Quantum hacking: how Eve can exploit component imperfections to control yet another of Bob's single-photon qubit detectors

***S. Sauge*[1], *V. Makarov*[2], *A. Anisimov*[3]**

1. Department of Microelectronics and Information Technology, Royal Institute of Technology (KTH), Sweden

2. Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway

3. Radiophysics Department, St. Petersburg State Polytechnic University, Russia

Security and integrity of the network and the traffic it carries is a key requirement in modern communication systems. Over the past twenty years, quantum key distribution (QKD) has gained world-wide attention. This is because security of its implementations is based on the impossibility, in principle, to reliably copy an a-priori unknown quantum state (no-cloning theorem). However, security also relies on the assumption that electro-optical devices which are part of quantum cryptosystems do not deviate from model assumptions made to establish security proofs. This second range of security threats, which target component imperfections, has already been successfully exploited by one of the authors to take control of commonly used single photon detectors, namely InGaAs-based modules at telecom wavelengths [1] and Silicon-based passively-quenched modules in the visible - near infrared range [2].

In this study, we investigated several possible attacks that an eavesdropper could launch against cryptosystems equipped with yet another commonly used Silicon photon counting detector module operating with active quenching and manufactured by Perkin Elmer (model SPCM-AQR). We showed that when the avalanche photo-diode (APD) of the detector gets illuminated with bright optical pulses (instead of single photons), the voltage at which the APD is biased drops by more than 12–14 V if the repetition rate of the bright pulses is large enough (above 70kHz here). Under those conditions, the detector thus becomes totally insensitive to single photons as well as dark counts and afterpulses, only producing an output pulse (a "click") when a brighter optical pulse is applied at its input, see Fig. 1 below.

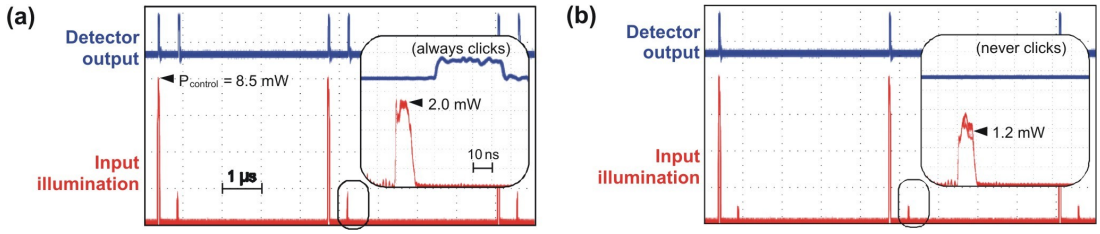

Fig. 1 Quantum hacking control mode – Detector output (blue curve) illuminated by a bright optical pulse (red curve) made of a *control* pulse (8.5 mW, 50 ns wide, 230 kHz repetition rate), which blinds all detectors at the receiving end, and a *signal* pulse, which above a certain intensity threshold makes the target detector click with sub-nanosecond time jitter, as shown on the picture (detectors always click in case a, never click in case b).

With such a control mode allowing to blind ("0") or make a detector click ("1") at will with unity probability and sub-nanosecond time jitter, an eavesdropper (Eve) could intercept each quantum bit encoded by the sender (Alice) with an exact replica of the detection apparatus used by the receiver (Bob), then send a faked state targeting the corresponding detector at the receiver's side, allowing her to get a complete copy of the cryptographic key without being noticed unless light intensity across the link is monitored.

As an example of such a faked state attack, let us consider a QKD scheme using single photon qubits encoded in polarization states |H> ("0"), |V> ("1") in the horizontal/vertical basis, and |D>= (|H> + |V>)/2 ("0") and |A>= (|H> - |V>)/2 ("1") in the conjugate basis. Let us assume that Eve targets detector "H" for a given qubit. Sending input illuminations of type (a) with 2 mW signal pulse for H polarization but *no* signal pulse for V polarization will make detector "H" click while keeping all three other detectors "V", "D" and "A" blind.

In conclusion, we have demonstrated a vulnerability of PerkinElmer SPCM-AQR detector module that may, at least under some conditions, be used to eavesdrop on a QKD system. For real world implementations, "quantum hacking" shall help uncovering and patching potential technological imperfections while QKD systems get incorporated to protect the integrity of data.

References

[1] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems", Phys. Rev. A **74**, 022313 (2006).

[2] V. Makarov, arXiv:0707.3987v2 [quant-ph].