Cracking quantum cryptography*

Vadim Makarov
Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway

Quantum key distribution (QKD) is a technique to securely grow a shared secret key between two remote parties [1]. Commercial implementations of QKD are available since 2005 and are used to secure network traffic (Fig. 1). QKD is proven unconditionally secure based on the laws of quantum physics [2]. However, security proofs necessarily assume an idealized model of equipment. Numerous discrepancies between the model and actual hardware have been found, leading to loopholes that can be used to eavesdrop the secret key.

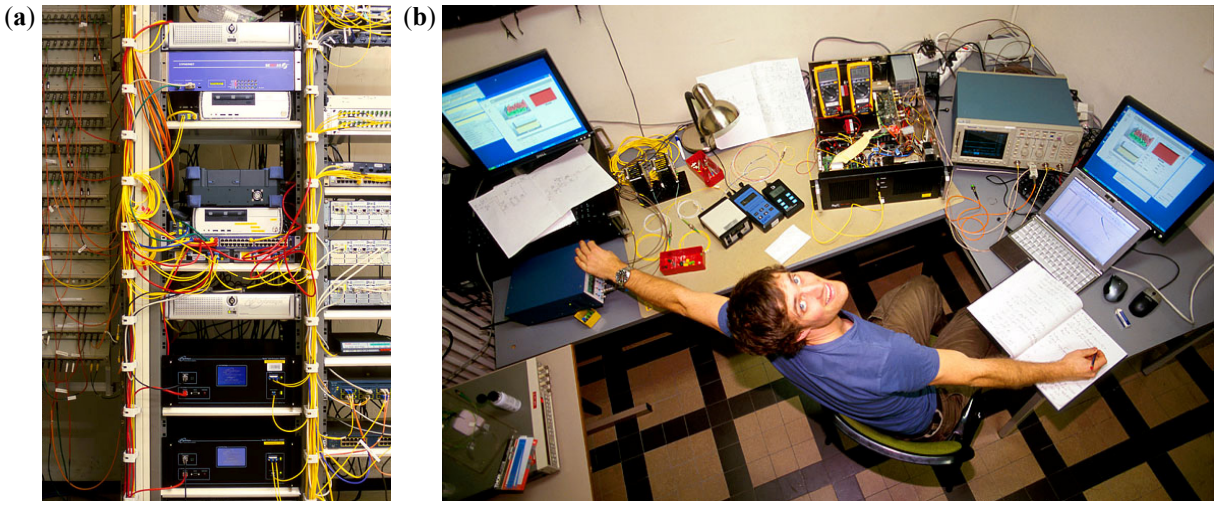

Fig. 1. Commercial QKD equipment vintage 2010. (**a**) Systems from ID Quantique installed together with high-speed classical link encryption equipment in a network node, encrypting all traffic with two other nodes. (**b**) A quantum hacker (L. Lydersen) at work, testing MagiQ Technologies QPN 5505 system for loopholes [5].

Several attacks on commercial QKD systems have been demonstrated, with various degrees of success. In a **time-shift attack**, variations of single-photon detection efficiency between quantum receiver's detectors are exploited to give an attacker a *partial* knowledge of the secret key [3]. In a **phase-remapping attack**, time-dependence of sender's phase modulation when preparing a quantum state is exploited to surreptitiously make a modified set of quantum states more easily distinguishable by the attacker [4]; however this attack introduces a high error rate and is discoverable under most QKD protocols. A **detector control attack** is free from these limitations, and allows the eavesdropper to obtain *full secret key* while remaining unnoticed by the legitimate parties [5]. The attack uses one of several mechanisms in the single-photon detector to force an avalanche photodiode to operate in a linear regime, not responsive to single photons but deterministically controllable by bright-light pulses. This vulnerability has been confirmed in both commercial QKD systems on the market as of 2010 [5]. A full field implementation of the detector control attack has been demonstrated on an installed connection using a research QKD system [6].

Partial countermeasures to these loopholes are possible, and some have been made by the manufacturers. However, the most general way to close the above loopholes is integrating them into a security proof. A countermeasure allowing a security proof that takes detector imperfections into account is being developed [7].

References

* Slides from this conference presentation will be available at http://www.iet.ntnu.no/groups/optics/qcr/other.html
[1] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," J. Cryptology **5**, 3 (1992).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301 (2009).
[3] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," Phys. Rev. A **78**, 042333 (2008).
[4] F. Xu, B. Qi, and H.-K. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," New J. Phys. **12**, 113026 (2010).
[5] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nat. Photonics **4**, 686 (2010); L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," Opt. Express **18**, 27938 (2010).
[6] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Perfect eavesdropping on a quantum cryptography system," arXiv:1011.0105 [quant-ph].
[7] L. Lydersen, V. Makarov, and J. Skaar, "Secure gated detection scheme for quantum cryptography" (unpublished).