ (dashed) from normal LLMs, on the left, and after Eve's hack that induced a separation of 459 ps, on the right. The logarithm of their ratio, quantifying the degree of mismatch (solid line), is at least an order of magnitude higher in the flanks after Eve's hack: the dash-dot line indicates zero mismatch. To eavesdrop successfully, Eve times the arrival of "appropriately bright" faked states at $t = t_0$ or t_1 in Bob.

→Eve	Eve→	Bob's result	Detection probability
$Z, 0$	$X, 1, \mu_0, t_0$	0	$\mathbf{q}_0 = d_0 + (1 - d_0) \times$ $(1 - \exp(-\mu_0 \eta_0(t_0)/2))$
		1	$\mathbf{q}_1 = d_1 + (1 - d_1) \times$ $(1 - \exp(-\mu_0 \eta_1(t_0)/2))$
		$0 \cap 1$	$\mathbf{q}_0 \mathbf{q}_1$
		loss	$1 - (\mathbf{q}_0 + \mathbf{q}_1 - \mathbf{q}_0 \mathbf{q}_1)$
$X, 0$	$Z, 1, \mu_0, t_0$	0	$\mathbf{r}_0 = d_0$
		1	$\mathbf{r}_1 = d_1 + (1 - d_1) \times$ $(1 - \exp(-\mu_0 \eta_1(t_0)))$
		$0 \cap 1$	$\mathbf{r}_0 \mathbf{r}_1$
		loss	$1 - (\mathbf{r}_0 + \mathbf{r}_1 - \mathbf{r}_0 \mathbf{r}_1)$
$X, 1$	$Z, 0, \mu_1, t_1$	0	$\mathbf{s}_0 = d_0 + (1 - d_0) \times$ $(1 - \exp(-\mu_1 \eta_0(t_1)))$
		1	$\mathbf{s}_1 = d_1$
		$0 \cap 1$	$\mathbf{s}_0 \mathbf{s}_1$
		loss	$1 - (\mathbf{s}_0 + \mathbf{s}_1 - \mathbf{s}_0 \mathbf{s}_1)$

TABLE I. Faked-state attack, given that Alice prepared bit 0 in the Z basis and that Bob measured in the Z basis (only matching basis at Alice and Bob remains after sifting). The first column contains the basis chosen by Eve and her measurement result. The second column shows parameters of the faked state resent by Eve: basis, bit, mean photon number, timing. The third column shows Bob's measurement result; $0 \cap 1$ denotes a double click. The last column shows the corresponding click probabilities (ignoring possible superlinearity effect in gated detectors [18]). Note: The first result ($\rightarrow$ Eve $\equiv Z, 0$) is twice as likely to occur as the other two.

posite bit value is suppressed due to negligible detection efficiency. As an example, assume that Eve measures bit 0 in the Z basis [in a phase-coded scheme, measuring in Z (X) basis $\Leftrightarrow$ applying $\varphi = 0$ $(\pi/2)$]. Then, she resends bit 1 in the X basis, timed to be detected at $t = t_0$ (see Fig. 3), where D1 is almost blind. Using the numerical data on the induced mismatch, Eq. 3 from [16] yields a QBER $< 0.5\%$ if the FSA is launched at times t_0 and t_1 where the efficiency mismatch is high.

However, it can be observed that the detection probabilities for D0 and D1 are quite low in this case. A considerable decrease in the rate of detection events in Bob could ensue an alarm. Also, the (relatively increased) dark counts would add significantly to the QBER. In fact, Eve needs to *match* the channel transmission T that Alice and Bob expect, without exceeding the QBER threshold at which they abort key generation [17]. Experimentally, we find that the abort threshold depends on the channel loss seen by Clavis2; for an optical loss of 1–6 dB (corresponding to $0.79 > T > 0.25$), it lies between 5.94–8.26%.

Eve solves these problems by increasing the mean photon number of her faked states. To evaluate her QBER, we elaborate the approach of [16] by generalizing table I from this reference. Our attack strategy, carefully accounting for all the involved factors, is summarized in Table I. For instance, in the first row we replace the probability of detection $\eta_0(t_0)/2$ by $1 - \exp(-\mu_0 \eta_0(t_0)/2)$ for a coherent-state pulse of mean photon number μ_0 impinging on Bob's detectors at time t_0. Including the effect of the dark counts into this expression, Bob's probability to register 0 becomes $\mathbf{q}_0 = d_0 + (1 - d_0)(1 - \exp(-\mu_0 \eta_0(t_0)/2))$, where d_0 is the dark count probability in detector D0. A row for double clicks, i.e. simultaneous detection events in D0 and D1, is added for every (re-sent) state.

Due to the FSA, the D0/1 click probability at time t no longer depends solely upon $\eta_{0/1}(t)$. Summing over all the states sent by Alice (by extending Table I), the total detection probabilities in D0 and D1 when the attack is launched at specific times t_0 and t_1 are

$$\begin{aligned} p_0(\mu_0, \mu_1) &= 0.75 + 0.25d - 0.25(1 - d) \times \\ &\quad \left(e^{-0.5\mu_0 \eta_{00}} + e^{-0.5\mu_1 \eta_{01}} + e^{-\mu_1 \eta_{01}}\right), \qquad (1) \\ p_1(\mu_0, \mu_1) &= 0.75 + 0.25d - 0.25(1 - d) \times \\ &\quad \left(e^{-0.5\mu_0 \eta_{10}} + e^{-0.5\mu_1 \eta_{11}} + e^{-\mu_0 \eta_{10}}\right). \qquad (2) \end{aligned}$$

Here $\eta_{jk} = \eta_j(t_k)$ with $j, k \in \{0, 1\}$ and $d = \text{mean}(d_0, d_1)$ are used to simplify the expressions. Similarly, one can compute the expression for $p_{0\cap 1}$, the total double-click probability. Eve's error probability, the arrival probability of the optical signals in Bob, and the QBER are

$$\begin{aligned} p_{\text{error}}(\mu_0, \mu_1) &= 0.75 + 0.25d - 0.5p_{0\cap 1} - 0.125 \times \qquad (3) \\ &(1 - d)\left(e^{-\mu_0 \eta_{10}} + 2e^{-0.5\mu_0 \eta_{10}} + e^{-\mu_1 \eta_{01}} + 2e^{-0.5\mu_1 \eta_{01}}\right), \\ p_{\text{arrive}}(\mu_0, \mu_1) &= p_0 + p_1 - p_{0\cap 1}, \qquad (4) \\ \text{QBER}(\mu_0, \mu_1) &= p_{\text{error}}(\mu_0, \mu_1)/p_{\text{arrive}}(\mu_0, \mu_1). \qquad (5) \end{aligned}$$

Here double clicks are assumed to be assigned a random bit value by Bob [25], causing an error in half the cases.

If Alice and Bob are connected back-to-back (channel transmission $T \approx 1$), the click probabilities in Bob should be slightly less than half of the peak values in Fig. 3. This is owing to optical losses ($\gtrsim 3$ dB) in Bob's apparatus.

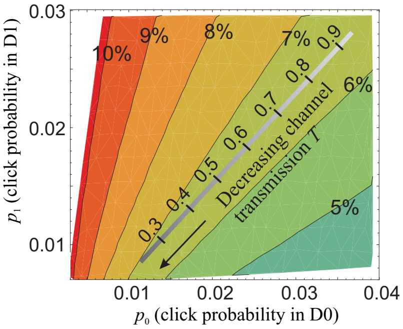


FIG. 4. Minimum QBER versus click probabilities in D0 and D1: Eve minimizes the error with a suitable choice of the mean photon number of the faked states (for this plot, $1 < \mu_0 < 100$ and $21 < \mu_1 < 120$ at Bob's detectors). The thick shaded line indicates Bob's detection probabilities. The QBER introduced by Eve stays below 7% for $T \gtrsim 0.25$.

Eve's constraints can now be formalized as: starting in the vicinity of $p_0 = 0.038$ and $p_1 = 0.032$, not only does she have to match Bob's expected detection rate for any given $T < 1$, but also keep the resultant QBER below the threshold at which Clavis2 aborts the key exchange. We assume Eve detects photons at Alice's exit using a perfect apparatus, and resends perfectly aligned faked states.

Substituting $t_1 = -1.32$ ns, $t_0 = 1.90$ ns (marked in Fig. 3) and $d = 2.4 \times 10^{-4}$ in Eqns. 1–5, Eve collects tuples [p_0, p_1, QBER] by varying μ_0 and μ_1 in a suitable range. Out of all tuples that feature the same detection probabilities (arising from different combinations of μ_0 and μ_1), Eve chooses the one having the lowest QBER. A contour plot in Fig. 4 displays this minimized error $\min_{\mu_0,\mu_1} \mathrm{QBER}\left((\mu_0, \mu_1)| (p_0, p_1)\right)$. The thick shaded line shows that for $T > 0.25$, Eve not only maintains the detection rates within 5% of Bob's expected values, but also keeps the QBER below 7% [**?**]; thus breaking the security of the system. Note that the simulation assumes a lossless Eve, but in principle she can cover loss from her realistic detection apparatus by increasing μ_0 and μ_1 further and/or including t_0 and t_1 in the minimization.

To counter this hack, Bob should randomly apply a phase of 0 or π (instead of $\pi/2$ uniformly) while performing LLM. This modification is implementable in software and has already been proposed to ID Quantique. More generally, a method to shield QKD systems from attacks that exploit DEM is described in Ref. [23].

In conclusion, we report a proof-of-principle experiment to induce a large detector efficiency mismatch in a commercial QKD system by deceiving a vital calibration routine. An optimized faked-state attack on such a compromised system would not alarm Alice and Bob as it would introduce a QBER $< 7\%$ for a large range of expected channel transmissions. Thus, the overall security of the system is broken. With initiatives for standardizing QKD [24] underway, we believe this report is timely and shall facilitate elevating the security of practical QKD systems.

Acknowledgments: We thank M. Legré from ID Quantique and N. Lütkenhaus for helpful discussions; Q. Liu, L. Meier and A. Käppel for technical assistance. This work was supported by the Research Council of Norway (grant no. 180439/V30), DAADppp mobility program financed by NFR (project no. 199854) and DAAD (project no. 50727598), and BMBF CHIST-ERA (project HIPERCOM). Ca. Wi. acknowledges support from FONCICYT project no. 94142.

* nitin.jain@mpl.mpg.de

[1] C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (IEEE, New York, 1984), pp. 175–179; P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000) and references therein.
[2] V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).
[3] V. Scarani and C. Kurtsiefer, arXiv:0906.4547.
[4] B. Huttner *et al.*, Phys. Rev. A **51**, 1863 (1995); N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).
[5] N. Gisin *et al.*, Phys. Rev. A **73**, 022320 (2006); A. Vakhitov *et al.*, J. Mod. Opt. **48**, 2023 (2001).
[6] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007); S. Nauerth *et al.*, New J. Phys. **11**, 065001 (2009).
[7] Y. Zhao *et al.*, Phys. Rev. A **78**, 042333 (2008).
[8] C.-H. F. Fung *et al.*, Phys. Rev. A **75**, 032314 (2007); F. Xu *et al.*, New J. Phys. **12**, 113026 (2010).
[9] L. Lydersen *et al.*, Nat. Photonics **4**, 686 (2010).
[10] L. Lydersen *et al.*, Opt. Express **18**, 27938 (2010); C. Wiechers *et al.*, New J. Phys. **13**, 013043 (2011).
[11] I. Gerhardt *et al.*, Nat. Comm. **2**, 349 (2011).
[12] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).
[13] V. Makarov, New J. Phys. **11**, 065003 (2009).
[14] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002).
[15] Datasheet of Clavis2, available at ID Quantique website `http://www.idquantique.com`.
[16] V. Makarov *et al.*, Phys. Rev. A **74**, 022313 (2006).
[17] D. Gottesman *et al.*, Quant. Inf. Comput. **4**, 325 (2004); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[18] L. Lydersen *et al.*, arXiv:1106.2119.
[19] D. Stucki *et al.*, New J. Phys. **4**, 41 (2002).
[20] D. S. Bethune and W. P. Risk, IEEE J. Quantum Electron. **36**, 340 (2000); M. Bourennane *et al.*, Opt. Express **4**, 383 (1999).
[21] Z. Yuan and A. Shields, Opt. Express **13**, 660 (2005).
[22] See Page 5 for experimental details.
[23] L. Lydersen *et al.*, Phys. Rev. A **83**, 032306 (2011).
[24] ETSI GS QKD 005 V1.1.1: "Quantum key distribution (QKD); Security proofs" (ETSI, 2010); T. Länger and G. Lenhart, New J. Phys. **11**, 055051 (2009).
[25] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).

Device calibration impacts security of quantum key distribution: Technical appendix

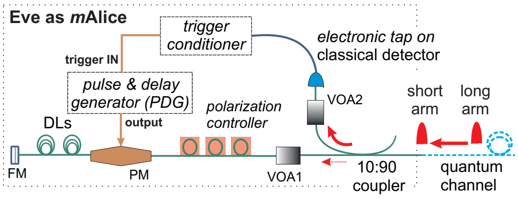


FIG. 5. Eve's implementation (mAlice) by modifying Alice's module: The onboard pulser driving the phase modulator (PM) is disconnected, and the PM itself is positioned *before* the 23.5 km delay loops (DLs). The trigger conditioner circuit allows (prevents) the pulse & delay generator to be triggered by the short arm (long arm) optical pulses. Newly added components to the original Alice module are labeled in italic. VOA: variable optical attenuator, FM: Faraday mirror.

Implementation of the hack: Here, we explain our experimental implementation of the scheme outlined in the Letter for deceiving Line Length Measurement (LLM), the calibration routine of the Clavis2 QKD system [15]. For this purpose, we rig the module of Alice as shown in Fig. 5. From now on, we call this manipulated device mAlice. An electronic tap placed on the classical detector (normally used by Alice for measuring the incoming optical power [5]) is conditioned appropriately with a homemade circuit. The output of this circuit provides the trigger for the pulse & delay generator (PDG, Highland Technology P400), which essentially drives the phase modulator (PM) in mAlice.

For experimental convenience, we also change the settings in the Clavis2 firmware (Bob's EEPROM specifically) such that during the execution of LLM, $\varphi_{\text{Bob}} = 0$ is applied instead of the usual $\pi/2$. This relaxes the requirement on Eve's modulation pattern: in comparison to the waveform in Fig. 2(b) in the Letter, the PDG needs to switch simply from 0 to V_π through the center of the optical pulse. This is in principle equivalent to the scheme in Fig. 2(b) in the Letter, while easier to implement. In other words, it does not affect a full implementation of Eve. Normally, Alice applies the phase modulation in a double pass by making use of the Faraday mirror. However, the PM in mAlice is shifted closer to Alice's entrance (i.e. before the delay loops) to enable a precise synchronization of the PDG. To ensure that the photons passing through the PM (in a single pass now) pick up the requisite 'π' modulation, a polarization controller is deployed before the PM.

Finally, the synchronization of the rising edge of Eve's modulation to the center of the optical pulse is performed by scanning the delay in the PDG (in steps of 5 ps) while monitoring the interference visibility [15]. As Eve's modulation flips the phase of the optical pulse through the center, the visibility reduces to zero. The corresponding delay setting of the PDG can then be used to induce the temporal efficiency mismatch between Bob's detectors D0 and D1, during the execution of LLM.

We emphasize that the mAlice module serves as a proof-of-principle implementation *only* for inducing the detector efficiency mismatch during the LLM. It should not be confused with Eve's intercept or resend modules, needed in the subsequent faked-state attack. Finally, note that Eve is free to modify Bob's pulses or replace them by her suitably-prepared pulses, and thus effectively control the amount of detection efficiency mismatch that can be induced.

Measurement of efficiency curves: Detection efficiencies $\eta_0(t)$ and $\eta_1(t)$ are estimated at single-photon level by scanning the detector gates in steps of 20 ps with an external laser (optical pulse-width $\sim$ 200 ps). We average the click probability per gate and subtract $d_{0/1}$ (the dark count rate in D0/1) from it. This gives a more accurate estimate of the efficiencies, especially in the flanks (see Fig. 3 in the Letter).

Paper J

Superlinear threshold detectors in quantum cryptography

Accepted for publication in Physical Review A.

arXiv: 1106.2119 [quant-ph]

Superlinear threshold detectors in quantum cryptography

Lars Lydersen,[1, 2, *] Nitin Jain,[3, 4] Christoffer Wittmann,[3, 4] Øystein Marøy,[1, 2]
Johannes Skaar,[1, 2] Christoph Marquardt,[3, 4] Vadim Makarov,[1, 2] and Gerd Leuchs[3, 4]

[1] *Department of Electronics and Telecommunications,*
Norwegian University of Science and Technology, NO-7491 Trondheim, Norway
[2] *University Graduate Center, NO-2027 Kjeller, Norway*
[3] *Max Planck Institute for the Science of Light, Günther-Scharowsky-Str. 1/Bau 24, 91058 Erlangen, Germany*
[4] *Institut für Optik, Information und Photonik, University of*
Erlangen-Nuremberg, Staudtstraße 7/B2, 91058 Erlangen, Germany

(Dated: August 18, 2011)

We introduce the concept of a superlinear threshold detector, a detector that has a higher probability to detect multiple photons if it receives them simultaneously rather than at separate times. Highly superlinear threshold detectors in quantum key distribution systems allow eavesdropping the full secret key without being revealed. Here, we generalize the detector control attack, and analyze how it performs against quantum key distribution systems with moderately superlinear detectors. We quantify the superlinearity in superconducting single-photon detectors based on earlier published data, and gated avalanche photodiode detectors based on our own measurements. The analysis shows that quantum key distribution systems using detector(s) of either type can be vulnerable to eavesdropping. The avalanche photodiode detector becomes superlinear towards the end of the gate. For systems expecting substantial loss, or for systems not monitoring loss, this would allow eavesdropping using trigger pulses containing less than 120 photons per pulse. Such an attack would be virtually impossible to catch with an optical power meter at the receiver entrance.

I. INTRODUCTION

Single photon detectors [1] can be regarded as essential parts of quantum information processing hardware, and are certainly crucial components in quantum key distribution (QKD) systems [2–7]. In QKD, the communicating parties Alice and Bob exploit the properties of quantum mechanics to reveal any eavesdropping attempt by the eavesdropper Eve. The security of QKD has been proven for perfect devices [4, 5]. However, when the security of QKD is to be proven for practical systems [8–16], it is necessary to construct models based on assumptions about the practical devices, and hence also about the single photon detectors.

With a few exceptions [17, 18], most single photon detectors suitable for QKD systems are threshold detectors that cannot resolve the number of photons in a pulse. They rather have a binary response distinguishing between zero, and 'one or more' photons, where a detection event is often referred to as a "click". Threshold detectors are usually characterized by their quantum efficiency η, which is the probability to detect a single photon. For multiphoton pulses, a very common assumption is that each photon within the pulse is detected individually with probability η. Then, the detection probability of a n-photon Fock state can be expressed as

$$p_{\mathrm{det}}(n) = 1 - (1-\eta)^n. \qquad (1)$$

We refer to threshold detectors with a multiphoton detection probability higher than the one given by Eq. (1) as *superlinear* threshold detectors. A superlinear threshold detector has a larger probability to detect multiple photons if it receives them nearly simultaneously, than if it receives each of the photons separately at different times. This effect is well known in multiphoton absorption by atoms [19], where the multiphoton absorption rate can be much higher for chaotic light than for laser light with the same mean intensity. Meanwhile for threshold detectors, superlinear response may also originate from how the entire device converts individual excitations into the macroscopic detection event.

The photon number of a coherent state follows a Poisson distribution with probability $p_n = \mu^n e^{-\mu}/n!$, where μ is the mean photon number. Therefore, if the detection probability of a n-photon Fock state is given by Eq. (1), a coherent state with mean photon number μ is detected with probability

$$p_{\mathrm{det}} = \sum_{n=0}^{\infty} \frac{\mu^n e^{-\mu}}{n!} p_{\mathrm{det}}(n) = 1 - e^{-\mu\eta}. \qquad (2)$$

Note that for a coherent state with mean photon number μ, a superlinear threshold detector with quantum efficiency η will have a higher detection probability than the one given by Eq. (2).

Insufficient models of single photon detectors have caused numerous security loopholes [15, 20–30] in QKD. For instance, the time-shift attack [21] based on detector efficiency mismatch [20] has been shown to break the security of a commercial QKD system [24]. More recently, the detector control attack [25–30] allows the eavesdropper to capture the full key without revealing her presence (via errors in the key). Specifically, the attack introduces zero quantum bit error rate (QBER). Furthermore,

[*] lars.lydersen@iet.ntnu.no

this attack which is based on bright illumination is implementable with current technology. Two commercial QKD systems were shown to be vulnerable to the attack [25–27], and a full eavesdropper has been implemented to capture the full key of an experimental QKD system under realistic conditions [29]. However, the power level (more than 500 µW) of the eavesdropper's illumination has led to discussions whether an optical power meter at the entrance of Bob can be used to detect these attacks [31–34].

In this paper we propose and analyze an attack against QKD systems with superlinear detectors (Sec. II). Note that the previously published detector control attack [25] is based on an extreme superlinear behavior of the detectors, and can therefore be considered a special case of the "imperfect" detector control attack presented here. Then we discuss how the attack would perform against superconducting single photon detectors [35, 36], which have been reported to exhibit superlinear behavior (Section III). In Sec. IV we show that APD-based gated detectors have a substantial superlinear response at the end of the gate. The superlinear behavior at the end of the gate allows eavesdropping with very faint trigger pulses [25, 32]. This *faint after-gate attack* will be virtually impossible to catch with an optical power meter at the entrance of Bob. At least one security proof covers QKD systems with superlinear detectors [16]. In Sec. V we show how the detector control attack relates to the security proof, and discuss possible countermeasures. Finally, we conclude in Sec. VI.

II. THEORY OF SUPERLINEAR DETECTOR CONTROL

The core of the previously proposed detector control attacks is the following [25]: in the Bennett-Brassard 1984 (BB84) [2] family of protocols, Eve uses a random basis to measure the quantum state from Alice. Then she resends her measurement result, not as a single photon, but rather as a bright pulse, called a trigger pulse, with a carefully selected optical power. Then, if Eve uses Bob's measurement basis, her trigger pulse is *always* detected by Bob. On the contrary, if Eve uses a basis not matching Bob's to measure the quantum state from Alice, her trigger pulse is *never* detected. This is possible because Bob's detectors are very superlinear: for less than a factor of two (3 dB) increase in trigger pulse power, the detection probability shoots from 0 to 100%. Since Eve uses the correct basis only half of the time, the total loss between Alice and Bob is 3 dB. For the differential-phase-shift protocol [37, 38] there is no basis choice, so the same factor of two (3 dB) superlinearity allows eavesdropping without extra loss [30]. The coherent one-way protocol [39, 40] is also vulnerable to the detector control attacks [30], but requires a more strict relationship between the superlinearities of the detectors in the system.

The previously proposed detector control attacks allow Eve to capture the full secret key without introducing any QBER. However, Alice and Bob usually tolerate a non-zero QBER (typically less than 11%). Therefore, Eve might introduce a small QBER without getting caught. What if the superlinearity of the detector is such that when Eve selects the right basis, the trigger pulse is detected with a *high* probability, while when Eve selects the wrong basis, the trigger pulse is detected with a *low* probability? One can immediately identify two consequences of this "imperfect" detector control attack: the non-unity detection probability when Eve uses the right basis will contribute extra to the loss. On the other hand, the non-zero detection probability when Eve uses the wrong basis will introduce a non-zero QBER.

We will here consider an active basis choice BB84 implementation using two detectors. In a passive basis choice BB84 implementation [41], Eve's trigger pulse will strike the detectors in both bases simultaneously for each bit. For this case, the QBER introduced by the attack depends on how Bob handles simultaneous clicks in both bases. Assume that Bob assigns a random bit value to these events. Then, if the probability for simultaneous clicks in both bases is non-zero, the QBER introduced by a "imperfect" detector control attack will be higher in a passive basis choice implementation than in an active basis choice implementation. In any case, for passive basis choice implementations, the theoretical QBER derived below can be used as a lower bound.

To calculate the QBER caused by this attack, let $p_{\mathrm{f},i}$ be the detection probability in detector i for the trigger pulse with full power. Likewise, let $p_{\mathrm{h},i}$ be the detection probability at detector i with half the power. We assume Eve resends the same power regardless of her detected bit value, that double clicks are assigned to a random bit value [42], and that Eve selects Bob's measurement basis with probability 1/2. When Eve resends in the wrong basis and Bob has a detection, the bit value will be erroneous with probability 1/2. Therefore, the QBER caused by the "imperfect" detector control attack is given by

$$\begin{aligned}\mathrm{QBER} &= \frac{1}{2}\frac{\text{Bob detects and Eve used wrong basis}}{\text{Bob has a detection}}\\ &= \frac{p_{\mathrm{h},0}+p_{\mathrm{h},1}-p_{\mathrm{h},0}p_{\mathrm{h},1}}{p_{\mathrm{f},0}+p_{\mathrm{f},1}+2(p_{\mathrm{h},0}+p_{\mathrm{h},1}-p_{\mathrm{h},0}p_{\mathrm{h},1})},\end{aligned} \tag{3}$$

where dark counts have been omitted. Errors originating from dark counts would add to the errors caused by the attack. However, in a good detector design the amount of errors from dark counts is minimized. Since we require the eavesdropper to reproduce the detection probability from normal operating conditions, the dark count probability would be minimized under attack as well. A high dark count probability, and thus a high error rate without the eavesdropper would leave the attack less room for errors to be introduced. However, an equivalent restriction on the attack is easier obtained by lowering the acceptance threshold for the QBER. Therefore, our analyses is limited to the QBER introduced by the attack, and dark counts are omitted. Assuming that both detectors have equal detection probabilities, $p_{\mathrm{f},i} = p_\mathrm{f}$ and $p_{\mathrm{h},i} = p_\mathrm{h}$, Eq. (3) simplifies to

$$\mathrm{QBER} = \frac{2p_\mathrm{h} - p_\mathrm{h}^2}{2p_\mathrm{f} + 2(2p_\mathrm{h} - p_\mathrm{h}^2)}. \tag{4}$$

As discussed above, the perfect detector control attack introduces 3 dB loss when applied against BB84 QKD systems with active basis choice in Bob's implementation, because Eve only selects the correct basis half of the time. If $\min_i p_{\mathrm{f},i} < 1$, the attack will cause an even higher loss. On the other hand, $\max_i p_{\mathrm{h},i} > 0$ will reduce the loss introduced by the attack. Therefore, the transmittance T when an "imperfect" detector control attack is applied against a BB84 QKD system with active basis choice is given by

$$T = \frac{1}{4}\left(p_{\mathrm{f},0} + p_{\mathrm{f},1}\right) + \frac{1}{2}\left(p_{\mathrm{h},0} + p_{\mathrm{h},1} - p_{\mathrm{h},0}p_{\mathrm{h},1}\right). \tag{5}$$

Note that T refers to the transmittance between Eve and Bob. If Eve uses imperfect detectors, this will add to the total loss observed by Alice and Bob. For the remainder of the paper, we simply consider Eve to use perfect detectors. Since Eve can place her detectors close to Alice, and she can use detectors with almost unity detection efficiency [18], this is an acceptable assumption. If both detectors have equal probabilities, Eq. (5) simplifies to

$$T = \frac{1}{2}p_\mathrm{f} + \frac{1}{2}\left(2p_\mathrm{h} - p_\mathrm{h}^2\right). \tag{6}$$

Note that in passive implementations of Bob, such as passive basis choice in BB84 [41], or in distributed phase reference protocols [37–40], there is no 3 dB loss due to basis choice. Therefore, the above expression for the transmittance T can be considered a lower bound also for such implementations.

In most cases, the eavesdropper can introduce substantial loss without getting noticed. With the notable exception of transition-edge sensors [18], the quantum efficiency of Bob's detectors is typically about 10% at telecom wavelengths [1]. Furthermore, an optical fiber usually exhibits a loss of about 0.2 dB/km at 1550 nm wavelength. Adding the loss owing to detector's quantum efficiency to the loss in the line at a typical distance of 50 km, Alice and Bob normally observe a total loss of 20 dB, corresponding to $T \sim 0.01$. In addition to this, there is loss in the optical path inside Bob's apparatus. However, Eve can always adjust the power in her trigger pulses to strike Bob's detectors with a given optical power. Therefore, by inserting her eavesdropping station into the line close to Alice's system, Eve has almost the full 20 dB at her disposal. In one case, a QKD system operating with loss up to 40 dB has been reported [43] (but the actual, tolerable loss might be less because there is no satisfactory security proof for the protocol used in Ref. [43]). Therefore, it seems that for many QKD setups, Eve can introduce loss of more than 20 dB without being revealed from the reduction in the transmittance.

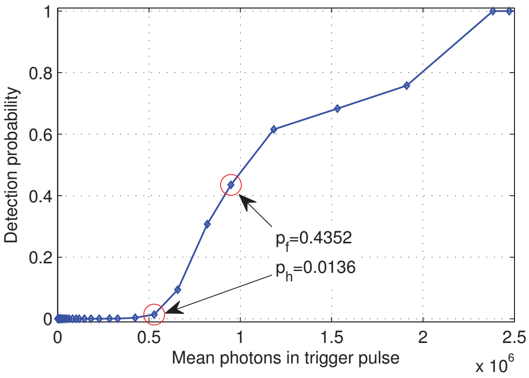


FIG. 1. (Color online) The detection probability versus mean photon number in the trigger pulse for the SSPD in Ref. [36], at 1550 nm and $I_b = 0.8I_c$. Count rates were extracted from Fig. 1 in Ref. [36], and divided by the pulse repetition frequency of 82 MHz to obtain the detection probability. The red circled data points were used to calculate the QBER and the transmittance from an attack.

III. SUPERLINEARITY OF SUPERCONDUCTING SINGLE PHOTON DETECTORS

Superconducting single photon detectors (SSPDs) based on superconducting nanowires [35] have been used for long-distance QKD experiments [43–47], due to their ultra low dark count rate and timing jitter. However, the need for cryogenic cooling to temperatures in the 2–4 K range has prevented them from being used in commercial QKD systems.

In SSPDs, the nanowire is cooled to the superconducting state. Then, then the nanowire is biased with a current I_b slightly lower than the critical current I_c. Because the wire is superconducting at I_b, there is no voltage drop over the device. A photon incident on the nanowire can create a normally-conducting hotspot, with the effect that the whole cross-section of the nanowire becomes normally conducting. This increases the voltage over the device. Afterwards, the cooling restores superconductivity in the nanowire, and the current increases back to the bias current. This dead time is usually about 10 ns. The biasing current I_b can be adjusted for a trade-off between high detection efficiency and low dark count rate.

Already in the first systematic investigation of the detection efficiency of SSPDs [36], superlinear behavior due to multiphoton absorption mechanisms was reported. The superlinear behavior is wavelength dependent, and is substantial at 1550 nm, which is the wavelength suitable for long-distance experiments. Figure 1 shows the detection count data for 1550 nm extracted from Fig. 1 in Ref. [36], processed as detection probability (count rate/trigger pulse rate), and plotted on a linear scale. The SSPD was biased at $I_b/I_c = 0.8$. The superlinear behavior is suitable for eavesdropping in QKD: by increasing the photon number, the detection probability increases sharply. Using trigger pulses containing 10^6 photons per pulse, Eq. (4) predicts a QBER of less than 3%, and Eq. (6) predicts a transmittance $T > 0.20$ (assuming reasonable errors in extracting the numerical data from the plot in Ref. [36]). Therefore, a QKD system using this SSPD would clearly be vulnerable to a detector control attack.

Judging by the low detection probability at one photon per pulse for this SSPD, the QKD experiments would use a higher bias current to get better sensitivity. Unfortunately, few publications seems to report the detection probabilities for pulses above the single photon level, especially for 1550 nm wavelength. The available literature shows that SSPDs are less superlinear at shorter wavelengths [36], and also less superlinear at higher bias currents [48]. However, note that any superlinear detector response must be handled in the security proof. Therefore, the reported data on SSPDs [36, 48] clearly shows that such a security proof is necessary for QKD systems using SSPDs.

IV. SUPERLINEARITY OF GATED APD-BASED DETECTORS

The gated APD-based detectors in the QKD system Clavis2 by ID Quantique exhibit substantial superlinear behavior far after the gate [27], or when blinded by bright illumination [25, 26]. However, as pointed out before [25, 31], the bright trigger pulses might be revealed by an optical power meter at the entrance of Bob. Here, we show that at the end of the gate, when the APD is biased close to the breakdown voltage, the superlinear response allows Eve to use very faint trigger pulses.

The detection probability during the gate was measured as follows: The gated InGaAs detectors in the QKD system Clavis2 were run with factory settings, but with the gating frequency reduced from 5 MHz to 98 kHz. The reduced frequency corresponds to the factory frequency with a detection in every gate, and afterpulse blocking (forced 10 µs deadtime after detection events to reduce dark counts) enabled. A short-pulsed laser (see Appendix A for the pulse shape) was attenuated to the appropriate mean photon number, and connected directly to the fiber pigtail of each detector. Then, the laser pulse was scanned through the gate in steps of 25 ps, and the detection probability was recorded in each step. The "quantum efficiency" η was measured by applying a coherent state $\mu = 1$, and solving η from Eq. (2). In fact, the detector is slightly superlinear, but a coherent state with $\mu = 1$ [49] contains only a small fraction of multiphoton pulses.

Once the quantum efficiency η is known, Eq. (2) can be used to calculate the expected detection probability for a coherent state with any mean photon number, assuming that each photon is detected individually. Figure 2 shows the detection probability of a coherent state for various mean photon numbers predicted by Eq. (2), compared to the actual detection probabilities measured in our experiment.

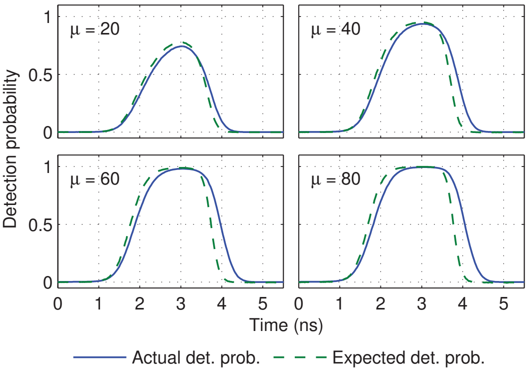


FIG. 2. (Color online) The measured detection probability for a coherent state with $\mu = 20$, 40, 60 and 80, compared to the expected detection probabilities predicted by Eq. (2). Data points are 25 ps apart. Data for detector 0 is shown; detector 1 behaved very similarly. When the mean photon number μ is increased, deviation between the expected detection probabilities and the actual measured detection probabilities increases, especially at the end of the gate. See also Fig. 3.

The measurement data matches the expected detector response fairly well until the falling edge of the gate. There, the measured detection probability becomes superlinear. One possible explanation for this could be the following: an avalanche, started by a photon in a localized spot, laterally spreads over time to encompass the entire junction area of the APD [50]. For detection events before the falling edge of the gate, the avalanche has sufficient time to spread and therefore the current reaches the same amplitude regardless of the number of photons absorbed in the APD [17]. At the end of the gate, an avalanche from a single photon absorption does not have sufficient time to spread to the entire junction area, and therefore only causes a small current insufficient of crossing the comparator threshold. However, multiple photon absorptions in different spots across the junction can start multiple small avalanches that together provide enough current to cross the comparator threshold. This is exactly the process exploited to make photon number resolving APD-based detectors [17]. Avalanche spreading assisted by secondary photons re-emitted by the APD, has already been used to explain avalanche development [50, 51]. Similarly, multiple photon absorptions caused by the multiphoton pulse could speed up the avalanche development.

For the gated APD-based detectors, the superlinear response can be exploited in a faint version of the after-gate attack [27]. From Eve's perspective, the original after-gate attack has some drawbacks. The attack may

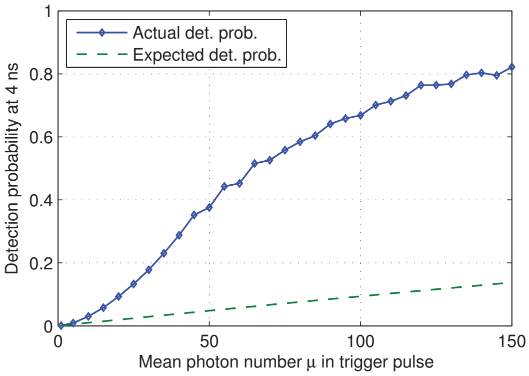


FIG. 3. (Color online) Detection probability at the falling edge of the gate (at the 4 ns point in Fig. 2). For $\mu < 40$, the shape of the actual detection probability is clearly superlinear, in contrast to the nearly linear expected detection probability.

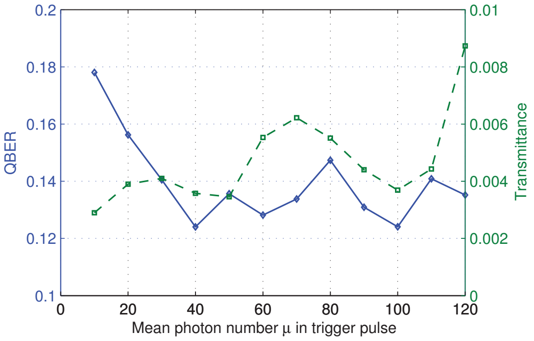


FIG. 4. (Color online) The minimum QBER (solid curve) caused by trigger pulses with various mean photon number calculated from Eq. (4) and the corresponding transmittance (dashed curve) calculated from Eq. (6). The data contains some noise due to fluctuations in applied power and/or fluctuations in the detection efficiency.

cause a substantial amount of errors in the key, because the bright pulses cause afterpulses with a random bit value. Furthermore, in principle, an optical power meter can be used to catch Eve's bright pulses. Also, removing gates randomly or as a part of afterpulse blocking (to avoid excessive dark counts) would reveal the attack because the trigger pulses would cause clicks regardless of the presence of a gate. Then, detection events without a gate applied would indicate the presence of the eavesdropper. Similarly, it has been noted that in the original after-gate attack could be countered by ignoring detection events outside the gate [33], while for this faint after-gate attack, the detections happen within the gate [34].

As discussed in Sec. II, having a "high" detection probability for a given trigger pulse power, and a "low" detection probability for a 3 dB dimmer trigger pulse is suitable for Eve's attack. Figure 3 shows the measured and expected detection probability at a single point at the falling edge of the gate. For less than 40 photons per trigger pulse, the APDs clearly exhibit superlinear response in favor of the eavesdropper.

The detection probability curve of the detector 0 (the results are very similar for detector 1) was used when calculating QBER and transmittance from Eqs. (4) and (6). Figure 4 shows the resulting QBER and the corresponding transmittance for various mean photon numbers in the trigger pulse, when the trigger pulse timing was optimized to minimize the QBER. The data indicates that a faint after-gate attack could cause a QBER around 13% with a transmittance of about 0.005, corresponding to 23 dB loss (for instance, for $\mu = 40$, $p_f = 0.0054$ and $p_h = 0.00089$ at the point 4.525 ns in Fig. 2). As discussed in Sec. II, this transmittance corresponds to Bob's detectors having 10% quantum efficiency, a line loss corresponding to about 50 km of fiber and another 3 dB loss in Bob's apparatus, which are reasonable values.

While most QKD systems do not accept QBER above 11% [5], there are post-processing protocols which accept QBER up to 20% [52]. Also note that the QBER introduced by the attack may be significantly lower with yet shorter trigger pulses, since they would better resolve the superlinear behavior at the falling edge of the gate. A relatively wide pulse we're using (Appendix A) arrives at both linear and superlinear regions of the gate. Therefore the superlinear response to it must be less than that to a narrower pulse arriving only at the most superlinear point in the gate.

The detectors in Clavis2 have been shown to exhibit detection efficiency mismatch [20, 24, 53]. Therefore, in the general case one would have to use different timings and/or different powers depending on the bit value, to avoid skewing the bit value distribution in the raw key. Also, the superlinearity could be exploited in other attacks, such as the faked-state attack [53, 54] and conventional quantum attacks, to make them more efficient [15].

ID Quantique has been notified about this loophole prior to the submission of the manuscript.

V. COUNTERMEASURES AND PROOF OF SECURITY

The security of QKD systems with arbitrary nonlinearities in Bob's system, and therefore superlinear threshold detectors has already been proved [16]. Without source imperfections and with symmetry in the two bases, the secret key rate is given by [16]

$$R \geq -h(\mathrm{QBER}) + \eta(1 - h(\mathrm{QBER})), \qquad (7)$$

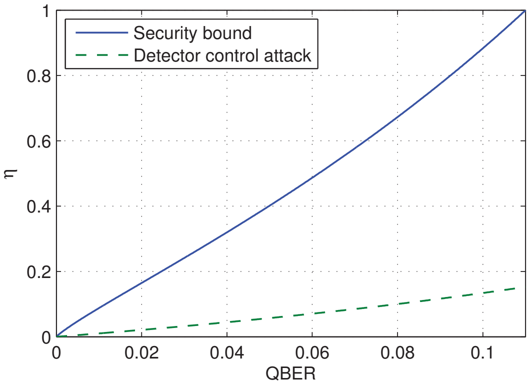


FIG. 5. (Color online) Comparison of the detector control attack and the bound from the security proof [16]. The region to the left of the security bound curve (solid curve) allows extraction a secure key. The region to the right of the detector control attack curve (dashed curve) is clearly insecure, because the attack presented in Sec. II can be applied. The region between the curves should be assumed insecure.

where $h(\cdot)$ is the binary entropy function, and η is the smallest detection probability of a non-vacuum state. If one further assumes that the probability to detect a multiphoton state is higher than a single photon, η is simply the quantum efficiency (the probability to detect a single photon).

As for the detector control attack, let us assume the worst-case superlinearity, namely that a single photon is detected with probability η, while a two-photon state is detected with probability 1. Then, Eve can use trigger pulses with two photons, and Eq. (4) simplifies to

$$\mathrm{QBER} = \frac{2\eta - \eta^2}{2 + 2(2\eta - \eta^2)}. \tag{8}$$

Figure 5 shows Eq. (7) for $R = 0$ and Eq. (8), comparing the "imperfect" detector control attack with the bounds derived in the security proof [16]. It shows that a sufficiently high detection probability, and thus quantum efficiency allows extraction of secret key regardless of any superlinear detector response. For instance, if the QBER is 5%, a quantum efficiency $\eta > 0.4$ allows the extraction of secret key. Note that a high quantum efficiency does not remove the superlinear effect, but then the security proof makes it possible to remove any knowledge Eve could have obtained exploiting the superlinear response, by (a large amount of) extra privacy amplification [55].

For gated systems, one possible countermeasure might be bit-mapped gating [56]. Then, the basis selector is used to randomize all detection events outside the center of the gate. Therefore, trigger pulses timed at the falling edge of the gate would cause random detections and thus a QBER of 50%. This would reveal Eve's presence. However, the security analysis for bit-mapped gating requires that each photon is detected individually during the transition of the basis selector. In practice, this means that the detectors must have a detection probability given by Eq. (2) in the center of the gate. Figure 2 shows that this is nearly the case. It might be possible to detect each photon completely individually in the middle of the gate by expanding the gate, or by shaping the applied electrical gate appropriately.

VI. SUMMARY AND CONCLUSION

In this paper we have analyzed the security of QKD systems using superlinear threshold detectors. The detector control attack previously reported [25] is based on very superlinear detection probability: when the amplitude of the trigger pulses is increased, the detection probability sharply increases from 0 to 100%. This allows eavesdropping the full key without causing any errors, the only side effect is 3 dB total loss. Here, the detector control attack is generalized to moderately superlinear detectors by accepting a limited amount of errors in the key, and/or accepting a higher loss. Note that in practice, a total loss of about 20 dB may be tolerable, as discussed in Sec. II.

Nanowire SSPDs [35] have been reported to have superlinear detection probability [36]. We have shown that by carefully selecting the trigger pulse amplitude, an eavesdropper would introduce a QBER of less than 3% when attacking the SSPD in Ref. [36]. The total loss caused by the eavesdropping would be less than 6 dB. Therefore, a QKD system using this detector would clearly be insecure.

Figures 2 and 3 show that the response of the APD-based gated detector is superlinear at the falling edge of the gate. Therefore, it is possible to attack the gated detectors with faint trigger pulses, with less than 120 photons per pulse. From the measurements, the attack would cause a QBER of about 13% and about 23 dB loss. Most QKD systems do not accept a QBER above 11% [5], but there are post-processing protocols allowing a QBER up to 20% [52]. Furthermore, we suspect that both the QBER and the loss could be reduced by using shorter trigger pulses [57]. Finally, even if the attack is not directly applicable to some QKD systems due to the QBER and/or loss threshold, the superlinear response of the APD-based detector shows that ordinary security proofs no longer apply to these systems. Therefore, these systems must use advanced security proofs to bound and remove Eve's partial knowledge from the moderate superlinear response.

The faint after-gate attack does not suffer from the limitations of the original after-gate attack [27]. In the faint after-gate attack, the afterpulsing is negligible. Furthermore, with less than 120 photons per pulse, the trigger pulses should be nearly impossible to catch with an optical power meter at the entrance of Bob. Also, removing gates randomly or due to after-pulse blocking will not

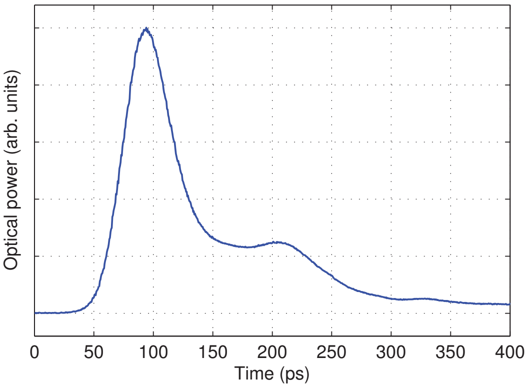


FIG. 6. (Color online) Pulse shape of the id300 short-pulsed laser, measured with a 45 GHz optical probe on a 12.5 GHz sampling oscilloscope at a pulse repetition rate of 100 kHz.

expose the attack [27] since such trigger pulse will not cause a click unless there is a gate present. Furthermore, the timing of the trigger pulse detection will be very similar to a normal detection inside the gate, and therefore difficult to discard based on timing [33].

If the detectors have an increasing detection probability for increasing photon number, a sufficiently high quantum efficiency makes it possible to remove Eve's knowledge using privacy amplification [55]. For gated APD-based detectors, bit-mapped gating [56] can be used if each photon is detected individually in the center of the gate.

Quantum key distribution has been proven secure for all future, so currently the challenge is to make a secure implementation. We believe that weeding out loopholes caused by the implementation is a necessary step towards achieving practical secure QKD, and that this work is crucial because it fully exposes the nature of the detector control attack.

ACKNOWLEDGMENTS

We acknowledge ID Quantique's valuable assistance in this project. We also acknowledge useful discussions with M. Akhlaghi. This work was supported by the Research Council of Norway (grant no. 180439/V30), DAADppp mobility program financed by NFR (project no. 199854), and DAAD (project no. 50727598). L.L. and V.M. acknowledge travel support from the Institute for Quantum Computing, Waterloo, Canada.

Appendix A: Pulse shape of id300

Figure 6 shows the pulse shape of the id300 short-pulsed laser [58]. This is the particular laser sample used in this experiment; other samples of this laser model may have a different pulse shape.

[1] R. H. Hadfield, Nat. Photonics **3**, 696 (2009).
[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, Bangalore, India, 1984) pp. 175–179.
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[8] D. Mayers, in *Proceedings of Crypto'96*, Vol. 1109, edited by N. Koblitz (Springer, New York, 1996) pp. 343–357.
[9] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[10] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).
[11] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. **4**, 325 (2004).
[12] H.-K. Lo and J. Preskill, Quant. Inf. Comp. **7**, 431 (2007).
[13] Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A **77**, 052327 (2008).
[14] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **9**, 131 (2009).
[15] L. Lydersen and J. Skaar, Quant. Inf. Comp. **10**, 60 (2010).
[16] Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).
[17] B. E. Kardynal, Z. L. Yuan, and A. J. Shields, Nat. Photonics **2**, 425 (2008).
[18] A. E. Lita, A. J. Miller, and S. W. Nam, Opt. Express **16**, 3032 (2008).
[19] B. R. Mollow, Phys. Rev. **175**, 1555 (1968).
[20] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006), erratum ibid. **78**, 019905 (2008).
[21] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **7**, 73 (2007).
[22] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).
[23] V. Makarov and J. Skaar, Quant. Inf. Comp. **8**, 622 (2008).
[24] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[25] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[26] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938

(2010).

[27] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).

[28] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, arXiv:0809.3408 [quant-ph].

[29] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).

[30] L. Lydersen, J. Skaar, and V. Makarov, J. Mod. Opt. **58**, 680 (2011).

[31] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nat. Photonics **4**, 800 (2010).

[32] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 801 (2010).

[33] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Appl. Phys. Lett. **98**, 231104 (2011).

[34] L. Lydersen, V. Makarov, and J. Skaar, arXiv:1106.3756 [quant-ph].

[35] G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, Appl. Phys. Lett. **79**, 705 (2001).

[36] A. Verevkin, J. Zhang, R. Sobolewski, A. Lipatov, O. Okunev, G. Chulkova, A. Korneev, K. Smirnov, G. N. Gol'tsman, and A. Semenov, Appl. Phys. Lett. **80**, 4687 (2002).

[37] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).

[38] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).

[39] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, arXiv:quant-ph/0411022v1.

[40] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).

[41] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).

[42] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).

[43] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photonics **1**, 343 (2007).

[44] R. H. Hadfield, J. L. Habif, J. Schlafer, R. E. Schwall, and S. W. Nam, Appl. Phys. Lett. **89**, 241129 (2006).

[45] D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, R. J. Hughes, and J. E. Nordholt, New J. Phys. **11**, 045009 (2009).

[46] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).

[47] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, Opt. Express **18**, 8587 (2010).

[48] M. K. Akhlaghi and A. H. Majedi, IEEE Trans. Appl. Supercond. **19**, 361 (2009).

[49] The coherent state with $\mu = 1$ was obtained by shining much brighter pulses into a power meter and calculating the energy per pulse. Then a controlled amount of optical attenuation was introduced to decrease the energy level of each pulse to $\mu = 1$.

[50] A. Spinelli and A. L. Lacaita, IEEE Trans. Electron Devices **44**, 1931 (1997).

[51] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, J. Mod. Opt. **51**, 1267 (2004).

[52] H. F. Chau, Phys. Rev. A **66**, 060302 (2002).

[53] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, arXiv:1103.2327 [quant-ph].

[54] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).

[55] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[56] L. Lydersen, V. Makarov, and J. Skaar, Phys. Rev. A **83**, 032306 (2011).

[57] Which we unfortunately did not have at our disposal for this experiment.

[58] id300, datasheet: `http://www.idquantique.com/images/stories/PDF/id300-laser-source/id300-specs.pdf`, visited 28. April 2011.

Paper K

Controlling an actively-quenched single photon detector with bright light

Submitted to Optics Express.

arXiv: 0809.3408 [quant-ph]

Controlling an actively-quenched single photon detector with bright light

Sebastien Sauge,[1] Lars Lydersen,[2,3] Andrey Anisimov,[4] Johannes Skaar,[2,3] and Vadim Makarov[2,*]

[1]*School of Information and Communication Technology,*
Royal Institute of Technology (KTH), Electrum 229, SE-16440 Kista, Sweden
[2]*Department of Electronics and Telecommunications,*
Norwegian University of Science and Technology, NO-7491 Trondheim, Norway
[3]*University Graduate Center, NO-2027 Kjeller, Norway*
[4]*Radiophysics Department, St. Petersburg State Polytechnical University,*
Politechnicheskaya street 29, 195251 St. Petersburg, Russia

(Dated: December 15, 2010)

We hack a commercial actively-quenched avalanche single-photon detector (PerkinElmer SPCM-AQR) commonly used for quantum cryptography. This study complements the recent hacking of passively-quenched and gated detectors by the same method, and thus demonstrates its generality. Bright illumination is used to blind the detector, such that it exits single-photon detection mode and instead operates as a mere classical photodiode. In this regime, the detector clicks controllably if a bright pulse is applied above a classical sensitivity threshold, allowing for an attack on quantum cryptography that eavesdrops the full secret key. The SPCM-AQR detector model exhibits three redundant blinding mechanisms: (1) overload of an opamp in the bias control circuit, (2) thermal blinding of the APD itself, and (3) overload of the DC/DC converter biasing the APD. This confirms that multiple loopholes may be left open if one does not examine closely non-idealities in components used for quantum cryptography implementations. To reach the security envisioned by theoretical proofs, this practice must change.

Over the past twenty years, quantum key distribution (QKD) has progressed from a tabletop demonstration to commercially available systems [1], with secure key exchange demonstrated up to 144 km in free-space [2] and 250 km in optical fibers [3]. Security of these cryptosystems is based on the impossibility, in principle, to reliably copy an *a priori* unknown quantum state, as accounted for by the no-cloning theorem [4]. However, security also relies on the assumption that the optical and electro-optical devices which are part of quantum cryptosystems do not deviate from model assumptions made to establish security proofs [5–11].

Recently, it has been demonstrated that both commercial QKD systems on the market can be fully cracked [12–14]. A tailored bright illumination was employed to remote-control gated avalanche photodiodes (APDs) used to detect single photons in these QKD systems. In another work, a full eavesdropper has been implemented on a research system using passively-quenched APDs [15]. The overall purpose of the work reflected in this paper is now to establish the generality of this attack, by extending its validity to QKD systems employing the most commonly used model of actively-quenched APD, PerkinElmer SPCM-AQR detector module [16]. Moreover, we wish to illustrate here that the principle of our attack can be exploited in numerous ways, leading in practice to several control modes of the APDs (three in the case of the detector tested in this paper). We now explain briefly the general scheme of attack, before embarking on particularities of this detector model.

From eavesdropper's point of view, the *intercept-resend attack* provides a general framework to exploit unaccounted non-idealities or operating modes of components. In this attack, we assume that the eavesdropper Eve owns an exact replica of receiver Bob's detection apparatus, with which she intercepts and measures the state of each qubit sent by Alice. To successfully eavesdrop, Eve must resend faked states [21] that will force her detection results onto Bob's in a transparent way. Ideally, the faked state should make the target detector click controllably (with unity probability and near zero time-jitter) while keeping any other detector blind (no click). In the Bennett-Brassard 1984 (BB84) [22] and similar four-state protocols, Bob must detect two bit values in two bases, which can be implemented with two pairs of detectors. One pair detects bit values "0" and "1", and a second pair (not necessary with active basis choice) detects in the conjugate measurement basis, which is randomly selected prior to detection of each qubit in order to guarantee security against eavesdropping. Thus in 50% of the cases, the qubit resent by Eve will be measured by Bob in the conjugate basis, resulting in a random outcome. Similarly, if the photonic qubit is replaced by a classical pulse of peak power P_{th}, an incompatible choice of basis will result in arrival of pulses of power $P_{\mathrm{th}}/2$ at both detectors. Let us now assume that under some conditions, detectors remain blind at power $P_{\mathrm{th}}/2$ and click controllably at threshold power P_{th}. With the latter pulse, Eve can selectively address the target detector without causing a click in the conjugate basis. This is illustrated in Fig. 1 in the case of a QKD system running a four-state protocol with polarization coding and passive choice of basis at Bob's side. After Bob reveals in which bit slots he has registered detections, Eve will have the same key bit sequence as Bob. Eve thus can extract the final secret key by listening to the classical public com-

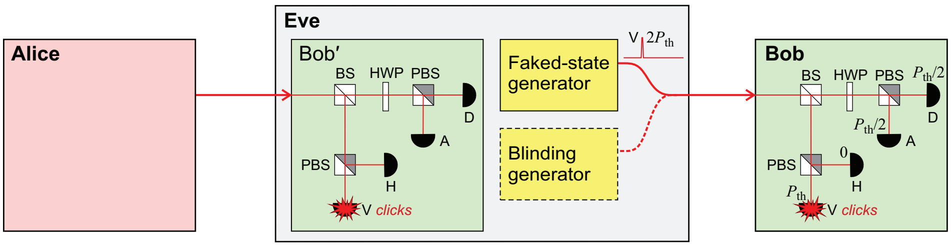


FIG. 1. (Color online) Intercept-resend (faked-state) attack Eve could launch against a QKD system which runs a four-state protocol with polarization coding and passive choice of basis [17–20]. In the example, Eve targets the detector recording vertically polarized qubits in the horizontal/vertical (H/V) basis. We assume here that detectors click controllably when illuminated by an optical pulse with peak power $\geq P_{\rm th}$, and that they are blind (or kept blind) at power $\leq P_{\rm th}/2$ (characteristics of the 'blinding generator' potentially needed to bring detectors in this working mode will be described later). To address the target detector, Eve sends a faked state with V polarization and power $2P_{\rm th}$, thus the V detector receives power $P_{\rm th}$ after basis choice, and clicks. The detectors recording polarized qubits in the conjugate (45°-rotated, D/A) basis each receive a pulse of power $P_{\rm th}/2$, and thus remain blinded. In the diagram: BS, 50:50% beamsplitter; PBS, polarizing beamsplitter; HWP, half-wave plate rotated 22.5°.

munication between Alice and Bob and doing the same post-processing operations as Bob [12, 15]. Thus, providing that the above assumption of the detector threshold behavior is satisfied, QKD systems using such detectors are vulnerable.

Let us now explain how this assumption can be fulfilled. Most QKD systems today use *avalanche photodiodes* (APDs) to detect single photons [23]. (The two notable exceptions are continuous-variable QKD systems [24–28] and those using superconducting detectors [3, 29, 30].) For single-photon sensitivity, APDs are operated in so-called Geiger-mode, i.e., they are biased above the breakdown voltage so that an absorbed photon triggers an avalanche. (In case of gated-mode operation, the APD is biased above breakdown only during the gate time to limit noise [12, 23].) The avalanche current is sensed by a comparator before the avalanche is quenched to reset the diode. Quenching is achieved by lowering (passively or actively) the bias voltage below breakdown. In the latter condition, however, the APD no longer behaves as a single-photon detector but as a classical linear photodiode generating photocurrent proportional to the optical illumination. It is thus insensitive to single photons, but also to noise sources (dark counts, afterpulses). However, it is still possible to make the APD click controllably since in this linear mode, the comparator threshold translates to a classical optical power threshold $P_{\rm th}$. Providing the threshold is well-defined, no click will ever occur at power $P_{\rm th}/2$, and Eve has at her disposal a very general attack for breaking the security of most APD-based QKD systems.

In the case of the two recently-hacked commercial QKD systems operating at telecom wavelengths [12], transition from Geiger to linear mode was achieved by using continuous-wave (c.w.) bright illumination to reduce APD bias voltage below breakdown. Equivalently, raising the breakdown voltage above the fixed bias voltage by heating the APDs also led to blinding and control of the detectors [14].

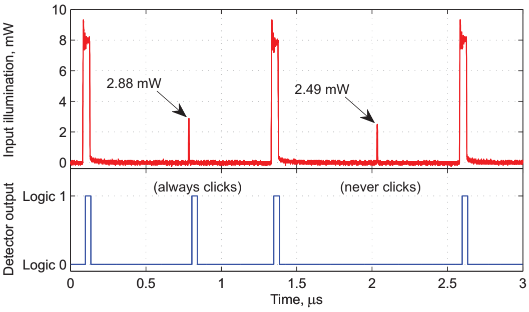


FIG. 2. (Color online) Oscillogram at detector output (lower trace) illuminated by bright optical pulses (upper trace) made of control pulses (808 nm, 8 mW, 50 ns wide, 800 kHz repetition rate) to blind the detector, and of weaker trigger pulses (8 ns wide). The trigger pulses make the detector click with unity probability and sub-nanosecond time jitter *only* above a certain power threshold. In the example, detector always clicks at $P_{\rm th} = 2.88$ mW peak power trigger pulses, never clicks at $\lesssim$2.49 mW.

In this paper, we illustrate further the generality of the attack by taking full control of a commercial detector model commonly used for QKD in the visible/near infrared range (PerkinElmer SPCM-AQR module [16]). In this case, we achieved transition to linear mode by applying not c.w. but instead bright pulsed illumination at the level of less than 10 mW at $\geq$70 kHz repetition rate. Between two pulses, the detector is blind to single photons, dark counts and afterpulses, and clicks controllably if a classical pulse $\geq P_{\rm th}$ is applied, as illustrated in Fig. 2.

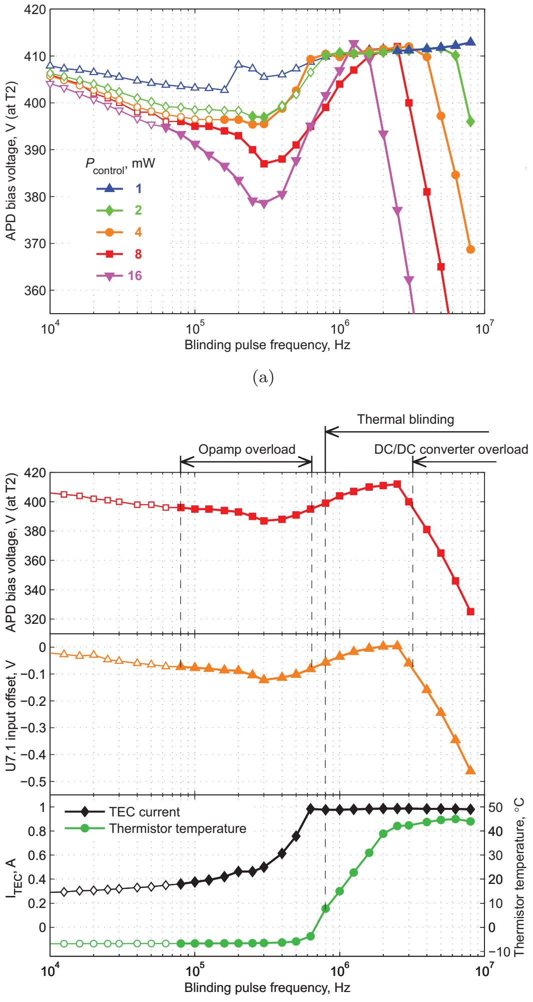
Fig. 3(a) shows at which optical pulse frequencies blinding of the detector is achieved, and the corresponding bias voltage at the APD. We identified three distinct mechanisms responsible for blinding. Each mechanism is activated in a different range of control pulse frequencies, as discussed below.

The first blinding mechanism corresponds to transition from Geiger to linear mode by lowering the APD bias voltage below breakdown. As the frequency of optical pulses increases, control first appears when the APD bias voltage drops by 12–15 V (Fig. 3(a)). To understand why it drops, let's consider the detector electrical circuit depicted in Fig. 4. When the APD is illuminated by a bright optical pulse, the current through it is not interrupted by the detection and quenching circuit (DQC) and is much larger than during an ordinary single-photon avalanche. A current limiting circuit (CLC) kicks in and limits the current pulse to about 10 mA. This current is drawn from the capacitor C9, whose other end is connected to the output of a low-power opamp U7.1. This opamp has a specified maximum load current significantly smaller than 10 mA. It gets overloaded by the current pulses, and unexpectedly develops a large static voltage offset between its inputs (see Fig. 3(b), middle chart). This negative offset effectively adds to the pre-set reference voltage at the opamp non-inverting input, and the feedback loop lowers the APD bias voltage proportionally.

At higher control pulse frequencies ~1 MHz, however, the disrupted opamp gets back into normal operation. At these frequencies, the duty cycle of the current pulses at the opamp output gets closer to 1/2, thus its sourcing peak current decreases while its sinking peak current grows; they become close in magnitude and now better suit opamp load capability. As a result, the APD bias is raised back to the nominal value. Yet, the detector remains blind. This occurs because the APD produces more heat through electrical power dissipated in it, as the frequency of control pulses increases. In normal operation, the APD is cooled to −7 °C with a thermoelectric cooler (TEC). The TEC heat removal capability and maximum current are inherently limited. As can be seen in the lower chart in Fig. 3(b), after a temperature controller reaches the maximum TEC current, the APD temperature quickly rises. The raised APD temperature in turn raises its breakdown voltage (by about 1.2 V/°C) above the bias voltage, which also leads to blinding. This thermal blinding behavior is the same as previously reported for gated detectors in the commercial QKD system Clavis2 (Fig. 5).

At even higher pulse frequencies, the bias voltage drops again below breakdown, while the detector is still under control. This is due to load capacity exhaustion of the high-voltage DC/DC converter U6 biasing the APD.

Above, we have demonstrated three distinct blinding modes in the SPCM-AQR detector model [16]. Some QKD experiments [20] use a four-channel version of this



(a)

(b)

FIG. 3. (Color online) Detector blinding: (a) APD bias voltage vs. frequency and peak optical power P_{control} of rectangular 50 ns wide input optical pulses. Normal bias voltage at low count rate for this detector sample is 410 V (the other detector sample we tested had bias voltage of 350 V). Filled symbols denote pulse parameters at which the detector got completely blind between the control pulses. (b) Parameters in the circuit vs. frequency of optical pulses with peak power $P_{\text{control}} = 8$ mW. Behavior of these parameters reveals three blinding mechanisms summarized over the top of the chart. The middle chart shows static voltage difference between the opamp inputs. The lower chart shows current of the thermoelectric cooler (TEC) and the temperature of the APD as measured by a thermistor mounted nearby at the cold plate of the TEC.

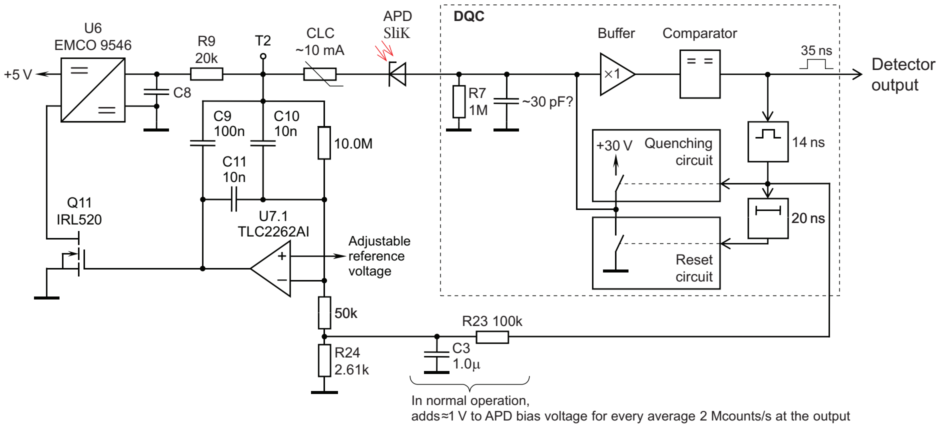


FIG. 4. Simplified reverse-engineered circuit diagram of PerkinElmer SPCM-AQR module. In normal operation, the cathode of the APD is biased at a constant high voltage, stabilized by a feedback loop containing an opamp U7.1 (Texas Instruments TLC2262), field-effect transistor Q11 and high-voltage DC/DC converter module U6 (EMCO custom model no. 9546). The anode of the APD is connected to a detection and quenching circuit (DQC). The DQC senses charge flowing through the APD during the avalanche, then briefly connects the APD anode to +30 V to lower the voltage across the APD below breakdown and quench the avalanche. The APD anode voltage is subsequently reset to 0 V, and the detector becomes ready for the next avalanche. (Note: the circuit diagram has been greatly simplified for the paper; do not use this figure for attempting detector repair or modification.)

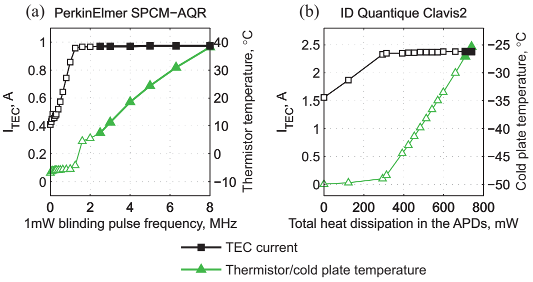


FIG. 5. (Color online) Comparison of thermal blinding characteristics of the PerkinElmer SPCM-AQR detector to the ones reported for ID Quantique's Clavis2 commercial QKD system [14]. Filled symbols denote regime in which the detector got completely blind between the control pulses.

detector module, PerkinElmer SPCM-AQ4C [31]. Our preliminary analysis indicates that it has a different bias control circuit that is not susceptible to the first blinding mechanism (opamp overload). However, it is likely susceptible to both thermal blinding and DC/DC converter overload, because it uses the same APD package and the same model of DC/DC converter.

The only *side effect* that betrays our attack is the simultaneous arrival at all detectors of the blinding pulses with a rate of at least 70 kHz. In some QKD systems, these may be ignored by Bob as falling outside his post-processing gating time window. In free-space systems operating in daylight [18, 19], these pulses may be mistaken by Bob for normal background count rates. The control pulses can be irregularly spaced to make them look more like background counts. We remark that the blinded state has some inertia (especially in the case of thermal blinding [14]) that should in principle allow Eve to apply the blinding pulses in bursts interleaved with quiet periods when only the trigger pulses are applied. We also note that both APDs used in the present study died suddenly after prolonged extensive testing, which may indicate that at least some of these control regimes reduce their lifetime.

Countermeasures for all detectors considered may include monitoring the incoming optical power, as well as monitoring the APD bias voltage, current and temperature. Single-photon sensitivity of Bob's APDs can be tested at random times by a calibrated light source placed inside Bob. Although development of countermeasures has begun [12, 32], no definite countermeasure has been finalized and tested by hacking at this time [33]. The most frequently proposed countermeasure is an optical power meter at Bob's entrance. Currently this should not be considered a sufficient countermeasure: it is unclear how to select the power meter threshold which must be derived from a security proof with a sufficiently general detector model.

In view of this study, complemented by the ones made on other APD models [12–15], we estimate that most of the QKD systems existing today are potentially vulnerable to our attack, the only 'detector-dependent' aspect here being the type of bright illumination (none, c.w., or pulsed) required to bring a particular APD into the linear regime. Our work emphasizes the need to investigate thoroughly vulnerabilities originating from unaccounted physical non-idealities of QKD components.

Financial support is acknowledged from the Research Council of Norway (grant no. 180439/V30), the ECOC'2004 foundation and the Research Council of Sweden (grant no. 621-2007-4647).

* makarov@vad1.com

[1] Commercial QKD systems are available from at least two companies: ID Quantique (Switzerland), `http://www.idquantique.com`; MagiQ Technologies (USA), `http://www.magiqtech.com`.

[2] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Nat. Phys. **3**, 481 (2007).

[3] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).

[4] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[5] D. Mayers, in *Proceedings of Crypto'96*, Vol. 1109, edited by N. Koblitz (Springer, New York, 1996) pp. 343–357.

[6] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[7] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[8] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. **4**, 325 (2004).

[9] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **9**, 131 (2009).

[10] L. Lydersen and J. Skaar, Quant. Inf. Comp. **10**, 0060 (2010).

[11] Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).

[12] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[13] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, e-print arXiv:1009.2683 [quant-ph].

[14] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, e-print arXiv:1009.2663 [quant-ph].

[15] I. Gerhardt, Q. Liu, J. Skaar, A. Lamas-Linares, C. Kurtsiefer, and V. Makarov, e-print arXiv:1011.0105 [quant-ph].

[16] PerkinElmer SPCM-AQR single photon counting module, data sheet, PerkinElmer (2005).

[17] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).

[18] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, New J. Phys. **11**, 045007 (2009).

[19] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New J. Phys. **4**, 43 (2002).

[20] C. Erven, C. Couteau, R. Laflamme, and G.Weihs, Opt. Express **16**, 16840 (2008).

[21] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).

[22] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, Bangalore, India, 1984) pp. 175–179.

[23] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, J. Mod. Opt. **51**, 1267 (2004).

[24] T. C. Ralph, Phys. Rev. A **61**, 010303 (1999).

[25] M. Hillery, Phys. Rev. A **61**, 022309 (2000).

[26] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).

[27] M. Heid and N. Lütkenhaus, Phys. Rev. A **76**, 022313 (2007).

[28] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, New J. Phys. **11**, 045023 (2009).

[29] G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, Appl. Phys. Lett. **79**, 705 (2001).

[30] A. Verevkin, J. Zhang, R. Sobolewski, A. Lipatov, O. Okunev, G. Chulkova, A. Korneev, K. Smirnov, G. N. Gol'tsman, and A. Semenov, Appl. Phys. Lett. **80**, 4687 (2002).

[31] PerkinElmer SPCM-AQ4C single photon counting module array, data sheet, PerkinElmer (2005).

[32] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nat. Photonics **4**, 800 (2010).

[33] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 801 (2010).

Paper L

Controlling a superconducting nanowire single-photon detector using tailored bright illumination

Submitted to New Journal of Physics.

arXiv: 1106.2396 [quant-ph]

Controlling a superconducting nanowire single-photon detector using tailored bright illumination

Lars Lydersen,[1, 2, *] Mohsen K. Akhlaghi,[3] A. Hamed Majedi,[3] Johannes Skaar,[1, 2] and Vadim Makarov[1, 2, †]

[1] *Department of Electronics and Telecommunications,*
Norwegian University of Science and Technology, NO-7491 Trondheim, Norway
[2] *University Graduate Center, NO-2027 Kjeller, Norway*
[3] *Department of Electrical & Computer Engineering and Institute for Quantum Computing,*
University of Waterloo, Waterloo, ON, N2L 3G1 Canada

(Dated: June 15, 2011)

We experimentally demonstrate that a superconducting nanowire single-photon detector is deterministically controllable by bright illumination. We found that bright light can temporarily make a large fraction of the nanowire length normally-conductive, can extend deadtime after a normal photon detection, and can cause a hotspot formation during the deadtime with a highly nonlinear sensitivity. In result, although based on different physics, the superconducting detector turns out to be controllable by virtually the same techniques as avalanche photodiode detectors. As demonstrated earlier, when such detectors are used in a quantum key distribution system, this allows an eavesdropper to launch a detector control attack to capture the full secret key without being revealed by errors in the key.

I. INTRODUCTION

Quantum key distribution (QKD) allows two parties, Alice and Bob, to generate a secret random key at a distance [1–4]. The key is protected by quantum mechanics: an eavesdropper Eve must disturb the signals between Alice and Bob, and therefore reveal her presence. QKD using perfect devices has been proven secure [5, 6].

Implementations of QKD have to use components available with current technology, which are usually imperfect. While there are numerous security proofs considering more realistic devices [7–15], these proofs assume that the imperfections are quantified in terms of certain source and detector parameters. Due to the difficulty of characterizing or upper bounding these parameters owing to limitations of these security proofs, it is common to use the more established security proofs for ideal systems also in practical implementations. With actual devices deviating from the ideal models, numerous security loopholes have therefore been identified [16–24], and in some cases exploited in eavesdropping experiments without [25, 26] and with [27, 28] secret key extraction by Eve. Finding and eliminating loopholes in implementations is crucial to obtain provable practical security.

As an example, several recent attacks have been based on bright-light control of avalanche photodiodes (APDs) [22, 23, 27–33]. Superconducting nanowire single-photon detectors (SSPDs) studied in this paper are based on different physics. However, as we will see, the principles of attacks on QKD systems using SSPDs are broadly similar to attacks on QKD systems using APDs: Eve uses a faked-state attack [34], can blind the detectors [22, 23], make them click with a classical threshold using a bright pulse [23] or let one detector temporarily recover from blinding [22]; also, detector's response to multiphoton pulses can be superlinear [33]. We refer to these principles through the paper.

Although SSPDs have been used in several QKD experiments [35–39], this detector technology is still in its infancy. No automated unattended operation of systems containing SSPDs has been reported. Technical aspects of SSPD operation, such as handling the latching behavior and converting the nanowire analog response into a digital detection signal, have only been studied in the normal single-photon counting regime. So far, no attempt has been reported to consider SSPD's nonidealities in order to attack a QKD system. This study thus serves as an *early warning.* Although we have done our experiments on only one detector sample, we show that control by bright light can be achieved through two separate mechanisms, and may thus be applicable to different detector electronics designs [40].

The paper is organized as follows. In Sec. II, we describe the SSPD under test. Sections III and IV deal with the SSPD in the latched and non-latched states; in each section we present the physics behind detector's reaction to bright-light illumination, then how it can be exploited to attack QKD. We discuss our findings and conclude in Sec. V.

II. DETECTOR DESIGN AND OPERATION

We performed our tests on an SSPD of a fairly standard configuration, which has been characterized in previous publications [41–43]. The SSPD chip was manufactured at the State Pedagogical University, Moscow, and consists of a 4 nm thick, 120 nm wide NbN nanowire on sapphire substrate, laid out in a $10 \times 10\,\mu$m meander pattern with 60% filling ratio. The chip is packaged and installed in a ~ 1 m long dipstick assembly (see

[*] lars.lydersen@iet.ntnu.no
[†] makarov@vad1.com

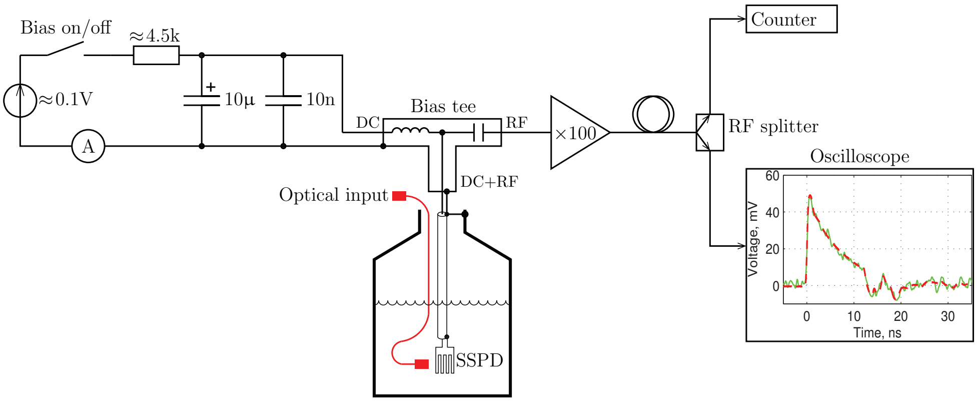


FIG. 1. (Color online) Detector circuit. The SSPD is biased from a battery-powered direct current (DC) source, an equivalent circuit diagram of which is shown. Pulses produced by the SSPD travel through ~ 1 m coaxial cable, bias tee (0.1–6000 MHz, Mini-Circuits ZFBT-6GW+), radio-frequency (RF) amplifier (voltage gain 100, 0.1–1500 MHz, Phillips Scientific 6954-S-100), ~ 1.5 m coaxial cable, and RF splitter (Mini-Circuits ZN2PD-9G-S+), to the counter and oscilloscope. Inside the oscilloscope box: normal single-photon response after the RF amplifier and splitter, shown as a single-shot trace with 2 GHz bandwidth (solid line) and averaged over many pulses (dashed line). Features appearing 12 ns after the leading edge are attributed to reflections due to impedance mismatch in the RF circuits.

Ref. [42] for details), lowered into a Dewar flask. During detector operation, the chip is immersed into liquid helium at 4.2 K. It is optically accessible through a single-mode fibre. The chip is connected to a room-temperature bias tee and wideband radio-frequency (RF) amplifier via a 50 Ω coaxial cable (Fig. 1). A battery-powered current source biases the superconducting nanowire with $I_\mathrm{b} = 22.5$ μA which is ≈ 0.85 of its critical current I_c (this I_b value provides the highest ratio of photon detection probability at 1550 nm to dark count rate, for this particular SSPD sample). The signal from the output of the RF amplifier is split to a 16 GHz single-shot oscilloscope (Tektronix DSA 71604) and a counter (Stanford Research Systems SR400). Detection efficiency for single photons at 1550 nm was 2.2×10^{-5} and the dark count rate was < 1 Hz. The detector sensitivity was polarization-dependent; in all experiments in this paper polarization was aligned to maximize the detection efficiency, using a fiber polarization controller.

One aspect of detector operation is how the analog pulse produced by a transient hotspot (see inset in Fig. 1) is converted into a detection event and assigned a particular timing. The analog pulse is well-defined, its magnitude and shape being nearly constant from one photon detection to another. Therefore almost any discriminator design would work for single-photon detection, and its implementation details (bandwidth, hysteresis, whether it is a threshold discriminator or a constant-fraction discriminator, etc.) are often omitted in the literature on SSPDs. However these details become more important for demonstration of detector control by bright light. We assume in this study that the analog pulse is sensed by a high-speed voltage comparator, and the detection event timing is registered by pulse's leading edge crossing a preset comparator threshold. Indeed this is how our SR400 counter operates: it has an adjustable threshold set with 0.2 mV resolution. In our setup, the counter works correctly (registering one count per one single-photon analog pulse) in a wide range of threshold settings, +4.4 to +37 mV. A detail not mentioned in the literature is what threshold level the comparator should be set at, within this working range. While the setting may not affect normal detector operation, only a part of this voltage range is reachable under bright-light control described in the following section.

Another interesting aspect of detector operation is latching. In single-photon detection regime, the hotspot after formation shrinks quickly and the nanowire returns to the superconducting state [44]. However the detector also has a stable *latched state,* when a larger self-heating hotspot persists indefinitely, at a steady current I_latched which is a fraction of I_b, and a large voltage across the SSPD. The detector is blind to single photons and does not produce dark counts in this regime. A properly designed SSPD does not enter the latched state after a single-photon detection [44, 45]. However it can still latch after an electromagnetic interference (which in our experiment was easily caused by switching on and off lights and other mains-powered electrical equipment in the same building). Latching also occurs after a brief bright illumination: as little as 50 nW, 5 ms long single light pulse at 1550 nm reliably latches the device. Increasing the bias current I_b very close to I_c also leads to latching. The only way to return the detector from the latched state into the normal regime is to temporarily reduce I_b below I_latched. In our experiment, and supposedly in most other experiments reported in the literature, this was performed manually.

III. DETECTOR CONTROL IN LATCHED STATE

A. Physics

In the latched state, the Joule heat generated in the normally-conductive fraction of the nanowire exactly balances the cooling. The length of the normally-conductive fraction changes with the voltage applied across the SSPD. We investigated this by replacing the battery-powered bias source with an external voltage source. In our experiment, I_{latched} was roughly 7 μA regardless of the voltage across the device, up to 10 V (we did not apply higher voltages to reduce a chance of electrical breakdown). At 10 V, the nanowire resistance was thus $\sim$ 1.4 MΩ. Above the superconducting transition temperature the resistance of the entire device is approximately constant, and is $\approx$ 2.3 MΩ [43]. Therefore we concluded that slightly over half its length was normally-conductive at 10 V. During the experiment, I_{latched} would randomly assume a value in the 6 to 8 μA range, which could correspond to the normally-conductive region shifting and "locking" to the local variations of nanowire thermal characteristics along its length.

Next, we investigated what happened when bright continuous-wave (CW) light was applied in the latched state. Under illumination, current I through the device dropped, with a different sensitivity at different voltages (Fig. 2(a)). When recalculated into device resistance (Fig. 2(b)), we see that at low source voltages the resistance increased by about the same amount (350–400 kΩ per 20 mW), while at 10 V the increase was smaller (~110 kΩ). Note that depending on optical coupling, illumination may be unevenly distributed along the nanowire.

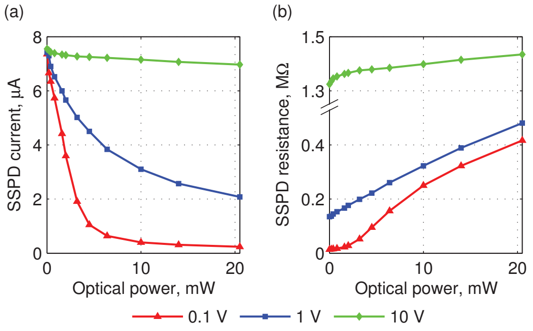


FIG. 2. (Color online) Response to continuous-wave (CW) light in the latched state. (a) Current I through the SSPD vs. optical power at 1550 nm, at different voltages V applied across the SSPD. (b) SSPD resistance $R = V/I$.

Implementation and maximum voltage of the bias source is yet another detail that varies between setups and is rarely specified in the literature. In our detector it is implemented as a $\approx$ 0.1 V voltage source in series with $\approx$ 4.5 kΩ resistor (see Fig. 1), with both voltage and resistance being trimmable in a small range to set precise I_{b} in the normal (non-latched) regime. When the SSPD resistance is zero, this bias circuit acts as a current source. However, in the latched state the SSPD resistance becomes larger than the circuit output impedance, thus it acts as a voltage source. Measurements done with this battery-powered bias circuit closely match the 0.1 V curve in Fig. 2.

B. Exploit

The eavesdropper Eve can latch the device by applying a single 5 ms long light pulse at 1550 nm. Latching occurs at any pulse power > 50 nW.

In the latched state, the SSPD is insensitive to single photons and produces no dark counts (similarly to blinding of APDs [22, 23]). However, the nanowire's response to bright illumination detailed in Sec. III A also holds on a nanosecond scale, and can be used to produce an electrical pulse after the RF amplifier and splitter (Fig. 3) [46]. The response is caused by a larger piece of the nanowire becoming normally conductive during the bright illumination, therefore causing an abrupt change in the resistance, just as a single photon causes an abrupt change in the resistance in the normal operating regime. Note that the electrical response to a bright trigger pulse saturates

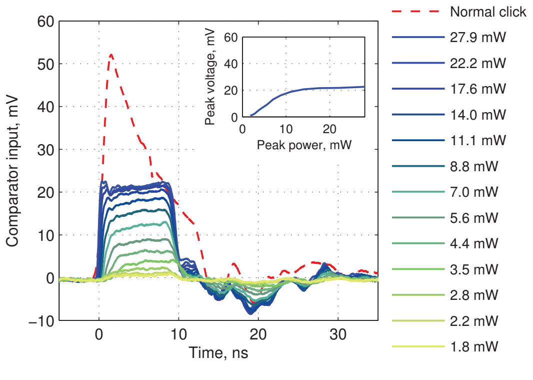


FIG. 3. (Color online) Electrical response in the latched state to the 10 ns, 1550 nm optical trigger pulse. All traces are averaged over 500 samples. The trigger pulse saturates at an electrical response of about 20 mV (see inset), compared to the normal detection event which reaches peak amplitude of about 50 mV.

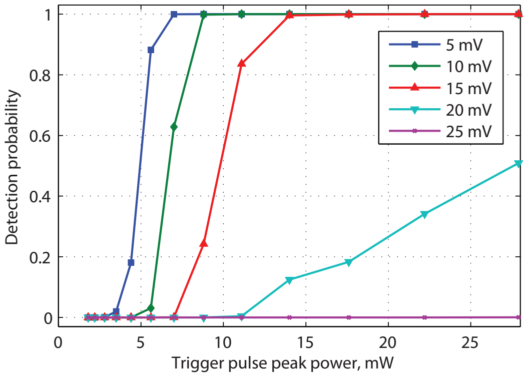


FIG. 4. (Color online) Detection probability of the 10 ns trigger pulse, depending on the comparator threshold. The probabilities were obtained by simulating a bandwidth-limited ideal comparator, requiring that the wideband signal recorded by the oscilloscope spent at least 3 ns above the threshold level to register a click. With SR400, jitter of comparator click in response to the bright pulse was ~ 0.5 ns full width at half maximum (FWHM).

at ~ 20 mV when optical power > 15 mW is applied, because at this power the current through the nanowire is reduced to almost zero.

Since this analog electrical pulse is sensed by a comparator, the detector has a highly superlinear detection probability of bright pulses [33]. The actual detection probability depends strongly on the comparator threshold (Fig. 4). With the comparator threshold in the 5–20 mV range, the detection probability is highly superlinear and increases quickly from negligible to a substantial value for a 3 dB increase in the optical power. A sufficient condition for a detector control attack is a large ratio of detection probabilities over a 3 dB change in the trigger pulse power [23, 33] (or 6 dB change in the trigger pulse power for distributed-phase-reference protocols [29]). Then Eve can intercept the quantum states from Alice, and resend bright trigger pulses corresponding to her detection to Bob [23, 33]. If Eve used a measurement basis not matching Bob's, she wants her pulse to remain undetected. Indeed when the pulse is measured by Bob in a different basis, it will be split to both detectors, corresponding to 3 dB reduction in its power, and almost never cause a click. Due to the large difference in detection probability for 3 dB change in the trigger pulse amplitude, a detector control attack would cause negligible errors and not expose eavesdropping, for the comparator threshold settings $\lesssim 20$ mV. Above ~ 20 mV the trigger pulses stop causing clicks at all, and this attack method no longer works. However, it may be possible to reach higher threshold settings using a different attack method described in the next section.

IV. DETECTOR CONTROL VIA DEADTIME EXTENSION

A. Physics

In this section we consider a non-latched, single-photon sensitive normally operating detector. The attack is based on detector's ability to form a hotspot in response to bright light when the current I through the SSPD is low. In addition, the hotspot formation probability at a low current is strongly superlinear. It is well-known that at relatively low values of the bias current I_{b}, multiphoton processes dominate the detector sensitivity [33, 47, 48]. Here we demonstrate that this effect becomes extreme during the normal recovery time after a photon detection.

In normal detector operation, after the hotspot formation, I drops to a fraction of I_{b} [44]. Then, I exponentially recovers to I_{b} at a slow rate, owing to a relatively large kinetic inductance of the superconducting nanowire (see dashed trace in Fig. 5). During the initial part of this recovery, the SSPD remains insensitive to single photons, but it can react to a bright illumination by forming another hotspot, with a higher illumination power being able to form a hotspot earlier in the recovery. This is illustrated in Fig. 5, which shows electrical response to a 48 ns long bright pulse. At 0.25 mW pulse power, the single-shot trace clearly shows that the SSPD forms a hotspot on average every 6 ns. At 0.5 mW, the period reduces to ~ 2.7 ns. At higher optical powers separate hotspot formations are no longer distinguishable, but the whole electrical pulse gets higher, indicating a lower average current through the nanowire during the optical pulse. Thus, during a sufficiently bright optical pulse, the electrical signal will stay above the comparator threshold. This allows Eve to extend the detector deadtime after the first photon detection, up to 500 ns with this detector setup, without causing latching.

We further quantify the hotspot formation probability during the recovery, by applying a 53 ps FWHM trigger pulse after the closing edge of the 48 ns, 2.5 mW pulse. (The recovery after the bright pulse should be similar to the recovery after a single-photon detection, however we focus on the former for reasons that will become apparent in the next subsection.) As far as we can see, response to this trigger pulse is probabilistic and binary: the hotspot either forms, or it does not (Fig. 6). In the former case the recovery resets and starts anew from a certain current value, in the latter case the recovery continues undisturbed. The probability that the trigger pulse causes a hotspot is plotted in Fig. 7. The measurement shows that the detection probability is reduced for at least 40 ns. It also shows that the detector is highly superlinear in at least the first 10 ns. During this time, a hotspot can be formed with unity probability using a sufficiently high-energy trigger pulse (~ 150 fJ), while the same trigger pulse attenuated by 20 dB (i.e., 100 times lower pulse energy) is very unlikely to cause a hotspot formation.

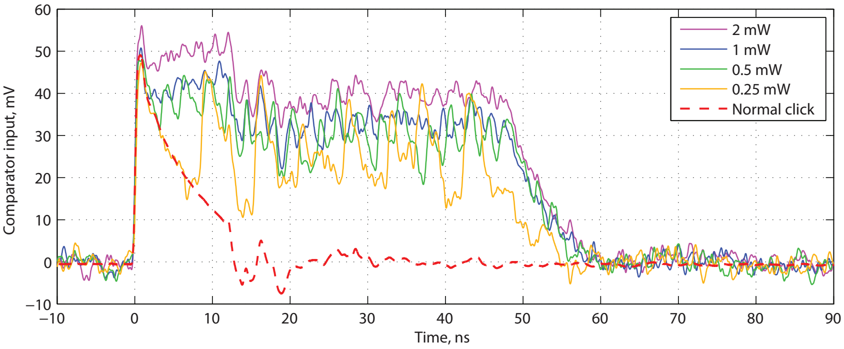


FIG. 5. (Color online) Electrical response in the non-latched state to the 48 ns, 1550 nm optical pulse. Single-shot traces with 2 GHz bandwidth for different pulse powers are shown, as well as an averaged normal single-photon response.

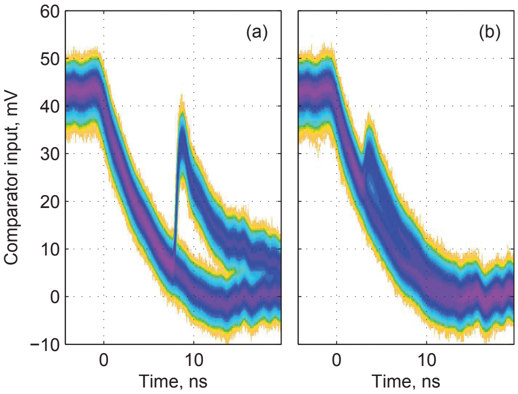


FIG. 6. (Color online) Accumulated 30,000 oscilloscope traces of the electrical response to the trigger pulse during the recovery from a 48 ns, 2.5 mW rectangular optical pulse. The trigger is (a) 8 ns into the recovery, 25 fJ energy, (b) 3 ns into the recovery, 78 fJ energy. In both cases the trigger pulse causes hotspot formation with roughly 50% probability, and resets the voltage to the same level. All oscillograms at trigger pulse delays ≥ 2 ns show the same behavior.

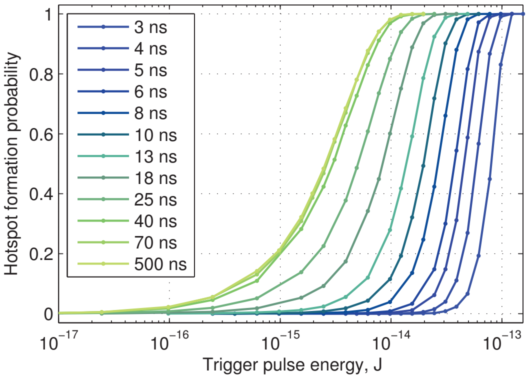


FIG. 7. (Color online) Hotspot formation probability vs. energy of a 53 ps wide trigger pulse, for different trigger pulse delays after the closing edge of a 48 ns, 2.5 mW rectangular optical pulse (both pulses at 1550 nm). The probabilities were extracted from recorded oscillograms similar to those shown in Fig. 6. 10^{-13} J corresponds to 780,000 photons contained in the trigger pulse.

B. Exploit

Extendability of SSPD's deadtime can be exploited in the earlier described attack [22] on the Bennett-Brassard 1984 (BB84) and similar protocols. We remark that the superlinearity is not required for this attack, but is helpful and makes it easier. Here we propose a version of this attack for differential-phase-shift QKD (DPS-QKD) systems [36, 49]. We explain the key component of the attack: how Eve can control Bob's SSPDs in the DPS-QKD system. Bob consists of an unbalanced Mach-Zehnder interferometer, and two detectors D0 and D1 (Fig. 8(a)). We assume that a properly implemented Bob will not accept clicks from both detectors for the duration of recovery after a click in one of the detectors, in order to avoid the detector deadtime and efficiency mismatch loopholes [18, 28]. As illustrated above, the expected recovery is ∼ 40 ns long. Eve begins by applying to both detectors a laser pulse longer than the recovery time (Fig. 8(b)), with phase φ changing in steps along the pulse such that its power splits equally to the two detectors. This pulse produces a double click at the beginning, which however can be timed to fall in between the bit slots and be discarded by Bob. Immediately after this long pulse, Eve applies a sequence of short pulses. Their phases are chosen to steer them primarily to one of the two detectors

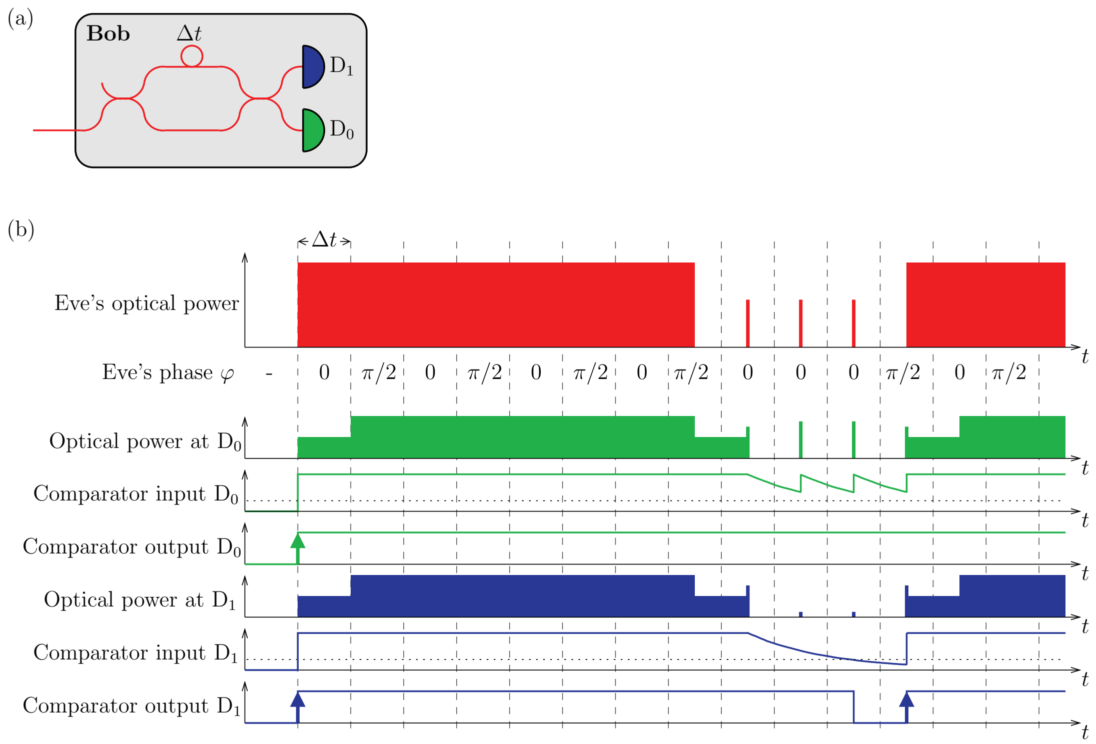


FIG. 8. (Color online) Proposed faked-state attack on the DPS-QKD system. (a) Bob's optical scheme. Δt is the time delay between the two interferometer arms. (b) Diagram showing Eve's optical output, how her light splits between the two Bob's detectors, and how the electrical signals in each detector react to it.

(similarly to [29, 50]) and form hotspots in that detector only, keeping the comparator input voltage above the threshold. In the other detector, the voltage is allowed to fall below the comparator threshold. Then a pulse is applied and causes a click only in the detector that has recovered. Eve can end her control diagram here, or repeat the long pulse (as shown in Fig. 8(b)) and then make another controlled click. The total length of such chained control diagram producing several controlled clicks is limited by low-frequency cutoff of the RF components, and in the case of our setup can be up to 500 ns. We remark that the short-pulsed parts of the diagram could in principle be replaced by a single phase-modulated long pulse, however short pulses may be easier to steer between Bob's detectors in case of sub-nanosecond Δt used in the modern DPS-QKD systems [36].

Interferometers used for DPS-QKD are of a sufficiently good quality to allow Eve an extinction ratio of at least 20 dB when routing her short pulses between the two Bob's detectors [36]. Examination of the recovery traces in Fig. 6 and hotspot formation probabilities in Fig. 7 suggests that the above control diagram will work. It should allow Eve to make clicks in Bob deterministically, or close to deterministically, in a wide range of comparator threshold voltages and Δt, even for $\Delta t = 100$ ps [36] or/and a threshold voltage above 20 mV. Eve should be able to vary the number of short pulses during the recovery to suit these system parameters, and still induce clicks in the correct detector most of the time.

Our present experimental setup did not allow us to verify this control diagram experimentally for all combinations of threshold voltages and Δt. However, we have verified that the detector is controllable as expected for a simulated $\Delta t = 5$ ns and threshold setting of 11.6 mV. We used a 2 mW peak power, 53 ns long pulse (with 1 mW, 5 ns steps at the sides as per diagram in Fig. 8(b)). We added 5 or 10 ns behind it a single 53 ps FWHM short pulse, and measured the click probability by the SR400 counter while varying the short pulse energy. With an energy difference that simulated interferometer extinction ratio of 20 dB, control over the detector was nearly perfect: probability of a click induced at 10 ns in the wrong detector was $< 0.005\%$, in the right detector $> 99.7\%$. At simulated 10 dB extinction ratio, the wrong detector click probability was $< 1\%$. Jitter of the clicks caused by the short pulse was 250 ps FWHM, while that of clicks caused by the long pulse leading edge was 170 ps FWHM.

V. DISCUSSION AND CONCLUSION

The experimental results show that the control of this SSPD is nearly perfect. Therefore, if this SSPD were used in a QKD system, an eavesdropper could use bright illumination to capture the full raw and secret key, while introducing negligible errors.

While the SSPD is based on different physics than the APD single-photon detector, the similarity in how they can be controlled is startling. Latching the SSPD using bright illumination can be considered as permanently blinding it, without the need for additional illumination to keep it blind. In the latched/blind state, the SSPD exhibits the same superlinear response to bright trigger pulses as a blind APD. Likewise, controlling the SSPD using deadtime extension is nearly identical to controlling the APD using deadtime extension: the only difference is that for this SSPD the low-frequency cut-off of the RF components (and on a longer time scale the latching phenomenon) limits how long the deadtime can be extended.

Countermeasures against bright illumination attacks have been discussed extensively [22, 23, 27, 32, 51–53], and most of the countermeasures are equally applicable to SSPD-based detectors. To summarize the discussion, detectors should be designed in a provably secure way. For instance, in an installed QKD system, latching can be avoided either by an automated reset, or by including a shunt resistor in parallel with the nanowire [54]. However, this does not guarantee that latching is precluded for all types of external input, and more importantly this countermeasure does not fit into a security proof. Therefore, detector control based on both latching and deadtime extension should be avoided by including a calibrated light source inside Bob, randomly testing, and thereby guaranteeing the single photon sensitivity at random times as modelled in the security proof [53].

As mentioned in the introduction, SSPDs are still in their infancy, and therefore our findings might not apply to other detector designs. However, our findings clearly demonstrate that unless detector control is specially considered during design, SSPDs may be controllable using bright illumination, just as their APD-based cousins. The early stage of SSPD technology is an excellent opportunity to avoid detector control vulnerability for future generations of SSPDs. Designing hack-proof detectors will be crucial for the success of QKD.

ACKNOWLEDGMENTS

We thank A. Korneev, R. Hadfield and V. Burenkov for useful discussions. This work was supported by the Research Council of Norway (grant no. 180439/V30), Ontario Center of Excellence (OCE) and National Research Council of Canada (NSERC). L.L. and V.M. thank Institute for Quantum Computing for travel support during their visit to Waterloo.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, Bangalore, India, 1984) pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[5] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[7] D. Mayers, in *Proceedings of Crypto'96*, Vol. 1109, edited by N. Koblitz (Springer, New York, 1996) pp. 343–357.
[8] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[9] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).
[10] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. **4**, 325 (2004).
[11] H.-K. Lo and J. Preskill, Quant. Inf. Comp. **7**, 431 (2007).
[12] Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A **77**, 052327 (2008).
[13] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **9**, 131 (2009).
[14] L. Lydersen and J. Skaar, Quant. Inf. Comp. **10**, 60 (2010).
[15] Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).
[16] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).
[17] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[18] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006), erratum ibid. **78**, 019905 (2008).
[19] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **7**, 73 (2007).
[20] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).
[21] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).
[22] V. Makarov, New J. Phys. **11**, 065003 (2009).
[23] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[24] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, arXiv:1103.2327 [quant-ph].
[25] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).

[26] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[27] I. Gerhardt, Q. Liu, J. Skaar, A. Lamas-Linares, C. Kurtsiefer, and V. Makarov, arXiv:1011.0105 [quant-ph].

[28] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, arXiv:1101.5289 [quant-ph].

[29] L. Lydersen, J. Skaar, and V. Makarov, J. Mod. Opt. **58**, 680 (2011).

[30] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).

[31] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, arXiv:0809.3408 [quant-ph].

[32] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010).

[33] L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, arXiv:1106.2119 [quant-ph].

[34] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).

[35] R. H. Hadfield, J. L. Habif, J. Schlafer, R. E. Schwall, and S. W. Nam, Appl. Phys. Lett. **89**, 241129 (2006).

[36] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photonics **1**, 343 (2007).

[37] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).

[38] D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, R. J. Hughes, and J. E. Nordholt, New J. Phys. **11**, 045009 (2009).

[39] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, Opt. Express **18**, 8587 (2010).

[40] Testing was restricted to one sample owing to difficulty of gaining access to more samples. One reason for this was that high-power illumination was initially assumed to be potentially lethal to the devices. However, the sample we tested survived undamaged. In fact, the measurement in Sec. III A suggests that the maximum temperature of the nanowire under 20 mW, 1550 nm continuous-wave illumination stayed relatively low, because only a part of the nanowire rose above the superconducting transition temperature of ∼ 10 K.

[41] M. K. Akhlaghi and A. H. Majedi, in *IEEE Lasers and Electro-Optics Society, 2008. LEOS 2008. 21st Annual Meeting of the* (2008) pp. 234–235.

[42] J.-L. F.-X. Orgiazzi and A. H. Majedi, IEEE Trans. Appl. Supercond. **19**, 341 (2009).

[43] Z. Yan, M. K. Akhlaghi, J. L. Orgiazzi, and A. H. Majedi, J. Mod. Opt. **56**, 380 (2009).

[44] J. K. W. Yang, A. J. Kerman, E. A. Dauler, V. Anant, K. M. Rosfjord, and K. K. Berggren, IEEE Trans. Appl. Supercond. **17**, 581 (2007).

[45] A. J. Annunziata, O. Quaranta, D. F. Santavicca, A. Casaburi, L. Frunzio, M. Ejrnaes, M. J. Rooks, R. Cristiano, S. Pagano, A. Frydman, and D. E. Prober, J. Appl. Phys. **108**, 084507 (2010).

[46] The measurement in Figures 3 and 4 was taken some days apart from the measurement in Fig. 2. Unfortunately it seems we had an optical and/or polarization alignment problem during the former: the detector is ∼ 3 times less sensitive in Figures 3 and 4 than in the rest of the paper, with its behaviour being otherwise consistent except for the scale factor of ∼ 3 on the optical power.

[47] A. Verevkin, J. Zhang, R. Sobolewski, A. Lipatov, O. Okunev, G. Chulkova, A. Korneev, K. Smirnov, G. N. Gol'tsman, and A. Semenov, Appl. Phys. Lett. **80**, 4687 (2002).

[48] M. K. Akhlaghi and A. H. Majedi, IEEE Trans. Appl. Supercond. **19**, 361 (2009).

[49] Y. Nambu, T. Hatanaka, and K. Nakamura, Jpn. J. Appl. Phys. **43**, L1109 (2004).

[50] V. Makarov and J. Skaar, Quant. Inf. Comp. **8**, 622 (2008).

[51] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nat. Photonics **4**, 800 (2010).

[52] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 801 (2010).

[53] L. Lydersen, V. Makarov, and J. Skaar, Phys. Rev. A **83**, 032306 (2011).

[54] R. Hadfield, private communication (2011).

Paper M

Comment on "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography"

Submitted to Applied Physics Letters.

arXiv: 1106.3756 [quant-ph]

Comment on "Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography"

Lars Lydersen,[1, 2, *] Vadim Makarov,[1, 2] and Johannes Skaar[1, 2]

[1] *Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway*
[2] *University Graduate Center, NO-2027 Kjeller, Norway*

Quantum key distribution (QKD) has initially been proven secure using ideal devices. However, implementations use imperfect devices available with current technology. Therefore, there are security proofs for QKD which model the devices to allow these imperfection, though at the expense of a lower secure key rate. To achieve provable security, it is crucial that the devices and implementations are verified to be within the models in the security proofs.

Security loopholes have been found originating from discrepancies between the actual implementations and the models in the security proofs. For instance, one such discrepancy allows the tailored bright illumination attacks [1–3], recently shown also to be applicable against superconducting single-photon detectors [4, 5]. In this case the loophole is caused by the response of qubit measurement devices (detectors) to swarms of qubits (bright illumination). The question is how to counter such loopholes.

In their paper, Yuan *et al.* propose to counter these bright illumination attacks by monitoring the avalanche photodiode (APD) current for "anomalously high values" [6]. The robustness of this countermeasure is shown by arguing that previously proposed attacks do not work anymore. First of all, this leaves the challenge of determining what is "anomalously high". In order to achieve provable security, this threshold must originate from a security proof. Secondly, the fundamental issue, namely that the detector response deviates from the models in the security proofs [7], is not solved by this countermeasure.

As discussed previously [8, 9], practical QKD cannot become provably secure by intuitive countermeasures against known attacks. This approach also requires manufacturers to make frequent, possibly costly upgrades to their systems. Loopholes should instead be countered by modifying the implementation and/or the security proofs such that the devices are within the models of the security proofs. This is the only way practical QKD can obtain the provable security that makes it superior to classical key distribution schemes. This is also how loopholes have been handled previously: for example, the photon-number splitting attack [10] led to more general security proofs [11] and eventually more efficient protocols to negate the decrease in the key rate [12]. In another example, detector efficiency mismatch [13], enabling for instance the time-shift attack [14, 15], is now included in security proofs [16, 17]. For the bright illumination attacks, we have proposed a secure detection scheme which integrates with security proofs [18]. In this scheme, a calibrated light source is used to verify the quantum efficiency in the center of the detector gate. Randomizing detection events outside the center of the gate provides a lower bound on the fraction of detections in the center of the gate.

In this particular case, we have already shown that an eavesdropper using temporally tailored light of short pulses containing less than 120 photons can threaten the security of QKD [4]. This faint after-gate attack would not be detectable with the countermeasure proposed by Yuan *et al.*, since the pulses would not cause an "anomalously high" current, but rather a current similar to the current caused by a single photon. Therefore, this serves as an example of the risk associated with closing loopholes in an intuitive way.

[1] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[2] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010).

[3] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).

[4] L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, arXiv:1106.2119 [quant-ph].

[5] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, arXiv:1106.2396 [quant-ph].

[6] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Appl. Phys. Lett. **98**, 231104 (2011).

[7] There are security proofs including this detector response in their model of the receiver (for instance Ref. [17]), but they predict zero secret key rate for such receivers.

[8] Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nat. Photonics **4**, 800 (2010).

[9] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 801 (2010).

[*] lars.lydersen@iet.ntnu.no

[10] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[11] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. **4**, 325 (2004).
[12] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[13] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006); Erratum ibid. **78**, 019905 (2008).
[14] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **7**, 73 (2007).
[15] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[16] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **9**, 131 (2009).
[17] Ø. Marøy, L. Lydersen, and J. Skaar, Phys. Rev. A **82**, 032337 (2010).
[18] L. Lydersen, V. Makarov, and J. Skaar, Phys. Rev. A **83**, 032306 (2011).