NTNU
Norwegian University of
Science and Technology

Security of QKD-systems with detector efficiency mismatch

Lars Vincent van De Wiel Lydersen

Master of Science in Electronics
Submission date: November 2008
Supervisor: Johannes Skaar, IET

Norwegian University of Science and Technology
Department of Electronics and Telecommunications

Problem Description

One of the most promising applications of quantum information theory is quantum key distribution (QKD). Unconditional security of QKD has been proved for ideal systems and also for systems with certain imperfections. QKD over distances of more than 100 km have been realized, both in optical fibers and free space. Today there are at least three commercial suppliers of QKD-systems.

Nevertheless, several security loopholes have been discovered in implementations, many of which exploit so called side-channels. One category of such imperfections is basis- and bit-dependent detector flaws, such as detector efficiency mismatch. The task is to study this loophole in detail, and try to close it such that QKD can approach unconditional security in real implementations.

Assignment given: 15. January 2008
Supervisor: Johannes Skaar, IET

Abstract

The rules of quantum mechanics makes it possible to exchange a secret key at a distance. This is called quantum key distribution (QKD). In theory the key exchange can be made completely secure. Real QKD implementations however, has numerous imperfections. Luckily one has also been able to prove the security of QKD with a large variety of imperfections. The field of QKD has matured over the recent years, and it has now reached commercial applications with photons as the quantum bits, and optical fibers as the quantum channel. Today there are at least three commercial vendors of QKD-systems.

We live in the times of *quantum hacking*. Researchers has begun the task of breaking the security of QKD-systems. Many new imperfections has been discovered, some of which might be used to break the security of QKD. This thesis is a study of the detector efficiency mismatch loophole. Most QKD-systems require two detectors, and it is virtually impossible to make two identical detectors with the exact same efficiency. What is worse, it turns out that the eavesdropper can often control the relative efficiencies of the two detectors trough some domain, for instance by controlling the timing, the frequency or the spacial mode of the photons. This can in turn be used by the eavesdropper to gain information about the secret key.

Previously the best known attack would compromise security if the detector efficiency mismatch of about 1:15. Here the current attacks on systems with detector efficiency mismatch are improved to compromise security for a mismatch of about 1:4. This is less than the mismatch found in a commercial QKD-system, so the attack could in principle be used to eavesdrop on this QKD-system.

One might try to close the loophole by modifying the implementation. One suggestion is the *four state Bob*. The problem is that this patch will in turn open other loopholes, and one of these loopholes reopen the detector efficiency mismatch loophole.

One can remove Eves information about the key by doing a sufficient amount of extra privacy amplification. Here a general security bound is presented, quantifying the required amount of extra privacy amplification to remove Eve's information about the key. The proof is more general than the previous security proof, and is valid for any basis dependent, possibly lossy, linear optical imperfections in the channel and receiver/detectors. Since this is more realistic assumptions for a QKD-implementation, the proof represents a major step of closing the loophole in real devices.

Contents

1 Introduction and history

The word cryptography originates from Greek and is composed by the words *kryptos* which means hidden, and *graphein* which means writing. Together it means that cryptography is the knowledge of writing messages such that its contents are hidden for anyone but the intended receiver. The ability to encrypt messages has been very important thoughout the times from ancient Greece, to today's widespread use of the internet. A new direction has evolved for the last 20 years, sprouting from quantum physics. Cryptography is no longer based on some complicated coding scheme, but is rather based on the laws of quantum mechanics.

1.1 Common terms in cryptography

Before going further into the field of cryptography it is usefull to establish some commonly used terms in cryptography. The task of finding weaknesses or breaking an 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 or cipher. The goal of all cryptographic schemes is that the sender commonly named *Alice* wants to send information to the receiver *Bob*, without the eavesdropper *Eve* getting any the information.

1.2 Classical cryptography

One of the first known ciphers is the so called *Caesars cipher*, used by Julius Caesar to communicate with his generals during his military campains. In Caesars cipher each letter of the plaintext was replaced by a letter some steps lower in the alphabet. The encryption is easily broken as one could try all 25 shifts in the alphabet to find the one which produces a meaningful meassage. The concept of replacing letters was actually used by the Germans in the famous Enigma machines during the second world war. Here the shift in the alphabet was changed for each letter in a complicated fashion.

The two main classes of classical cryptographic schemes is called *symmetric key*, and *asymmetric key* cryptography. In symmetric key cryptography also called *private key* cryptography, Alice and Bob shares a secret, private, and preferably random keystring[1]. This key can then be used to encrypt and decrypt messages in some cryptographic scheme.

Gilbert Vernam invented the *One-time pad* cipher in 1917 [1]. In the one-time

[1] If the keystring is not random, it reduces an brute-force attack since Eve only has to search for the probable keystrings. An example of this is the dictionary attacks used today, where the attacker assumes that a common word is used.

pad the ciphertext is obtained by performing an exclusive or (XOR) operation[2] with each bit of plaintext and a bit of the secret key. 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. The unconditional security (see section 4.3) of the one-time pad was proved from information theoretic principles by Shannon in 1949 [2]. This result is important and simple to show, so let us revise it here. Assume a n-bit message $M \in (\mathbb{Z}_2)^n$ where $P(M = m)$ followes some probability distribution. Further assume a random, secret key $K \in (\mathbb{Z}_2)^n$ where $P(K = k) = 1/2^n$. Let the ciphertext be denoted by $c \in (\mathbb{Z}_2)^n$. All possible keys k maps m into all possible ciphers c in $(\mathbb{Z}_2)^n$. Therefore 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

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

Now we can use Bayes theorem to find that

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

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

Shannon further proved that any unconditional secure encryption scheme consumes at least as many bits of secret key as the message. This establishes the key distribution problem since it is difficult to estimate in before hand the amount of required key needed later. This has lead to then developed of cryptographic schemes where less key is consumed at the expense of a slightly weaker security level. The most important schemes are RC4, DES and AES which are widely used in computers today.

The key distribution problem has also lead to asymmetric key cryptography. This is also called *public key* 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 [3]. Two years later came the now so widely used RSA algorithm [4]. 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

[2] The XOR operation is equal to adding modulo 2 bitwise. Another way of looking at the XOR operation in the one-time pad is that it inverts the message bit if the secret key bit is 1 and leaves it untouched otherwise.

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 since the encryption key can be made publicly available. An eavesdropper obtains the encryption key and the ciphertext. It turns out that finding the decryption key with the knowledge of the encryption key is a factorisation problem which takes an exponential amount of time[3] with currently known algorithms on a classical computer. By selecting the proper keylength the average time to find the private key can be made arbitrarily large. It is however unclear if more efficient factorisation algorithms exist. One can conclude that 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 [5]. This makes public key cryptography is insecure in the presence of a scalable quantum computer. Even without quantum computers public cryptography offers no *forward secrecy.* Eve could could store the public key and the ciphertext until sufficient computational power is available, and decrypt the communication some time in the future.

This is where quantum cryptography comes to an rescue! The strange laws of quantum mechanics allows Alice and Bob to generate a secret, random key at a distance.

1.3 The history of quantum cryptography

In 1984 Charles Bennett and Gilles Brassard suggested the use of elementary particles to generate a secret random key at a distance [6]. The intuition comes from the fact that the laws of quantum mechanics generally does not allow a measurement of the properties of a particle without disturbing them. Alice sends random bits encoded in the properties of such particles to Bob. These random bits will later be used as a private key. If Eve tried to eavesdrop on the bits she would have to impose some disturbance to the properties particles while measuring them, and would therefore reveal her presence. If the particles were received undisturbed, the laws of quantum mechanics guarantees that no one has knowledge of the key. This means that the security of the key distribution is no longer based on computational complexity, but rather the known laws of physics.

The term quantum cryptography is somewhat inaccurate, the correct term is *quantum key distribution* (QKD) which is the term I will use troughout this thesis. The distributed key could now be used in a classical symmetric cryptographic

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

scheme, for instance the one-time pad which gives unconditional security.

The protocol proposed in 1984 is now known as the BB84 protocol from the names of its inventors. In essence 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 random bit. If they used different basis they discard the bits. Their common random bits is a private secret key. To check for eavesdropping they publicly compare a part of their key. A full review of BB84 is given in section 3.1.

Independently and without knowledge of Bennett and Brassards findings, Arthur Ekert proposed to use entangled states to perform key distribution [7]. His intuition came from the fact measuring each of the two particle in an entangled state the measurement results will be completely correlated, even if the two particles are measured at a distance. These strong quantum correlations will necessarily violate the Bell inequalities [8]. Any measurement on an entangled state, it brings "local reality" [9] to the properties of the particle such that further measurements will not violate the Bell inequalities, and therefore it is possible to reveal any eavesdropper. In fact, one could even allow the eavesdropper to produce the entangled states.

The protocol Ekert proposed with entangled states is named the E91 or the Ekert protocol. Here Alice and Bob each has a half of entangled state. Then they measure in one of two bases to obtain the bits in the secret key. Again the same basis choice gives perfectly correlated results, so the bits where Alice and Bobs picked different bases are discarded. 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 [10, 11].

In 1992 Bennett showed that it is possible to perform QKD with only two non-orthogonal states [12] in the so called B92 protocol.

The first experimental demonstration of a QKD-system was conducted by Bennett et al. in 1992 [13]. The experiment was on a lab bench with a 32 cm free space quantum channel, with the quantum states encoded in the polarization of photons. After this the interest for QKD rapidly increased, as did the experimental activity. Soon QKD was demonstrated in an optical commercial optical telecomcable over 23 km [14]. Currently the distances has been increased to 200 km for an optical fibre [15], and 144 km free space [16]. Today there exists more than three commercial companies which supply QKD-systems.

Theory also came a long way from the introduction of QKD in 1984. The first important discovery was privacy amplification [17], which makes it possible to remove Eve's partial knowledge about the secret key by discarding some of the key in from a public discussion. Afterwards the first security proofs for BB84 was established [18, 19, 20, 21], proving the unconditional security of BB84 under ideal conditions. In turn, people started considering the security of QKD with real devices and many security loopholes were closed [22, 23, 24]. Unfortunately most of the security analysis up until this time used an insufficient security definition (see section 4.2). In 2005 a new composable security definition was found [25], and subsequently most of the existing security proofs has been updated or patched to fit the requirements of the new security definition.

Recently multiple security loopholes has been found in various implementations, reaching beyond the assumptions considered in previous security proofs [26, 27, 28, 29, 30, 31]. Many of them are caused by so called *side channels* where Eve obtains information about the key by listening on various sources from the implementation, rather than eavesdropping on the quantum states them selves. The field of hacking QKD-systems is referred to as *quantum hacking*. This thesis is a study to close the security loophole caused by detector efficiency mismatch [26].

2 Theory and prerequisites

This section will briefly review some basic theory to give a general framework to understand concepts and theory about QKD. It mainly follows the book of Nielsen & Chuang [32] which is an excellent source of more in-depth material about the topics covered in this section.

2.1 Quantum mechanical bits

In general one may use the term quantum states, but in quantum information terms it is more common to talk about quantum mechanical bits, or *qubits*. A qubit is a quantum mechanical system in a two-dimensional state space. A quantum state can be imprinted in one or more qubits. Examples of physical systems corresponding to a single qubit is the polarization of a single photon or the spin of the electron.

While classical bits has the value 0 or 1, qubits can also be in a superposition of 0 and 1. The states 0 and 1 are denoted by $|0\rangle$ and $|1\rangle$ in Dirac notation. In general the state of a qubit may be expressed as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{3}$$

where $\alpha, \beta \in \mathbb{C}$. A measurement on the state $|\psi\rangle$ gives the result 0 with probability $|\langle 0|\psi\rangle|^2 = |\alpha|^2$. Likewise the result 1 will occur with probability $|\beta|^2$, thus $|\alpha|^2 + |\beta|^2 = 1$ since the result must be either 0 or 1.

The states $|0\rangle$ and $|1\rangle$ is known as the computational basis. The states are orthogonal, $\langle n|m\rangle = \delta_{nm}$ where $n, m \in \{0, 1\}$ and δ_{nm} is the Kronecker delta. $|0\rangle$ and $|1\rangle$ represent a basis so an arbitrary state $|\psi\rangle$ can be expressed as a sum of the basis states as in equation (3). Usually $|0\rangle$,$|1\rangle$ are the eigenstates of the Pauli Z operator, so the $|0\rangle$,$|1\rangle$ basis is called the Z basis.

Any basis can be used to express the states of a qubit. The eigenstates of the Pauli X operator is another important basis. Commonly called the X basis it can be expressed as

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \tag{4a}$$

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle. \tag{4b}$$

The X basis is orthogonal, $\langle +|-\rangle = 0$. A point of great importance is that given a qubit in one of the states in equation (4), a measurement in the computational basis ($|0\rangle$,$|1\rangle$) gives the results 0 and 1 with equal probabilities

$$|\langle 0|+\rangle|^2 = |\langle 1|+\rangle|^2 = |\langle 0|-\rangle|^2 = |\langle 1|-\rangle|^2 = \frac{1}{2}. \tag{5}$$

The state $|\psi\rangle$ in equation (3) can be expressed in the X basis (4) as

$$|\psi\rangle = \alpha'|-\rangle + \beta'|+\rangle = \frac{1}{\sqrt{2}}(\alpha - \beta)|-\rangle + \frac{1}{\sqrt{2}}(\alpha + \beta)|+\rangle. \tag{6}$$

2.2 Quantum computations and measurements

One of the postulates of quantum mechanics states that the time evolution of closed quantum systems is described by unitary transformations, i.e. that

$$|\phi(t_2)\rangle = U|\phi(t_1)\rangle, \tag{7}$$

where $U^\dagger U = I$ and t_1,t_2 are different times. This restricts the possible operations on qubits. Equation (7) makes it impossible to copy a qubit state, also known as the No-Cloning Theorem. This extremely important result is easily proved following [33]. A quantum cloning circuit is shown in figure 1. The lower left bit is an ancilla bit in a standard state which is to be transformed to $|\phi\rangle$ by the cloning circuit. Applying the circuit at both $|\psi\rangle$ and $|\varphi\rangle$ givens

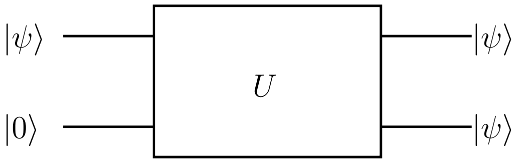

Figure 1: Quantum bit cloning circuit. The lower left bit is an ancilla bit in a standard state.

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle, \tag{8a}$$
$$U|\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle. \tag{8b}$$

Multiplying (8a) with (8b) transposed from the left gives

$$\langle\varphi|\langle 0|U^\dagger U|0\rangle|\psi\rangle = \langle\varphi|\psi\rangle = (\langle\varphi|\psi\rangle)^2, \tag{9}$$

which is valid only if $\langle\varphi|\psi\rangle$ equals to 0 or 1. This corresponds to ψ and φ being orthogonal, thus cloning a set of quantum states is impossible unless the set of states is orthogonal.

One can also interact with a qubit by measuring. First of all, measurements does not necessarily reveal the state of the system. In equation (3) the coefficients α and β are generally not accessible from a single measurement. They can however be estimated by the measurement statistics from preparing and measuring the state $|\psi\rangle$ many times.

Secondly after a measurement, the system is left in the state of the measurement result. If one measure a qubit in the $|+\rangle$ state in the Z basis, and obtain the measurement result 0, the qubit will be in the $|0\rangle$ state afterwards. The fact that one may perturb the system by measuring is a concept of great importance when proving the security of QKD. It may also appear quite counterintuitive as many other quantum mechanical phenomena.

2.3 Classical Information Theory

This section covers the most important results in classical information theory relevant for this thesis. For a full description see [34].

The core of classical information theory is to quantify the information of a stochastic variable X. The *Shannon entropy* of the stochastic variable X is a measure of how much information gained on average by an outcome of X, denoted by x. The Shannon entropy is given by

$$H(X) = -\sum_{x \in X} p(x) \log_2 p(x), \tag{10}$$

where $p(x) = P(X = x)$. $H(X)$ is the uncertainty about the outcome of the stochastic variable X. A nice interpretation comes from Shannon's noiseless coding theorem: the average number of bits required to store an outcome x is given by $H(X)$. As an simple example, assume four outcomes with equal probability 1/4. Then at least $H(X) = \log_2 4 = 2$ bits must be used to record an outcome. In other words, by getting to know the outcome we get 2 bits of information. As a different example, let only one of the four states occur. Now $H(X) = 0$, we get no information from an outcome x since the outcome is known in advance.

The entropy of binary probability distributions is frequently used, and is simply called the *binary entropy function* given by

$$H_{\text{bin}}(X) = h(X) = h(p) = -p \log_2 p - (1-p) \log_2 (1-p). \tag{11}$$

The binary entropy function is plotted in figure 2. Note that $h(1/2) = 1$. An important property of the binary entropy function is that it is *concave*. Graphically this means that all straight lines cutting the graph in figure 2 are below the graph. In an equation this can be expressed as

$$h(\sum_i p_i x_i) \geq \sum_i p_i h(x_i), \tag{12}$$

where p_i is the probability that the outcome is given by the binary probability distribution $\{x_i, 1 - x_i\}$.

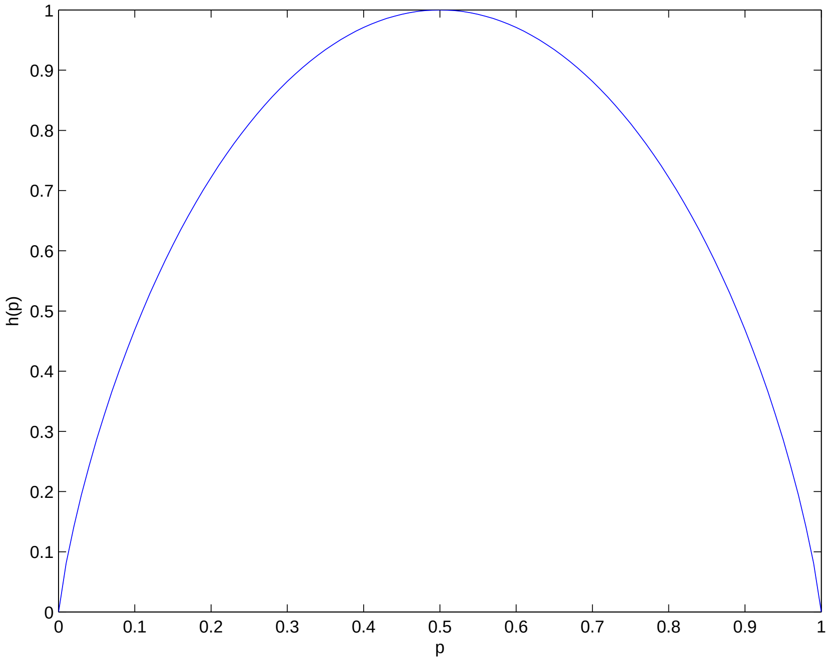

Figure 2: Plot of the binary entropy function given by equation (11).

Let X and Y be two random variables. Then the *joint entropy* of X and Y is defined as

$$H(X,Y) = -\sum_{x\in X, y\in Y} p(x,y)\log_2 p(x,y), \tag{13}$$

where $p(x,y) = P(X=x, Y=y)$. The *conditional entropy* of Y when X is known is given by

$$\begin{aligned} H(Y|X) = H(X,Y) - H(X) &= -\sum_{x\in X, y\in Y} p(x,y)\log_2 p(y|x) \\ &= \sum_{x\in X} p(x)H(Y|X=x), \end{aligned} \tag{14}$$

where the last equality is obtained by using that $p(x,y) = p(y|x)p(x)$. The conditional entropy can be interpret as the uncertainty about the outcome of X, when we already know the outcome of Y. The most important quantity of this section is the *mutual information* of X and Y, given by

$$\begin{aligned} I(X:Y) &= H(X) + H(Y) - H(X,Y) = H(X) - H(X|Y) \\ &= H(Y) - H(Y|X). \end{aligned} \tag{15}$$

$I(X:Y)$ is a measure of the mutual information content of the two stochastic variables X and Y.

All the quantities are summarized in the Venn diagram in figure 3.

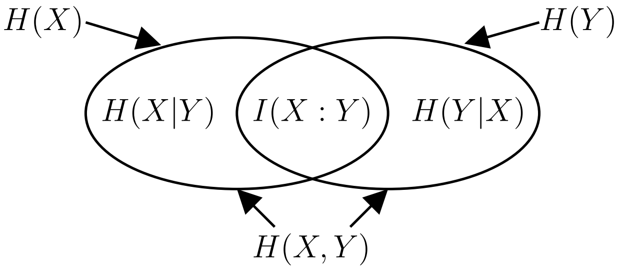

Figure 3: Venn diagram of the joint entropy, the conditional entropies and the mutual information of the stochastic variables X and Y.

Now consider the case when both X and Y are binary stochastic variables, that is $x, y \in \{0, 1\}$. Let X and Y have uniform probability distributions. Then $H(X) = H(Y) = h(1/2) = 1$. Further let y be equal to x with probability $1-p$ for both values of x, in other words $P(X = 0, Y = 0) = P(X = 1, Y = 1) = 1 - p$ and $P(X = 0, Y = 1) = P(X = 1, Y = 0) = p$. This is a typical scenario where Alice sends an equal amount of both bit values, and Bob has the receive error probability p. Under this conditions the mutual information can be found by using equations (15) and (14)

$$I(X:Y) = h(Y) - \sum_{x \in X} p(x) H(Y|X = x) = 1 - h(p). \tag{16}$$

This expression for the mutual information will be used frequently. Note that the mutual information increases very fast when the error probability p approaches 0 or 1[4]. Expression (16) with the inequality (12) shows that having many different error probabilities for different groups of bits, yields a higher mutual information, than having the same average error probability for all bits.

2.4 Optimal measurement on two non-orthogonal states

Information theory can be used to show a result which will be needed later: assume that the two bit values are encoded in two non-orthogonal states. The task of identifying the bit value is equal to identifying the state of the qubit. Further we can allow the two states to have non equal a priori probabilities. What is the maximum mutual information between the receiver measuring the qubits, and the sender of the qubits?

[4] Having an error probability equal to 1 means that the two bit strings are the inverse of each other. Knowing the inverse of an bit string is the same as knowing the bit string itself.

The fact that the two states are non-orthogonal makes it impossible to measure the bit value encoded in the states deterministically. If this was possible it would allow a qubit cloning circuit!

When the states have equal a priori probabilities, the problem has a known solution [35, 36]. Let $|\psi_0\rangle$ and $|\psi_1\rangle$ denote the two states which have the same a priori probabilities, and let the angle between the states be denoted by φ. Then the optimal measurement gives a probability p of a correct measurement equal to

$$p = \frac{1}{2} + \frac{1}{2}\sin\varphi. \tag{17}$$

Several papers [35, 37, 38, 39] claim to have found the optimal measurement on two non-orthogonal states with different a priori probabilities. Most of the calculations of this information assumes that the optimal measurement is a projective measurement. The only paper attempting a rigorous proof is [37]. I find the proof incomplete as it assumes only two POVM elements in the measurement without justification. It is not obvious to me that the optimal measurement has only two POVM elements. In fact [40] gives an example where three non projective POVM elements give more information than two projective measurement elements. Since many recognized sources use the result that the optimal measurement is projective [35, 39, 41], I choose to do so without fully accepting the proof [37].

Now let us optimize the measurement by assuming that the measurement is projective. Let the a priori probabilities of $|\psi_0\rangle$ and $|\psi_1\rangle$ be q and $1-q$. Figure 4 gives a geometric representation of the states and measurement operators. Here the angle θ is the variable to optimize. With the coordinate system in figure 4, the states ($|\psi_0\rangle$,$|\psi_1\rangle$) and the measurement operators ($|P_0\rangle$,$|P_1\rangle$) can be expressed as

$$|\psi_0\rangle = |0\rangle \tag{18a}$$
$$|\psi_1\rangle = \cos\varphi|0\rangle + \sin\varphi|1\rangle \tag{18b}$$
$$|P_0\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle \tag{18c}$$
$$|P_1\rangle = \sin\theta|0\rangle + \cos\theta|1\rangle. \tag{18d}$$

For a given angle θ, the probability of measuring the correct bit value is given by

$$\begin{aligned} p &= q|\langle P_0|\psi_0\rangle|^2 + (1-q)|\langle P_1|\psi_1\rangle|^2 \\ &= q\cos^2(\theta) + (1-q)\sin^2(\theta+\varphi), \end{aligned} \tag{19}$$

where q is the a priori probability for state $|\psi_0\rangle$. The θ which maximizes p, θ' is

$$\tan 2\theta' = \frac{\sin 2\varphi}{\frac{q}{1-q} - \cos 2\varphi}. \tag{20}$$

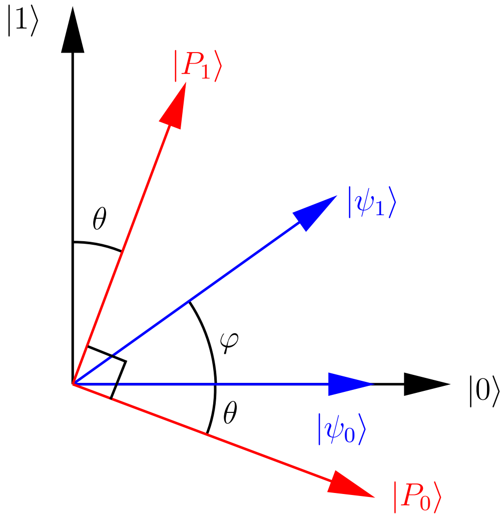

Figure 4: A geometric representation of states and the projective measurement operators. The two states to be distinguished are $|\psi_0\rangle$ with a priori probability q and $|\psi_1\rangle$ with a priori probability $1-q$, and the projective measurement operators are $|P_0\rangle$ and $|P_1\rangle$. φ is the angle between the states and θ is the angle to optimize.

The maximum probability of measuring the correct bit value is therefore

$$\begin{aligned} p = q\cos^2((1/2)\arctan(\frac{\sin 2\varphi}{\frac{q}{1-q}-\cos 2\varphi})) \\ + (1-q)\sin^2(\varphi + (1/2)\arctan(\frac{\sin 2\varphi}{\frac{q}{1-q}-\cos 2\varphi})). \end{aligned} \tag{21}$$

If $q = 1/2$ the expression reduces to equation (17) as expected.

The case to be considered here is the following; the sender *Alice* sends the bit values 0 and 1 with equal probabilities. *Eve* receives the two bits encoded in two non-orthogonal states. For each bit a third party *Fred* has some information of the bit value in terms of a probability distribution q,$1-q$ for the bit value. Fred gives this information to Eve who use it to improve her measurement. See figure 5. Let A denote Alice's bits and hence Alice's information, and let E denote Eve's bits and Eve's information. Then under these conditions the mutual information between the sender Alice and the receiver Eve (who has Fred's information) is symmetric, and is given by equation (16)

$$I(A:E)) = 1 - h(p), \tag{22}$$

where p is given by equation (21). The result differs from the result in [37, 38, 39]. This is because the papers maximise the information from a measurement on two

$$\begin{tikzcd}
\textbf{Alice} \arrow[r] & \textbf{Fred} \arrow[r] & \textbf{Eve} \\
\{\frac{1}{2},\frac{1}{2}\} \arrow[r] & \{q,1-q\} \arrow[r] & \{p,1-p\}
\end{tikzcd}$$

Figure 5: Alice sends the two bit values with equal probabilities. Fred has knows the bit value probability q and which he gives to Eve. She does her final measurement to achieve the final bit probability p.

bits which are sent with different a priori probability. The information calculated in these papers can be expressed in our terms as $I(A:(E|F))$. It can be shown that

$$I(A:E) = I(A:F) + I(A:E|F). \tag{23}$$

The Venn diagram in figure 6 shows the information of Alice, Fred and Eve. Note

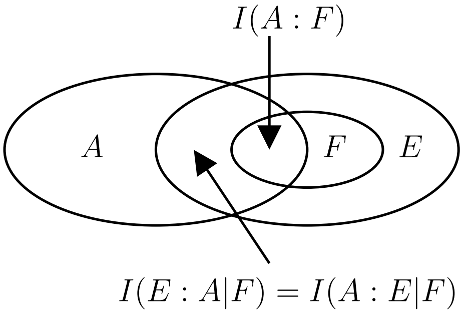

Figure 6: Venn diagram of the information of Alice, Fred and Eve. Since Fred gives all his information to Eve, F is contained in E.

that $H((A|F)|E) = H(A|(F,E))$. Further note that since F is contained in E, $H(F,E) = H(E)$. It is now possible to show the result (23) by using the definition of mutual information (15):

$$\begin{aligned} I(E:A|F) + I(A:F) &= H(A|F) - H((A|F)|E) + H(A) - H(A|F) \\ &= H(A) - H((A|F)|E) = I(A:(F,E)) \\ &= H(F,E) - H((F,E)|A) = H(E) - H(E|A) \\ &= I(A:E). \end{aligned} \tag{24}$$

An expression for the information $I_0 = I(A:E|F)$ can for instance be found as equation (3.263) in [39]. $I(A:F)$ is given by $1-h(q)$ from equation (16). It is verified numerically that $I(A:E) = 1-h(p) = I(A:E|F)+I(A:F) = I_0+1-h(q)$ for all q, so the result (22) coincides with the previous results [37, 38, 39].

3 Principles of QKD

3.1 BB84 protocol

The BB84 protocol is the first QKD-protocol which was proposed, implemented and proved unconditionally secure [6, 10, 42, 11]. It has the advantage of being very intuitive and easy to understand, but it might not be the optimal protocol to implement in practice.

QKD-protocols usually require Alice and Bob to be connected with a quantum channel which can carry qubits, and a classical channel. Eve is allowed to do anything allowed by the physical laws of nature with the quantum channel. The classical channel is authenticated[5] by Alice and Bob, thus Eve can read all the information on the classical channel but is not able to alter the information on the classical channel. To authenticate the channel a parts of a previously secret key is used[6]. Therefore QKD is often referred to as a secret growing protocol.

BB84 protocol:

1. Alice generates $4m + \epsilon$ random classical bits, and for each bit she randomly chooses the X or the Z basis. For each bit she generates a qubit and sends it to Bob. If the bit is 0 she sends $|0\rangle$ or $|-\rangle$, and if the bit is 1 she sends $|1\rangle$ or $|+\rangle$.

2. Bob measures the $4m + \epsilon$ qubits in a random basis; either the X or the Z basis. As seen in section 2.1 Bob's measurement result will be equal to Alice bit if they used the same basis. Otherwise the measurement result will be random. This initial key is often called the *raw key.*

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

4. Alice randomly selects half of the remaining bits and publicly announces the bit values. Bob compares Alice bit values with his measurement results to

[5] Unconditionally secure authentication schemes exists. Note however, that breaking the authentication after the secret key is generated does not compromise the security of the key. Therefore it is sufficient with protocols that guarantee the security for a limited amount of time.

[6] At first this might seem as a drawback in 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 communicates directly to Eve. Therefore all protocols require some preshared information about the parties. In QKD this is a random, private, 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.

probe for Eve's presence. From this set they can estimate the quantum bit error rate (QBER), and if it is sufficiently low they continue the protocol with the remaining m bit key. Otherwise discard the key and start over again.

5. This step is called *reconciliation.*Using the QBER estimate Alice sends Bob error correcting data to obtain equal keys. Further Alice and Bob calculates an upper bound on Eve's information about the key. They then perform privacy amplification (see section 3.3) to fully remove Eve's information about the key. In this step the m bit erroneous, partly secure key is reduced to an n bit identical, unconditionally secure key.

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

3.2 Example of an attack

Lets examine some simple attack strategies, and why they fail. 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 just measure her copy and obtain the bit value. But the no-cloning theorem (see section 2.2) makes it impossible to copy the qubit, so this strategy is physically impossible.

Let us see what happens if Eve tries to measure on the qubits sent by Alice. Since she does not know the basis used by Alice and Bob, she randomly makes a guess and randomly chooses the X or Z basis. For half the bits she will guess the correct basis, and she obtains the correct bit value. The qubit is unaffected by Eve's measurement, and Bob's measurement result will correspond to Alice bit value. No QBER is introduced. For the other half of the bits Eve will use the opposite basis as Alice and Bob. On those bits the probability to measure the same bit value as Alice is 50%. Further the qubit is passed on to Bob in the wrong basis, so independently of Eve's measurement, result Bob will have a 50% probability of measuring the bit value Alice sent. In other words Eve's attack will introduce a 50 % QBER for half of the bits, making a total of 25 % QBER.

This type of attack is called an *intercept-resend* attack, and will always compromise the security of the QKD. Obviously the acceptable QBER must be under 25 %. For a full discussion on the acceptable QBER see section 4.5. Eve could achieve an arbitrary low QBER by attacking just a fraction of the bits. Therefore a non zero QBER means that Eve might have some information about the key.

3.3 Privacy amplification

Assume that Alice and Bob has a 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* [17].

An nice intuitive algorithm goes as following: Alice announces that the two of the bits are to be replaced with the XOR of the two bit values. Now if Eve had the correct bit values with a 75 % probability she has the correct XOR with probability $0.75^2 + 0.25^2 = 0.625$. Thus Eve's information about the bit was reduced by discarding one bit.

In practice privacy amplification algorithms are a little bit different. It has turned out that the only privacy amplification algorithm that preseve composability (see section 4.2) is so called two-universal hashing. A hash function takes all 2^n inputs of length n to an output of length $m < n$. Since $n > m$ 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 $x, x' \in (\mathbb{Z}_2)^n$ then $p(f(x) = f(x')) \leq 1/2^m$. Alice and Bob randomly choose a function $f \in \mathcal{F}$, and lets the secret key be $s = f(x)$ 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 $f(x')$.

3.4 Implementations of QKD

An implementation of a QKD-system requires a physical realisation of qubits. The physical qubit must necessarily be some small particle obeying quantum mechanics. Further it should retain its quantum state for an arbitrarily long time (have a long coherence time). Finally the particles should be easy to prepared and measure. Today the only suitable particle is the photon as it is the only particle to keep its state while being transported over an acceptable distance. Light has been used by the telecom industry many years fibers, so sources and detectors has been explored in depth. The quantum state can be encoded into the polarization or the phase of the single photons.

A single photon source is difficult to manufacture, so most QKD-systems use faint laser pulses. The photon number of a laser pulse follows a Poisonian distribution. Attenuating the pulse to a low mean photon number gives a low probability of sending multiphotons.

With photons the quantum channel is either free space, or optical fibers. The main non-ideal effect from the channel is that both free space and optical fibers introduce substantial loss.

To detect single photons, most of the current QKD-systems use avalanche photon diodes (APDs). This is a highly reversed biased p-n junction. When a photon arrives it creates an electron-hole pair, and an avalanche of holes and electrons is generated in a self-amplifying process. This can be detected as a large current running trough the diode. After a detection event the current has to be stopped, and the device has to be reverse biased again. This operation is called *quenching* and causes a moment where the diode is insensitive to incoming photons, also called *dead time*.

Since any number of photons could cause a detection event, this is not really single photon detection, but rather threshold detection. It should also be noted that detectors do not have full quantum efficiency, a single photon incident to the detector does not always cause a click. Typical values is a quantum efficiency of 3-50 %.

An important parasitic effect is the *dark counts*. A dark count is a detection event which occurred without any photon incident to the detector, usually caused by thermal excitations. This is a challenge in QKD-systems since dark counts contributes to the QBER. When the dark count rates are to high to operate QKD-systems the detectors are usually gated. Then the detector is only sensitive during a time window when a photon is expected to arrive. This is the case for InGaAs APDs which are used in most setups with optical telecom fibers.

Figure 7 shows an example of a polarization encoded QKD-system. Alice system has four laser diodes, each followed by a 0, 45, 90 or 135 degrees polarizer. The random bit and basis choice is done by randomly toggling one of the four laser

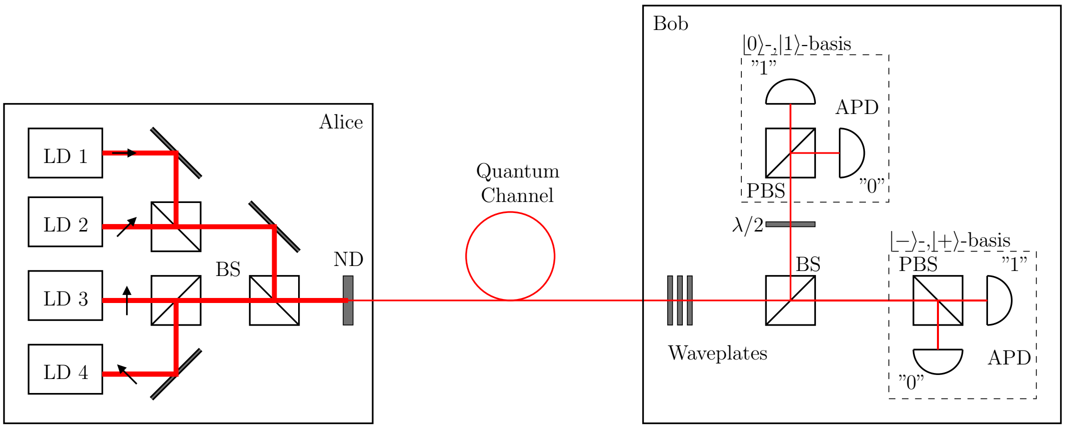

Figure 7: An implementation using the polarization of single photons. LD: laser diode. BS: beam splitter. ND: neutral density filter. PBS: polarizing beam splitter. $\lambda/2$: half wave-plate. APD: avalanche photodiode.

diodes, whose output is merged into a single beam. Finally a neutral density filter attenuates the beam to a sufficiently low mean photon number. In Bob's apparatus waveplates is used to revert any polarization transformation from the channel. Bob's basis choice is passively implemented by using a 50/50 beamsplitter. In one of the arms a half wave-plate is inserted to flip the basis. The detection of the two bit values is just a polarizing beam splitter with one APD in each arm. When a polarization encoded implementation was used in an optical telecom fiber over a distance of 23 km, it turned out that the heavily time-variant polarization transform of the fiber made the setup instable [14]. Polarization encoding is however suitable for implementations using free space [43].

In optical fibers QKD it is more suitable to use the phase of the single photons to encode the qubits. Figure 8 shows an example of such an implementation which is a large Mach-Zehnder interferometer used with single photons, and where Alice and Bob controls the phase shift in each arm. Alice setup consists of a source directly followed by a fiber coupler. Alice controls a phase modulator in one of the arms after the fiber coupler. Choosing a random bit and basis is equivalent to applying a random phase shift $\varphi_A \in \{0,\pi/2,\pi,3\pi/2\}$. In this setup, the quantum channel connecting Alice and Bob is two optical fibers. Bob controls a phase modulator located in the other arm, and his basis choice is performed by randomly setting the phase shift of his phase modulator $\varphi_B \in \{0, \pi/2\}$. After the phase modulator the two optical fibers are input to a beam splitter where each arm is terminated in an APD. If the phase difference $\varphi_A - \varphi_B$ is equal to 0 or π, the photon will exit a deterministic arm from Bob's beam splitter. If $\varphi_A - \varphi_B$ is equal to $\pi/2$ or $3\pi/2$, a random detector will fire. This is summarized in table 1. From the table it is easy to realize that a phase encoded system is topologically equal to the polarization encoded system.

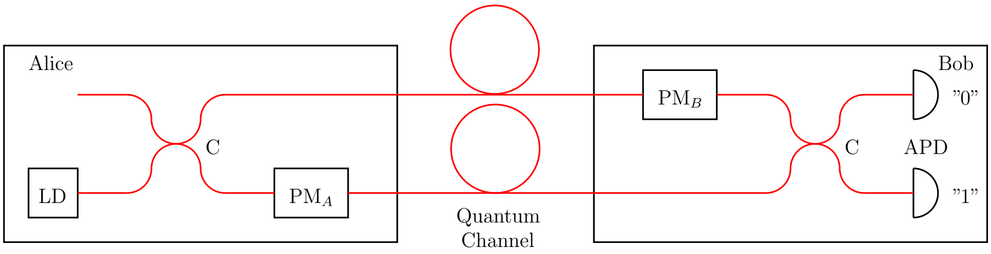

Figure 8: An implementation using the phase of single photons. LD: laser diode. C: fiber coupler. PM$_A$: Alice's phase modulator. PM$_B$: Bob's phase modulator. APD: avalanche photodiode. Alice randomly choose a phaseshift $\varphi_A \in \{0,\pi/2,\pi,3\pi/2\}$. Bob randomly choose a phase shift $\varphi_B \in \{0,\pi/2\}$. This setup is topologically equal to the polarization encoded system in figure 7.

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 1: The relation between Alice and Bobs bits, basis choice, measurements and the settings of the phase modulators.

The requirement with two optical fibers is of great disadvantage. In practice it turns out to be very difficult to keep the two arms in the interferometer stable. Two optical fibers is also twice the cost, thus a single fiber is preferable.

Figure 9 shows a phase encoded system which only require a single optical fiber. Bob generates a bright laser pulse which is injected into the system trough a circulator. Bob keeps his phase modulator at zero and the pulse is split into two different pulses distinctly polarized by the polarizing beam splitter. The two strong pulses travel to Alice where parts is split of into a classical detector to reveal any strong pulses interrogating the system [44, 45, 46, 47]. The other parts travel trough the phase modulator where Alice phase modulates only one the first pulse. Subsequently the pulses are reflected trough a Faraday mirror and attenuated to prevent multiphotons. Back at Bob the pulses are split according to their polarization, and Bob applies his basis choice in the phase modulator

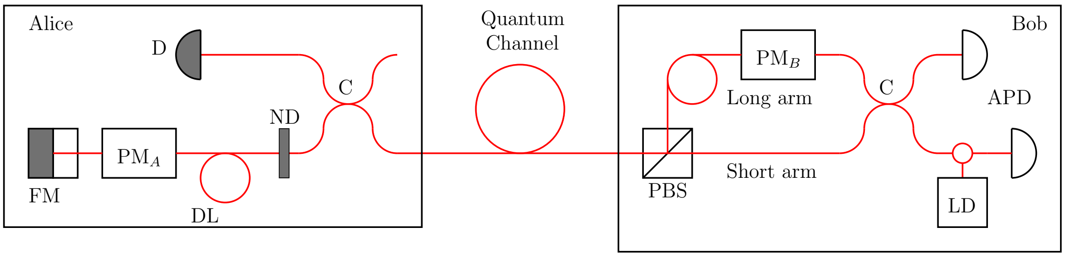

Figure 9: An implementation using the phase of single photons. FM: Faraday mirror. PM$_A$: Alice's phase modulator. C: fiber coupler. DL: optical delay line. ND: neutral density filter. D: classical detector. PBS: polarizing beamsplitter. PM$_B$: Bob's phase modulator. APD: avalanche photodiode.

before the pulses are detected according to table 1. Sending the pulses back, reflecting them in a Faraday mirror and sending them forth again will revert any transformation caused by the optical fiber. The system has been labled the *plug-and-play* system since it can use previously deployed optical fibers. The system has been implemented in experiments [48, 44] and is commercially available.

4 Security of QKD

4.1 Classes of attacks

So far the security of QKD has been based on the intuition that Eve cannot measure the qubits without disturbing their state. Quantum physics however, allow for much more powerful interactions than a measurement. Normally Eve's attacks are classified as follows:

- 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 3.2. A other more general attack could be to let the quantum system from Alice interact with a probe[7], and measure the probe later. There are different opinions whether the measurement of the probe is allowed after the classical post-processing [11], but I will use the term individual attack even if the probe is measured after the classical post-processing. Note that in any case every probe only interact with a single system from Alice, and every probe is measured equally.

- 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 interaction 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 use the same probe for many bits. Luckily there exists a theorem called the *exponential De Finetti theorem* which states that in the asymptotic limit of infinite keys, any coherent attack is not better than a

[7] A probe is a small quantum system i.e. a number of quantum bits starting in a standard state.

collective attack [49]. The theorem makes it is sufficient to prove the security against collective attacks.

4.2 Security definition

In the framework of QKD we would like a device which gives a random, secret key to Alice and Bob, while the information given to Eve is zero. This means that the best thing Eve could do is to try to guess the key. Unfortunately there exists no such device, so one need to loosen the security definition in a way, while making a framework in which leaked to the eavesdropper is quantified. The first attempt to create a feasible security definition was the following: "A QKD protocol is defined as being *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 string must also be essentially random." The security definition is very intuitive: the protocol should normally succeed, and Eve's mutual information with the key can be chosen arbitrarily small. Under this security definition the achievable secret key rate R is [50]

$$R \geq \min \left\{ I(A:E), I(B:E) \right\}. \tag{25}$$

In retrospect it turned out that the definition above was insufficient. The main reason is that the definition only considers the classical information *after* everybody has performed measurement on their quantum systems. Quantum mechanics however are quite counterintuitive, and it turns out that if Eve is given one extra bit of information before she measure her probe, this could unlock *more* than one bit of information. This extra information could easily come from some known-plaintext[8] attack when Alice and Bob applies the key in a one-time pad. The security criterion also turned out to lack *composabiltiy.* If the ϵ-secure secret key is used in an ϵ'-secure[9] task one need an estimate of the security of the composed process.

A proper security definition was found in 2005 [25]. The success criterion is equal but Eve's knowledge about the key is reformulated. 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. Then the key is ϵ-secure if $\frac{1}{1} || \rho_{ABE} - \rho_S \otimes \rho_E ||_1 \leq \epsilon$.

First of all ϵ has a nice interpretation in the new security definition. ϵ is the distinguishability advantage, meaning that the probability that Eve use her

[8] In a known-plaintext attack the eavesdropper knows some of the plaintext which is encrypted. An example could be the header of an e-mail, which is essentially equal every time. With the one-time pad the knowledge of some of the plaintext will reveal some of the secret key.

[9] The one-time pad is an example of a scheme which is 0-secure.

information to distinguish the QKD-system from a perfect QKD-system is given by ϵ.

The new security definition is composable, 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 the proper security definition, many of the security proofs and security frameworks are formulated for the old security definition. Luckily patches has been found for most security proofs and frameworks. Note also that the expression for the secret keyrate in equation (25) is still valid for security proofs restricted to individual attacks.

4.3 Unconditional security

It is possible to prove that QKD is *unconditionally secure*. Unconditional security means that the security is proved without restricting the attacker in computational power, time or physical access to the communication channel. Classical public key cryptography is an example of the contrary, where the security is proved with assumptions on the computational power of the adversary.

There are however some obvious assumptions in QKD[11]:

- Eve does not get any information about Alice and Bob's bases or bits from their QKD-systems, neither passively where the apparatus sends some signature in some domain, nor actively by interrogating their equipment.

- Random numbers are from true random number generators.

- Alice and Bob use a unconditionally secure authentication scheme on the classical channel (such schemes exists, for instance Wegman-Carter authentication).

- No physical theory invalidates the parts of quantum mechanics used for QKD, such as the uncertainty relation and the no-cloning theorem.

4.4 Optimal individual attack

The complexity of an attack on a QKD-system makes the range of possible attacks very large. Therefore only a small number of attacks has been analysed in depth. In the chase for the strongest possible attack the optimal individual attack has been found [41]. The attack is intuitive: the qubit from Alice interacts with a probe, which is measured after Alice and Bob reveals the basis. See figure 10 for the attack setup.

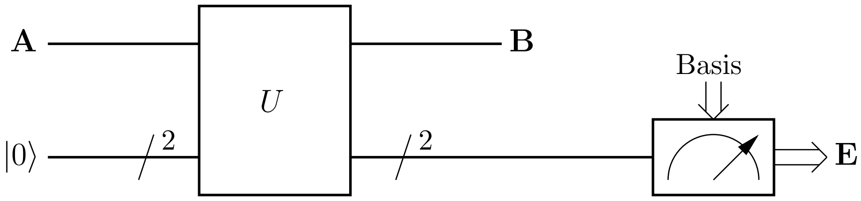

Figure 10: Schematics of the optimal individual attack. Eve's probe interacts with the bit from Alice trough an unitary transformation U. The basis information is used to optimize the measurement.

Without going into to much detail the main results are simply presented. After the basis is revealed Eve possesses one of two states [41]:

$$\rho_0 = (1-\delta)|\xi_0\rangle\langle\xi_0| + \delta|\zeta_0\rangle\langle\zeta_0|, \tag{26a}$$

$$\rho_1 = (1-\delta)|\xi_1\rangle\langle\xi_1| + \delta|\zeta_1\rangle\langle\zeta_1|, \tag{26b}$$

where δ is the QBER measured by Alice and Bob. The states used to express Eve's density operators in equation (26) can be expressed as

$$|\xi_0\rangle = |0\rangle|0\rangle, \tag{27a}$$

$$|\zeta_0\rangle = |0\rangle|1\rangle, \tag{27b}$$

$$|\xi_1\rangle = (\cos\theta|0\rangle + \sin\theta|1\rangle)|0\rangle, \tag{27c}$$

$$|\zeta_1\rangle = (\cos\varphi|0\rangle + \sin\varphi|1\rangle)|1\rangle, \tag{27d}$$

where the $|0\rangle$,$|1\rangle$ is used as a basis.

This means that the two bit values are encoded in two non-orthogonal states. Eve's task is to separate between the states labeled with 0 and 1 to determine the bit value. This can be done in the following way: The ξ states and the ζ states are orthogonal as seen by the second qubit in equation (27). This means that Eve is able to deterministically discriminate between them without disturbing the quantum state. In terms of the states expressed as above this corresponds to the projective measurement described by

$$P_\xi = I \otimes |0\rangle\langle 0|, \tag{28a}$$

$$P_\zeta = I \otimes |1\rangle\langle 1|. \tag{28b}$$

One remarkable feature of this attack is that Eve knows which bits are erroneous at Bob. If Eve obtains measurement result P_ξ, the bit is correct at Bob, while the measurement result P_ζ corresponds to a erroneous bit which contributes to the

QBER. In this attack alone this does not compromise security since Eve can read the error correcting data anyways.

Independent of the measurement result Eve's has two non-orthogonal states. [41] shows that Eve has the maximum mutual information with Alice when she has the same probability of measuring the correct bit value regardless of Bob's measurement result i.e. that $\theta = \varphi$. The angle φ is related to the introduced QBER δ as

$$\cos\varphi = 1 - 2\delta. \tag{29}$$

Regardless of which subspace Eve is considering, she now has to separate between the states $|0\rangle$, and $\cos\varphi|0\rangle + \sin\varphi|1\rangle$. This problem was considered in section 2.4 and the optimal measurement is given by equation (17) and gives a probability equal to

$$p = \frac{1}{2} + \frac{\sin\varphi}{2} = \frac{1}{2} + \sqrt{\delta(1-\delta)}, \tag{30}$$

where p is the probability for a correct measurement result. Eve's mutual information with Alice is given by equation (16)

$$I(A:E) = 1 - h(\frac{1}{2} + \sqrt{\delta(1-\delta)}), \tag{31}$$

where $h(\cdot)$ is the binary entropy function given by equation (11). $\delta = 1/2$ means that Eve takes the qubit, and sends a standard state to Bob. Then $I(A:E) = 1$ as expected. Likewise $\delta = 0$ meaning no interaction between the bit and the probe gives $I(A:E) = 0$.

Alice and Bob's mutual information is simply $I(A:B) = 1 - h(\delta)$. Since this is an individual attack the secure rate can be calculated by equation (25). Solving $R = 0 \Rightarrow I(A:B) = I(A:E)$ for δ gives

$$\delta = \frac{1}{2} - \frac{1}{2\sqrt{2}} \approx 14.6\%. \tag{32}$$

To my knowledge this is the best conventional attack found to date, and it compromises the security at 14.6 % QBER. In this respect it also constitutes an upper bound for the acceptable QBER. The attack is not implementable with current technology, since it requires both a quantum non-demolition measurement and quantum memory to store the probes. The attack has however been simulated [51].

4.5 Koashi's framework for proving security

It turns out to be extremely complicated to prove the security of QKD-protocols directly. Therefore the security proofs for QKD are usually constructed in the following way: first the security is proved for a virtual protocol. Then the real protocol is seen as a simplification, or some special case of the virtual protocol.

The security of QKD has been proved using several different frameworks [18, 19, 20, 21, 52, 53]. Most security profs with imperfections has used the entanglement approach to prove the security. To close the security loophole considered in this thesis the framework from Koashi [52, 54] is used, so this framework is sketched. Note that a patch has been found to let this framework fit the new security definition from section 4.2.

Koashi's security proof is based on the uncertainty principle. Here the intuition in the proof and the procedure of the proof is presented, rather than the rigorous proof it self. Assume that N qubits are measured in either the X or the Z basis, corresponding to observables $X \otimes X \otimes ... \otimes X \equiv X^{\otimes N}$ or $Z \otimes Z \otimes ... \otimes Z \equiv Z^{\otimes N}$. The entropic uncertainty relation [55] can then be formulated as:

$$H\left(X^{\otimes N}\right) + H\left(Z^{\otimes N}\right) = N. \tag{33}$$

Here $H(\cdot)$ denotes the entropy of the stochastic process from measuring in a basis. The idea is to use the entropic uncertainty relation (33) to upper bound Eve's information on the key.

The two bases are symmetric with respect to each other, so without lack of generality we assume that Alice and Bob always use the Z basis[10]. Let δ_{bit} and δ_{phase} be the QBER estimate in the Z and X basis.

For the N bits Eve's result is not dependent on what Bob is doing. Therefore, assume that Bob is measuring in the X basis. Bob does not measure in the X basis in reality, it is just used to estimate how well Bob could do such a measurement. Therefore Bob is allowed to do anything permitted by the laws of physics during the virtual X measurement.

Since the QBER in the X basis is estimated to be δ_{phase}, the entropy of the virtual X measurement is simply given by $Nh(\delta_{\text{phase}})$, where $h(\cdot)$ is the binary entropy function. This means that the best Z measurement anyone but Alice could do (including both Bob and Eve) has entropy equal to

$$H\left(Z^{\otimes N}\right) \geq N\left(1 - h(\delta_{\text{phase}})\right). \tag{34}$$

This is an upper bound on Eve's information about Alice bits; Eve need at least $H\left(Z^{\otimes N}\right)$ bits to have a perfect copy of the key. These bits are secret to Eve, and can thus be used as a secret key. Alice and Bob do however not have identical keys, because the QBER in the Z basis is non-zero. Classical error correction would require $Nh(\delta_{\text{bit}})$ bits of communication. Alice and Bob could simply use

[10] This is easily seen by labeling Alice and Bob basis choice as the Z basis, and labeling the opposite basis the X basis.

$Nh(\delta_{\text{bit}})$ bits of previously established secret key to encrypt this classical error correction. Thus the net secret key rate (secret bits pr. sifted bit) is given by

$$R \geq 1 - h(\delta_{\text{bit}}) - h(\delta_{\text{phase}}). \tag{35}$$

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

$$R \geq 1 - 2h(\delta). \tag{36}$$

Solving $R = 0$ gives $\delta = 0.11 = 11\%$. This bound can be used for the QBER in the absence of imperfections.

5 Implementation caused loopholes

The unconditional security of BB84 with *perfect* devices was established in section 4.5. The overview of some actual implementations in section 3.4 clearly shows that practical QKD face numerous imperfections, and some of them may cause security loopholes.

A loophole can be closed in two different ways. One possibility is to alter the implementation. This is necessary if the loophole completely reveals Alice bit value. An example of this is the recent discovery that Eve can control APDs with a powerful laser [30]. The disadvantages by changing the implementations are numerous. First of all it usually increases the complexity of the setup, and can open new implementation caused loopholes. One other disadvantage is that securing existing setups can be hard, and even impossible.

The other possibility is to include the imperfection in the security proofs, and increase the amount of privacy amplification. Many imperfections has been dealt with in this way [22, 23, 24]. The biggest advantage is that existing QKD installations can be secured with a simple software/firmware update. One disadvantage is that the secure key rate will be reduced, and this is the most important parameter in current commercial QKD devices. It is however not obvious that changing the implementation will perform better; adding components in the optical pathway will always increase the loss and therefore reduce the key rate.

5.1 The photon number splitting attack

The first big loophole that caught the community's attention is caused by the combination of coherent laser sources, large loss in the optical fiber and the limited quantum efficiency of the detectors. In security analysis one must assume that all loss is caused by Eve. In practice one could imagine that Eve replaces the fiber with a lossless quantum teleportation device.

The faint lasers does not always send single photons. The number of photons n in a coherent state is Poisson distributed

$$p_n = \frac{\mu^n e^{-\mu}}{n!}, \tag{37}$$

where μ is the mean number of photons per pulse. Usually $\mu \approx 0.1$ in practical devices. This means that the probability of sending an photon at all is given by

$$p_{n>0} = 1 - p_0 = 1 - e^{-\mu} \approx \mu. \tag{38}$$

When at least one photon is sent, the probability that more than one photon is sent is given by

$$\frac{p_{n>1}}{p_{n>0}} = \frac{1 - p_1 - p_0}{1 - p_0} = \frac{1 - \mu e^{-\mu} - e^{-\mu}}{1 - e^{-\mu}} \approx \frac{\mu}{2}. \tag{39}$$

Now Eve could attack the system with the photon number splitting attack (PNS attack). Since the photon number measurement commutes with measuring the polarization or the phase of the photon, it is possible for Eve to do a quantum non-demolition measurement and measure the photon number without disturbing the quantum state. If the pulse contains more than one photon Eve could split off, and store at least one photon until the basis is revealed. This would give Eve full information about the bit value.

This is not a problem alone, since most half of the pulses contains single photons. One must however assume that the loss is caused by Eve, so she might measure the photon number, and only remove single photons. Therefore one must assume that all loss is single photons and that all multiphotons are used in the PNS attack. A full deviation on how this limits the acceptable loss, and thus the transmission length can be found in [22]. It however simple to show how the rate R scales with the transmittance t. It is easy to realize that the number of bits sent by Alice and detected by Bob is given by $t\mu\eta$, where η is the detection probability of Bob's detector. Remember that μ was the probability to send a photon at all. The information lost to Eve in form of multiphotons is given by $\mu\frac{\mu}{2}\eta$. Eve's equipment can be placed right after Alice equipment, so Eve does not suffer the loss in the channel t. The bit must however be detected by Bob. Therefore an simplified expression for the rate is given by

$$R = t\mu\eta - \frac{\mu^2}{2}\eta. \tag{40}$$

Optimisation gives $\mu = t$, thus the rate scales as $R \propto t^2$. Further the dark counts will lower bound the rate so t can not become arbitrarily low. The first way to tackle this problem was with a new protocol called the SARG04 protocol [56]. In this protocol the rate scales as $R \propto t^{\frac{3}{2}}$.

The proper solution turned to be *decoy states* [57, 58, 59]. Instead of using a single mean photon number μ, Alice might choose randomly from several different intensities $\mu_1, \mu_2, ...$ It is impossible for Eve to determine which intensity is used by Alice, so she has to treat the pulses independently of the photon number used by Alice. In the post processing stage Alice and Bob estimate the transmittance for each mean photon number $t_1, t_2, ...$, and the QBER for each mean photon number $\delta_1, \delta_2, ...$ From this parameters it is possible to estimate the transmittance for each specific photon number which makes it possible to estimate the actual number of both single and multiphotons which actually arrived. This makes the rate scale with t again[11].

5.2 Detector efficiency mismatch (DEM)

As mentioned in section 3.4 it is common to gate the detectors to avoid high dark counts, especially in optical fiber QKD because the best optical transmission window is compatible with the InGaAs bandgap. During the time window, there is the transient where the detector efficiency is rising, followed by the transient where the detector efficiency is falling. The timing of the qubits is such that they usually arrive in the middle of the time window.

Most protocols, and all BB84 setups require Bob to detect two bit values. This require two detectors or time-multiplexing on one detector. In either case the detector efficiency curves from the gating are to some extent misaligned. This is due to small differences in optical pathway, finite manufacturing in electric circuitry and finite precision in the APDs themselves. In practice DEM is unavoidable from an alignment and manufacturing point of view.

The flaw with misaligned efficiency curves is commonly called *detector efficiency mismatch* (DEM) [26, 27]. Eve is often able to control the relative efficiencies in systems with DEM to some extent. Figure 11 shows an example of mismatched efficiency curves. Here Eve could control the relative efficiencies trough the arrival time of the photon. The concept of DEM goes beyond the time domain. There are examples where systems exhibit DEM in both the spacial domain and the frequency domain [60]. Figure 12 shows the efficiency curves of a commercially available QKD-system [28].

[11] Eve could still apply the PNS attack, but Alice and Bob would know the nature of the attack and properly privacy amplificate to obtain a secure key. If the secret key rate drops below 0 due to the PNS attack, Alice and Bob just discard the key. At first this makes it seem like the PNS attack still is a threat, but if Eve's goal was to avoid the generation of a secure key she could simply use scissors to cut the fiber.

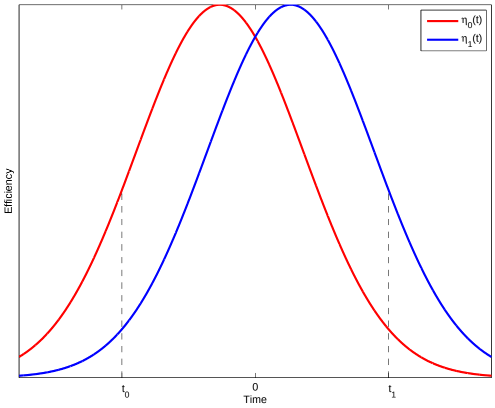

Figure 11: Example of detector efficiency curves exhibiting efficiency mismatch. $\eta_0(t)$ and $\eta_1(t)$ is the detector efficiencies of detector 0 and 1.

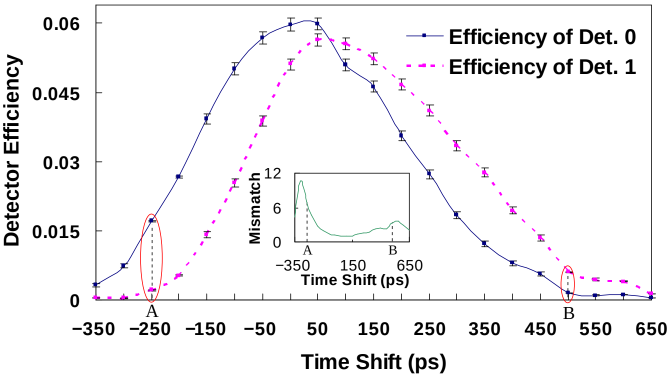

Figure 12: Efficiency curves measured on a commercially available QKD-system by Zhao et al. [28].

For the following subsections, most of the attacks based on DEM can be characterized by a single parameter. More specifically, let the efficiency of detector 0 be given by $\eta_0(t)$ and the efficiency of detector 1 be given by $\eta_1(t)$. Let t_0 be the timing that minimizes $\eta_1(t_0)/\eta_0(t_0)$. This is the timing where the probability to detect the bit value 0 is the largest compared to the probability to detect the bit value 1. Equally let t_1 be the timing that minimizes $\eta_0(t_1)/\eta_1(t_1)$. To simplify all analysis, one can choose to use the maximum contrast [26]

$$\eta = \min\left\{\frac{\eta_1(t_0)}{\eta_0(t_0)}, \frac{\eta_0(t_1)}{\eta_1(t_1)}\right\}, \tag{41}$$

and assume that this detector contrast exists for both bit values. This is a pessimistic assumption for Alice and Bob as one of the detector contrasts may be less than this maximum contrast. Note that $\eta = 0$ corresponds to full contrast, which means that there exist times when only one of the detectors is able to detect an incoming photon. Since lost bits are discarded in the key, one may assume that the most efficient detector has a detector efficiency of 1 without loss of generality. This is the full symmetrization assumption $\eta_0(t_0) = \eta_1(t_1) = 1$ and $\eta_0(t_1) = \eta_1(t_0) = \eta$. Under this assumption one find $\eta \approx 1/4$ for the system in figure 12.

A commonly mentioned countermeasure is called four-state Bob. A full discussion about this countermeasure is left for the paper in section 6.

5.3 Faked states attack

The first attack exploiting the DEM loophole is called the *faked-states attack* [26]. This is an intercept-resend attack, but the states resent to Bob are different from the measurement result. This way she can make Bob discard the bits if his basis does not coincide with Eves.

Faked states attack:

1. Eve measures the state from Alice, randomly choosing the X or the Z basis. Example: Eve measures 1 in the X basis.

2. The state sent to Bob is the opposite bit value in the opposite basis. The timing is such that the measured bit value has a large probability of being detected compared to the opposite bit value. Example: since Eve measured 1 in the X basis she sends a 0 in the Z basis timed to arrive at t_1.

Lets finish the example to see why this actually works:

- First assume that Alice and Bob choose the opposite basis from Eve, the Z basis. The bit values has full symmetry, so assume Alice sent the bit value 0.

Bob receives the state $Z0$ from Eve timed to arrive at t_1. Since Bob measures in the Z basis, the bit will always be incident to the 0 detector, but due to the timing t_1 the detector detecting 0 is very inefficient. Therefore there is a very high probability that the bit is lost.

- Assume that Alice and Bob choose the same basis as Eve, the X basis. Since Eve measured $X1$, the state sent by Alice must have been $X1$. Bob measures $Z0$ in the X basis. Then the photon has a 50/50 probability of hitting either detector 0 or 1. But again, the timing t_1 ensures that only the detector with value 1 has a high detection probability, so with a high probability Bob reads the same bit value as Eve which is the bit value sent by Alice. Otherwise the bit is likely to be lost.
- To summarize the losses, if Eve used the correct basis about half the bits are lost. If Eve used the incorrect basis about all the bits are lost. Therefore the visibility is reduced to 25 %. But most systems have loss, so Eve can compensate for the reduced visibility by increasing the intensity of the laser which is used to generate the faked states.

The attack is an intercept-resend attack. In terms of mutual information it constitutes a Markov-chain ($A \rightarrow E \rightarrow B$), so $I(A,E) \geq I(A,B)$. As shown in [26] the introduced QBER is given by

$$\text{QBER} \equiv \delta = \frac{2\eta_0(t_1) + 2\eta_1(t_0)}{\eta_0(t_0) + 3\eta_0(t_1) + 3\eta_1(t_0) + \eta_1(t_1)} = \frac{2\eta}{1+3\eta}. \tag{42}$$

$I(A:B)$ is given by equation (16) and is

$$I(A:B) = 1 - h(\delta) = 1 - h(\frac{2\eta}{1+3\eta}), \tag{43}$$

where $h(\cdot)$ is the binary entropy function given by equation (11). The mutual information between Alice and Eve $I(A:E)$ is found to be [26]

$$I(A:E) = 1 - \delta = 1 - \frac{2\eta}{1+3\eta} = \frac{1+\eta}{1+3\eta}. \tag{44}$$

This attack will always give Eve full control over the key as for all intercept-resend attacks: The limiting factor in this attack is that when the DEM becomes sufficiently small, the introduced QBER will become large (approach 25 % as for the intercept-resend attack in section 3.2). If Alice and Bob keep the key with a QBER < 11 %, the system is insecure when

$$\eta < \frac{\delta}{2-3\delta} = \frac{0.11}{1.67} \approx 0.066 \approx 1/15. \tag{45}$$

One has been able to adapt the faked states attack to many other protocols [29]. The faked states has also been used in together with other loopholes [61].

5.4 Time-shift attack

In the time-shift attack Eve simply randomly choose the timing of each bit [27]. When one of the detectors is more efficient that the other, this also makes the bit value corresponding to the detector more probable than the other. In this way Eve gains information about the bit value from the fact that Bob detected the bit.

Assume symmetry as presented in section 5.2. Let t_0 be the timing when detector 0 has unity efficiency, and detector 1 has η efficiency. Likewise let t_1 be the timing when detector 1 has unity efficiency, and detector 0 has η efficiency. Let Eve randomly choose the timing t_0 or t_1. When a bit is detected, the probability that the bit value corresponds to the timing of the bit is equal to

$$p = \frac{1}{1+\eta}. \tag{46}$$

This means that Eve's guessing probability on the bit is not 1/2 any more. Therefore Eve's mutual information with the key is given by equation (16)

$$I(A:E) = 1 - h(p) = 1 - h(1/(1+\eta)), \tag{47}$$

where $h(\cdot)$ is the binary entropy function given by equation (11).

The time-shift attack will not provide Eve full information about the key unless $\eta = 0$. Still it is easy to implement, and it does not introduce any QBER. Therefore it is suitable for use together with other attacks. It is also apparently resistant to the four-state Bob patch, but this discussion is left for the article.

Recently Zhao et. al. has been able to compromise security of a practically out-of-the-box commercial QKD-system based on the phase-encoding setup from figure 9 using the time-shifting attack [28]. This is due to the fact that the key rate cannot be arbitarily low in real devices. The only modification was to introduce a more narrow pulsed laser at Bob, but this is a nonessential modification as Eve could narrow the pulses in the quantum channel after the pulses left Alice [26].

5.5 Improved faked states attack

The faked states attack from section 5.3 is not optimised. First of all, the attack is limited by the introduced QBER, rather than the fact that the secure rate drops to zero. Therefore it is possible to attack only a fraction of the bits, and still compromise the security of the key. To improve the attack even further one could attack the other fraction with the time-shift attack, since this attack introduces zero QBER. An exciting feature of the improved attack is that it is also implementable with current technology, figure 13 shows the full setup of the eavesdropper.

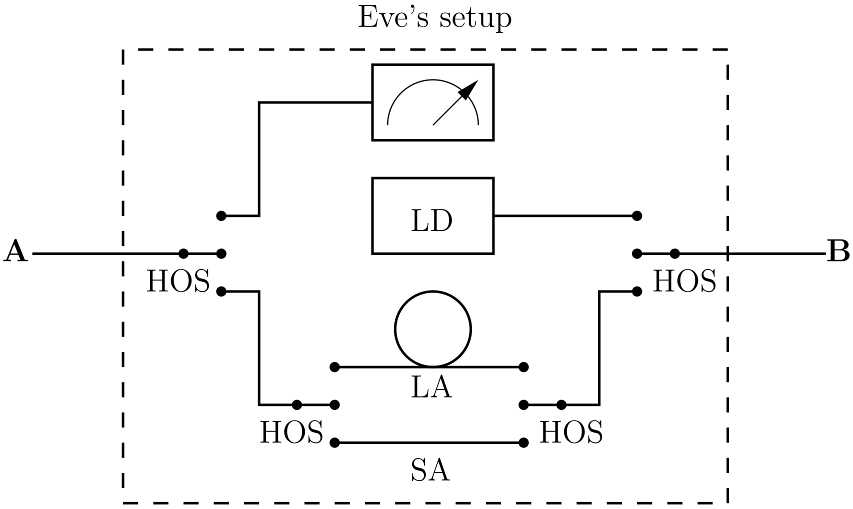

Figure 13: Eve's setup. LD: laser diode. HOS: high-speed optical switch. LA: long arm (large delay). SA: short arm (short delay). For a fraction of the bits, Eve measures the bit and sends Bob a fake state. For the other fraction of the bits she performs time-shifting to avoid introducing a to high QBER.

Let δ be the QBER which Alice and Bob observe. To achieve this QBER, Eve could use the faked states attack on a fraction $r = \delta/\delta_{\text{Faked states}} = \delta(1+3\eta)/(2\eta)$ of the bits. Eve's mutual information with Alice will simply be a weighted sum of the information from each attack

$$\begin{aligned} I(A:E) &= r\left(\frac{1+\eta}{1+3\eta}\right) + (1-r)\left(1-h(\frac{\eta}{1+\eta})\right) \\ &= \frac{1+\eta}{2\eta}\delta + \left(1-\frac{1+3\eta}{2\eta}\delta\right)\left(1-h(\frac{\eta}{1+\eta})\right) \\ &= 1-\delta-h(\frac{\eta}{1+\eta})\left(1-\frac{1+3\eta}{2\eta}\delta\right), \end{aligned} \tag{48}$$

for $\delta_{\text{Faked states}} > \delta$. If $\delta_{\text{Faked states}} < \delta$ Eve can just apply the faked states attack alone.

As before $I(A:B) = 1-h(\delta)$[12]. The equation $I(A:E) = I(A:B)$ can be solved numerically with respect to η, to measure the strength of this attack. $\delta = 0.11$ gives $\eta \approx 0.215$ which corresponds to a DEM about 1:5. This means that

[12] One might wonder why $I(A:B)$ is not given by a weighted sum as for $I(A:E)$. This is because Alice and Bob does not know which attack is used on each bit, they just observe the average QBER and apply both error correction and privacy amplification to the full key.

the improved faked states attack compromises the security of QKD-systems with $\eta < 0.215$, which is close to the η found in present QKD-systems.

5.6 Optimal individual attack

In the optimal individual attack from section 4.4, the final step is to distinguish between two non-orthogonal states. With the information from the time-shifting attack the measurement of the probe could be significantly improved. Figure 14 outline Eve's setup for the improved optimal individual attack.

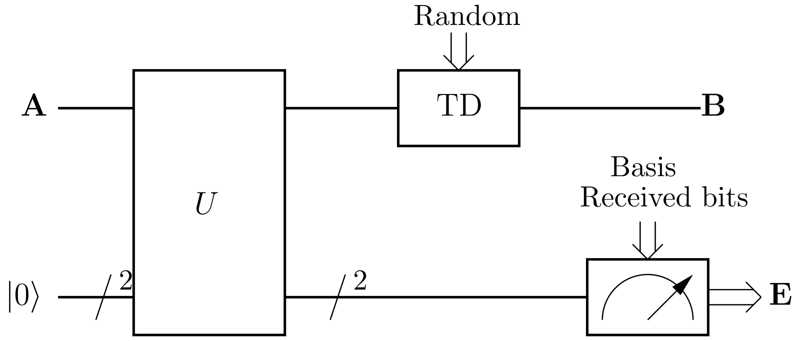

Figure 14: Eve's setup. TD: Timing device to adjust the timing of the qubits. The timing device could for instance be two arms of different lengths, and two high speed optical switches as the lower part of figure 13.

The time-shift attack does not introduce any QBER, and is therefore suitable to combine with the optimal individual attack. But if QBER is present, the time-shift attack is less efficient since Eve's ability to predict which detector a bit is sent to is reduced. Suppose for instance that the bit value is 1, and Eve chooses t_0. Then there is a slight probability that the bit will be erroneous and go to the 0 detector. Eve reads this as if the bit was 0, but the bit value is 1. The conclusion is that QBER reduces the information in the time-shift attack. The optimal individual attack however, has the strange property that Eve knows which bits are erroneous. Therefore the information from the time-shift attack is unreduced when combined with the optimal individual attack.

With the knowledge of the a priori probabilities of the two non-orthogonal states, Eve can improve her measurement. The improved measurement was discussed in section 2.4 and the mutual information between Alice and Eve was given by equation (22), namely

$$I(A:E) = 1 - h(p'). \tag{49}$$

where p' is the probability that Eve measured the correct bit value. Here p' is given by equation (21) which is

$$\begin{aligned} p' &= p\cos^2((1/2)\arctan(\frac{\sin 2\varphi}{\frac{p}{1-p}-\cos 2\varphi})) \\ &\quad + (1-p)\sin^2(\varphi+(1/2)\arctan(\frac{\sin 2\varphi}{\frac{p}{1-p}-\cos 2\varphi})), \end{aligned} \tag{50}$$

with $p = 1/(1+\eta)$, and the angle φ given as a function of the introduced QBER δ by equation (29).

The mutual information between Alice and Bob is given by equation (16), $I(A:B) = 1-h(\delta)$, where δ is the QBER. If one assume that Alice and Bob keep the key if the QBER is less than 11 %, and solve $I(A:B) = I(A:E)$ one get $\eta \approx 0.25$. This means that without countermeasures, the attack would break the security of the commercial system considered in [28].

6 Paper with security proof

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

Lars Lydersen[1, *] and Johannes Skaar[1]

[1] *Department of Electronics and Telecommunications,*
Norwegian University of Science and Technology, NO-7491 Trondheim, Norway

(Dated: November 3, 2008)

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, linear optical imperfections in the receiver/detectors.

PACS numbers: 03.67.Dd

I. INTRODUCTION

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

In practical QKD systems there will always be imperfections. The security of QKD systems with a large variety of imperfections has been proved [5, 9–11]. 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 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.

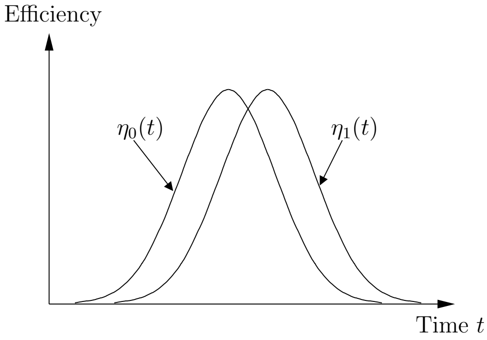

FIG. 1: An example of mismatched efficiency curves for two detectors in the time-domain. The functions $\eta_0(t)$ and $\eta_1(t)$ are the efficiencies of detector 0 and 1, respectively. The parameter t can be used to parameterize other domains as well.

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 attack has a major advantage because 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

[*] Electronic address: lars.lydersen@iet.ntnu.no

time-shift attack [17].

A possible countermeasure for systems with DEM is called *four-state Bob* [13, 16, 18, 19]. 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 [20–23] to read Bob's phase modulator settings. This will give Eve the mapping of the bit values to the detectors after the bits have been detected by Bob. Therefore, it is possible that the system may still be vulnerable to the time-shift attack.

Fung et al. found a security proof for QKD systems with DEM [14], quantifying the amount of extra privacy amplification required to remove Eve's knowledge about the key. 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 will first consider a powerful attack that even applies to implementations with four-state Bob, emphasizing the seriousness of the DEM vulnerability (Section II). The attack is a combination of an optimal individual attack, the time-shift attack, and a large pulse attack. Then we will provide a compact 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 modes associated with different bit values or t's, 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 with and without misalignment.

II. ATTACKS ON SYSTEMS WITH FOUR-STATE BOB

We will now discuss and concretize the possibility of attacking a system with four-state Bob using a large pulse attack [13, 16, 20–23]. 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.

If Eve reads Alice's modulator setting, the security will be seriously compromised, as Eve would get bit and/or basis information before the qubit enters Bob's apparatus. 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 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 qubit 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. Following the line of thought from Alice's setup does not work at Bob's apparatus. Using a beam splitter together with an intensity detector, or placing an attenuator at the entrance of Bob's setup will make the key rate suffer; the input of Bob's setup is precious single photons. The most practical solution seems to be an optical circulator combined with an intensity detector [22]; however, even then the key rate will be reduced due to additional loss. 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. In what follows, we will consider the latter solution, i.e., we assume that Eve is able to read Bob's phase modulator setting after Bob's detection.

The optimal individual attack in the absence of imperfections is known [24]. Here Eve lets the qubit from Alice interact with a probe, and measures the probe after the basis is revealed. This measurement involves separation between two non-orthogonal states, corresponding to the two bit values. In the presence of DEM and four-state Bob, we improve the attack as follows: In addition to using a probe, Eve launches a time-shift attack combined with a large pulse attack. Then she uses the information from the time-shift attack to optimize the measurement of the probe.

To analyze the attack, consider two points of time t_0 and t_1 such that $\eta_1(t_0)/\eta_0(t_0) = \eta_0(t_1)/\eta_1(t_1) = \eta$. After the public discussion, Eve has to separate between two non-orthogonal states with the probabilities $\{1/(1+\eta), \eta/(1+\eta)\}$. The optimal measurement on two non-orthogonal states with different *a priori* probabilities has been proved to be a projective measurement [25]. The key rate when Eve performs this attack (given one-way classical communication) is

$$R = h(p) - h(E), \tag{1}$$

where E is the QBER, and $h(\cdot)$ is the binary entropy function. The probability p of Eve measuring the correct bit value, is given by

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

where φ is related to the QBER by

$$\cos(\varphi) = 1 - 2E. \tag{3}$$

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 (1), and setting $E = 0.11$ gives $\eta = 0.25$. This value is larger than a corresponding η value found in a commercial QKD system [17]. Therefore, this attack could be used to compromise the security of such QKD systems, *even* if the system is patched with four-state Bob. Note that this attack works even if the mismatch is only 1/4 of the required mismatch for the faked-states attack [13]. Fig. 3 shows which η values compromise the security as a function of the QBER.

III. SECURITY ANALYSIS

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 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 uses decoy states [26–28]. Alice's source is otherwise assumed perfect: It emits an incoherent mixture of photonic number states, randomly in the X or Z bases, with no correlation between the bases and the photon number statistics [29].

The state space accessible to Eve consists of all photonic modes supported by the channel. Bob's two detectors may 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 transformations C_Z and C_X, acting on the channel modes after Eve's intervention. Here X and Z denote the bases chosen by Bob. With singular value decomposition, we can write

$$C_Z = U_Z F_Z V_Z C, \tag{4}$$

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; however, as lossless linear optical elements they act trivially on the vacuum subspace. More precisely, taking U_Z as an example, it transforms an arbitrary state as follows:

$$a|0\rangle + b|0^{\perp}\rangle \to a|0\rangle + b|0^{\perp'}\rangle. \tag{5}$$

Here a and b are complex numbers, $|0\rangle$ is the vacuum state of all modes, and $\langle 0^{\perp}|0\rangle = \langle 0\perp'|0\rangle = 0$. The diagonal matrix F_Z represents the different efficiencies of the two detectors (in addition to mode-dependent absorptions in the receiver), and satisfies

$$|F_Z|^2 = \mathrm{diag}\left[\eta_{Z0}(t_1)\;\;\eta_{Z1}(t_1)\;\;\eta_{Z0}(t_2)\;\;\eta_{Z1}(t_2)\ldots\right]. \tag{6}$$

Here $\eta_{Z0}(t_j)$ and $\eta_{Z1}(t_j)$ can be viewed as the efficiencies of detector 0 and 1, respectively, in the absence of U_Z and V_Z. The parameters $t_j, j = 1, 2, \ldots$ label the different modes. For example, t_j may correspond to different temporal modes. 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.

Note that the operators $C_Z = U_Z F_Z V_Z C$ and $C_X = U_X F_X V_X C$ are classical transformations (or transfer matrices) operating on the physical, photonic modes (e.g. temporal modes and polarization modes). For example, the general, unitary matrix V_Z is the result of sending the modes through a network isomorphic to the type in [30]. Each mode can contain any photonic state such as number states or coherent states. The quantum mechanical operators operating on the photonic states are infinite dimensional even though the matrices C_Z and C_X have finite dimension.

Having absorbed the detector efficiencies into C_Z, we can now represent Bob's detectors as perfect two-outcome detectors. Dark counts are modeled by Eve sending pulses, and for double click events, Bob assigns a random value to his bit [11]. 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.

We will prove security using Koashi's argument [29, 31]. To do this, we must consider how well Bob is able to predict a virtual X-basis measurement at Alice's side (assuming Alice's bits can be regarded as the outcome of a measurement on an entangled pair of states [29]).

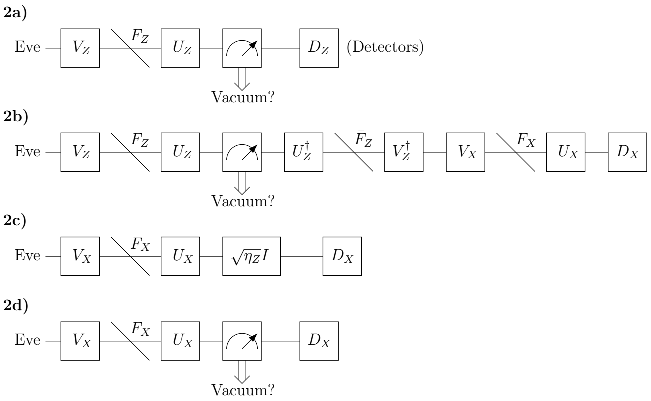

FIG. 2: a) Actual protocol. b) Estimation of Alice's virtual X-basis measurement. c) Simplification of Fig. 2b from Bob's point of view. d) Actual parameter estimation in the X-basis.

Bob does not perform such a measurement in practice; thus in this measurement we may let Bob do everything permitted by quantum mechanics, as long as he does not alter the information given to Eve.

Consider 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 $C_X = U_X F_X V_X$. 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

$$\bar{F}_Z F_Z = \sqrt{\eta_Z} I, \tag{7}$$

where

$$\eta_Z = \min_{ij} \{\eta_{Zi}(t_j)\}. \tag{8}$$

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 to determine Bob's measurement statistics. First of all, in light of (5) the unitary operator $U_Z^\dagger$ commutes with Eve's vacuum measurement. Thus we move it to the left, and annihilate it with U_Z. Next, we would like to move $\bar{F}_Z$ to the left. However, this filter does not commute with Eve's vacuum measurement. Nevertheless, we argue that Bob's measurement statistics are independent of the order of Eve's vacuum measurement and $\bar{F}_Z$.

For this argument, we introduce an extra vacuum measurement right before U_X, assuming nobody records the outcome. Clearly, Bob's measurement statistics are not altered by the presence of this extra measurement. The filter F_X consists of beam splitters, and in the next paragraph we will show that we may put another vacuum measurement before it, without changing the measured output state. Commuting this new measurement through V_X and $V_Z^\dagger$ we realize that the vacuum measurement to the left of $\bar{F}_Z$ may be omitted. Then $\bar{F}_Z$ goes together with F_Z to make $\sqrt{\eta}_Z I$. We can now move $V_Z^\dagger$ and annihilate it with V_Z. Thus, from Bob's point of view, 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.

A single beam splitter takes an arbitrary, single-mode density operator

$$\rho = \sum_{mn} \rho_{mn} |m\rangle\langle n| \tag{9}$$

to

$$\mathcal{F}(\rho) = \sum_{mnk} \rho_{mn} a_{mnk} |k\rangle\langle k+n-m|. \tag{10}$$

Here $|n\rangle$ denotes the number state, and the coefficients a_{mnk} are nonzero only for $\max\{0, m-n\} \leq k \leq m$. A vacuum measurement on $\mathcal{F}(\rho)$ leads to $P\mathcal{F}(\rho)P + (I - P)\mathcal{F}(\rho)(I-P)$, where P is the projector onto the vacuum state. From (10) it follows that $P\mathcal{F}(\rho)P$ is only dependent on the diagonal elements of ρ; thus this term is invariant if we make a vacuum measurement of ρ before applying $\mathcal{F}$. The remaining term $(I-P)\mathcal{F}(\rho)(I-P)$ is only dependent on ρ_{mn} for $m, n \geq 1$; thus it is invariant if we make a vacuum measurement before applying $\mathcal{F}$. Generalizing to the case with several beam splitters acting on each mode separately, is straightforward.

Let Q_X be the detection rate in the X basis, and $q_X^{(1)}$ the fractions of those detection events that originate from single photons at Alice. Morever, let $e_X^{(1)}$ be the QBER for single photon events in the X-basis. These parameters can be estimated by the decoy state method, and will be assumed known. Consider the estimation in Fig. 2b-c. Let N be the number of states sent by Alice. 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 $\sqrt{\eta}_Z I$. 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. 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 $Q_Z N - \eta_Z q_X^{(1)} Q_X N[1 - h(e_X^{(1)*})]$. In our analysis we have ignored the events associated with Alice sending the vacuum state [29]; their contribution will only give a marginally larger rate.

We can now use Koashi's security proof to establish the number of secure key bits $Q_Z N R$ in the asymptotic limit $N \to \infty$:

$$\begin{aligned} Q_Z N R &= Q_Z N - Q_Z N h(E_Z) \\ &\quad -Q_Z N + \eta_Z q_X^{(1)} Q_X N \left[1 - h(e_X^{(1)*})\right] \\ &= -Q_Z N h(E_Z) + \eta_Z q_X^{(1)} Q_X N \left[1 - h(e_X^{(1)*})\right]. \end{aligned} \tag{11}$$

Here E_Z is the QBER as measured in the Z basis.

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. 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,

$$e_X^{(1)*} \leq \frac{e_X^{(1)}}{\eta_Z(1 - e_X^{(1)}) + e_X^{(1)}} \leq e_X^{(1)}/\eta_Z. \tag{12}$$

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

$$R_Z \geq -h(E_Z) + \eta_Z q_X^{(1)} Q_X/Q_Z \left[1 - h(e_X^{(1)}/\eta_Z)\right]. \tag{13}$$

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

$$R_X \geq -h(E_X) + \eta_X q_Z^{(1)} Q_Z/Q_X \left[1 - h(e_Z^{(1)}/\eta_X)\right]. \tag{14}$$

Ineqs. (13) and (14) 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 (13) to that of Ref. [14], we let Alice only send single photons. The rate then becomes

$$R \geq -h(E) + \eta[1 - h(E/\eta)], \tag{15}$$

where we have assumed symmetry between the bases, and therefore omitted the Z and X subscripts. The rate (15) coincides with the rate found in [14] (see Subsection **??** for a discussion on how to identify η). Note, however, that (15) 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 (12) can be replaced by $e_X^{(1)*} = e_X^{(1)}$. Then (15) is improved to

$$R \geq -h(E) + \eta[1 - h(E)]. \tag{16}$$

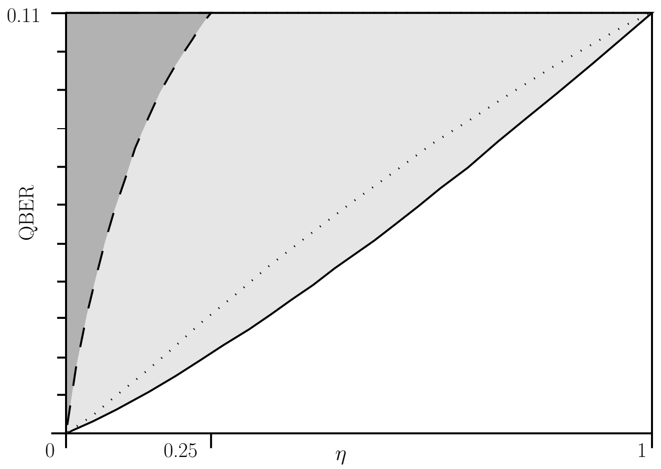

FIG. 3: Security bounds when Alice sends single photons ($q_Z^{(1)} = q_X^{(1)} = 1$), assuming symmetry between the bases. The bounds are found by setting the associated key generation rates equal to zero. Solid line: General security bound, as resulting from (15). Dotted line: Security bound (16) assuming Eve sends single photons. Dashed line: The attack from Section II, as resulting from (1).

Fig. 3 shows the security bounds resulting from (15) and (16) when the right-hand side is set equal to zero.

IV. EXAMPLES

A. 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 $C_X = F_X H C = F_Z H C$, where H is a block-diagonal matrix consisting of 2×2 Hadamard matrices $H^{(2)}$, interchanging the bases Z and X for each time:

$$H = \mathrm{diag}\left[H^{(2)} \;\; H^{(2)} \;\; H^{(2)} \;\; \ldots\right]. \tag{17}$$

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

$$F_Z = F F', \tag{18}$$

where

$$F'^2 = \mathrm{diag}\left[\eta'(t_1) \;\; \eta'(t_1) \;\; \eta'(t_2) \;\; \eta'(t_2) \ldots\right], \tag{19}$$

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 (13) is therefore the minimum diagonal element of $|F|^2$:

$$\eta_Z = \min_t \min \left\{ \frac{\eta_{Z0}(t)}{\eta_{Z1}(t)}, \frac{\eta_{Z1}(t)}{\eta_{Z0}(t)} \right\}. \qquad (20)$$

B. DEM and misalignments

In addition to the detector efficiency mismatch in Subsection IV A, 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 $C_X = F_X V_X H C$. Assuming no coupling between different temporal modes (no multiple reflections), V_Z and V_X are block-diagonal matrices. For example,

$$V_Z = \mathrm{diag}\left[V_1^{(2)} \;\; V_2^{(2)} \;\; V_3^{(2)} \;\; \ldots \right], \qquad (21)$$

where $V_j^{(2)}$ are unitary 2×2 matrices. Here we have used the same order of modes as in the original definition (6). Taking $F_X = F_Z$ and factorizing as in Subsection IV A, we find that the parameter $\eta_Z = \eta_X$ again is given by (20). The secure key generation rate is then found from (13).

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 (8). For unnormalized detection efficiencies, this definition can be rewritten

$$\eta_Z = \frac{\min_{i,t}\{\eta_{Zi}(t)\}}{\max_{i,t}\{\eta_{Zi}(t)\}}. \qquad (22)$$

Eq. (22) is obtained by absorbing the maximum detector efficiency $\max_{i,t}\{\eta_{Zi}(t)\}$ into C. Omitting the requirement $F_X = F_Z$, (22) must be rewritten as

$$\eta_Z = \frac{\min_{i,t}\{\eta_{Zi}(t)\}}{\max\left(\max_{i,t}\{\eta_{Zi}(t)\}, \max_{i,t}\{\eta_{Xi}(t)\}\right)}. \qquad (23)$$

C. 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 (23).

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

$$\eta > \frac{\min_{t,\mathrm{basis,bit}}(\text{detection efficiency}) - \delta}{\max_{t,\mathrm{basis,bit}}(\text{detection efficiency}) + \delta}. \qquad (24)$$

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.

V. 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.

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.

To demonstrate the seriousness of the detection efficiency loophole, we have argued that even with a four-state Bob patch, QKD systems may be vulnerable to a powerful attack. The 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 (13) and (14) for estimating the required amount of privacy amplification.

[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, Physical Review Letters **67**, 661 (1991).

[3] C. H. Bennett, Physical Review Letters **68**, 3121 (1992).

[4] N. Gisin, G. G. Ribordy, W. Tittel, and H. Zbinden, Reviews of Modern Physics **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, Journal of the Association for Computing Machinery **48**, 351 (2001).

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

[8] P. W. Shor and J. Preskill, Physical Review Letters **85**, 441 (2000).

[9] H. Inamori, N. Lütkenhaus, and D. Mayers, e-print quant-ph/0107017 (2001).

[10] M. Koashi and J. Preskill, Physical Review Letters **90**, 057902 (2003).

[11] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Information & Computation **4**, 325 (2004).

[12] I. Csiszàr and J. Körner, IEEE Transactions on Information Theory **24**, 339 (1978).

[13] V. Makarov, A. Anisimov, and J. Skaar, Physical Review A **74**, 022313 (2006), ibid. **78**, 019905 (2008).

[14] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quantum Information & Computation **9**, 131 (2009).

[15] V. Makarov and J. Skaar, Quantum Information & Computation **8**, 0622 (2008).

[16] B. Qi, C. H. F. Fung, H.-K. Lo, and X. F. Ma, Quantum Information & Computation **7**, 73 (2007).

[17] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, e-print quant-ph/0704.3253v1 (2007).

[18] M. LaGasse, US patent application 20050190922 (2005).

[19] P. Møller Nielsen, C. Schori, J. Lykke Sørensen, L. Salvail, I. Damgård, and E. Polzik, Journal of Modern Optics **48**, 1921 (2001).

[20] G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Journal of Modern Optics **47**, 517 (2000).

[21] D. S. Bethune and W. P. Risk, IEEE Journal of Quantum Electronics **36**, 340 (2000).

[22] A. Vakhitov, V. Makarov, and D. R. Hjelme, Journal of Modern Optics **48**, 2023 (2001).

[23] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Physical Review A **73**, 022320 (2006).

[24] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Physical Review A **56**, 1163 (1997).

[25] L. B. Levitin, in *Quantum Communications and Measurement*, edited by V. P. Belavkin, O. Hirota, and R. L. Hudson (Plenum Press, New York, 1995), pp. 439–448.

[26] W. Y. Hwang, Physical Review Letters **91**, 057901 (2003).

[27] X.-B. Wang, Physical Review Letters **94**, 230503 (2005).

[28] H.-K. Lo, X. F. Ma, and K. Chen, Physical Review Letters **94**, 230504 (2005).

[29] M. Koashi, e-print quant-ph/0609180v1 (2006).

[30] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Physical Review Letters **73**, 58 (1994).

[31] M. Koashi, Journal of Physics Conference Series **36**, 98 (2006).

7 Conclusion and further work

An extensive analysis of QKD-systems with detector efficiency mismatch has been conducted. Both lower and upper security bounds on the secret key rate has been found.

The known attacks of systems with detector efficiency mismatch has been improved. Earlier the best known attack would compromise the security of a QKD-system if the efficiency mismatch of the detectors was about 1:15. The attack from section 5.5 will compromise the security of a QKD-system when the efficiency mismatch of the detectors is about 1:5. The nice feature of this attack is that it is implementable today. The attack in section 5.6 will compromise the security of a QKD-system when the efficiency mismatch is about 1:4. This attack is not implementable with current technology, but it shows the severeness of the detector efficiency mismatch loophole. The attack could even be used against systems with the four state Bob patch, if it is combined with a large pulse attack. Experimental measurements of the DEM on a commercially available QKD-system indicates that both attacks could be used to eavesdrop on current QKD-systems. Even if Eve could get only partial information about the key, this would hurt QKD since QKDs main advantage over classical cryptography is the unconditional security.

A security bound has been established to quantifying the amount of privacy amplification required to remove Eve's information about the secret key. The bound is more general than the previous bound [60], and is valid for any basis dependent, possibly lossy, linear optical imperfections in the channel and receiver/detectors. Some of the major improvements includes removing the squashing assumption, making the proof valid for multiphotons. This is a very important step towards making the proof applicable to real systems. With the security bound a QKD-manufacturer can characterise the QKD-system, and perform extra privacy amplification to keep the security intact. Further a software/firmware update to existing systems could reestablish the security.

There is much experimental work to be done. First of all one should put some effort into characterising the DEM of real commercial systems. Multiple reflections should get special attention, since it easily gives a complete DEM. New detector circuitry could perhaps limit the DEM by only allowing detections in the middle of the window? One other aspect is that it might turn out that it is impossible to measure the quantities used for the security proof. If this is the case, one should modify the security proof to base it on measurable parameters. This would require a close cooperation between theorists and experimentalists.

On the theoretical side, the security proof could be extended in at least three directions. One could consider the polarization based, passive basis setup in figure 7. The system allows mode mixing between the bases, which is not considered in the current proof. Entangle based systems face a different problem: both Alice and Bob has DEM, and the mismatch can be different at Alice and Bob. In such setups Eve might use the spacial mode of the photon to control the relative efficiencies. The third, and perhaps a more long term goal should be to do finite key analysis.

The most important point is that effort should still be put into breaking the security of QKD-systems. This is the only way real implementations can approach perfect security sometime in the future.

References

[1] 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.

[2] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.

[3] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22:644–654, 1976.

[4] R. L. Rivest, A. Shamir, and L. M. Adleman. A method of obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[5] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Scientific and Statistical Computing*, 26:1484, 1997.

[6] 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*, pages 175–179, Bangalore, India, 1984. IEEE Press, New York.

[7] A. K. Ekert. Quantum cryptography based on bell theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[8] J. S. Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38:447–452, 1964.

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

[10] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without bell's theorem. *Physical Review Letters*, 68:557–559, 1992.

[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *e-print quant-ph/0802.4155*, 2008.

[12] C. H. Bennett. Quantum cryptography using any 2 nonorthogonal states. *Physical Review Letters*, 68(21):3121–3124, 1992.

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

[14] A. Muller, H. Zbinden, and N. Gisin. Quantum cryptography over 23 km in installed under-lake telecom fibre. *Europhysics Letters*, 33(5):335–339, 1996.

[15] 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(6):343–348, 2007.

[16] 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. Entanglement-based quantum communication over 144km. *Nature Physics*, 3(7):481–486, 2007.

[17] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[18] D. Mayers. Advances in cryptology. In N. Koblitz, editor, *Proceedings of Crypto ´96*, volume 1109, pages 343–357. Springer, New York, 1996.

[19] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999.

[20] P. W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, July 2000.

[21] D. Mayers. Unconditional security in quantum cryptography. *Journal of the Association for Computing Machinery*, 48(3):351–406, 2001.

[22] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quantum Information & Computation*, 4(5):325–360, 2004.

[23] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *e-print quant-ph/0107017*, 2001.

[24] M. Koashi and J. Preskill. Secure quantum key distribution with an uncharacterized source. *Physical Review Letters*, 90(5):057902, 2003.

[25] R. Renner and R. Koenig. Universally composable privacy amplification against quantum adversaries. In Joe Kilian, editor, *Second Theory of Cryptography Conference, TCC 2005*, volume 3378 of *LNCS*, pages 407–425. Springer Verlag, Berlin, February 2005. Also available at http://arxiv.org/abs/quant-ph/0403133.

[26] V. Makarov, A. Anisimov, and J. Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 74(2):022313, 2006. ibid. **78**, 019905 (2008).

[27] B. Qi, C. H. F. Fung, H.-K. Lo, and X. F. Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Information & Computation*, 7(1-2):73–82, 2007.

[28] Y. Zhao, C.-H. Fred Fung, B. Qi, C. Chen, and H.-K. Lo. Experimental demonstration of time-shift attack against practical quantum key distribution systems. *e-print quant-ph/0704.3253v2*, 2007.

[29] V. Makarov and J. Skaar. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *Quantum Information & Computation*, 8:0622, 2008.

[30] V. Makarov. Exploiting saturation mode of passively-quenched APD to attack quantum cryptosystems. *e-print quant-ph/0707.3987*, 2007.

[31] Y. Zhao, B. Qi, and H.-K. Lo. Quantum key distribution with an unknown and untrusted source. *Physical Review A*, 77(5):052327, 2008.

[32] P. Møller Nielsen, C. Schori, J. Lykke 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.

[33] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, Cambridge, 2000.

[34] Thomas M. Cover and Joy A. Thomas. *Elements of information theory.* Wiley, Hoboken, N.J., 2nd edition, 2006.

[35] Asher Peres. *Quantum theory concepts and methods.* Fundamental theories of physics vol. 72. Kluwer Acadamic, Dordrecht, 1995.

[36] C. A. Fuchs and C. M. Caves. Ensemble-dependent bounds for accessible information in quantum-mechanics. *Physical Review Letters*, 73(23):3047–3050, 1994.

[37] L. B. Levitin. Optimal quantum measurements for two pure and mixed states. In V. P. Belavkin, O. Hirota, and R. L. Hudson, editors, *Quantum Communications and Measurement*, pages 439–448. Plenum Press, New York, 1995.

[38] L. B. Levitin. Physical information theory part II: Quantum systems. In *Workshop on Physics and Computation, 1992. PhysComp '92.*, pages 215–219, 1992.

[39] C.A. Fuchs. *Distinguishability and Accessible Information in Quantum Theory.* Ph.d. thesis, 1996.

[40] A.S. Holevo. Information-theoretical aspects of quantum measurement. *Problems of Information Transmission*, 9(2):110–118, 1973.

[41] 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(2):1163–1172, 1997.

[42] N. Gisin, G. G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, 2002.

[43] 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(6906):450–450, October 2002.

[44] G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden. Fast and user-friendly quantum key distribution. *Journal of Modern Optics*, 47(2-3):517–531, 2000.

[45] D. S. Bethune and W. P. Risk. An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light. *IEEE Journal of Quantum Electronics*, 36(3):340–347, 2000.

[46] 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(13):2023–2038, 2001.

[47] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, 73(2):022320, 2006.

[48] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden. Automated 'plug & play' quantum key distribution. *Electronics Letters*, 34(22):2116–2117, 1998.

[49] R. Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649, 2007.

[50] I. Csiszàr and J. Körner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[51] T. Kim, I. S. Wersborg, F. N. C. Wong, and J. H. Shapiro. Complete physical simulation of the entangling-probe attack on the bennett-brassard 1984 protocol. *Physical Review A*, 75(4):042327, 2007.

[52] M. Koashi. Simple security proof of quantum key distribution via uncertainty principle. *Journal of Physics Conference Series*, 36:98, 2006.

[53] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, 72(1):012332, 2005.

[54] M. Koashi. Efficient quantum key distribution with practical sources and detectors. *e-print quant-ph/0609180v1*, 2006.

[55] H. Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.*, 60(12):1103–1106, 1988.

[56] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5):057901, 2004.

[57] W. Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters*, 91(5):057901, 2003.

[58] H.-K. Lo, X. F. Ma, and K. Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94(23):230504, 2005.

[59] X.-B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical Review Letters*, 94(23):230503, 2005.

[60] 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(1 & 2):131–165, 2009.

[61] 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(3):032314, 2007.