nature COMMUNICATIONS

ARTICLE

Received 14 Jan 2011 | Accepted 11 May 2011 | Published 14 Jun 2011

DOI: 10.1038/ncomms1348

Full-field implementation of a perfect eavesdropper on a quantum cryptography system

Ilja Gerhardt[1,*], Qin Liu[2,*], Antía Lamas-Linares[1], Johannes Skaar[2,3], Christian Kurtsiefer[1] & Vadim Makarov[2]

Quantum key distribution (QKD) allows two remote parties to grow a shared secret key. Its security is founded on the principles of quantum mechanics, but in reality it significantly relies on the physical implementation. Technological imperfections of QKD systems have been previously explored, but no attack on an established QKD connection has been realized so far. Here we show the first full-field implementation of a complete attack on a running QKD connection. An installed eavesdropper obtains the entire 'secret' key, while none of the parameters monitored by the legitimate parties indicate a security breach. This confirms that non-idealities in physical implementations of QKD can be fully practically exploitable, and must be given increased scrutiny if quantum cryptography is to become highly secure.

[1] Centre for Quantum Technologies, Department of Physics, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore. [2] Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway. [3] University Graduate Center, NO-2027 Kjeller, Norway. *These authors contributed equally to this work. Correspondence and requests for materials should be addressed to Q.L. (qin.liu@iet.ntnu.no); questions about quantum cryptography system should be addressed to C.K. (christian.kurtsiefer@gmail.com); questions about the hacking hardware should be addressed to V.M. (makarov@vad1.com).

Secret communication provided by cryptography is needed in many activities of the human civilization—military, commerce, government and private affairs. The long history of cryptography is a continual cat-and-mouse game of cryptographic systems being broken and replaced with new, stronger ones[1]. Quantum cryptography, as one of the latest techniques, promised for the first time a security, which is not based on mathematical conjectures but on the laws of physics[2,3]. Technologically, quantum cryptography has matured to experiments up to 250 km distance[4], and several commercial systems are available. Although security of the quantum key distribution (QKD) protocol is unconditionally proven[5,6], deviations of actual hardware from the idealized model still present a challenge. Various attacks have been proposed exploiting imperfections of components in QKD scheme: light modulators[7,8], photon sources[9,10] and detectors[11–17]. However, none of these proposals implemented an attack that eavesdropped the secret key, leaving the question of practicality of technological vulnerabilities unresolved.

We chose one of the proposed attack methods, fully implemented an eavesdropper Eve, and used it to attack an installed QKD line. The QKD system under attack is a well-designed one used previously in several experiments[18–20], and openly documented[21]. We treated QKD hardware and software as 'given' and kept all its settings as they had been set for QKD before this study. The hardware and software are assumed fully known to Eve, according to Kerckhoffs' principle[22].

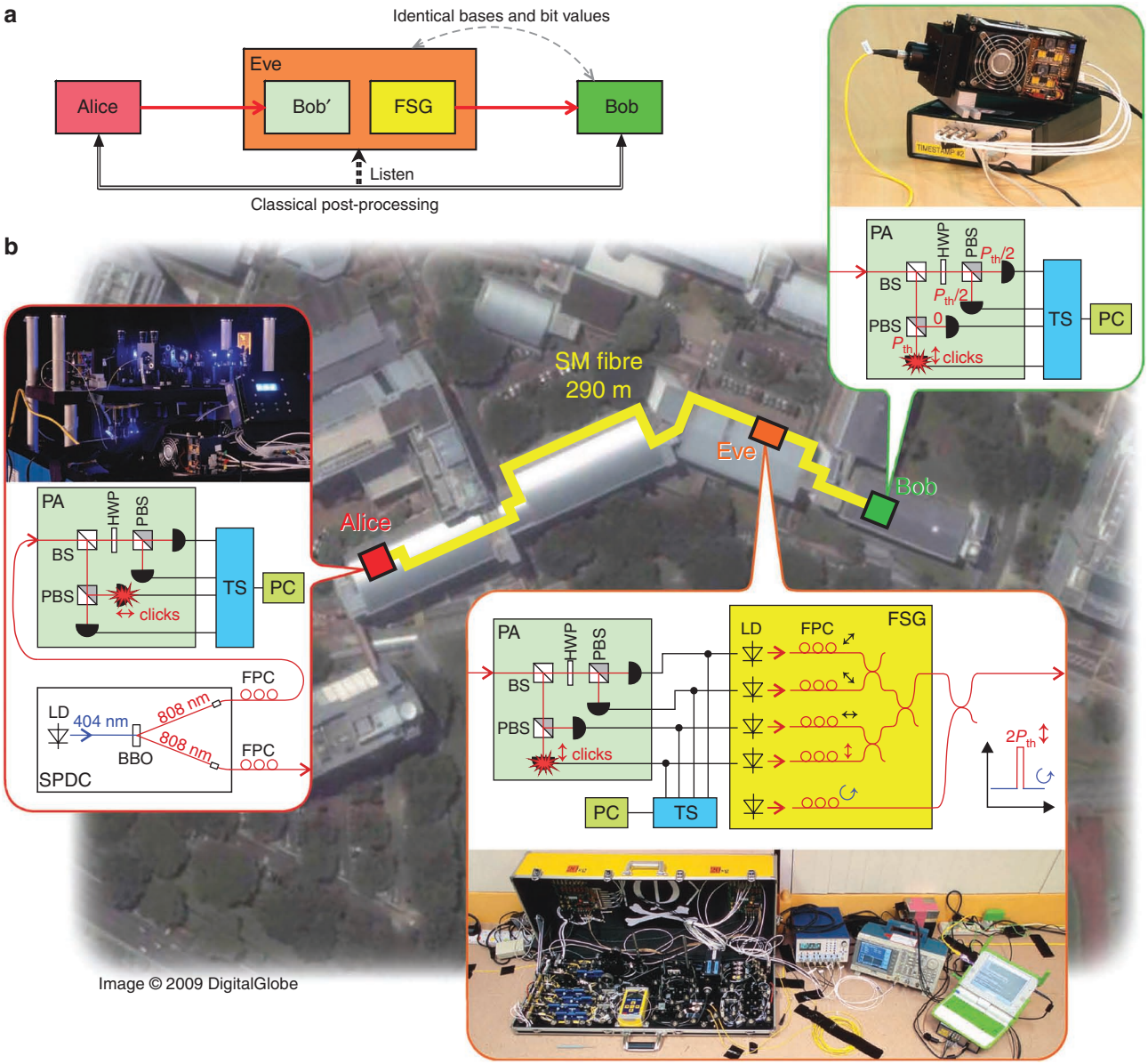

Figure 1 | Eavesdropping experiment. (**a**) Principle of the faked-state attack. (**b**) Attack on installed QKD system spanning four buildings at the campus of the National University of Singapore. In Alice, polarization-entangled photon pairs were produced in a type-II spontaneous parametric down-conversion (SPDC) source[18,20]. One photon was measured locally by Alice; the other one was sent through a 290 m single-mode (SM) fibre line to Bob. Eve was inserted at a mid-way point. All three parties used identical polarization analysers (PA); clicks were registered with timestamp (TS) units. Under attack, Bob's detectors clicked controllably when illuminated by an optical pulse with peak power $\geq P_{th}$. In the example, to address the target detector for vertically polarized photons, Eve sent a faked state with vertical polarization and peak power $2P_{th}$. Each of Bob's detectors in the conjugate (45° rotated) basis received a pulse of peak power $P_{th}/2$, and thus remained blinded. See also 'Complete Eve's setup' section in Methods. In the diagram: BS, 50/50% beamsplitter; PBS, polarizing beamsplitter; HWP, half-wave plate; FPC, fibre polarization controller; BBO, β-barium-borate crystal.

In this paper, we demonstrate the full-field implementation of this eavesdropping attack in realistic conditions over a 290-m fibre link between the transmitter Alice and the receiver Bob. From multiple QKD sessions over a few hours, Eve obtains the same 'secret' key as Bob, while the usual parameters monitored in the QKD exchange are not disturbed, leaving Eve undetected.

Results

The faked-state attack. We have chosen a 'faked-state attack' (Fig. 1a)[23]. Eve uses a replica of the legitimate receiver unit (Bob′) to intercept and measure all quantum states sent by Alice. She further uses a faked-state generator (FSG) to force Bob to output identical bases and bit values, so that Eve and Bob have the same raw key. Eve also records unencrypted communication in the classical channel, and computes the final secret key (identical to Alice's and Bob's) by repeating the same sifting, error correction and privacy amplification procedures[3,6] as Bob. Unlike the traditional intercept-resend attack[2,3], the faked-state attack does not introduce errors in the key and therefore is not detected by the QKD protocol.

Eve's full control of Bob's detection outcomes is crucial to the success of the faked-state attack. Several technological vulnerabilities allow for the needed degree of control[12,15,17,23]. We have chosen to exploit blindability and controllability of single-photon detectors under strong illumination[15,16]. The QKD system under attack uses passively quenched single-photon avalanche photodiodes (APDs; Fig. 2a). Ordinarily, the arrival of a single photon generates an electron-hole pair that leads to an avalanche in the APD. The resulting current spike is detected by a comparator and a pulse-shaper as the arrival of a single photon, a 'click'. Spurious capacitances of the device result in a finite recharging time and cause a detector deadtime of ~1 μs. If the illumination level is increased such that no full recharge occurs between individual photons, the avalanche becomes progressively smaller. Under higher illumination conditions, it falls below the comparator threshold and can not be identified as a click; the detector becomes blind (Fig. 2b). Hence, by injecting high light levels into the channel, it is straightforward for Eve to indefinitely blind Bob's detectors. Under these illumination conditions, the APD no longer behaves as a single-photon detector, but as a classical photodiode generating photocurrent proportional to the optical power. A strong light pulse with peak power above a threshold P_{th} generates a current spike that mimics the signal of a legitimate photon (Fig. 2c)[16].

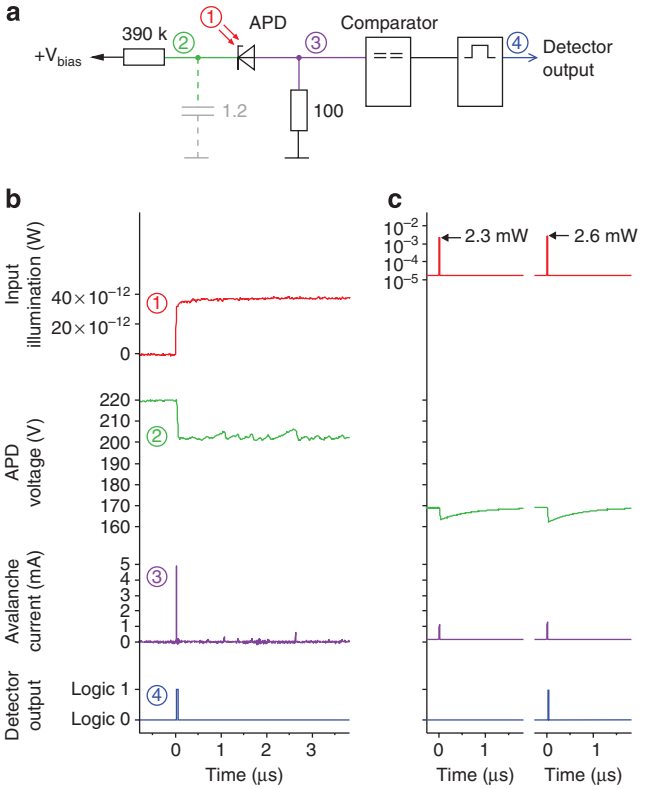

Figure 2 | Detector blinding and control. (**a**) Circuit diagram of the custom-built single-photon detectors used in the QKD system under attack[18–20]. An avalanche photodiode (APD, C30902S, PerkinElmer) is biased 15 V above its breakdown voltage from a voltage supply $+V_{bias}$≈220 V. The avalanche current is fed by a charge stored in a small stray capacitance (≈1.2 pF) and is detected via a voltage spike at the 100 Ω resistor. The avalanche quickly self-quenches becuse of discharge of the capacitance and concomitant bias voltage drop; its recharge and recovery of single-photon sensitivity takes ~1 μs. (**b**) Oscillograms show one of the detectors blinded after switching on 38 pW continuous-wave (c.w.) illumination. (**c**) Oscillograms show the same detector blinded with 17 μW c.w. illumination. A superimposed optical trigger pulse with a peak power of 2.3 mW never causes a click, whereas one with P_{th} = 2.6 mW always does.

Experimental implementation. This QKD implementation has four detectors and uses a four-state protocol with polarization coding and passive basis choice (Fig. 1b). Eve can blind all detectors using a laser diode (LD) emitting continuous-wave circularly polarized light, which splits evenly between Bob's detectors. To selectively make one detector click while keeping the other three blinded, Eve adds a linearly polarized pulse of the same polarization as the target detector, and peak power $2P_{th}$. By using four LDs aligned to vertical, horizontal and ±45° polarizations, Eve has the option to deliberately launch a click in any of Bob's detectors. She then executes the faked-state attack.

Before attack, we inserted Eve into the line and manually aligned her polarizations to match Bob's detector settings. Then we characterized fidelity of her control over Bob. During a 5 min session Eve received 8,736,719 clicks and resent an equal number of faked states to Bob. Of the latter, 99.75% caused clicks in Bob, and more importantly those clicks were always produced in the intended detector (Table 1). As the synchronization protocol involves Bob sending to Alice precise timing of every click registered[21], Eve can easily identify and discard the few faked states that did not register at Bob, and that will be discarded in the reconciliation between Alice and Bob. After this, she has an identical record with Bob. Owing to small imperfections in tuning Eve's FSG ('Complete Eve's setup' section in Methods), Bob had a probability of 5×10^{-7} to register simultaneous clicks in two detectors, corresponding to four events in 323 s. In this QKD implementation, such double clicks were treated as noise and discarded (which is obviously insecure but easily patchable by assigning instead random bit values[24]). We remark that our control scheme could be extended to reproduce arbitrary clicks in several detectors with a more complex FSG, which is, however, not needed in the present experiment.

QKD performance and key extraction. After Eve's calibration, we ran multiple 5–10 min QKD sessions over a few hours, some with Eve inserted in the fibre line and some without. We recorded performance statistics, all public communication data between Alice and Bob, and the generated keys. During QKD, the legitimate parties monitor key rates to check the line transmission. Figure 3 shows results from two typical sessions, one eavesdropped and one not. As expected, inserting Eve does not alter the rates. Small differences in rate averages of the two sessions are not caused by eavesdropping but rather are normal medium-term alignment fluctuations in this QKD system. The quantum bit error ratio of 5–6% is typical for this experiment[18–20], and well below the security limit for the Bennett–Brassard–Mermin 1992 (BBM92) protocol used here[6].

Table 1 | Fidelity of Eve's control over Bob.

Faked states sent by Eve		Clicks at Bob			
		V	**−45°**	***H***	**+45°**
1,702,067	***V***	1,693,799 99.51%	0	0	0
2,055,059	**−45°**	0	2,048,072 99.66%	0	0
2,620,099	***H***	0	0	2,614,918 99.80%	0
2,359,494	**+45°**	0	0	0	2,358,418 99.95%

The 4×4 matrix shows the total number of clicks in each of Bob's detectors, as well as their percentage in respect to the faked states sent with the same polarization. The data was recorded during a 5 min long diagnostic-mode session. The lack of off-diagonal elements proves that a click is never launched in a wrong detector. Double clicks are not included. The overall click rate is close to 100%, leading to virtually no loss in the line Eve–Bob.

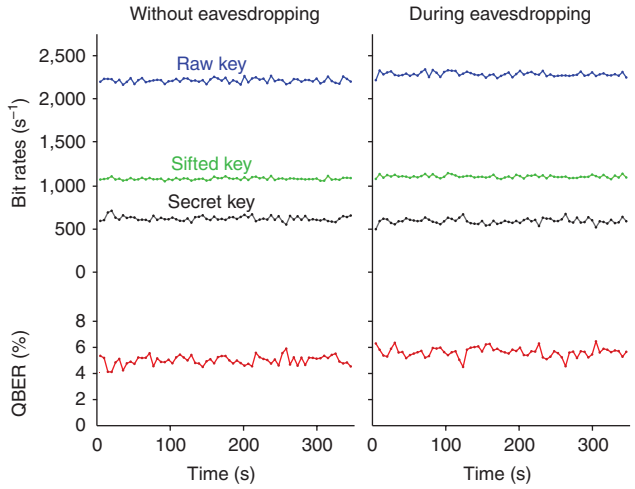

Figure 3 | QKD performance with and without eavesdropping as measured by Alice and Bob. Session without Eve in the fibre line (left). Eve installed (right). The traces in the top chart correspond to the raw key rate, sifted key rate and final secret key rate after error correction and privacy amplification[18,20]. The bottom chart shows the quantum bit error ratio (QBER).

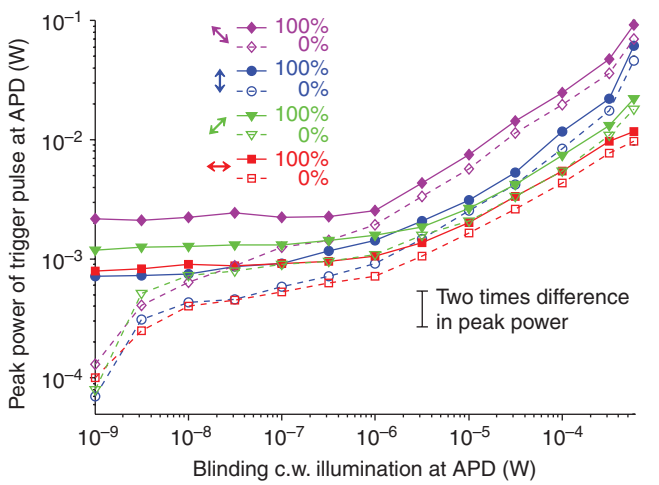

Figure 4 | Click thresholds of the four detectors in Bob's PA versus blinding c.w. power. The dashed curves show the highest peak pulse power at which the detector still never clicks. The solid curves show the lowest peak pulse power at which it always clicks. Between these two thresholds, click probability of each detector increases gradually. The detector recording photons of horizontal polarization (curves with squares) was the one tested in Figure 2.

In the sessions in which Eve was connected, she extracted Bob's sifted key from her clicks and the recorded public communication Alice–Bob. Alice and Bob identify photon pairs by time-tagging each detector click and exchanging these times over the public channel[21]. This allows them to synchronize their clocks and to keep track of what photons were detected. Bob also announces his detection bases, and Alice answers for which Bob's clicks she detected the other photon of the pair in the same basis (these pairs form the sifted key). As no measurement outcomes are revealed, this information can be entirely public. In the present implementation, this channel is established over a transmission control protocol and internet protocol (TCP/IP) wireless connection, and is passively wiretapped by Eve. She watches the discussion, synchronizes her clock with Bob's clock, then sifts her key keeping only those of her clicks which are also kept by Alice and Bob in the sifted key. We ran Eve's processing script on recorded experimental data and verified that in all eavesdropped QKD sessions, Eve's sifted key was identical to Bob's (the script and data sample are available, 'Raw experimental data and Eve's key extraction software' section in Methods).

If the source analysers and transmission medium were perfect, this sifted key would directly constitute the secret key. Under realistic conditions, the sifted keys of Alice and Bob are not identical (the difference being quantified by the quantum bit error ratio). Further steps of error correction and privacy amplification complete the public exchange Alice–Bob to produce the secret key[3,6]. As Eve has the same sifted key as Bob, she can apply the same processing as Bob to it, and is guaranteed to produce the same secret key.

Discussion

The particular weakness exploited in this work can be closed by developing suitable countermeasures[25]. Single-photon sensitivity of Bob's APDs can be tested at random times by a calibrated light source placed inside Bob. The incoming blinding light may be detected, either by a separate watchdog detector or by monitoring electrical and thermal parameters of the APDs. Eve introduces 212 ns time delay ('Jitter and insertion delay introduced by Eve' section in Methods), however, monitoring may be impractical, and Eve can compensate this delay by shortening the fibre line. Eve's need to calibrate her FSG before the attack cannot be considered a reliable deterrent, because she may calibrate non-obtrusively[23]. Other countermeasure proposals that break the described attack exist and may be relatively easy to implement. However, a countermeasure that incorporates into the existing security proofs[6,5,26,27] and thus closes this loophole definitely, such as the one in ref. 25, has not yet been implemented.

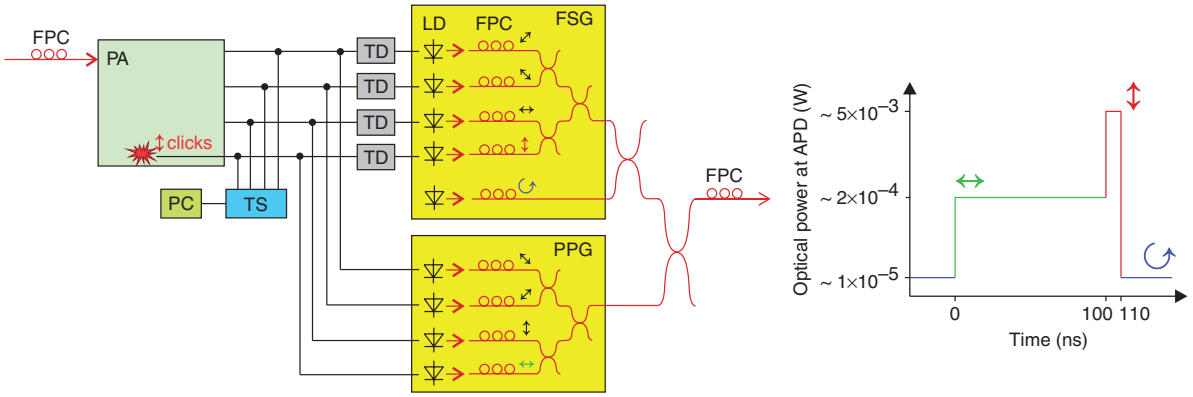

Figure 5 | Complete Eve's setup forming an improved control diagram. This setup was used for all eavesdropping experiments reported in this article. Four LDs followed by FPCs comprise a pre-pulse generator (PPG). Timing of each main trigger pulse is adjusted by a trimmable time-delay (TD) circuit. The FPC before the PA is used to align Eve's polarization reference frame after inserting her into the line (similarly to the manual FPC used in Alice's setup for alignment during QKD system installation).

In conclusion, we have demonstrated a complete and undetected eavesdropping attack against an established QKD system. The success of this demonstration proves that a technological imperfection in a QKD system can be fully exploited using off-the-shelf components. As there is a variety of potentially exploitable loopholes in both research and commercial QKD systems[7,8,10–17,23], Eve can design a tailored attack on one or the other implementation problem. We have briefly discussed how one particular loophole can be closed. However, a more pointed question is what problems still lurk unnoticed in the gap between the theoretical description and the practical systems[28]. Just as in classical cryptography, an ongoing search for backdoors is required to build hardened implementations of quantum cryptography for real-world use.

Methods

Complete Eve's setup. The task of Eve's FSG is to make the target detector at Bob click, while keeping his other detectors silent. An optical pulse of a peak power P_{th} at the target detector causes it click with 100% probability. In order for the FSG depicted in Figure 1b to work, a pulse of power $P_{th}/2$ should never cause the two conjugate-basis detectors to click. Unfortunately, for the actual Bob's polarization analyser this condition did not hold, because one of its detectors turned out to have significantly higher click thresholds than the other three (Fig. 4). Note that for blinding power $>1\,\mu W$, the click thresholds of all four detectors rose uniformly. We tried to change the circular blinding polarization to elliptical, such that the detector with higher click threshold received much less blinding power than the other three. This achieved almost perfect fidelity of Eve's control over Bob, with diagonal elements $>96.2\%$ (in terms of Table 1) and off-diagonal elements $<0.005\%$. The latter meant Eve had slightly less than full information on the sifted key, compromising the security but requiring an additional cryptanalytic task to complete the eavesdropping.

We then improved the control method by including a polarized pre-pulse that dynamically increased blinding power at the orthogonal-basis detectors 100 ns before the main trigger pulse was sent (Fig. 5). These pre-pulses were emitted by four additional laser diodes. With this setup, clicks never occurred in a wrong detector. When we calibrated Eve's control of Bob by sending the same faked state at a fixed rate, the click probability in any target detector was 100%, and double clicks did not occur. However, as we discovered later in the recorded experimental data, a cross-talk between adjacent faked states (which could be as closely spaced as 550 ns during eavesdropping) led to slightly $<100\%$ click probability, as Table 1 illustrates. There were also a few double clicks. Nevertheless, Eve managed to recover complete sifted key by proper post-processing, which shows robustness of this control method.

Jitter and insertion delay introduced by Eve. After initially inserting Eve into the line, her four detection and Bob control channels had slightly different insertion delays (varying by $\lesssim$1 ns). As Alice and Bob used a tight coincidence window to identify photon pairs, we had to equalize Eve's insertion delays by adjusting the time-delay circuits (shown in Fig. 5). As can be seen in Figure 6, the resulting relative coincidence time distributions were indistinguishable from those without eavesdropping. The jitter between photon pairs stayed about the same and was

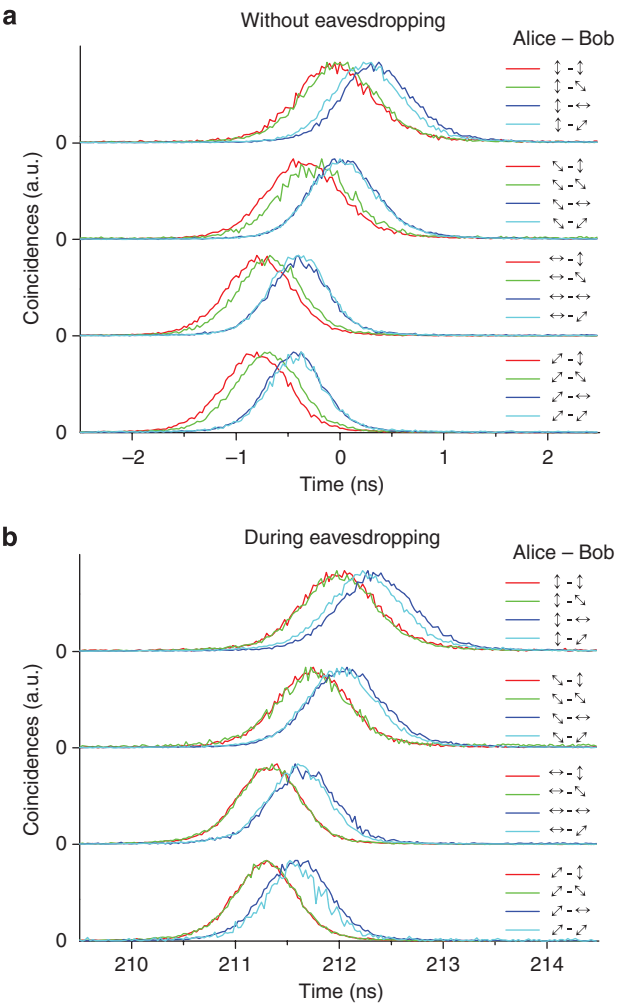

Figure 6 | Coincidence timing distributions for all 16 detector combinations Alice–Bob, measured at outputs of Alice's and Bob's detectors and normalized. (**a**) Distributions without eavesdropping. The full-width at half-magnitude (FWHM) averaged over the 16 coincidence peaks is 761 ps. The QKD software corrects for relative time shift between the peaks via a set of calibration constants. (**b**) Distributions with Eve inserted into the line, after time-delay adjustment. The FWHM averaged over the 16 peaks is 779 ps.

dominated by timing jitter of the single-photon detectors, ≈500 ps full-width at half-magnitude for each detector.

As Figure 6 shows, Eve introduced an overall insertion delay of 212 ns. This went without any consequence, because Alice and Bob synchronized their clocks by photon coincidences, which is a common practice in QKD systems of this type. In general, the propagation delay is not authenticated and is not a part of the QKD security. We remark that if Alice and Bob synchronized their clocks in some independent way (which is probably impractical), Eve could cancel her insertion delay by shortening the fibre-optic line and/or bypassing a part of the line by spatially separating her polarization analyser and FSG and establishing a line-of-sight radio-frequency link between them, in which signals travel ~1.5 times faster than in fibre[23]. These tricks would not apply to systems using a free-space line-of-sight QKD link[18–20,29–32], but so far none of them implemented a clock synchronization method that would fail because of Eve's insertion delay.

Raw experimental data and Eve's key extraction software. There were four eavesdropped QKD sessions over 2 h. For example, the second session lasted 5 min and produced a 393,323-bit sifted key, which was identical between Bob and Eve. The raw data recorded during this session and the script used to extract Eve's sifted key can be found in a single archive file: http://www.vad1.com/eve-extract-sifted-key.zip (74 MiB). The minimum disc space required is 125 MiB, including files generated by running the script.

The main script to do Eve's key extraction, named eve_extract_sifted_key.m, can be found in the directory scripts-matlab, while the other files in this directory are functions called by the main script, and a log file proclog.txt will be generated after running the script. The script is implemented in MATLAB. We have tested it under both Windows and Linux.

The directory data-raw contains the raw experimental data from this session, recorded during the experiment. To obey realistic eavesdropping conditions, Eve only gets access to the classical channel where the transmission is public (and to her own computer), but not to Bob's or Alice's computers. Hence, the script is run only on the timing and basis choice data sent from Bob to Alice (the subdirectory alice-receivefiles), the sifting response returned from Alice (the subdirectory bob-receivefiles), and Eve's own recorded click data (the subdirectory eve-raw-events). Although not used by the extraction script, both sifted and final secret keys recorded in Alice's and Bob's computers are also provided in the archive, to satisfy a curious reader. The final secret key is 218,462 bit long.

After running the script, Eve's sifted key will be extracted and stored in a new directory named data-produced-by-scripts. The script then does a bitwise comparison between Eve's and Bob's sifted keys, and reports the number of discrepancies (which is zero for all eavesdropped QKD sessions). For convenience, both Bob's and Eve's sifted keys are also saved as two sets of ASCII files.

All data are partitioned into files by epoch (defined as a time span of 2^{29}ns≈0.537 s), except the final secret key which is stored in blocks of nine epochs. All file formats are openly defined and documented[21], and have been used in several QKD experiments previously[18–20].

References

1. Singh, S. *The Code Book* (Random House, 1999).
2. Bennett, C. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Proc. IEEE Int. Conf. on Comp. Sys. Signal Process (ICCSSP)* 175–179 (1984).
3. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *J. Cryptology* **5,** 3–28 (1992).
4. Stucki, D. *et al.* High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.* **11,** 075003 (2009).
5. Gottesman, D., Lo, H.- K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.* **4,** 325–360 (2004).
6. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
7. Vakhitov, A., Makarov, V. & Hjelme, D. R. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *J. Mod. Opt.* **48,** 2023–2038 (2001).
8. Xu, F., Qi, B. & Lo, H.- K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.* **12,** 113026 (2010).
9. Félix, S., Gisin, N., Stefanov, A. & Zbinden, H. Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses. *J. Mod. Opt.* **48,** 2009–2021 (2001).
10. Nauerth, S., Fürst, M., Schmitt-Manderbach, T., Weier, H. & Weinfurter, H. Information leakage via side channels in freespace BB84 quantum cryptography. *New J. Phys.* **11,** 065001 (2009).
11. Kurtsiefer, C., Zarda, P., Mayer, S. & Weinfurter, H. The breakdown flash of silicon avalanche photodiodes—backdoor for eavesdropper attacks? *J. Mod. Opt.* **48,** 2039–2047 (2001).
12. Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **74,** 022313 (2006), erratum: *ibid.* **78**, 019905 (2008).
13. Lamas-Linares, A. & Kurtsiefer, C. Breaking a quantum key distribution system through a timing side channel. *Opt. Express* **15,** 9388–9393 (2007).
14. Zhao, Y., Fung, C.- H. F., Qi, B., Chen, C. & Lo, H.- K. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **78,** 042333 (2008).
15. Sauge, S., Lydersen, L., Anisimov, A., Skaar, J. & Makarov, V. Controlling an actively-quenched single photon detector with bright light. *Preprint at arXiv:0809.3408 [quant-ph]* (2008).
16. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4,** 686–689 (2010).
17. Wiechers, C. *et al.* After-gate attack on a quantum cryptosystem. *New J. Phys.* **13,** 013043 (2011).
18. Marcikic, I., Lamas-Linares, A. & Kurtsiefer, C. Free-space quantum key distribution with entangled photons. *Appl. Phys. Lett.* **89,** 101122 (2006).
19. Ling, A. *et al.* Experimental quantum key distribution based on a Bell test. *Phys. Rev. A* **78,** 020301 (2008).
20. Peloso, M. P., Gerhardt, I., Ho, C., Lamas-Linares, A. & Kurtsiefer, C. Daylight operation of a free space, entanglement-based quantum key distribution system. *New J. Phys.* **11,** 045007 (2009).
21. QCrypto: an open source code for experimental quantum cryptography, http://code.google.com/p/qcrypto/.
22. Kerckhoffs, A. La cryptographie militaire. *J. des Sci. Militaires* **IX,** 5–38 (1883).
23. Makarov, V. & Hjelme, D. R. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **52,** 691–705 (2005).
24. Lütkenhaus, N. Estimates for practical quantum cryptography. *Phys. Rev. A* **59,** 3301–3319 (1999).
25. Lydersen, L., Makarov, V. & Skaar, J. Secure gated detection scheme for quantum cryptography. *Phys. Rev. A* **83,** 032306 (2011).
26. Fung, C.- H. F., Tamaki, K., Qi, B., Lo, H.- K. & Ma, X. Security proof of quantum key distribution with detection efficiency mismatch. *Quant. Inf. Comp.* **9,** 131–165 (2009).
27. Marøy, Ø., Lydersen, L. & Skaar, J. Security of quantum key distribution with arbitrary individual imperfections. *Phys. Rev. A* **82,** 032337 (2010).
28. Scarani, V. & Kurtsiefer, C. The black paper of quantum cryptography: real implementation problems. *Preprint at arXiv:0906.4547v1 [quant-ph]* (2009).
29. Rarity, J. G., Gorman, P. M. & Tapster, P. R. Secure key exchange over 1.9 km free-space range using quantum cryptography. *Electron. Lett.* **37,** 512 (2001).
30. Hughes, R. J., Nordholt, J. E., Derkacs, D. & Peterson, C. G. Practical free-space quantum key distribution over 10 km in daylight and at night. *New J. Phys.* **4,** 43 (2002).
31. Kurtsiefer, C. *et al.* A step towards global key distribution. *Nature* **419,** 450 (2002).
32. Ursin, R. *et al.* Free-space distribution of entanglement and single photons over 144 km. *Nat. Phys.* **3,** 481–486 (2007).

Acknowledgments

This work was supported by the National Research Foundation and the Ministry of Education, Singapore, and the Research Council of Norway (grant no. 180439/V30). L. Lydersen and V. Scarani are thanked for useful discussions. We thank the OLPC project for providing a notebook for the eavesdropper.

Author contributions

V.M. conceived the idea. Q.L., I.G., A.L.-L., C.K. and V.M. prepared and conducted the experiment. Q.L. and A.L.-L. processed the recorded data with help of I.G. and C.K. Q.L., A.L.-L., I.G. and V.M. wrote the paper. J.S. supervised the NTNU team. C.K. and V.M. supervised the project.

Additional information

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: Gerhardt, I. *et al.* Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* 2:349 doi: 10.1038/ncomms1348 (2011).