Optical and Quantum Electronics (2023) 55:888
https://doi.org/10.1007/s11082-023-05170-4

Analysis of single photon detectors in differential phase shift quantum key distribution

Vishal Sharma[1]

Received: 29 April 2023 / Accepted: 8 July 2023 / Published online: 23 July 2023

Abstract
In the current research work, an analysis of differential phase shift quantum key distribution using InGaAs/InP and Silicon-APD (avalanche photodiode) as single photon detectors is performed. Various performance parameters of interest such as shifted key rate, secure key rate, and secure communication distance obtained are investigated. In this optical fiber-based differential phase shift quantum key distribution, it is observed that Si-APD under frequency conversion method at telecommunication window outperforms the InGaAs/InP APD.

Keywords InGaAs/InP-APD · Si-APD · Dark current · Differential phase shift quantum key distribution · Quantum bit error rate · Secure key generation · Hybrid attacks

1 Introduction

Quantum key distribution (QKD) shares the secure secret key among the authenticated users, where unconditional security is achieved by the postulates of quantum mechanics, and different from the classical cryptography where computational complexity is the basis for the entire cryptography system. Many research communities (Lütkenhaus 2000; Waks et al. 2002; Sharma and Bhardwaj 2022) performed security tests and detailed analysis under the realistic scenarios, and concluded that source characteristics such as single or entangled photons are one of the performance deciding factors for any quantum-cryptography system. Quantum key distribution was first implemented in 1992 (Bennett et al. 1992) and desired improvements were developed in (Sharma and Banerjee 2019, 2020, 2018; Gobby et al. 2004; Sharma and Bhardwaj 2022; Sharma et al. 2015, 2016, 2018; Sharma 2018; Raj et al. 2019).Quantum technologies are nowadays being deployed in many interdisciplinary industrial applications (Sharma et al. 2021; Sharma 2014; Sharma and Pancharia 2015). Wavelength at 1550 nm is the desired 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

✉ Vishal Sharma
bits.vishal11@gmail.com

[1] Instrumentation and Applied Physics, Indian Institute of Science, Bengaluru, CV Raman Road, 560012 Bengaluru, Karnataka, India

photon based quantum key distribution protocols implemented experimentally such as Bennett-Brassard 1984 (BB84) protocol, the entanglement-based Bennet-Brassard-Mermin 1992 (BBM92) protocol (Honjo et al. 2004). In the present work, we consider differential-phase-shift quantum key distribution (DPS-QKD) protocol (Inoue et al. 2003; Sharma 2016), deploying weak coherent pulse train (Inoue et al. 2002, 2003), implemented under optical-fiber-based experimental parameters based on InGaAs/InP and silicon-APD at telecommunication wavelengths. For efficient detection of single-photons at 1550 nm, we use frequency-up conversion technique (Langrock et al. 2005). 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 (Pelc et al. 2012; Sharma and Banerjee 2019), and tuning the experimental parameters to provide very low losses and provides higher secure key rate (SKR) Sharma and Sharma (2014) as compared to InGaAs/InP-APD. In addition to these, further, we analyze vulnerability of DPS-QKD under different hybrid attacks.

2 Single photon detectors at third telecommunication window

2.1 Single photon detectors

Single-photon detection in optical fiber-based quantum key distribution (QKD) has been investigated in many applications where InGaAs/ InP avalanche photodiodes were used due to their experimental properties in QKD systems (Yoshizawa et al. 2004; Bethune et al. 2004; Stucki et al. 2001; Bourennane et al. 2001; Gobby et al. 2004). Further, it was analyzed that due to trapped charge carriers, these detectors suffer from after-pulse effects, low quantum efficiencies and hence results in relatively large dark count rates. These drawbacks degrade the performance of InGaAs/InP avalanche photodiodes in gated-mode operation. Under such conditions (in gated mode), the detector works above the breakdown threshold for a limited duration which indicates performance improvement in terms of high photon detection efficiency with comparatively less dark counts. After a short interval of time, it returns below breakdown for the time duration enough for the trapped charge carrier to leak away. In gated mode operation, the device is allowed to work at mega-hertz rates, for which trapping lifetime spans microsecond timing. Hence, we are able to reduce the after pulse probability by the fraction of gate width to the time separation between gates. At this point, it is very important to notice the significance of the gate frequency which is one of the performance deciding factor in almost all type of QKD applications, which decides the pulse repetition rate, and further limits the achievable communication rate. In addition to this, semiconductor material's response time is one of the important parameters which decides the rate of dark counts produced and responsible for limiting the communication distance achieved, and moreover, all these are affected by gate width. In general, gate widths of 1-2 ns at $\sim$ 1 MHz pulse repetition frequency are deployed with final dark counts of 10^{-5} /gate order. In the current analysis of DPS-QKD, we are deploying two single photon detectors, Si-APD [28] and InGaAs/ InP APDs.

2.2 Single-photon detection with frequency up-conversion

A periodically poled lithium niobate (PPLN) is deployed for sum-frequency generation (Roussev et al. 2004), and a strong pump at 1320 *nm* is allowed to interact with a single

photon at 1550 *nm*. This technique is applied in the 1550 *nm* up-conversion single-photon detector (Langrock et al. 2005). With the use of the PPLN waveguide, it becomes possible to convert a signal of very high conversion efficiency to a 700 *nm* sum-frequency output. This is achieved due to the guided wave structure of PPLN waveguide, where the presence of quasi-phase-matching pattern and the tight mode confinement over longer interaction lengths exist. Further, by applying these methods, silicon APD detects the converted information carriers (photons). We are deploying two single photon detectors, Si-APD, and InGaAs/ InP APDs. Out of these two detectors, Si-APD is mostly preferred in all industrial and real-field QKD (Quantum Key Distribution) applications. This is because of its high quantum efficiency in the NIR (near infrared region), low after-pulse effects, and low dark-count rates, low dead time(45 ns), and a timing resolution as low as (40 ps) [28]. These unique characteristics of silicon APD outperforms InGaAs/ InP APDs in almost all QKD applications where single-photon detection is achieved with increased value of timing accuracy and stability up to a count rate of 20 MHz. Sharma and Banerjee (2019); Pelc et al. (2012), [28]. The Geiger mode characteristic of Si-APD, which is also known as nongated mode of operation, is based on low-after-pulse probability, and helps in achieving higher communication rate in practical QKD systems. Further, dead time of Si-APD diminishes the secure key generation rate, here in Si-APD, it is low dead time(45 ns). During this time period that further gives a photodetection event, the photodiode cannot reply to next occurrences, and, finally, a larger amount of photon flux saturates the set-up. In the up-conversion process, both the quantum efficiency η_{up} and the dark-count rate D_{up} depend on pump power p (Langrock et al. 2005). In Si-APD, 0.46 value of quantum efficiency is obtained, when the 100% photon conversion condition is met, it is possible in the case when the phase-matching condition in the waveguide is met and enough pump power is present for the said process. In a waveguide, due to three-wave interactions based on coupled-mode theory, the fitting curve is obtained from the following relation

$$\eta_{up}(p) = a_1 \sin^2(\sqrt{a_2 p}), \tag{1}$$

where p is in mW, and values of a_1, and a_2 are 0.465, and 79.75, respectively.

We believe that the dark-count rate is controlled by the below mentioned nonlinear process. At first, the pump photons are dispersed by the fiber and phonons of the PPLN waveguide via a spontaneous Raman scattering mechanism. This method escalates straightaway with the pump power, and produces a spread of Stokes photons, which contains 1550 nm signal wavelength. Afterwards, the noise photons combine with the pump photons in the waveguide via the phase-matched sum-frequency generation approach, and generate dark counts. The combined process produces a precise quadratic dependence of the dark counts on the pump power, as shown in Fig. 2. The following expression generates an accurate polynomial fitting curve

$$D_{up}(p) = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + b_4 p^4, \quad (s^{-1}), \tag{2}$$

where the values of b_0, b_1, b_2, b_3, and b_4 are 50, 826.4, 110.3, −0.403, and 0.00065, respectively. The value of power p is given in mW.

Dark counts are also generated by the parametric fluorescence process and up-conversion of noise signal photons [39, 40]. Here, we find the quadratic relation between the dark counts and associated pump power. In such fluorescence processes in the frequency conversion detector, 8.9-μ m idler photons are absorbed in lithium niobate, and hence more dark counts are produced because of the spontaneous Raman scattering and

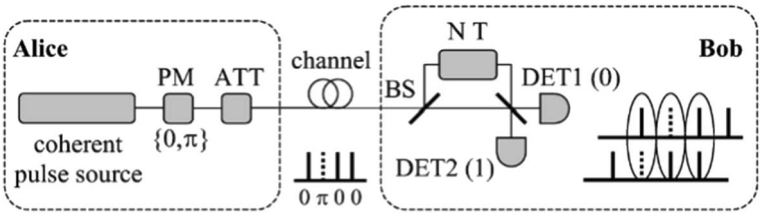

Fig. 1 DPS-QKD protocol (Inoue et al. 2003). Phase Modulator (PM), Attenuator(ATT), Beam Splitter(BS) and Detector(DET)

the the process described. Further, these undesired dark counts can be minimized by interchanging the signal wavelengths and pump [12], which is the important process generated in a waveguide, where thermal process of excited vibrational states produces anti-Stokes scattering gain.

Dark counts limit the performance of the up-conversion detector. The waveguide bandwidth decides the number of dark counts which is also responsible for the number of noise photons. For a detector with B_d bandwidth, the parameter $D_{up\ Hz}$ is defined as $D_{up\ Hz} = D_{up}/B_d\ \ s^{-1}Hz^{-1}$, where the term B_d is the dark count per mode. In general, an ideal communication system can be taken into consideration in which the bit rate B is equal to the bandwidth B with a matched filter. Here the measurement time window for such an ideal communication system is $1/B$. Based on similar concepts, performance of quantum key distribution systems are based on a very important parameter known as dark counts per time window, d_{up} is equal to D_{up} Hz. Further, considering the optimum filtering case, d_{up} is independent of the bit rate B. In InGaAs/ InP APD in gated mode operation, with $1/B$ gate width, and d_{APD} is the dark counts per gate, which is computed by D_{APD}/B, the term $D_{APD}(s^{-1})$ is known as the dark-count rate of the InGaAs/ InP APD. In InGaAs/ InP APD, $D_{APD} = 10^4,\ \ s^{-1}$ is used. Table 1 represents the dark-count quantities used in the current research work, where bit rate is denoted by symbol B and the waveguide bandwidth is represented by B_d. In the up-conversion process, the normalized noise equivalent power(NEP) $\frac{\sqrt{2D_{up}}}{\eta_{up}}$ is reduced, which is related to $D_{up} = 6.4 \times 10^3\ \ s^{-1}$ and $\eta_{up} = 0.075$. Here the parameter D_{up} Hz is computed at the operating point of the detector. For one of the cases, if the bandwidth, $B_d = 50$ GHz for an up-converter detector, which results in 1.3×10^{-7} as an optimum value of d_{up}. These manipulations are prior estimations that play an important role in many practical QKD applications for deciding QKD performance parameters of interest. Frequency-up conversion methods used in quantum communication systems improve the detection performance at telecommunication wavelength. Further, waveguide bandwidth also affects the number of dark counts in Si-APD and its characteristics also depend on pump power. We investigate all these factors in detail in the coming sections.

Table 1 Dark count parameters for frequency up-conversion

	InGaAs/InP APD	Up-converter
Dark count rate (s^{-1})	D_{APD}	D_{up}
Dark counts per mode ($s^{-1}Hz^{-1}$)	–	$D_{up}Hz = \frac{D_{up}}{B_d}$
Dark counts per time window/gate	$d_{APD} = D_{APD}\frac{1}{B}$	$d_{up} = D_{up}Hz$

3 Differential phase shift quantum key distribution protocol

DPS-QKD possesses many non-orthogonal states with many pulses, as shown in Fig. 1 (Inoue et al. 2003). These pulses, in highly attenuated coherent states are randomly phase modulated $\{0, \pi\}$. Bob applies random modulation on the delay time, NT, where N is a positive integer, and T is the reciprocal of the clock frequency, detector clicks based 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. Alice comes to know which detector clicked.Based on these events, Alice and Bob assign the bit values to the detectors. This protocol is protected from the individual attacks because the two non-local pulses are used for information encoding in terms of the difference of their respective phase information.

Based on the number of detected photons, we calculate the sifted key rate, and the secure rate is manipulated from the photon splitting and general individual attacks.

Further, we perform the security analysis of DPS-QKD under some of the well-known eavesdropping attacks such as Beam-splitter attack and Intercept-resend attack. Due to the fact that, the encoded information of the differential phase of two successive nonlocal pulses is transmitted which provides the secure protocol and the protocol becomes robust against the said attacks (Inoue and Honjo 2005; Honjo et al. 2007). To investigate the secure communication rate under the said attacks we need to find out the privacy amplification shrinking factor (τ) with respect to average collision probability (p_c) under various attacks.

Bob's photon detection probability is expressed as

$$p_{click} = p_{signal} + p_{dark}, \tag{3}$$

where,

$$p_{signal} = \mu\eta 10^{-(\alpha L + L_r)/10}, \tag{4}$$

$$p_{dark} = 2d, \tag{5}$$

where μ is the mean photon number per pulse, α is the optical fiber loss coefficient in dB/km, η denotes the detector quantum efficiency, L_r is the losses in the receiver unit, L is the communication link in km, between the two authentic users, say Alice and Bob, d denotes the dark counts per measurement time window. In p_{dark}, 2 denotes the number of detectors used at the Bob's detection unit. In the ideal case $\mu = 1$, and in a Poisson source, μ is a free variable which has to tune for optimum performance (Gisin et al. 2002).

$$e = \frac{(\frac{1}{2}p_{dark} + b\ p_{signal})}{p_{click}}, \tag{6}$$

where, e and b denote the error rate and baseline system error rates, respectively.

The value of $f(e)$ is based on the error-correction algorithm as mentioned in Table 2 (Brassard and Salvail 1994).

In privacy amplification procedure, the main shrinking factor $\tau(e, \beta)$ is written as

$$\tau = -log_2 p_c \tag{7}$$

Table 2 Error-correction algorithm given in Brassard and Salvail (1994)

e	$f(e)$
0.01	1.16
0.05	1.16
0.1	1.22
0.15	1.35

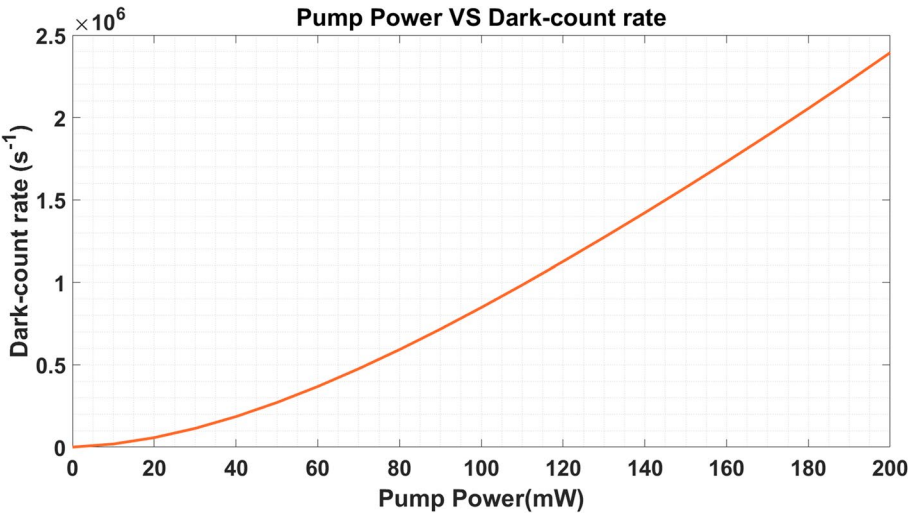

Fig. 2 Dark count dependency on the applied pump power

where p_c is the average collision probability, which shows the amount of Eve's mutual information with Bob and Alice.

The following expression is generated for τ.

$$\tau(e,\beta) = -\beta log_2\left[\frac{1}{2} + 2\left(\frac{e}{\beta}\right) - 2\left(\frac{e}{\beta}\right)^2\right] \tag{8}$$

Source emits photons where fraction of single-photon states is written as

$$\beta = \frac{p_{click} - p_m}{p_{click}}, \tag{9}$$

where the p_m is associated with the probability of the multi-photon quantum states. In case of an ideal single-photon state, $p_m = 0$ or $\beta = 1$. In another type of source the value of p_m, e.g. the probability of photon emission in Poisson source is expressed as

$$p_m = 1 - (1+\mu)e^{-\mu} \tag{10}$$

The term β decides the photon number splitting (PNS) attack. Eve makes PNS attack to steal the information fully or partially decided by the term β. Her quantum nondemolition measurements of the photon number in each pulse hide her presence in between the communication line without producing any significant errors. As the source emits multiple

photons, Eve takes advantage of that by taking one photon in quantum memory, and performing a delayed quantum measurement on the photon after the basis announcement made by Bob. The PNS attack is the main obstacle that limits the performance of the laser source used in BB84 QKD protocol experiments. The loss in the secure communication rate with the communication distance, $10^{\frac{-aL}{10}}$, for small error rate and $p_{dark} \ll p_{signal} \ll 1$. In another case, under the same operating conditions, when the deployed source is an ideal single-photon source, it is observed that $R_{BB84} \approx \frac{1}{2} \nu p_{signal}$.

Here in all the security analysis we assume that Eve is technically sound and possesses a quantum memory with infinitely long coherence time because the authentic users (here Alice and Bob) can announce the basis measurement related outcomes with long delay. On the other hand, if Eve does not have such a quantum memory she has to perform polarization measurement with arbitrary random basis selection. In such case, we can write Equation (8) as follows

$$\tau(e, \beta) = -\frac{1+\beta}{2} log_2 \Big[\frac{1}{2} + 4\Big(\frac{e}{1+\beta}\Big) - 8\Big(\frac{e}{1+\beta}\Big)^2\Big] \tag{11}$$

BB84 protocol can be designed to be robust against photon number splitting attack by deploying decoy states (Lo et al. 2005; Ma et al. 2005; Wang et al. 2005), or altering the sifting procedure (Scarani et al. 2004). In addition to these, secure communication distance is achieved by using Poisson sources in BB84 QKD protocol.

3.1 Beam-splitter attack

Alice transmits multiple photons to Bob, these photons are intercepted by Eavesdropper to get the replica of the coherent quantum states. In this strategy, Eve deploys a beam splitter with transmission η_{BS}. There are other possibilities, where Eve uses lossless fiber in place of lossy fiber. In addition to these, Eve replaces inefficient detectors by ideal detectors at the receiver end (at Bob's end). The probability, p_{signal}, is equivalent to Eq. (5), and is known as Bob's signal photon detection probability. Eve tries to unchange this probability value so that she can hide her presence, for that she changes the value of the beam-splitter transmission η_{BS} to

$$\eta_{BS} = \eta \ 10^{-(\alpha L + L_r)/10}, \tag{12}$$

The necessary parameters for the above equation is already mentioned. Eve at this stage can use an interferometer with $M\tau$ delay time selected randomly from Bob's, to get insight from the intercepted pulses. The amount of information measured can be calculated as follows. The expressions for the detection probability at Bob's and Eve's end for a given time slot are written as $\mu(1-\eta_{BS})$ and $\mu\eta_{BS}$, respectively. The term μ represents the value of mean photon number. Further, the detection probability at the same time instance is expressed as $\mu^2\eta_{BS}(1-\eta_{BS})$. Analyzing further, it is observed from the concept of conditional probability that the value of probability for an Eavesdropper received a particular bit at a given point of time where Bob has already detected the photon at that particular time frame is written as $\mu^2\eta_{BS}(1-\eta_{BS})/\mu\eta_{BS} = \mu(1-\eta_{BS})$. The expression $\frac{1}{N}$ represents the probability value that the Eavesdropper randomly selected M overlaps Bob's N. At this stage, it can be written that the probability value achieved by Eavesdropper in comparison to Bob is $\mu(1-\eta_{BS})/N$. This expression for the obtained probability by Eavesdropper is valid only and only when she is not well equipped with a quantum memory for infinitely

long coherence time. On the other hand, Eavesdropper can be equipped with a quantum memory to store the incoming photon pulses and by the time she listens to Bob's announcement to frame her strategy accordingly. To be successful in her information-gaining strategy, Eve should possess a quantum memory with long coherence time, as the authentic users, Alice and Bob, can randomly delay their individual announcements. Here, Eavesdropper deploys an optical switch with a suitable interferometer in place of a beam splitter to access the pulses for which Bob already gained the differential phase information. Hence, using this technique, there is a significant information gain to Eve, which is equal to $2\mu(1-\eta_{BS})$. Finally, using this attack strategy, Eavesdropper obtains $p_c = 1$ amount of information which corresponds to the fraction of bits equal to $\mu(1-\eta_{BS})/N$ or $2\mu(1-\eta_{BS})$. Here the BS (Beam-Splitter) attack does not introduce errors in the two authentic communicating parties, Alice and Bob. The rest of the bit fractions are given by (i) In the absence of quantum memory

$$\gamma_1 = 1 - \mu\frac{(1-\eta_{BS})}{N} = 1 - \frac{\mu}{N} + \frac{p_{signal}}{N}, \tag{13}$$

(ii) In the presence of quantum memory

$$\gamma_2 = 1 - 2\mu(1-\eta_{BS}) = 1 - 2\mu + 2p_{signal}, \tag{14}$$

3.2 Intercept-resend attack

Eavesdropper applies Intercept-resend attack which is another strategy applied on the photon pulses being sent from Alice to Bob. In such a strategy, *MT* time difference based two pulses are hacked by the Eavesdropper, they are passed via an interferometer with the same delay, further differential phase measurement takes place, and based on the outcomes Eve sends it to Bob. By this strategy, Eve splits a single photon into two with correct phase difference which is difficult to detect her presence, and hence Bob considers it as sent correctly by Alice. In this way, the Eavesdropper hides her presence. Bob can detect her presence when he measures with the probability value $(1 - 1/2N)$ and the delay value, $N \neq M$. Hence, this gives the error value equivalent to $1/2(1 - 1/2N)$. In such a situation, Eve can try the value $2e/(1 - 1/2N)$ of the pulse pair, which is less than the error rate, where e is the error rate. For obtaining full information by the Eavesdropper, the probability value is $1/2N$.

In case of the combined attacks (beam-splitter and intercept-resend attacks), Eve is unknown to the bits $p_c = \frac{1}{2}$ which are equal to $\gamma - \frac{e}{N(1-1/2N)}$. In this case, privacy amplification shrinking factor is computed as follows

$$\tau(e,\gamma) = \gamma - \frac{e}{N(1-1/2N)} \tag{15}$$

Here Eqs. 13 and 14 are used to calculate γ. Now we can express the secure communication rate equation for Differential Phase-QKD under the combined attack (beam-splitter and intercept-resend attacks).

$$R_{dpsqkd} = \nu\, p_{click}\{\tau(e,\gamma) + f(e)[elog_2 e + (1-e)log_2(1-e)]\} \tag{16}$$

Here transmission repetition rate is represented as ν. The dark count probability, p_{dark}, is written as

$$p_{dark} = 2d \tag{17}$$

The error rate expression is defined in Eq. (6), and Table 2 shows the values of $f(e)$. Under the condition, $p_{dark} \ll p_{signal} \ll 1$, we obtain the values from Equation 16, $R_{dpsqkd} \approx \nu(1-\frac{\mu}{N})p_{signal}$, in the absence of quantum memory, or $R_{dpsqkd} \approx \nu(1-2\mu)p_{signal}$, in the presence of quantum memory. These are satisfying with Gisin et al. (2004); Lo et al. (2005).

4 Results and discussion

With the described parameters and two types of detectors, we investigated the performance of Differential Phase shift QKD using frequency up-conversion. The values of the parameters under investigation are $\alpha = 0.2dB/km$ at 1550 nm, baseline system error rate, $b = 0.01$, extra loss at receiver end is $L_r = 1$ dB. Here the secure communication rate in DPS-QKD is optimized with respect to the value of the mean photon number, μ. Too low value of μ generates high dark counts, and too high values of μ is responsible for photon-number splitting attack.

It is clear from the simulated results obtained by Equation (16), and as shown in all the Figures (from Figs. 3, 4, 5 6, 7, 8, 9, 10, 11, 12) that the performance of the considered DPS-QKD protocol with two types of single photon detectors is greatly affected by detector quantum efficiency η, transmission repetition rate, ν, dark counts, d, and

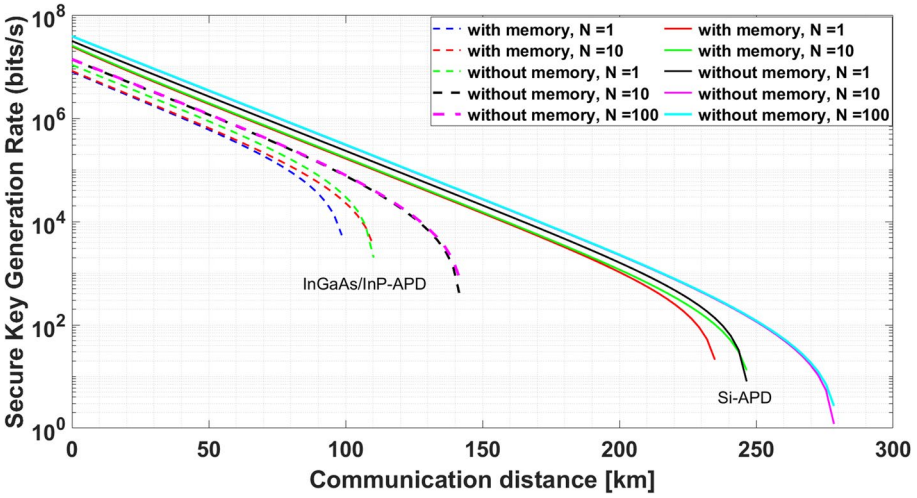

Fig. 3 Secure key generation under the considered attacks, $b = 0.01$; $\mu = 0.2$; $f = 1.16$; $\nu = 1 * 10^9$; $\eta_1 = 0.155$; $\eta_2 = 0.35$; $\alpha = 0.21$; $L_{r1} = 3.0$; $L_{r2} = 2.1$; $d_1 = 9.2 * 10^{-6}$; $d_2 = 3.5 * 10^{-8}$; $N_1 = 1$; $N_2 = 10$; $N_3 = 100$; $t_{d1} = 200 * 10^{-9}$; $t_{d2} = 45 * 10^{-9}$. Here subscript 1 and 2 denote InGaAs-APD and Si-APD, respectively

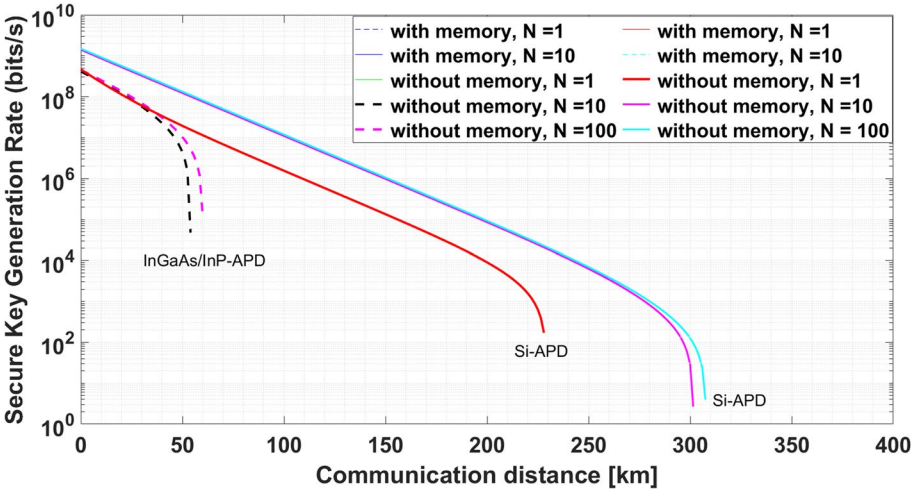

Fig. 4 Secure key generation under the considered attacks, $b = 0.01$; $\mu = 0.77$; $f = 1.16$; $\nu = 10 * 10^9$; $\eta_1 = 0.155$; $\eta_2 = 0.35$; $\alpha = 0.21$; $L_{r1} = 3.0$; $L_{r2} = 2.1$; $d_1 = 2.0 * 10^{-3}$; $d_2 = 3.5 * 10^{-8}$; $N_1 = 1$; $N_2 = 10$; $N_3 = 100$; $t_{d1} = 200 * 10^{-9}$; $t_{d2} = 45 * 10^{-9}$. Here subscript 1 and 2 denote InGaAs-APD and Si-APD, respectively

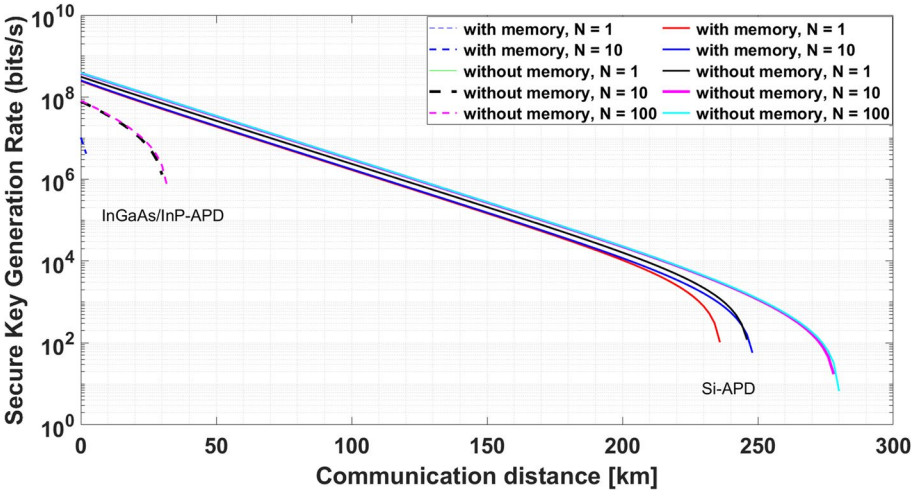

Fig. 5 Secure key generation under the considered attacks, $b = 0.01$; $\mu = 0.2$; $f = 1.16$; $\nu = 10 * 10^9$; $\eta_1 = 0.155$; $\eta_2 = 0.35$; $\alpha = 0.21$; $L_{r1} = 3.0$; $L_{r2} = 2.1$; $d_1 = 2.0 * 10^{-3}$; $d_2 = 3.5 * 10^{-8}$; $N_1 = 1$; $N_2 = 10$; $N_3 = 100$; $t_{d1} = 200 * 10^{-9}$; $t_{d2} = 45 * 10^{-9}$. Here subscript 1 and 2 denote InGaAs-APD and Si-APD, respectively

after pulse probability. Due to non-gated mode operation of Si-APD with considerable timing jitter values, we achieve better results at 1 GHz and 10 GHz. The performance limiting factor is dead time, t_d, in such cases. Here, in Poisson process, the two events occurring probability value in case of larger time t_d is given as $e^{-\delta \nu p_{click} t_d}$, here the value of δ depends on the number of used detectors. Here, the value of $t_d = 45$ ns, is taken into

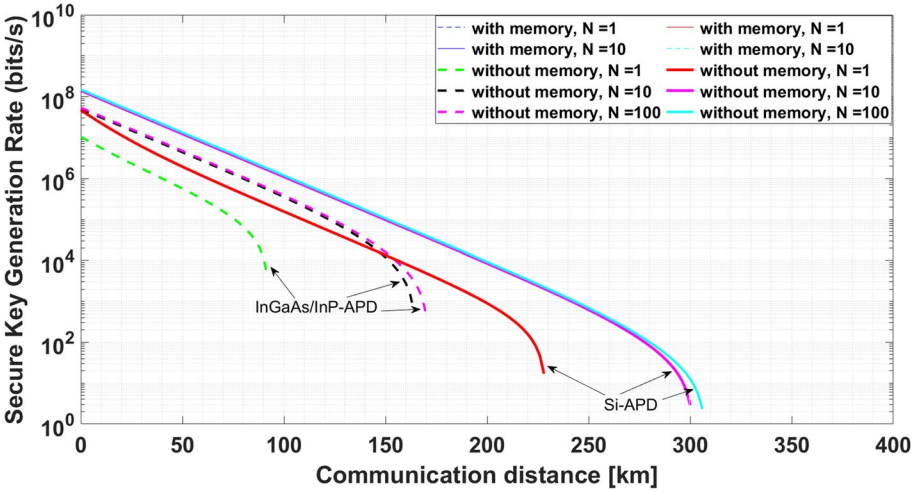

Fig. 6 Secure key generation under the considered attacks, $b = 0.01$; $\mu = 0.77$; $f = 1.16$; $\nu = 1 * 10^{9}$; $\eta_1 = 0.155$; $\eta_2 = 0.35$; $\alpha = 0.21$; $L_{r1} = 3.0$; $L_{r2} = 2.1$; $d_1 = 9.2 * 10^{-6}$; $d_2 = 3.5 * 10^{-8}$; $N_1 = 1$; $N_2 = 10$; $N_3 = 100$; $t_{d1} = 200 * 10^{-9}$; $t_{d2} = 45 * 10^{-9}$. Here subscript 1 and 2 denote InGaAs-APD and Si-APD, respectively

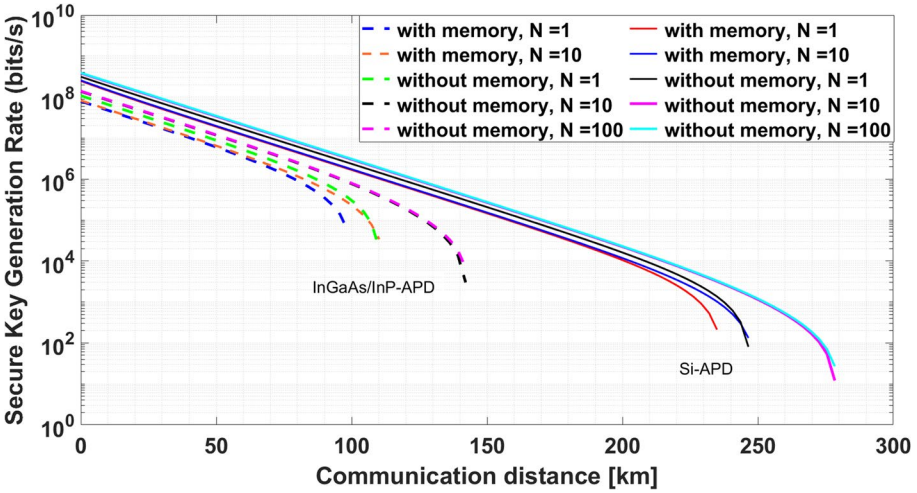

Fig. 7 Secure key generation under the considered attacks, $b = 0.01$; $\mu = 0.2$; $f = 1.16$; $\nu = 10 * 10^{9}$; $\eta_1 = 0.155$; $\eta_2 = 0.35$; $\alpha = 0.21$; $L_{r1} = 3.0$; $L_{r2} = 2.1$; $d_1 = 9.2 * 10^{-6}$; $d_2 = 3.5 * 10^{-8}$; $N_1 = 1$;$N_2 = 10$; $N_3 = 100$; $t_{d1} = 200 * 10^{-9}$; $t_{d2} = 45 * 10^{-9}$. Here subscript 1 and 2 denote InGaAs-APD and Si-APD, respectively

consideration. Using proper curve fitting method Inoue et al. (2003), we can tune the communication distance achieved with the pump power, p. Hence, the obtained optimum results as shown from Figs. 3, 4, 5 6, 7, 8, 9, 10, 11, 12 with the consideration of all such situations and the values of different parameters are mentioned in the caption of each Figures from Figs. Fig. 3, 4, 5 6, 7, 8, 9, 10, 11, 12 reflect the optimum results

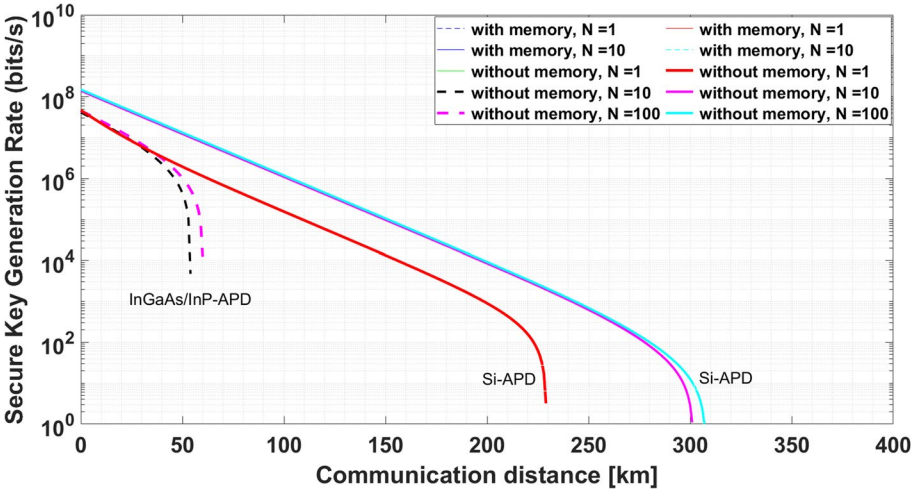

Fig. 8 Secure key generation under the considered attacks, $b = 0.01$; $\mu = 0.77$; $f = 1.16$; $\nu = 1 * 10^{9}$; $\eta_1 = 0.155$; $\eta_2 = 0.35$; $\alpha = 0.21$; $L_{r1} = 3.0$; $L_{r2} = 2.1$; $d_1 = 2.0 * 10^{-3}$; $d_2 = 3.5 * 10^{-8}$; $N_1 = 1$; $N_2 = 10$; $N_3 = 100$; $t_{d1} = 200 * 10^{-9}$; $t_{d2} = 45 * 10^{-9}$. Here subscript 1 and 2 denote InGaAs-APD and Si-APD, respectively

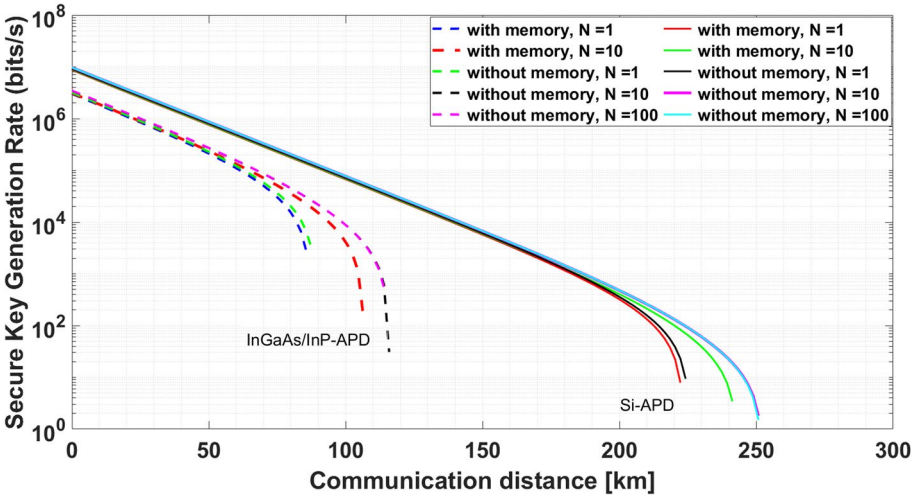

Fig. 9 Secure key generation under the considered attacks, $b = 0.01$; $\mu = 0.05$; $f = 1.16$; $\nu = 1 * 10^{9}$; $\eta_1 = 0.155$; $\eta_2 = 0.35$; $\alpha = 0.21$; $L_{r1} = 3.0$; $L_{r2} = 2.1$; $d_1 = 9.2 * 10^{-6}$; $d_2 = 3.5 * 10^{-8}$; $N_1 = 1$; $N_2 = 10$; $N_3 = 100$; $t_{d1} = 200 * 10^{-9}$; $t_{d2} = 45 * 10^{-9}$. Here subscript 1 and 2 denote InGaAs-APD and Si-APD, respectively

of secure key rates ranging from 10^7 bits/sec to 10^9 bits/sec, in the range of 200 km to 310 km communication distance.

Here, we observe that DPS-QKD performs efficiently under the PNS (photon-number splitting) attack, as described in the section of security analysis. In the simulated results we observe that, in the case when Eve has quantum memory, from Eq. (14), PNS attack does

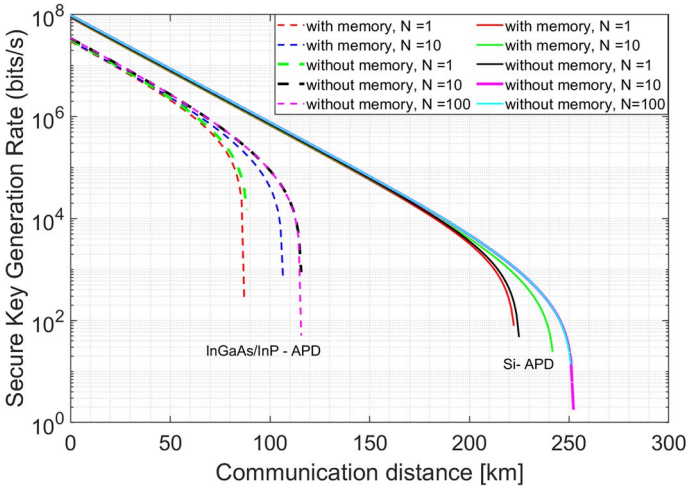

Fig. 10 Secure key generation under the considered attacks, $b = 0.01$; $\mu = 0.05$; $f = 1.16$; $\nu = 10 * 10^9$; $\eta_1 = 0.155$; $\eta_2 = 0.35$; $\alpha = 0.21$; $L_{r1} = 3.0$; $L_{r2} = 2.1$; $d_1 = 9.2 * 10^{-6}$; $d_2 = 3.5 * 10^{-8}$; $N_1 = 1$; $N_2 = 10$; $N_3 = 100$; $t_{d1} = 200 * 10^{-9}$; $t_{d2} = 45 * 10^{-9}$. Here subscript 1 and 2 denote InGaAs-APD and Si-APD, respectively

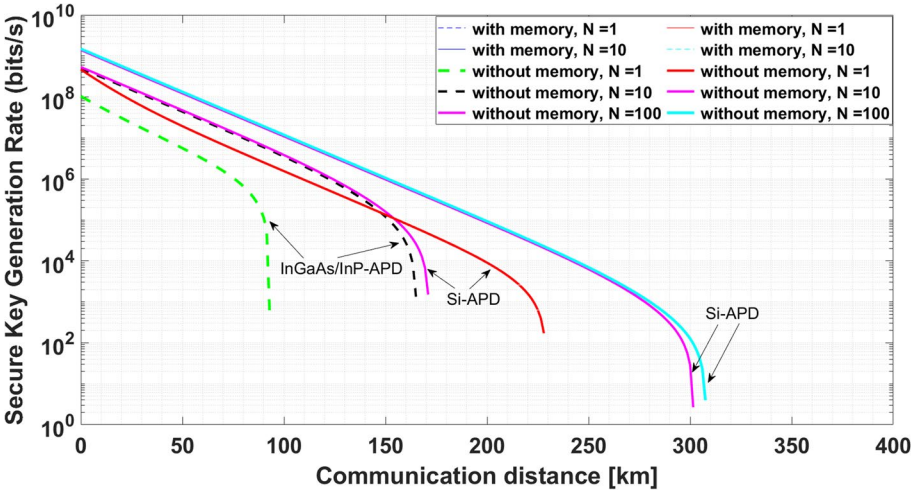

Fig. 11 Secure key generation under the considered attacks, $b = 0.01$; $\mu = 0.77$; $f = 1.16$; $\nu = 10 * 10^9$; $\eta_1 = 0.155$; $\eta_2 = 0.35$; $\alpha = 0.21$; $L_{r1} = 3.0$; $L_{r2} = 2.1$; $d_1 = 9.2 * 10^{-6}$; $d_2 = 3.5 * 10^{-8}$; $N_1 = 1$; $N_2 = 10$; $N_3 = 100$; $t_{d1} = 200 * 10^{-9}$; $t_{d2} = 45 * 10^{-9}$. Here subscript 1 and 2 denote InGaAs-APD and Si-APD, respectively

not affect the performance, the reason is that this attack is independent of delay term, N. On the opposite side, when Eve has no quantum memory with an infinitely long coherence time, the performance (secure key rate and communication distance) is severely affected, as shown in the simulated Figures. As shown in the results, when we tune the considered parameters, and delay parameter, N ($N = 1$, 10, 100), we achieve secure key rates ranging

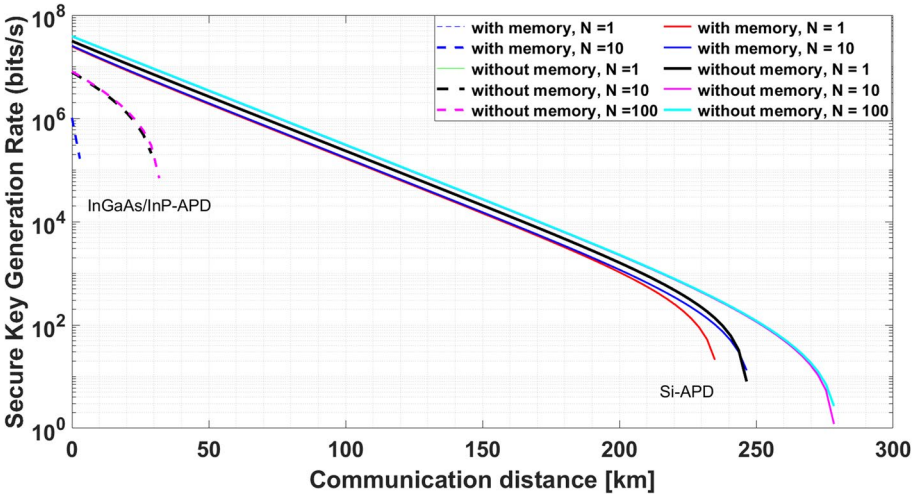

Fig. 12 Secure key generation under the considered attacks, $b = 0.01$; $\mu = 0.2$; $f = 1.16$; $\nu = 1 * 10^9$; $\eta_1 = 0.155$; $\eta_2 = 0.35$; $\alpha = 0.21$; $L_{r1} = 3.0$; $L_{r2} = 2.1$; $d_1 = 2.0 * 10^{-3}$; $d_2 = 3.5 * 10^{-8}$; $N_1 = 1$; $N_2 = 10$; $N_3 = 100$; $t_{d1} = 200 * 10^{-9}$; $t_{d2} = 45 * 10^{-9}$. Here subscript 1 and 2 denote InGaAs-APD and Si-APD, respectively

from 10^7 bits/sec to 10^9 bits/sec, in the range of 200 km to 310 km communication distance. These optimum values of performance parameters of DPS-QKD prove its practical feasibility under all the considered conditions. Under two types of detectors used, Si-APD outperforms under frequency up-conversion in terms of considered performance parameters.

5 Conclusion

The simulated protocol achieves improved results in terms of secure key generation rate, which indicates that the two APDs under consideration performs much better by deploying frequency conversion technique in a Periodically poled lithium niobate (PPLN) waveguide. Moreover, it is clearly shown in the results that Si-APD with frequency up conversion provides enhanced communication distance and secure key generation rates as compared to InGaAs-APD which are also practically feasible in real field applications where single photon detection is required at telecommunication wavelength within the acceptable quantum bit error rates. In the current research work, two types of single photon detectors at telecom wavelength are analyzed, one type of detector is InGaAs/ InP APD and another one is based on frequency up-conversion method in PPLN waveguide and further detected by silicon APD. In addition to this, security analysis under certain attacks and communication rate equations are derived and analyzed for DPS-QKD protocol. Our simulation results clearly indicate that Si-APD with frequency up conversion outperforms InGaAs/ InP APD under the considered parameter values and the hybrid attacks discussed. The improved simulation results for sifted key rate, secure key rate and quantum bit error rates are clearly highlighted which proves that Si-APD with frequency up-conversion outperforms InGaAs/ InP APD. Further, Eve's capabilities were analyzed with and without memory, which affects the performance of the overall quantum communication system. Under such conditions, from the simulated results it is clearly observed that at high frequencies i.e. 1 GHz

and 10 GHz it is possible to reach more than 300 km with considerably high secure key rates. To overcome the problems generated from birefringence and chromatic dispersion in fiber cables, it is required to deploy dispersion compensation methods (Fasel et al. 2004) and phase-encoding protocols (Honjo et al. 2004). These efforts will further improve the discussed performance parameters in realistic quantum communication scenarios.

Acknowledgements Author acknowledges 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.

Author contributions V.S. has directly participated in the planning, execution, and analysis of this study. V.S. drafted the manuscript. V.S. has read and approved the final version of the manuscript.

Funding V.S. would like to 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.

Data availability Not applicable.

Declarations

Conflict of interest The author declares that he has no competing interests.

Ethical Approval Not Applicable - The manuscript does not contain any human or animal studies.

Consent for publication Author is accepting to submit and publish the submitted work.

References

Albota, M.A. and Wong, F.N.C.: Efficient single-photon counting at 1.55 μm by means of frequency upconversion

Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental quantum cryptography. J. Cryptol. **5**, 3–28 (1992)

Bennett, CH and B Gilles, Proceedings of the IEEE international conference on computers, systems and signal processing, IEEE New York, **5**, pages 3–28, (1984)

Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68**(5), 557 (1992)

Bethune, Donald S., Risk, William P., Pabst, Gary W.: A high-performance integrated single-photon detector for telecom wavelengths. J. Mod. Opt. **51**(9–10), 1359–1368 (2004)

Bourennane, M., Karlsson, A., Ciscar, J.P., Mathés, M.: Single-photon counters in the telecom wavelength region of 1550 nm for quantum information processing. J. Mod. Opt. **48**(13), 1983–1995 (2001)

Brassard, G., Salvail, L.: Advances in cryptology Eurocrypt'93. Lect. Notes Comput. Sci. **765**, 410–423 (1994)

Fasel, Sylvain, Gisin, Nicolas, Ribordy, Grégoire., Zbinden, Hugo: Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: A comparison of two chromatic dispersion reduction methods. Eur. Phys. J. D-Atom., Mol., Opt. Plasma Phys. **30**(1), 143–148 (2004)

Fasel, S., Alibart, O., Tanzilli, S., Baldi, P., Beveratos, A., Gisin, N., Zbinden, H.: High-quality asynchronous heralded single-photon source at telecom wavelength. New J. Phys. **6**(1), 163 (2004)

Gisin, N., Ribordy, G., Zbinden, H., Stucki, D., Brunner, N. and Scarani, V.: Towards practical and fast quantum cryptography, arXiv preprint quant-ph/0411022, 2004

Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145–195 (2002)

Gobby, C and Yuan, ZL and Shields, AJ, Unconditionally secure quantum key distribution over 50km of standard telecom fibre, arXiv preprint quant-ph/0412173, (2004)

Gobby, C.: Yuan, ZL and Shields, AJ,: Quantum key distribution over 122 km of standard telecom fiber. Appl. Phys. Lett. **84**, 3762–3764 (2004)

Honjo, T., Takesue, H., Kamada, H., Nishida, Y., Tadanaga, O., Asobe, M., Inoue, K.: Long-distance distribution of time-bin entangled photon pairs over 100 km using frequency up-conversion detectors. Opt. Express **15**(21), 13957–13964 (2007)
Honjo, T., Inoue, K., Takahashi, H.: Differential-phase-shift quanum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer. Opt. Lett. **29**, 2797–2799 (2004)
https://www.idquantique.com/quantum-sensing/products/id100/
https://www.aureatechnology.com/images/produits
Inoue, K., Waks, E., Yamamoto, Y.: Differential phase shift quantum key distribution. Phys. Rev. Lett. **89**(3), 037902 (2002)
Inoue, K., Honjo, T.: Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. Phys. Rev. A **71**(4), 042305 (2005)
Inoue, K., Waks, E., Yamamoto, Y.: Differential-phase-shift quantum key distribution using coherent light. Phys. Rev. A **68**(2), 022317 (2003)
Lütkenhaus, N.: Security against individual attacks for realistic quantum key distribution. Phys. Rev. A **61**(5), 052304 (2000)
Langrock, Carsten and Diamanti, Eleni and Roussev, Rostislav V and Yamamoto, Yoshihisa and Fejer, Martin M and Takesue, Hiroki, Highly efficient single-photon detection at communication wavelengths by use of upconversion in reverse-proton-exchanged periodically poled LiNbO waveguides, Optics letters, Optica Publishing Group, **30 (13)**, pages 1725–1727, (2005)
Lo, H.-K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. **94**(23), 230504 (2005)
Ma, X., Qi, B., Zhao, Y., Lo, H.-K.: Practical decoy state for quantum key distribution. Phys. Rev. A **72**(1), 012326 (2005)
Pelc, J.S., Zhang, Q., Phillips, C.R., Yu, L., Yamamoto, Y., Fejer, M.M.: Cascaded frequency upconversion for high-speed single-photon detection at 1550 nm. Opt. Lett. **37**(4), 476–478 (2012)
Raj, Arockia Bazil and Sharma, Vishal and Banerjee, Subhashish, Quantum-based satellite free space optical communication and microwave photonics, Principles and Applications Free Space Optical Communications, IET Telecommunications Series, **78**, (2019)
Roussev, R.V., Langrock, C., Kurz, J.R., Fejer, M.M.: Periodically poled lithium niobate waveguide sum-frequency generator for efficient single-photon detection at communication wavelengths. Opt. Lett. **29**(13), 1518–1520 (2004)
Sharma, V., Banerjee, S.: Quantum communication using code division multiple access network. Opt. Q. Electron. **52**(8), 1–22 (2020)
Sharma, V., Shukla, C., Banerjee, S., Pathak, A.: Controlled bidirectional remote state preparation in noisy environment: A generalized view. Q. Inf. Process. **14**, 3441–3464 (2015)
Sharma, Vishal, Thapliyal, Kishore, Pathak, Anirban, Banerjee, Subhashish: A comparative study of protocols for secure quantum communication under noisy environment: single-qubit-based protocols versus entangled-state-based protocols. Q. Inf. Process. **15**, 4681–4710 (2016)
Sharma, V., Shrikant, U., Srikanth, R., Banerjee, S.: Decoherence can help quantum cryptographic security. Q. Inf. Process. **17**, 1–16 (2018)
Sharma, V.: Quantum Communication under noisy environment: From theory to aapplications, Indian Institute of Technology Jodhpur, (2018)
Sharma, V. and Banerjee, S.: Analysis of quantum key distribution based satellite communication, In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-5. IEEE, 2018
Sharma, Vishal, Banerjee, Subhashish: Analysis of atmospheric effects on satellite-based quantum communication: A comparative study. Q. Inf. Process. **18**(3), 1–24 (2019)
Sharma, Vishal, Sharma, Richa: Analysis of spread spectrum in MATLAB. Int. J. Sci. Eng. Res. **5**(1), 1899–1902 (2014)
Sharma, V.: Effect of Noise on Practical Quantum Communication Systems. Def. Sci. J. **66**(2), 186–192 (2016)
Sharma, V., Gupta, S., Mehta, G., Lad, B.K.: A quantum-based diagnostics approach for additive manufacturing machine. IET Collab. Intell. Manuf. **3**(2), 184–192 (2021)
Sharma, Vishal: Feasibility of temperature sensors in railway coaches. Int. J. Sci. Eng. Res. **5**(2), 881–884 (2014)
Sharma, V., Panchariya, P.C.: Experimental use of electronic nose for odour detection. Int. J. Eng. Syst. Modell. Simul. **7**(4), 238–243 (2015)
Scarani, V., Acin, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys. Rev. Lett. **92**(5), 057901 (2004)

Sharma, V. and Bhardwaj, A.: Analysis of differential phase shift quantum key distribution using single-photon detectors, In 2022 International Conference on Numerical Simulation of Optoelectronic Devices (NUSOD), IEEE, pages 17–18, (2022)

Stucki, D., Ribordy, G., Stefanov, A., Zbinden, H., Rarity, J.G., Wall, T.: Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APDs. J. Mod. Opt. **48**(13), 1967–1981 (2001)

Vandevender, A.P., Kwiat, P.G.: High efficiency single photon detection via frequency up-conversion. J. Mod. Opt. **51**(9–10), 1433–1445 (2004)

Wang, X.-B.: Beating the photon-number-splitting attack in practical quantum cryptography. Phys. Rev. Lett. **94**(23), 230503 (2005)

Waks, E., Zeevi, A., Yamamoto, Y.: Security of quantum key distribution with entangled photons against individual attacks. Phys. Rev. A **65**(5), 052310 (2002)

Yoshizawa, A., Kaji, R., Tsuchida, H.: 105 km fiber-optic quantum key distribution at 1550 nm with a key rate of 45 kHz. Jpn. J. Appl. Phys. **43**(6A), 35 (2004)