Inducing a detector efficiency mismatch to hack a commercial quantum key distribution system

N. Jain[1,3], L. Lydersen[2,5], C. Wittmann[1,3], C. Wiechers[1,4], D. Elser[1,3], Ch. Marquardt[1,3], V. Makarov[2] and G. Leuchs[1,3]

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

Quantum key distribution (QKD) is poised to be the first widespread implementation of quantum communication. In principle, it offers unconditional security: an eavesdropper introduces errors and thus cannot remain concealed from the legitimate parties. However, in practical implementations the actual security depends on a host of technological and protocol-operational components. Eve could exploit imperfections in Alice's or Bob's equipment (such as source or detectors) remotely, or vulnerabilities in the actual implementation of the abstract QKD protocol. Several such attacks have been proposed [1,2], and various proof-of-principle demonstrations on commercial QKD devices have been performed in recent years [3–5].

Detector efficiency mismatch can be used to compromise the security of QKD cryptosystems by exploiting variations in the detection efficiency as a function of some parameter that is controllable by Eve [2]. We propose and experimentally demonstrate a hack to induce a large and deterministic temporal efficiency mismatch between the two detectors of Clavis2, a commercial QKD system from ID Quantique [6].

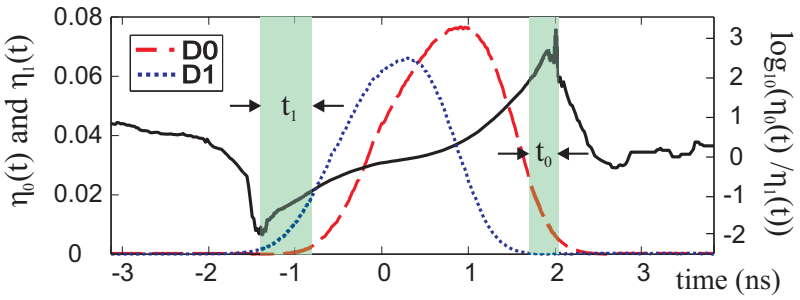

Fig. 1 Induced mismatch and Eve's faked-state attack: Efficiencies $\eta_0(t)$ and $\eta_1(t)$ measured at the single-photon level, with a time shift of 450 ps. The logarithm of their ratio quantifies the degree of mismatch (solid line). In comparison to the uncompromised case, the degree of mismatch is found to be at least two orders of magnitude higher in the flanks. To eavesdrop successfully, Eve times 'bright' faked states to arrive at times $t = t_0$ or $t = t_1$ (shaded vertical regions).

A calibration sequence named line length measurement (LLM) performs temporal calibration of the gating window in the self-stabilized interferometric plug-and-play setup of Clavis2 [7]. By controlling the activation instants of the gates of the two detectors D0 and D1, any existing mismatch between the respective temporal efficiencies $\eta_0(t)$ and $\eta_1(t)$ is minimized.

Eve exploits a weakness in the implementation of LLM and obtains a time shift of the order of 450 ps. The induced mismatch shown in Fig. 1 serves as a straightforward improvement in launching the time-shift attack [5]. Alternatively, a faked-state attack can be devised based on the scheme in [2]. We develop a strategy for Eve to minimize the quantum bit error rate (QBER) under realistic conditions by optimizing the mean photon number of the faked states – in form of coherent pulses – and timing them appropriately at some time $t = t_{0(1)}$, where D1(0) is nearly blind (refer Fig. 1). The security of the system is then fully compromised as Eve's attack results in a QBER below 11% without Bob noticing any deviation from his expected detection rate. To prevent this hack, we also propose a simple countermeasure which has already been communicated to ID Quantique [6].

References

[1] V. Makarov and D. R. Hjelme, J Mod. Opt. **52**, 691 (2005); B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Info. Compu. **7**, 73 (2007); C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).
[2] V. Makarov, A. Anisimov and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[3] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, Nat. Photonics **4**, 686 (2010); C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, Ch. Marquardt, V. Makarov and G. Leuchs, arXiv:1009.2683 (2010); L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, Opt. Exp. **18**, 27938 (2010)
[4] F. Xu, B. Qi and H.-K. Lo, New J. Phys. **12**, 113026 (2010)
[5] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[6] ID Quantique URL `http://www.idquantique.com`; the company uses our discoveries to improve their QKD system
[7] D. Stucki et al, New J. Phys. **4**, 41 (2002); ID Quantique QKD System id 3100 Clavis2 User Guide (2008).