Faking photon number on transition-edge sensor

Poompong Chaiwongkhot,[1,2,*] Anqi Huang,[3,†] Jiaqiang Zhong,[4] Hao Qin,[5] Sheng-cai Shi,[4] and Vadim Makarov[6,7,8]

[1] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[2] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[3] *Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha 410073, People's Republic of China*
[4] *Purple Mountain Observatory and Key Laboratory of Radio Astronomy, Chinese Academy of Sciences, 8 Yuanhua road, Nanjing 210034, People's Republic of China*
[5] *CAS Quantum Network Co., Ltd., 99 Xiupu road, Shanghai 201315, People's Republic of China*
[6] *Russian Quantum Center, Skolkovo, Moscow 143025, Russia*
[7] *Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information, University of Science and Technology of China, Shanghai 201315, People's Republic of China*
[8] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*

Transition-edge sensor (TES) [1, 2] is a photon detector with ability to discriminate photon number state. Here, we report experimental demonstration of two vulnerabilities in TES against an adversary Eve who tries to take control the detection outcome. The system under test is a fiber-coupled TES designed for 1550 nm wavelength. The TES current signal is amplified by a low-noise DC-SQUID sensor followed by an electrical amplifier at room temperature.

First, we found that Eve could fake a photon number detection result by sending multiple photons with a proportionally lower photon energy. Our first experiment shows that the response signal of single-photon detection from a 450 nm photon overlaps with two-photon detection from 780 nm and three-photon detection from 1550 nm photons. This shows that the response in TES detection alone cannot be used as a real-time channel monitoring or characterization of source quality in quantum cryptosystem.

In the second experiment, we found that the TES sensitivity to photon energy can be controlled. We show that the sensitivity of TES decreases as temperature increases, which could be induced by coupling bright continuous-wave laser through the TES input fiber. Furthermore, the photon number output could be replicated by coupling additional bright pulsed laser with a proper peak power.

Using this, we model a faked-state attack on a BB84 quantum key distribution (QKD) system [3] assuming it uses the TES under test as its detector. Our analysis shows that, by setting her blinding laser power to 0.25 nW and her fake pulsed signal peak power to 0.48 pW, Eve could perform an intercept-and-resend attack while inducing 7.4% error rate. This error rate is lower than the abort threshold of the BB84 protocol, thus the security of the key could be compromised. Figure 1 shows a histogram of TES output to single photon detection during normal operation as well as its response under the faked-state attack. Similar attacks on other QKD protocols could be considered [4].

This, to our knowledge, is the first demonstration of potential vulnerabilities of TES to hacking attacks. Countermeasures to such attacks will need to be considered in the future, if TES begin getting employed in secure quantum communication schemes.

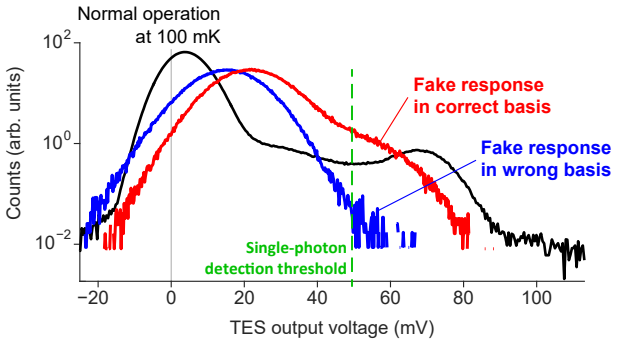

FIG. 1. Attack modeled on BB84 QKD system with TES as a detector. The response under normal condition (black) contains a zero-photon response (left peak) and single-photon response (right peak). The threshold (green vertical dashed line) mark the minimum TES voltage output that the system in our model would register as a detection. The fake response is shown for two cases where Bob and Eve pick the same (red) and different (blue) measurement basis.

* poompong.ch@gmail.com
† angelhuang.hn@gmail.com

[1] D. Fukuda, G. Fujii, T. Numata, A. Yoshizawa, H. Tsuchida, H. Fujino, H. Ishii, T. Itatani, S. Inoue, and T. Zama, Metrologia **46**, S288 (2009).
[2] A. J. Miller, A. E. Lita, B. Calkins, I. Vayshenker, S. M. Gruber, and S. W. Nam, Opt. Express **19**, 9102 (2011).
[3] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[4] L. Lydersen, J. Skaar, and V. Makarov, J. Mod. Opt. **58**, 680 (2011).