Influence of avalanche-photodiode dead time on the security of high-speed quantum-key distribution systems

Hai Xu[1, 2], Lijun Ma[1], Joshua C. Bienfang[1], Xiao Tang[1]
[1] *National Institute of Standards and Technology, 100 Bureau Drive Stop 8900, Gaithersburg, MD 20899*
[2] *University of Maryland Baltimore County, 1000 Hilltop Circle, Dept. of CSEE, Baltimore, MD 21250*
hai.xu@nist.gov, xiao.tang@nist.gov

Abstract: We study the correlation in the sifted key induced by the dead time of Geiger-mode avalanche photodiodes (APDs) in quantum cryptographic systems. A simultaneous hold-off of the APDs (SHA) technique eliminates these correlations.

OCIS codes: (060.2330) Fiber Optics Communications; (040.5570) Quantum detectors;

1. Introduction

It is of great interest to develop high-speed quantum key distribution (QKD) systems in short-distance fiber networks, such as local area networks (LANs). The short distance allows propagating light around 850 nm, at which silicon avalanche photodiodes (Si-APD) with low dark counts can detect photons at a rate well above 1 MHz when operating in free-running mode. Recently a QKD system was reported with a bit repetition rate of 312 Mbps, yielding a sifted-key rate of 1.0 Mbps and a quantum bit error rate (QBER) of 1.3% [1]. For a QKD system at even higher speeds, one major limitation is the dead time (t_d) of the Si-APD — the hold-off time following each detection event [2]. During the dead time, the bias voltage across the p-n junction of the device is below the breakdown level and no photon can be detected [3]. Because the photon detection rate of one APD cannot exceed $1/t_d$, the sifted-key rate cannot exceed $2/t_d$ in either of the B92 and BB84 protocols. Moreover, as the sifted-key rate approaches $2/t_d$ the dead time can induce significant correlations in the sifted-key bit values [4]. For example, in B92, during the dead time of one APD, the other APD is likely to detect a photon and hence will generate a sifted-key bit with value different from the preceding bit. Thus neighboring sifted-key bits are correlated. To avoid such correlations, one can simultaneously hold off all APDs when any of them is in the dead time. With this technique, called the SHA in this paper, we believe the sifted-key rate of QKD systems with Si-APD can approach $1/t_d$ without inducing correlations.

For the first time to our knowledge, we present a quantitative study of the above correlation issue. We conduct a Monte Carlo simulation of the QKD system in Ref. [1], and calculate the probability that two adjacent sifted-key bits are different. The simulation results agree well with the experiment, and show that in the B92, this probability can be larger than 0.9 at sufficiently high bit repetition rates. Potentially, such correlations could induce significant security loss. In comparison, the probability approaches 0.62 in BB84. Consequently, besides the well-known higher security [5], BB84 is also less sensitive to security loss induced by the dead time. We also simulate the SHA scheme. With this technique, the probability remains 0.5 for both protocols as the repetition rate increases. By this means, we expect that secure QKD with sifted-key rates approaching $1/t_d$ is achievable at high repetition rates.

2. System configuration and simulation setup

Figure 1(a) shows schematically the QKD system [1] that we simulate. We use the Monte Carlo method to simulate the key distribution. For example, in the B92 protocol the single-photon sources (faint laser) LD-1A and LD-2A are modulated by two 10^9-long random bit sequences, which are complementary to each other, respectively. The generated single-photon trains are polarization-encoded, combined, and sent to Bob through 1-km fiber. The losses of the fiber are simulated by random elimination of photons.

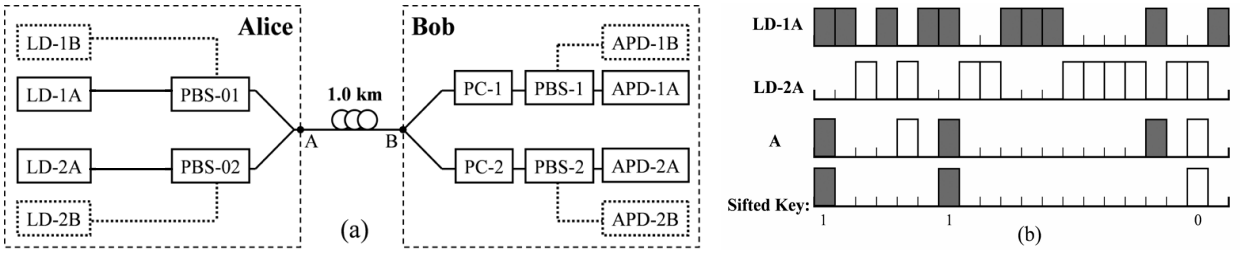

Fig. 1. (a) Schematic diagram of the QKD system. In BB84, two additional single-photon sources (LD-1B and LD-2B) and APDs (APD-1B and APD-2B) are used. The orientations of PCs and PBS are adjusted according the protocol. (b) Schematic display of random bit sequences used to modulate LDs, the combined single-photon train at A, and the sifted keys. The grey bars represent photons from LD-1A (with key bit value "1") and white bars represent photons from LD-2A (key bit value "0").

At Bob, each surviving photon randomly enters either the upper or lower path with equal probability. The polarization compensators (PCs) compensate for the polarization transformation in the transmission. Then the PBS eliminates the polarization-incompatible photons and passes half-compatible photons with a probability of 0.5. The remaining photons are detected by each APD with 45% efficiency. At last, the detected bits from all APDs are combined to form the sifted keys. All polarizing beam splitters (PBS) are assumed with infinite extinction ratio, which is a good approximation to the 23-dB extinction ratio reported in Ref. [1]. The APDs operate in the free-running mode with $t_d \approx 50$ ns. Without SHA, we block an APD for $t_d \times \nu$ of subsequent bits when it detects a photon, where ν is the bit repetition rate. With SHA, all APDs are blocked for $t_d \times \nu$ of subsequent bits after a detection. A similar process is also used in the BB84 protocol except that the bits detected with wrong bases are further sifted off.

3. Results and discussion

Figure 2 shows the results from the Monte Carlo simulation. In Fig. 2(a) and (b) the mean photon number is set to 0.1 at the output of Alice and the transmission loss is 5.0 dB, the same as those in Ref. [1]. Figure 2(a) shows the probability that two neighboring sifted-key bits have different values in the B92 and BB84, both with and without the SHA. As shown in Fig. 2(a), without SHA, significant correlation arises as the bit repetition rate increases so that the sifted-key rate approaches the limit of the APDs $2/t_d$ (Fig. 2(b)). In particular, with B92 the probability is larger than 0.9. For B92 systems operating at such high repetition rates, during the dead time of one APD there is a large probability that the other APD can detect a photon and generate a key bit with a value different from the preceding bit. In BB84, due to the random choice of bases, the next key bit could be encoded with different base but have the same bit value. Therefore, the correlation between neighboring keys is less and the probability approaches 0.62.

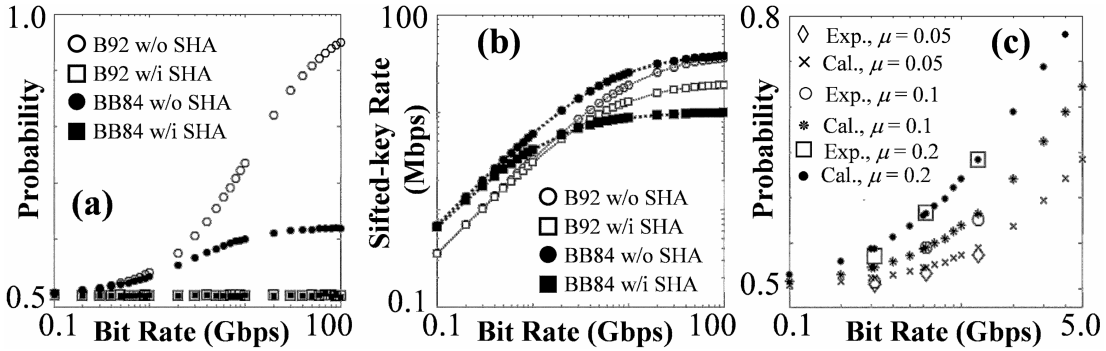

Fig. 2. (a) Probability that two neighboring bits are different with and without SHA, in B92 and BB84 protocol, (b) corresponding sifted-key rate, and (c) a comparison between simulation (Cal.) and experiment (Exp.) in B92 without SHA.

Figure 2(a) also shows that when one applies the SHA scheme, the probability of neighboring keys being different remains 0.5 independent of the repetition rate. One trade-off of this de-correlation is the decrease of the ultimately available sifted-key rate. In this case, all APDs are simultaneously available or idle, and thus the sifted-key rate approaches $1/t_d$ in B92 and $1/(2t_d)$ in BB84 (half of keys being sifted), as shown in Fig. 2(b).

We also measured the probability of different neighboring key bits in a B92 polarization-coded system without SHA, which is similar to the one in Fig. 1(a) except that the transmission loss is reduced to 2.0 dB by shortening the fiber and the mean photon number at Alice m is varied. Then we recalculated the probability using experimental parameters. As shown in Fig. 2(c), the simulation results agree well with the experiment. The slight difference is likely due to polarization drift during the measurement. The calculated sifted-key rate, which is not shown here, also agrees well with the experiment. As shown in the figure, if we further increase the mean photon number or the repetition rate from those in [1], without SHA the probability that the other APD detects a photon during the dead time becomes non-negligible and therefore, the correlation between neighboring sifted-key bits becomes observable. We are currently investigating the security implications of such correlations both experimentally and theoretically.

4. References

1. Xiao Tang, Lijun Ma, Alan Mink, Anastase Nakassis, Barry Hershman, Joshua Bienfang, Ronald F. Boisvert, Charles Clark, and Carl Williams, "High Speed Fiber-Based Quantum Key Distribution using Polarization Encoding," *Proceedings of SPIE* **5893**, Optics and Photonics Conference, San Diego, California, USA, July 31 – August 4, 2005.
2. D. Stucki, N. Gisinm O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," *New J. Phys.* **4**, 41, (2002).
3. M. Ghioni, A. Giudicem S. Cova, and F. Zappa, "High-rate quantum key distribution at short wavelength: performance analysis and evaluation of silicon single photon avalanche diodes," *J. MOD. Opt.* **50**, 2251- 2269 (2003).
4. André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden, "Optical random quantum generator," *J. Mod. Optic*. **47**, 595- 598 (2000).
5. N. Gisinm G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.* **74**, 145-195 (2002).