Passively quenched avalanche photodiode의 포화 모드를 이용한 양자암호 시스템 공격에 대한 연구

Exploiting the saturation mode of passively quenched avalanche photodiodes to attack quantum cryptosystems

V. Makarov[1]

Department of Physics, Pohang University of Science and Technology, 790-784 Pohang, South Korea
Department of Electronics and Telecommunications,
Norwegian University of Science and Technology, NO-7491 Trondheim, Norway
(Sibmitted January 8, 2008)

Quantum key distribution (QKD) is a technique for generating a secret random cryptographic key over an insecure optical communication channel [1]. Experimental QKD has grown from a proof-of-the principle experiment assembled on an optical table eighteen years ago to commercially available equipment today and numerous experiments over more than 100 km distance in optical fiber and in free space. Security of QKD is based, in principle, on the laws of quantum mechanics. Strict security proofs of its unconditional security now exist. However, a number of security studies concern imperfections of real hardware that have not been accounted properly in the security proof. My study is one of these: it investigates a component commonly used in QKD systems, a single-photon detector (SPD). Many SPDs used today are based on a passively quenched avalanche photodiode (APD).

Passively quenched APD responds to light linearly only up to a certain intensity; at higher input intensities the output count rate of the detector begins to saturate, peaks, then as the illumination further increases it drops to zero and the SPD becomes blinded (Fig. 1). This behavior seems to be inherent to the passively quenched design. I have tested two different models of SPD, both of which exhibit this behavior similarly: a modern do-it-yourself design by the National University of Singapore (henceforth model 1), and an old SPD module SPCM-200-PQ manufactured by EG&G (henceforth model 2). Why the saturation occurs becomes clear from the electrical circuit diagram of the detector (Fig. 2). When there are no photons coming and no current flowing through the APD, it is biased above the breakdown voltage. When a photon strikes the APD, it causes an avalanche, during which the small parasitic capacitances (~1 pF, shown on the circuit diagram in gray) quickly discharge through the APD, the voltage drops and the avalanche self-quenches. The discharge pulse is monitored by a fast comparator. Subsequently, the capacitances slowly charge through the large-value bias resistor. The APD is incapable of producing avalanches of sufficient amplitude to flip the comparator be-

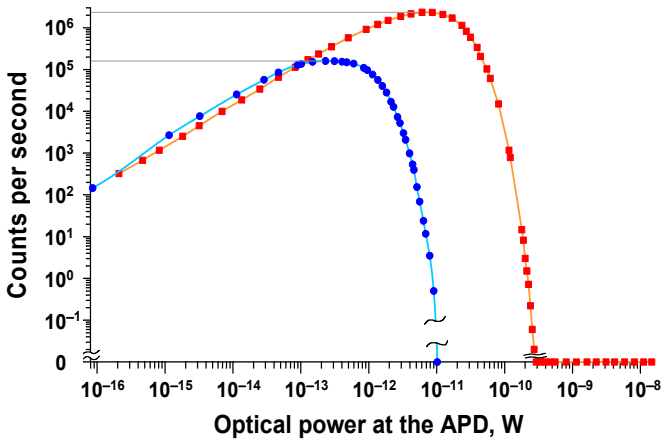

Fig. 1. Saturation curves of the SPDs. Circles: National University of Singapore design, squares: EG&G SPCM-200-PQ.

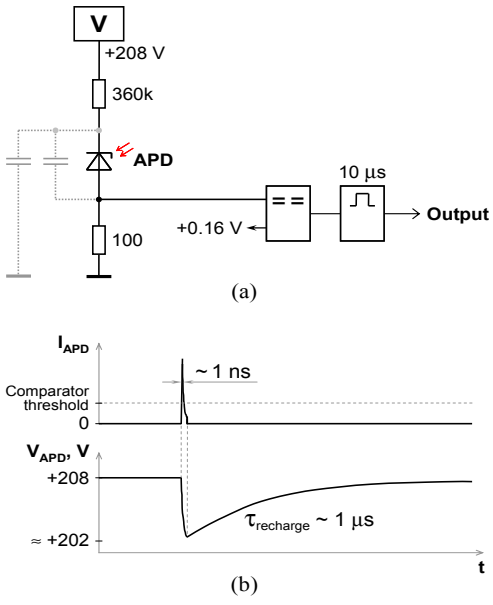

Fig. 2. SPD model 1: (a) equivalent circuit diagram; (b) current through the APD and voltage at the APD during avalanche and subsequent recharge.

[1] Email: makarov@vad1.com

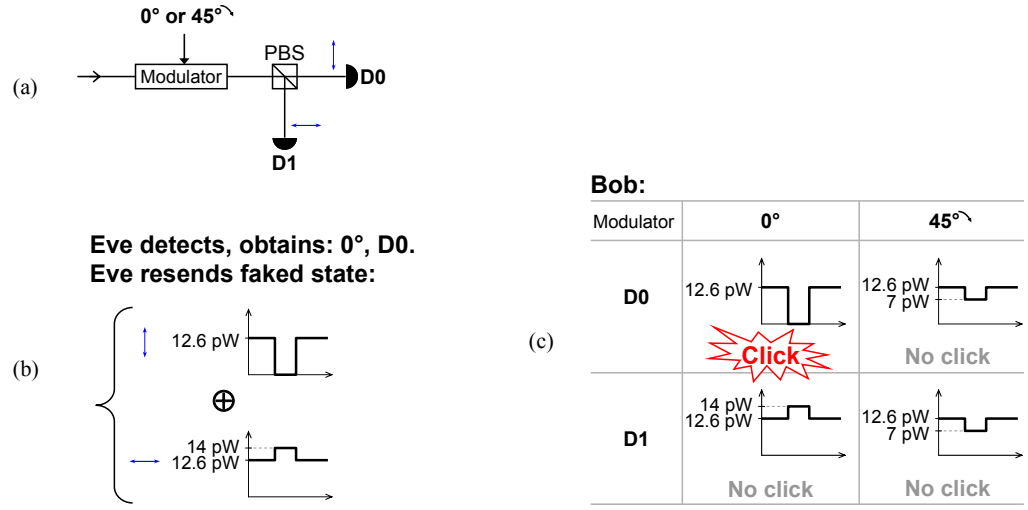

Fig. 3. Attack against a QKD system: (a) an equivalent optical scheme of Bob; (b) an example of faked state Eve re-sends; (c) intensity diagrams caused by this faked state at Bob's detectors for his two possible basis choices.

fore the voltage restores, which takes about 1 μs time. If photons come too often, they produce small avalanches that constantly discharge the APD and the voltage at it never has a chance to reach the sensitivity threshold, thus the detector becomes blinded. As you can see from Fig. 1, the blinding optical power is rather low.

In all normal uses, including uses in QKD systems, the SPD works in the linear part of its characteristic. The saturation and blinding regime is not useful and is avoided. I have found a "useful" application for the blinding regime. The application is: attacking a QKD system.

First, consider how the attacker Eve can control a single SPD. If Eve keeps it constantly illuminated at 12.6 pW or above, the SPD remains blinded and produces no output pulses. If, however, Eve interrupts the illumination for 2 μs, the capacitances have time to charge and the SPD recovers sensitivity. When Eve switches on light at the end of the gap, the SPD produces a single count event (perhaps the first photon from Eve causes a single-photon count), then the SPD becomes blinded again. The blinding power and gap width listed above are for the SPD model 1 and have been experimantally tested. For model 2 these values will be somewhat different, but I have tested that it can also be controlled by Eve with the same outcome.

Let's now consider theoretically how Eve can attack a QKD system that uses two detectors of this type. We take a system with polarization encoding and active basis choice at Bob as an example (I remark that several other types of QKD systems can be attacked similarly). Bob's optical scheme in such a system is shown in Fig. 3(a). Bob first applies, depending on his random choice of detection basis, either no rotation (0°) or 45° polarization rotation to the input light state. Then, light is split at the polarizing beamsplitter (PBS) into the SPDs D0 and D1. Eve conducts a *faked states attack* against this system. She uses a replica of Bob's setup to detect every Alice's photon, then creates and sends to Bob a specially constructed light pulse called a *faked state.* The faked state only causes a detection event at Bob when he chooses the same basis as Eve, and in this case the detection event will be in the same Bob's detector as Eve's earlier detection outcome. Let's suppose for certainty that Eve has detected Alice's photon in the 0° basis, and observed a click in her detector D0. She sends to Bob an incoherent mixture of vertical and horizontal polarizations with the intensity diagrams shown in Fig. 3(b) (the mixture is sent continuously during the attack, while the faked state is merely a temporary intensity deviation). It is easy to see that these polarization components route to two Bob's detectors differently depending on his choice of detection basis, and only cause a click in D0 when he chooses the 0° basis; in the 45° basis both Bob's detectors remain blinded (a temporary drop of power to 7 pW causes no click). Thus, every time Bob "detects a photon", it is detected by him in the same basis and with the same bit value as Eve has detected it.

During the attack, in about half of the cases Eve detects Alice's photon in a wrong basis, but all these bits in the key are later discarded by Alice and Bob at the sifting stage of the classical post-processing part of the QKD protocol. The bits remaining in the key are where Alice, Eve and Bob all have the same basis and bit value. Eve's attack is successful: it causes zero errors in the key, and she has full information about the key.

Monitoring input light intensity at Bob would protect from this attack, but no reported QKD experiments do it. Additional aspects of this attack and more detailed tests of the SPD model 1 can be found in Ref. 2.

[1] N. Gisin *et al.,* Rev. Mod. Phys. **74**, 145 (2002); H.-K. Lo and N. Lütkenhaus, arXiv:quant-ph/0702202.
[2] V. Makarov, arXiv:0707.3987 [quant-ph].