QKD information leakage due to blackflashes in single photon avalanche photodiodes

Colin Lualdi,[1,*] Daniel Stack,[1,†] and Stephen Pappas[1]

[1] *Quantum Information Sciences Group, The MITRE Corporation, 200 Forrestal Road Princeton, NJ 08540*

(Dated: July 8, 2016)

ABSTRACT

Quantum Key Distribution (QKD) promises a theoretically unbreakable cryptosystem by employing the probabilistic nature of quantum measurement over mutually unbiased bases. However, it has been shown that QKD systems possess security vulnerabilities due to engineering and technical imperfections in practical implementations. Attacks exploiting various points of accidental information leakage have been described in the literature, with examples including the faked states and Trojan-horse attacks. However, there is a particular vulnerability in the photon detectors of a QKD system that has not been well investigated. Many QKD systems employ single photon avalanche diodes (SPADs) as their means for detecting quantum states in the form of individual photons as required by QKD protocols like BB84. A significant fraction of SPADs are either of the silicon or InGaAs type, due to the former's prevalence in quantum optics laboratories and the latter's wavelength compatibility with existing telecommunications fiber networks. Avalanches of the charge carriers in both Si and InGaAs SPADs are known to be accompanied by photon emission due to electron-hole recombination. These "backflashes" may be coupled back into the quantum channel and detected by an eavesdropper [1]. The eavesdropper could potentially then exploit this information leakage to deduce the states of the original information-carrying photons measured by the legitimate QKD receiver without increasing the quantum bit error rate (QBER) and thus remain hidden. This backflash represents a potentially significant vulnerability to existing QKD systems and yet there has not been much research on the subject since it was first reported for Si SPADs with a free-space quantum channel [1]. Additionally, a recent article reports that backflashes from InGaAs SPADs are a potential security vulnerability to a fiber-based QKD system [2]. Both reports are limited to experimentally showing that information leakage due to backflashes in both Si and InGaAs SPADs is significant if preventive measures are not taken.

Having recognized that backflashes in SPADs constitute a significant source of information leakage, our research aims to further characterize these events in an attempt to determine practical means for an eavesdropper to extract information by intercepting such secondary signals. We investigate the presence of correlations between the backflash pulse and the state of the original photon. Correlations may be found in, but are not limited to, the timing, polarization, and spectral characteristics of the backflashes. Multiple SPADs are examined to determine if individual detectors exhibit unique backflash characteristics, a property that an eavesdropper may exploit to determine the basis states measured by the receiver. We conduct this investigation for both Si and InGaAs SPADs to compare the security (or lack thereof) of both types for QKD implementations.

* clualdi@princeton.edu

† dstack@mitre.org

[1] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, Journal of Modern Optics **48**, 2039 (2001), http://dx.doi.org/10.1080/09500340108240905.

[2] A. Meda, I. P. Degiovanni, A. Tosi, Z. L. Yuan, G. Brida, and M. Genovese, ArXiv e-prints (2016), arXiv:1605.05562 [quant-ph].