LETTERS
PUBLISHED ONLINE: 29 AUGUST 2010 | DOI: 10.1038/NPHOTON.2010.214
nature photonics

Hacking commercial quantum cryptography systems by tailored bright illumination

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

The peculiar properties of quantum mechanics allow two remote parties to communicate a private, secret key, which is protected from eavesdropping by the laws of physics[1–4]. So-called quantum key distribution (QKD) implementations always rely on detectors to measure the relevant quantum property of single photons[5]. Here we demonstrate experimentally that the detectors in two commercially available QKD systems can be fully remote-controlled using specially tailored bright illumination. This makes it possible to tracelessly acquire the full secret key; we propose an eavesdropping apparatus built from off-the-shelf components. The loophole is likely to be present in most QKD systems using avalanche photodiodes to detect single photons. We believe that our findings are crucial for strengthening the security of practical QKD, by identifying and patching technological deficiencies.

The field of quantum key distribution has evolved rapidly in recent decades. Today, quantum key distribution (QKD) implementations in laboratories can generate key over fibre channels with lengths up to 250 km (ref. 6), and a few QKD systems are even commercially available, promising enhanced security for data communication.

In all proofs for the security of QKD, assumptions are made for the devices involved. However, the components used for experimental realizations of QKD deviate from the models in the security proofs. This has led to iterations in which security threats caused by deviations have been discovered, and the loopholes have been closed either by modification of the implementation, or more general security proofs[7–9]. In other cases, information leaking to the eavesdropper has been quantified[10,11].

Attacks exploiting the most severe loopholes are usually experimentally unfeasible with current technology. A prominent example is the photon number splitting attack[12], which requires the eavesdropper Eve to perform a quantum non-demolition measurement of the photon number sent by Alice. The attack is still unfeasible, and has been nullified by improved QKD protocols[13,14]. In contrast, a more implementation-friendly attack is the time-shift attack[15] based on detector efficiency mismatch[16]. Experimentally however, this attack only gave a small information-theoretical advantage for Eve when applied to a modified version of a commercial QKD system[17]. In the attack, Eve captured partial information about the key in 4% of her attempts, such that she could improve her random (brute-force) search over all possible keys.

In this Letter, we demonstrate how two commercial QKD systems id3110 Clavis2 and QPN 5505, from the commercial vendors ID Quantique and MagiQ Technologies, can be fully cracked. We show experimentally that Eve can blind the gated detectors in the QKD systems using bright illumination, thereby converting them into classical, linear detectors. The detectors are then fully controlled by classical laser pulses superimposed over the bright continuous-wave (c.w.) illumination. Remarkably, the detectors exactly measure what is dictated by Eve; with matching measurement bases Bob detects exactly the bit value sent by Eve, whereas

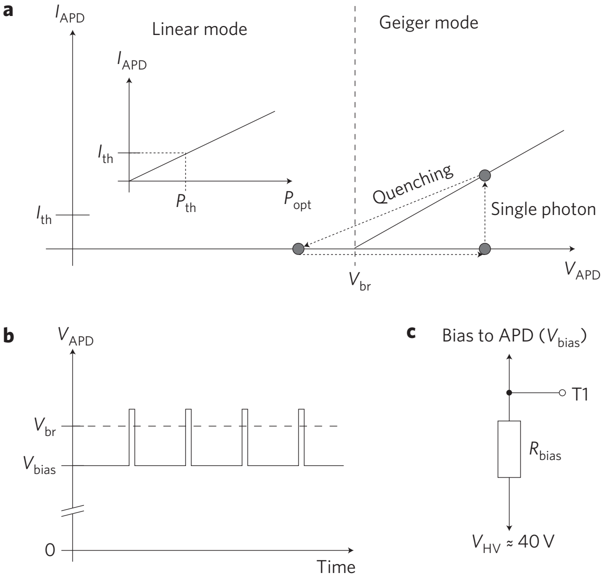

Figure 1 | APD as a single-photon detector. a, In Geiger mode, where the APD is reverse-biased above the breakdown voltage V_{br}, an absorbed single photon causes a large current I_{APD} through the APD. A detection signal called a 'click' occurs when I_{APD} crosses the threshold I_{th}. Afterwards, V_{APD} is lowered below V_{br} to quench the avalanche, before returning to Geiger mode. Below V_{br}, in the linear mode, the current I_{APD} is proportional to the incident optical power P_{opt}. Then I_{th} becomes an optical power threshold P_{th}. **b**, Commercial systems use gated detectors, with the APDs in Geiger mode only when a photon is expected, to reduce false detections called 'dark counts'. In practice, the APD is biased just below V_{br}, and periodical ~3 V voltage pulses create Geiger mode time regions, so-called 'gates'. **c**, In both systems, the bias high-voltage supply V_{HV} has impedance R_{bias} ($R_{bias} = 1$ kΩ in Clavis2 and 20 kΩ in QPN 5505) before V_{bias} is applied to the APD at the point T1. Therefore, any current through R_{bias} reduces V_{bias} (see Supplementary Section I for more details).

---

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

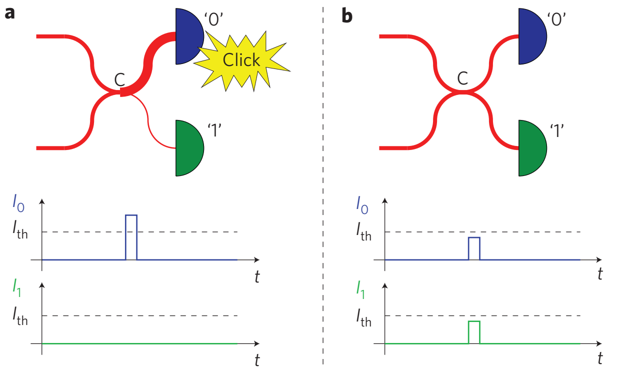

Figure 2 | How Eve's trigger pulses are detected by Bob. Schemes show the last 50/50 coupler (C) and Bob's detectors in a phase-encoded QKD system. Line thickness represents optical power. I_0/I_1 is the current running through APD 0/1. **a**, Eve and Bob have selected matching bases, and Eve has detected the bit value 0. Therefore the trigger pulse from Eve interferes constructively and its full power hits detector 0. The current caused by Eve's pulse crosses the threshold current I_{th} and causes a click. **b**, Eve and Bob have selected opposite bases. The trigger pulse from Eve does not interfere constructively and half of its power hits each detector. This causes no click as the current is below the threshold I_{th} for each detector.

with incompatible bases the bit is undetected by Bob. Even the detectors' dark counts are completely eliminated (but can be simulated at will by Eve). Based on these experimental results we propose in detail how Eve can attack the systems with off-the-shelf components, obtaining a perfect copy of the raw key without leaving any trace of her presence.

Today most QKD systems use avalanche photodiodes (APDs) to detect single photons[18]. To detect single photons, APDs are operated in Geiger mode (Fig. 1). However, all APDs spend part of the time biased under the breakdown voltage, in the linear mode. During this period, the detector remains sensitive to bright light, with a classical optical power threshold P_{th}. If Eve has access to the APDs in the linear mode, she may eavesdrop on the QKD system with an intercept-resend (faked-state[19,20]) attack as follows. Eve uses a copy of Bob to detect the states from Alice in a random basis. Eve resends her detection results, but instead of sending pulses at the single photon level she sends bright trigger pulses, with a peak power just above P_{th}. Bob will only have a detection event if his active basis choice coincides with Eve's basis choice (Fig. 2), otherwise no detector clicks. This causes half of the bits to be lost, but in practice this is not a problem because transmittance from the output of Alice to Bob's detectors is much lower than 1/2. Also Bob's APDs rarely have a quantum efficiency over 50%, but the trigger pulses always cause clicks. For a Bob using passive basis choice, Eve launches the peak power at just above $2P_{th}$, because half of the power hits the conjugate basis detectors[20]. Then Bob's detector always clicks.

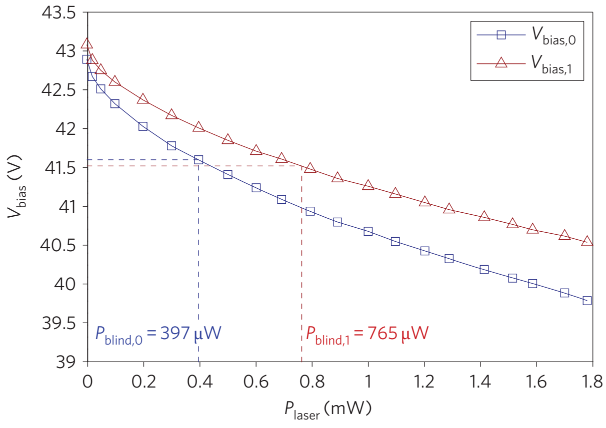

Figure 3 | Bias voltage at T1 versus c.w. laser power for Clavis2. Detector 0 is blind (dark count rate exactly zero) at $P_{laser} > 397$ μW, and detector 1 is blind at $P_{laser} > 765$ μW. QPN 5505 has similar characteristics; due to the larger value of R_{bias}, its detector 0 goes blind at $P_{laser} > 60$ μW and detector 1 goes blind at $P_{laser} > 85$ μW (see Supplementary Section II for more details of QPN 5505 blinding).

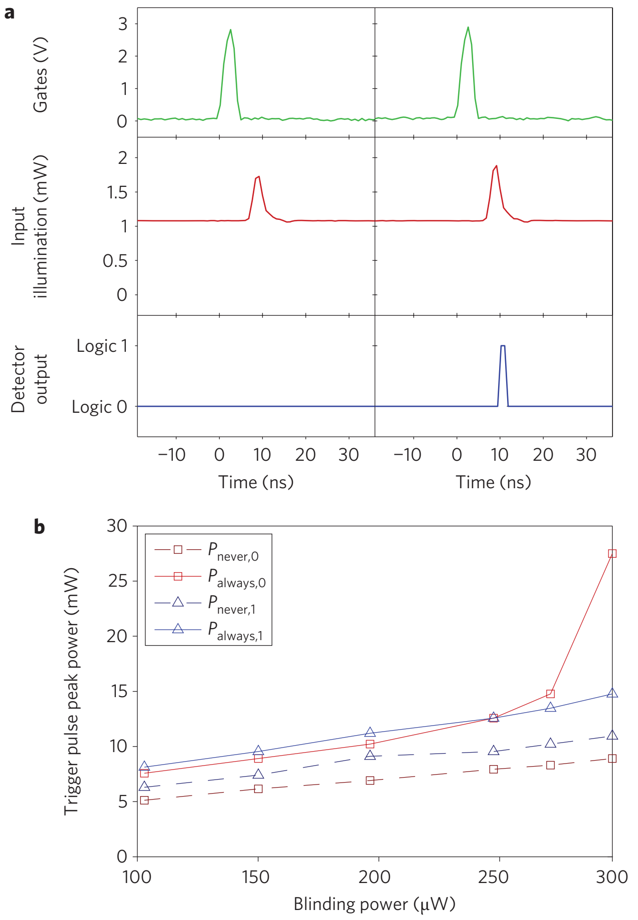

Figure 4 | Detector control. a, Electrical and optical signal oscillograms when detector 0 in Clavis2 is blinded by 1.08 mW c.w. illumination, and controlled by a superimposed 2.5-ns-long laser pulse timed slightly behind the gate (see Supplementary Section III for detailed measurement setup). The superimposed $P_{never,0} = 647$ μW (detector 1: $P_{never,1} = 697$ μW) trigger pulse never causes a detection event, whereas the $P_{always,0} = 808$ μW ($P_{always,1} = 932$ μW) trigger pulse always causes a detection event. **b**, Click thresholds versus the applied c.w. blinding illumination for the QPN 5505. When the blinding power increases, $P_{always,0}$ diverges, perhaps because the bias voltage is approaching the punch-through voltage of the APD (see Supplementary Section II).

After the raw key exchange, Bob and Eve have identical bit values and basis choices. Because Alice and Bob communicate openly during sifting, error correction and privacy amplification[5], Eve simply listens to this classical communication and applies the same operations as Bob to obtain the identical final key.

The attack is surprisingly general. All commercial QKD systems and the vast majority of research systems use APD-based detectors, which all operate their APDs part time in linear mode. Detectors with passively and actively quenched APDs can also be kept in linear mode through blinding[20,21]. The attack works equally well

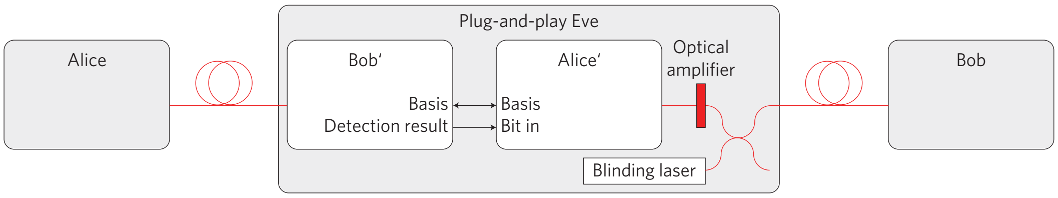

Figure 5 | Proposed plug-and-play Eve. In the plug-and-play scheme[24], the laser pulses travel from Bob to Alice and back to Bob, passing Bob's interferometer twice. Therefore, polarization drift in the fibre and drift in Bob's interferometer are automatically compensated. Eve consists of copies of Alice (Alice′) and Bob (Bob′), which share bit and basis settings, a blinding laser, and an optical amplifier used to obtain the proper trigger pulse power. Owing to the plug-and-play principle, any environmental perturbations in the fibres Alice–Bob′ and Alice′–Bob are automatically compensated. See Supplementary Section IV for a more detailed scheme.

on the Scarani–Acin–Ribordy–Gisin 2004 (SARG04)[14] and decoy-state BB84[13] protocols as well as the normal BB84 protocol[4]. With suitable modifications it applies to differential phase shift (DPS)[22], and given the right set of detector parameters to coherent one-way (COW)[23] protocols.

Note that the threshold P_{th} should be sufficiently well defined for perfect eavesdropping. To be precise, let detector i always click from a trigger pulse of optical peak power $\geq P_{\mathrm{always},i}$, and never click from a trigger pulse of optical peak power $\leq P_{\mathrm{never},i}$. The requirement for Eve to be able to make any single detector click, while none of the other detectors clicks, can be expressed in terms of the click thresholds as

$$\max_i\left\{P_{\mathrm{always},i}\right\} < 2\left(\min_i\left\{P_{\mathrm{never},i}\right\}\right) \qquad (1)$$

When eavesdropping, simply applying trigger pulses between the gates populates carrier trap levels in the APD, thus raising the dark count probability and causing a too high quantum bit error rate (QBER). To avoid this, Bob's detectors were blinded[20,21]. The detectors are then insensitive to single photons and have no dark counts. Outside the gates the APD is biased below the breakdown voltage, and the current caused by illuminating the APD is increasing with respect to the incident optical power. A current through the APD will decrease the bias voltage over the APD due to the presence of R_{bias} (Fig. 1c) and the internal resistance of the APD. Figure 3 shows the bias voltage drop at the point T1 in Clavis2 under c.w. illumination.

The blinding is caused by the drop of V_{bias} such that the APD never operates in the Geiger mode, but rather is a classical photodiode at all times. The voltages $V_{\mathrm{HV},0/1}$ of the high-voltage supplies do not change; the entire change of V_{bias} is due to the resistors R_{bias}. Although shorting this resistor seems like an easy countermeasure, at least for Clavis2 this does not prevent blinding. With higher illumination the electrical power dissipated in the APD generates substantial heat. Raised APD temperature increases its breakdown voltage by about 0.1 V $^{\circ}$C^{-1} while V_{bias} remains constant, which also leads to blinding (at several times higher power level, 4–10 mW).

To demonstrate detector control in Clavis2, each detector was blinded with 1.08 mW optical power with a 2.5-ns-long trigger pulse superimposed slightly after the gate. Note that a shorter trigger pulse can be timed inside the gate. Figure 4a shows the response of detector 0 in Clavis2 to trigger pulses at the click thresholds.

Similarly, for the QPN 5505, the trigger pulse was timed with its leading edge about 5 ns after the gate. Figure 4b shows the click thresholds for the detectors when blinded with 100–300 μW c.w. blinding illumination. In this case, for blinding power levels of 100–250 μW, the detectors remain silent at a power level of $\leq 0.61 P_{\mathrm{always},1}$.

For both systems the click thresholds fulfil equation (1), so perfect eavesdropping is possible. Further, both systems under investigation operate according to the plug-and-play principle[24], which allows an easily installable plug-and-play eavesdropper (Fig. 5).

A full eavesdropper based on bright-light detector control has previously been implemented and tested under realistic conditions on a 290-m experimental entanglement-based QKD system (Gerhardt, I. *et al.*, unpublished results). Because the attack is clearly implementable, building a full eavesdropper for a commercial cryptosystem would not further expose the problem. A better use of effort is to concentrate on thoroughly closing the vulnerability. An optical power meter at Bob's entrance with a classical threshold seems like an adequate countermeasure to prevent blinding. However, the power meter output should be included in a security proof. Furthermore, the click threshold at the transition between linear and Geiger mode may be very low, allowing practically non-detectable control pulses. How to design hack-proof detectors is unclear to us at this stage, and all future detectors clearly must be tested for side channels.

We believe that openly discovering and closing security loopholes is a necessary step towards practical and secure QKD, as it has been for multiple security technologies in the past. For example, RSA public key cryptography has been subject to extensive scrutiny, which has led to the discovery of effective attacks based on implementation loopholes[25]. In our view, quantum hacking is an indication of the mature state of QKD rather than its insecurity. Rather than demonstrating that practical QKD cannot become provably secure[26], our findings clearly show the necessity of investigating the practical security of QKD. Any large loopholes must be eliminated, and remaining imperfections must be incorporated into security proofs.

Both ID Quantique and MagiQ Technologies were notified about the loophole before this publication. ID Quantique has implemented countermeasures. According to MagiQ Technologies the system QPN 5505 has been discontinued; newer models of their system have not been available for our testing.

Received 2 April 2010; accepted 11 July 2010;
published online 29 August 2010

References

1. Mayers, D. Advances in cryptology. *in Proceedings of Crypto '96*, Vol. 1109 (ed. Koblitz, N.) 343–357 (Springer, 1996).
2. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283,** 2050–2056 (1999).
3. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441–444 (2000).
4. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 175–179 (IEEE Press, 1984).
5. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
6. 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).
7. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.* **4,** 325–360 (2004).

8. 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).
9. Lydersen, L. & Skaar, J. Security of quantum key distribution with bit and basis dependent detector flaws. *Quant. Inf. Comp.* **10,** 60–76 (2010).
10. Lamas-Linares, A. & Kurtsiefer, C. Breaking a quantum key distribution system through a timing side channel. *Opt. Express* **15,** 9388–9393 (2007).
11. 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).
12. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61,** 052304 (2000).
13. Hwang, W. Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
14. Scarani, V., Acin, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **92,** 057901 (2004).
15. Qi, B., Fung, C.-H.F., Lo, H.-K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quant. Inf. Comp.* **7,** 73–82 (2007).
16. 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).
17. 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).
18. Cova, S., Ghioni, M., Lotito, A., Rech, I. & Zappa, F. Evolution and prospects for single-photon avalanche diodes and quenching circuits. *J. Mod. Opt.* **51,** 1267–1288 (2004).
19. Makarov, V. & Hjelme, D. R. Faked states attack on quantum cryptosystems. *J. Mod. Opt.* **52,** 691–705 (2005).
20. Makarov, V., Anisimov, A. & Sauge, S. Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by Eve. Preprint at <http://arXiv:quant-ph/0809.3408v2>.
21. Makarov, V. Controlling passively quenched single photon detectors by bright light. *New J. Phys.* **11,** 065003 (2009).
22. Takesue, H. *et al.* Differential phase shift quantum key distribution experiment over 105 km fibre. *New J. Phys.* **7,** 232 (2005).
23. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87,** 194108 (2005).
24. Muller, A. *et al.* 'Plug and play' systems for quantum cryptography. *Appl. Phys. Lett.* **70,** 793–795 (1997).
25. Boneh, D. Twenty years of attacks on the RSA cryptosystem. *Notices Am. Math. Soc.* **46,** 203–213 (1999).
26. Scarani, V. & Kurtsiefer, C. The black paper of quantum cryptography: real implementation problems. Preprint at <http://arXiv:quant-ph/0906.4547v1>.

Acknowledgements

This work was supported by the Research Council of Norway (grant no. 180439/V30). The authors acknowledge the overall cooperation and assistance of the Max Planck Institute for the Science of Light, Erlangen, and G. Leuchs personally. L.L. and V.M. thank the Group of Applied Physics at the University of Geneva, ID Quantique and armasuisse Science and Technology for their hospitality, discussions, cooperation and loan of equipment. The Service of Radiology of the Cantonal Hospital of Geneva is thanked for their quick help in revealing the internal layers in the multilayer printed circuit board of a commercial detector.

Author contributions

V.M. conceived the idea and planned the study. L.L. and V.M. conducted the Clavis2 experiment with the help of C. Wiechers, D.E. and C. Wittmann. L.L. and V.M. conducted the QPN 5505 experiment. L.L. and J.S. wrote the paper and Supplementary information, with input from all authors. J.S. and V.M. supervised the project.

Additional information

The authors declare no competing financial interests. Supplementary information accompanies this paper at www.nature.com/naturephotonics. Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/. Correspondence and requests for materials should be addressed to L.L.