Can Eve control PerkinElmer actively-quenched single-photon detector?

V. Makarov (1), A. Anisimov (2), S. Sauge (3)

1: Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway; makarov@vad1.com

2: Radiophysics Department, St. Petersburg State Polytechnic University, Russia

3: Department of Microelectronics and Information Technology, Royal Institute of Technology (KTH), Sweden

Abstract

We show how PerkinElmer SPCM-AQR detector module can be controlled by an eavesdropper using bright optical pulses, by exploiting an obscure flaw in the detector electrical circuit. First experimental results are reported. This loophole may make possible an attack against quantum cryptosystems that use these detectors.

During the last 19 years, quantum key distribution (QKD) has progressed from a tabletop demonstration to commercially available systems and numerous experiments, some over >100 km distance. As QKD enters the commercial market, it becomes increasingly important to verify the actual security level of its implementations, and search for possible loopholes.

Many QKD systems, more than 30 reported experiments, employ Si avalanche photodiodes (APDs) for detection of single photons in the 500–900 nm wavelength range. There are two widely used detector electronic schemes for Si APDs: passive-quenching and active-quenching. Roughly half of these QKD experiments use detectors with one scheme, and the other half use the other. We have previously demonstrated that passively-quenched detectors have a loophole [1]. An eavesdropper Eve can take control of them using moderately bright light, and may be able to successfully attack a QKD system, unless extra countermeasures are implemented. In this paper, we consider an actively-quenched detector model, PerkinElmer SPCM-AQR detector module. Until recently, this has been the only commercially available Si single-photon detector model. Either this exact model or its quad version (SPCM-AQ4C) are used in most experiments that employ actively-quenched detectors.

Our testing has shown that the electrical circuit of the SPCM-AQR module exhibits at least four different “strange behaviors” when the optical input of the module is illuminated by light waveforms with peak optical power between 1 and 10 mW (at 780 nm). We do not see how three of these behaviors could be immediately useful for Eve, and omit their description for brevity. However, the fourth behavior can, under some conditions, be used by Eve to control Bob’s detectors and stage a successful intercept-resend attack. The part of the detector electrical circuit relevant to understanding this control method is shown in Fig. 1. To the left of the APD is a high-voltage power supply. In normal single-photon regime, it provides stable bias voltage at the cathode of the APD (the two detector samples we tested had bias voltages of 350 V and 410 V). The current limiting circuit does not notably reduce the cathode voltage during normal single-photon avalanches. To the right of the APD, a circuit connected to its anode senses the onset of avalanche. Active quenching is accomplished by connecting the anode of the APD to +30 V, which lowers the voltage across the APD below the breakdown voltage. 20 ns after quenching, the circuit is reset by briefly connecting the

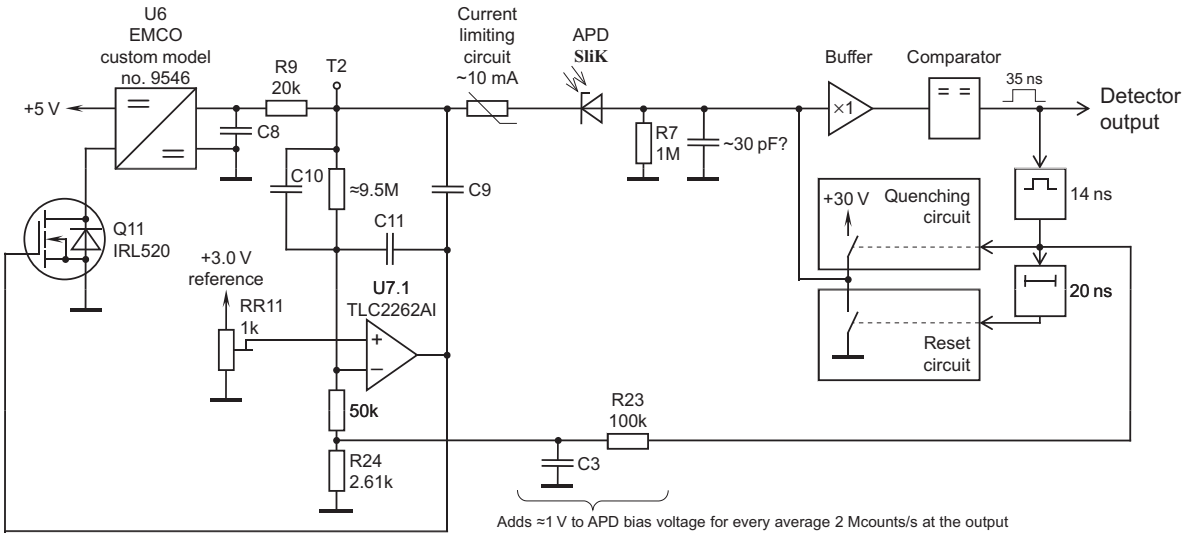

Figure 1: PerkinElmer SPCM-AQR module. Equivalent diagram of the high-voltage power supply, avalanche sensing and quenching circuitry (reverse engineered from sample with PCB labeled “EG&G P/N 2580883 rev. G”).

anode of the APD to the ground.

When the APD is illuminated by a bright optical pulse, the current through it is much larger than during the normal single-photon avalanche. The current limiting circuit kicks in and limits the current pulse to about 10 mA. This current is drawn from the decoupling capacitor C9. The other end of C9 is connected to the output of a low-power operational amplifier U7.1 (Texas Instruments TLC2262). This op amp is relatively slow and has maximum load current several times less than 10 mA. Over the next microsecond following the current pulse that exceeds the op amp load capacity, its output voltage produces a 1 V deep dip. The output of the op amp controls, through a high-power MOSFET Q11, the miniature high-voltage power supply module U6. In result, when the APD is illuminated by bright optical pulses with a certain frequency, the input power of U6 is regularly disrupted with the same frequency. The switching circuitry inside U6 appears to phase lock or fractionally phase lock to the frequency of disruptions, and U6 significantly reduces its output voltage, depending on the frequency and intensity of the optical pulses (Fig. 2). When the APD bias voltage drops by more than 12–14 V, the detector becomes *totally insensitive to single photons, dark counts and afterpulses,* only producing an output pulse when a brighter optical pulse is applied at its input.

Let's see how Eve can use this detector control method to eavesdrop on a QKD system. For example, consider a QKD system running a four-state protocol with passive basis choice at Bob (which many of the systems that use Si detectors implement; e.g., [2]). Eve must find a way to address just one of Bob's four detectors [1]. In our case, she can do this by launching

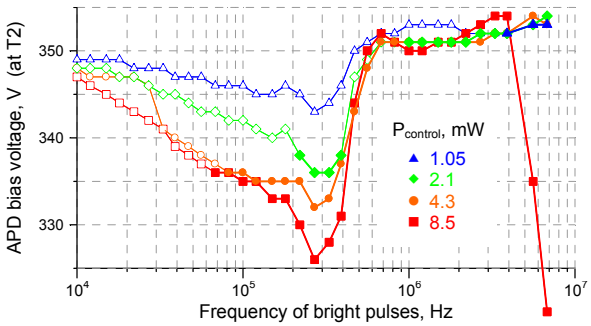

Figure 2: APD bias voltage vs. frequency and peak optical power $P_{control}$ of rectangular 50 ns wide input optical pulses. Normal bias voltage at low count rate for this detector sample is 350 V. Filled symbols denote pulse parameters at which the detector got under complete control, with its output pulse rate being exactly equal to the optical pulse rate. Outside the control range, random pulses were present at the output at typically much higher rate. (The input pulses do not have to be very regular to get the detector under control; we also tried a fast deeply frequency modulated pulse sequence, and it worked.)

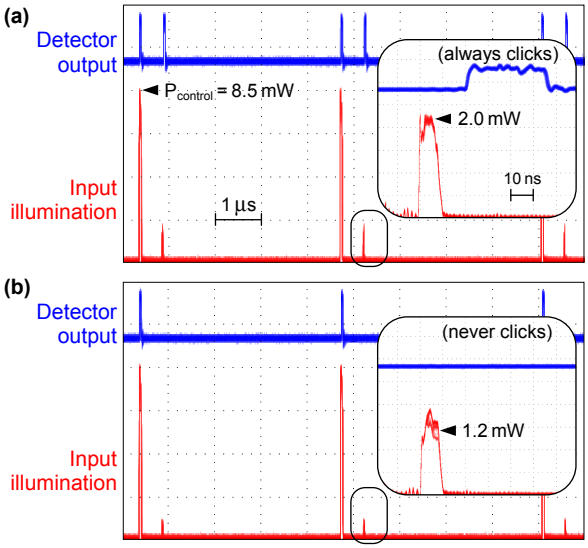

Figure 3: Two control intensity diagrams and the resulting output signal of the detector. The large (control) optical pulses are 50 ns wide.

a bright optical pulse in the quantum state corresponding to the target detector (e.g., vertically polarized bright pulse for the vertical polarization detector). In addition, she must make sure that this light pulse only causes a click when applied to the detector at a nominal intensity, while *not* causing a click at half the intensity, so that the two other detectors in the conjugate basis do not produce clicks. Unfortunately, the regular light pulses that reduce the bias voltage cannot be used for this purpose: at much less than half their intensity, they still cause clicks. What Eve can do, however, is to use a shorter and less intense pulse in between these pulses, as depicted in Fig. 3. The observed jitter of detector output signal was ≲1 ns. We have tested two detector samples, and they responded (or not responded) to the depicted input light pulses identically.

Since Eve now has a method to produce a click in Bob's detector of her choice, she may try to run an intercept-resend attack (faked states attack), get a complete copy of the key, and remain unnoticed [1]. The only thing that betrays her presence are simultaneous pulses at at least 70 kHz rate from all Bob's detectors. In some QKD systems, these may be ignored by Bob as falling outside his post-processing gating time ranges. In free-space systems operating in daylight, these pulses may be mistaken by Bob for normal background count rate. We also feel that there might be more tricks Eve can play with this nice detector to control it and hide her presence. We are continuing this study.

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.

References

1. V. Makarov, arXiv:0707.3987 [quant-ph].
2. C. Erven *et al.,* arXiv:0807.2289 [quant-ph].