Analysis of Differential Phase Shift Quantum Key Distribution using single-photon detectors

Vishal Sharma
Instrumentation and Applied Physics
Indian Institute of Science, Bengaluru
CV Raman Road, Bengaluru, Karnataka-560012
Email: vishalsharm1@iisc.ac.in

Asha Bhardwaj
Instrumentation and Applied Physics
Indian Institute of Science, Bengaluru
CV Raman Road, Bengaluru, Karnataka-560012
Email: asha@iisc.ac.in

***Abstract*—We investigated the performance of differential phase shift quantum key distribution using InGaAs/InP and Silicon-APD (avalanche photo diode) for generating secure keys, secure communication distance, and bit error rates under the various operating conditions.We compare the quantum bit error rate and the secure key generation rate as a function of communication length.Our simulation results show that with frequency conversion at telecommunication wavelength the silicon-APD contributes in enhanced communication rates and higher communication distances than InGaAs/InP APD for optical fiber-based quantum key distribution applications.**

I. Introduction

Quantum key distribution was first demonstrated in 1992 [1] and further many attempts have been made to achieve higher communication rate and highest possible communication distance [3], [5], [7], [11].Quantum technologies are nowadays being deployed in many industrial applications [13].The third telecommunication window at 1550 nm is the preferred one for practical deployment of quantum communication, as it provides less losses (0.2 dB/km) as compared to 1300 nm wavelength which offers higher losses (0.35 dB/km). There are various single photon based quantum key distribution protocols implemented experimentally such as Bennett-Brassard 1984 (BB84) protocol, the entanglement-based Bennet-Brassard-Mermin 1992 (BBM92) protocol [2]. Several experimental setup for optical fiber-based quantum key distribution has made tremendous progress at 1 GHz system clock frequency by reaching at more than 100 km secure communication distance [4]. The analysis made based on various experiments conclude that the performance of the quantum cryptography systems are affected mostly by single and entangled photon sources, and depends on the characteristics of single-photon detectors. In the present work, we consider differential-phase-shift quantum key distribution (DPS-QKD) protocol [6], implemented under optical-fiber-based experimental parameters based on InGaAs/InP and silicon-APD at telecommunication wavelengths.We use silicon-APD due to its unique properties and advantages such as high quantum efficiency, low dark counts rates with high timing accuracy and excellent timing stability, with suitable wavelength conversion to 1550 nm [7], [8], [10], [12] and tuning the experimental parameters to provide very low losses and provides higher secure key rate (SKR) [9].

II. Differential Phase Shift Quantum Key Distribution protocol

DPS-QKD posses many non-orthogonal states with many pulses, as shown in Fig. 1 [6]. These pulses, in highly attenuated coherent states are randomly phase modulated $\{0, \pi\}$. Bob, in the interferometer, at the receiver end, applies random modulation on the delay time, NT, where N is a positive integer, and T is the reciprocal of the clock frequency, which detector clicks depends on the phase difference of the two pulses which are having a NT time difference.Bob announces the value of N and the time instances on which the photon was detected. From this and her modulation data Alice comes to know which detector clicked.Based on these events, Alice and Bob, assign the bit values to the detectors.Since the bit information is encoded in the differential phase of two non-local pulses, hence the protocol considered is secure against the individual attacks.Based on the number of detected photons, we calculate the sifted key generation rate, and SKR is evaluated with the consideration of photon splitting and general individual attacks.The sifted key generation rate in the DPS-QKD system is given

$$R_{sifted} = \nu\mu T e^{-\nu\mu T t_d/2}, \tag{1}$$

where mean photon number is μ, system clock frequency is ν, blocking time of the discriminator is t_d. The overall efficiency, $T = \eta_d\eta_t$, where transfer efficiency is η_t, and the detector efficiency is η_d of the detector. $\eta_t = 10^{-\frac{(L_f l + L_d)}{10}}$, which depends on communication length, l (in km). In the present work, at telecommunication wavelength, we consider fiber loss (in dB/km), L_f = 0.21 dB/km, and L_d is the internal loss in the detector (in dB).The dark counts and after pulsing events are responsible to contribute in quantum bit error rate (QBER), expressed as

$$e \approx \frac{(e_b + p_{ab}/2)p_{click} + p_d}{p_{click}} \tag{2}$$

where p_{click} represents total probability of the event counts, the overall after pulsing probability is p_{ab} with $200\,ns$ blocking time, base error e_b, and the dark count probability per gate is p_d. After error correction and privacy amplification SKR is given by

978-1-6654-7899-1/22/$31.00 ©2022 IEEE

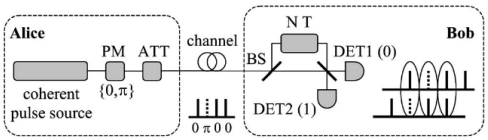

Fig. 1. DPS-QKD protocol [6]. PM refers for phase modulator, attenuator is denoted by ATT, BS refers for a beam splitter and DET refers for a detector.

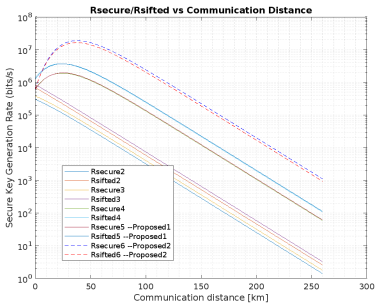

Fig. 2. Secure and sifted key generation rate as a function of communication distance.

$$R_{secure} = R_{sifted}\Big\{ -[1-2\mu(1-T)]log_2 \times \Big[1-e^2-\frac{(1-6e)^2}{2}\Big] + f(e)\times[elog_2 e+(1-e)log_2(1-e)]\Big\} \quad (3)$$

$\eta_{d1} = 0.155; \eta_{d2} = 00.14; \eta_{d3} = 00.13; \eta_{d4} = 00.085; \eta_{d5} = \eta_{d6} = 00.35; f(e) = 1.16; p_{d1} = 6.8 * 10^{-5}; p_{d2} = 2.0 * 10^{-3}; p_{d3} = 1.0 * 10^{-5}; p_{d4} = 9.2 * 10^{-6}; p_{d5} = 7.00 * 10^{-6}; p_{d6} = 3.5 * 10^{-8}; e_{b1,b2,b3,b4} = 0.01; e_{b5} = e_{b6} = 0.015; p_{ab1,ab2,ab3,ab4} = 0.013; p_{ab5} = p_{ab6} = 0.5; L_{f1,f2,f3,f4,f5,f6} = 0.21; L_{d5} = 3.0; L_{d1,d2,d3,d4,d6} = 2.1; V_c = 0.95; \mu = 0.77; \nu_1 = 10 * 10^6; \nu_2 = 14 * 10^6; \nu_3 = 500 * 10^6; \nu_4 = 800 * 10^6; \nu_5 = 1 * 10^9; \nu_6 = 10 * 10^9; p_{click1,click2,click3,click4} = 6.8 * 10^5; p_{click5} = p_{click6} = 20.0 * 10^6;$ $t_{d1,d2,d3,d4} = 200ns; t_{d5} = t_{d6} = 45ns.$

The subscripts from 1 to 4 are used for InGaAs/InP-APD, whereas the subscripts 5 and 6 are used for Si-APD. For each subscript corresponding colour plots are shown in the simulated results (Fig. 2 and 3). Probability of avalanche generation per gate pulse is p_a, blocking time of the discriminator is t_d. The remaining parameters are already described. From Fig. 2, we observe that for Si-APD, at 10 GHz system clock, the SKR is 1.33×10^7 bits/s over 40 km (parameters corresponds to subscript 6). This performance improvement is due to its higher quantum efficiency, low dark counts and low after pulse probability, we obtain SKR more than 1.3×10^3 bits per second at a communication distance of 260 km within the acceptable quantum bit error rate of 11% (Fig. 3).The results show that Si-APD in DPS-QKD with frequency-up conversion outperforms InGaAs/InP-APD in terms of sifted key and secure key generation rates, and falls within the practically acceptable QBER of 11%.

III. Conclusion

We simulated DPS-QKD protocol under the two types of APDs with the use of Si-APD frequency conversion that

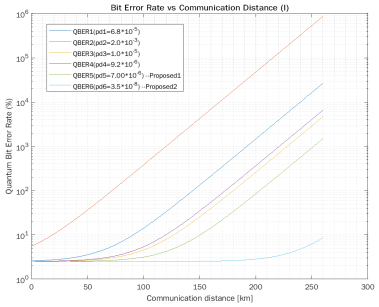

Fig. 3. Quantum bit error rate as a function of communication distance.

results in achieving optimum values of the performance parameters as compared to InGaAs/InP APD. In our future research work, we will compare DPS-QKD with BB84 and BBM92 protocols under the same conditions and hybrid attacks.

Acknowledgment

Authors acknowledge Indian Institute of Science, Bangalore for providing the support by the project Centre for Excellence in Quantum Technology (No. 4(7)/2020-ITEA), funded by the Ministry of Electronics and Information Technology, Government of India.

References

[1] Bennett, Charles H and Bessette, François and Brassard, Gilles and Salvail, Louis and Smolin, John, Experimental quantum cryptography *J. Cryptology*, **5**, pages 3–28, (1992).

[2] Honjo, T and Inoue, K and Takahashi, H, Differential-phase-shift quanum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer *Opt. Lett.*, **29**, pages 2797–2799, (2004).

[3] Sharma, Vishal and Banerjee, Subhashish, Quantum communication using code division multiple access network *Optical and Quantum Electronics*, **52**(8), pages 1–22, (2020).

[4] Gobby, C and Yuan, aZL and Shields, AJ, Quantum key distribution over 122 km of standard telecom fiber *Appl. Phys. Lett.*, **84**, pages 3762-–3764, (2004).

[5] Sharma, Vishal and Banerjee, Subhashish, Analysis of quantum key distribution based satellite *In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1-5. IEEE, 2018.

[6] Inoue, K and Waks, E and Yamamoto, Y, Differential-phase-shift quantum key distribution using coherent light *Physical Review A*, **68**(2), pages 022317, (2003).

[7] Sharma, Vishal and Banerjee, Subhashish, Analysis of atmospheric effects on satellite-based quantum communication: a comparative study *Quantum Information Processing*, **18**(3), pp. 1–24, 2019.

[8] Pelc, JS and Zhang, Q and Phillips, CR and Yu, L and Yamamoto, Y and Fejer, MM Cascaded frequency upconversion for high-speed single-photon detection at 1550 nm *Optics letters*, **37**(4), pages 476–478, (2012).

[9] Sharma, Vishal and Sharma, Richa, Analysis of spread spectrum in MATLAB *International Journal of Scientific Engineering Research*, **5**(1), pp. 1899-1902, 2014.

[10] https://www.idquantique.com/quantum-sensing/products/id100/.

[11] Sharma, Vishal, Effect of Noise on Practical Quantum Communication Systems *Defence Science Journal*, **66**(2), (2016).

[12] Perikala, Manasa and Bhardwaj, Asha Excellent color rendering index single system white light emitting carbon dots for next generation lighting devices *Scientific reports*, **11**(1), pages 1–11, (2021).

[13] Sharma, Vishal and Gupta, Shantanu and Mehta, Gaurav and Lad, Bhupesh K A quantum-based diagnostics approach for additive manufacturing machine *IET Collaborative Intelligent Manufacturing*, **3**(2), pages 184–192, (2021).