Scientific African 14 (2021) e01008

Contents lists available at ScienceDirect

Scientific African

journal homepage: www.elsevier.com/locate/sciaf

Loss-tolerant prepare and measure quantum key distribution protocol

Mhlambululi Mafu[a,*], Comfort Sekga[a], Makhamisa Senekane[b]

[a] Department of Physics and Astronomy, Botswana International University of Science and Technology, P/Bag 16, Palapye, Botswana
[b] Institute of Intelligent Systems, University of Johannesburg, Corner Kingsway and University Road, Auckland Park, Johannesburg 2092, South Africa

ARTICLE INFO

Article history:
Received 12 March 2021
Revised 12 July 2021
Accepted 7 October 2021

Editor: DR B Gyampoh

Keywords:
Loss-tolerant
Quantum key distribution
Quantum non-demolition measurements
Finite key analysis
Photon-number splitting attacks

ABSTRACT

We propose a modified version of the Bennett–Brassard 1984 quantum key distribution protocol intended to tolerate losses, certain forms of noise, and the so-called photon-number splitting attack. These are the issues facing the realization of practical quantum key distribution. The modified protocol is based on quantum non-demolition measurements for systems using weak coherent pulses. Our scheme ensures that emissions corresponding to zero photon pulses, multi-photon pulses, and detector double-clicks are discarded before sifting to improve sifting efficiency and increase the secret key rate. Moreover, we perform the finite key analysis to obtain the maximal achievable secret-key fraction and the corresponding optimal number of signals. Also, we compare our proposed protocol to the decoy-state quantum key distribution protocol. We observe that our proposed quantum key distribution scheme enables a more extended transmission distance than the decoy-state quantum key distribution protocol. Thus, this an advance in quantum communication because current limitations on quantum key distribution involve transmitting secret keys over more considerable distances in the presence of noise or losses in optical fibres.

Introduction

Quantum key distribution (QKD), one aspect of quantum cryptography, provides a way to share a secret key between Alice and Bob, with negligibly small information leakage to an eavesdropper, Eve. QKD exploits the properties of quantum mechanics to exchange cryptographic keys in such a way that is provable and guarantees security [1–3]. Ever since its inception back in 1984 [4], QKD has evolved into one of the most mature applications of quantum information science [5,6]. Thus, QKD forms one of the critical technologies in the 4th Industrial Revolution to guarantee the security of digital communication [7]. QKD achieves this goal by establishing secret keys to be used in subsequent cryptographic applications for which the requirements, the context of use, and the security properties can vary [8]. As researchers continue to refine this technology, quantum communications have already been demonstrated in some real-world applications [9]. For instance,

[*] Corresponding author.
E-mail address: mafum@biust.ac.bw (M. Mafu).

https://doi.org/10.1016/j.sciaf.2021.e01008

some applications are in the banking and finance industry, credit card industry, government and defence industry, health care data, protection of sensitive data in remote data centres, lotteries and online gaming, and electronic voting [10–12]. Notably, the ID Quantique has successfully demonstrated the use of quantum communications in the banking and financial industry to secure client sensitive data [13]. Moreover, QKD has been integrated into existing telecommunication networks to secure communication links, for instance, in Durban, South Africa [14], securing ballot transmissions to counting transmissions during the federal elections in Switzerland in 2007 [15]. Considering that Africa missed the previous Industrial Revolutions, the adoption of quantum technologies provides an opportune moment to become a key player in delivering novel disruptive technologies in the digital world [16,17]. Thus, our proposal contributes to addressing the challenge of distributing secure key over more considerable distances in the presence of noise or losses in optical fibres. Consequently, it is paramount for Africa to join this bandwagon and make a significant contribution and a massive impact on the continent and position itself as a key player for this QKD technology in the world.

However, one of the challenges facing practical QKD systems is exchanging a reasonably long secure key between two communicating parties separated arbitrarily by long distances. This is due to losses inherent in the quantum transmission channel [18]. Therefore, in this work, we propose a prepare and measure loss-tolerant BB84 (LTBB84) QKD scheme that reduces losses that could be attributed to Eve and show that such losses could be catered for during sifting. Though the BB84 protocol has been proven to be unconditionally secure; it is not tolerant to loss, noise, multi-photon signals of the source and various arbitrary attacks, especially the Photon-Number Splitting (PNS) attacks and side-channel attacks [19–21]. The novelty presented in this work is that the legitimate parties perform quantum non-demolition (QND) measurements and use only those cases in which Alice and Bob registered single-photon events. On Alice's side, combining an attenuated laser source with postselection based on a QND measurement has the effect of simulating a single-photon source. QND measurement of a single photon provides an avenue for precise measurement and versatile applications in quantum communications. The impact of a single photon QND measurement on Bob's side is to avoid errors induced by dark counts. This increases the possible transmission distance of the proposed protocol, which is a critical consideration in QKD implementations. This procedure improves the sifting efficiency and leads to an increase in the secret key generation rate. Also, we discuss the resilience of the protocol against the Photon-Number Splitting (PNS) attacks [20]. The PNS attacks decrease the security of QKD implementations that use weak coherent pulses, which constitute the most available photon sources. Finally, we show that the proposed LTBB84 QKD protocol displays improved secret key rates as a function of distance compared to the BB84 protocol. Except for this introduction, the remainder of this paper is divided into six sections. Section 2 provides background information about the existing loss tolerant BB84 protocol and quantum non-demolition (QND) measurements. It is followed by Section 3, which discusses how the proposed LTBB84 QKD scheme works. Section 4 provides the asymptotic-key and finite-key analyses, respectively, while Section 5 discusses the protocol's resilience against PNS and detector blinding attacks. The last section concludes this paper.

Background information

Loss-tolerant QKD

Various proposals of loss-tolerant QKD schemes have been studied by Tamaki et al. [22] and Vallone et al. [24]. The former scheme addresses the state preparation scheme's deficiencies, while the latter focuses on the detection scheme's deficiencies. The goal in both schemes is to find ways on how the key generation rates and distance covered can be improved. In particular, in the scheme by Tamaki et al. (2014), it was found that the eavesdropper can manipulate the state preparation flaws and introduce channel losses which leads to low key generation rates, hence lower-key transmission distance. Furthermore, the authors show how using a scheme with low detection efficiency can realise secure key generation rates compared to other protocols. However, in our proposal, we develop a scheme that reduces the losses attributed to Eve. In particular, we demonstrate that such losses could be catered for during the sifting process. This approach dramatically results in an improvement in the sifting efficiency and leads to increased secret key rates.

Quantum non-demolition measurement (QND)

QND is a type of measurement which does not change the signal states [25]. This is because the measurement commutes with the density matrices of the source. The QND measurement procedure allows the error-free detection of the number of photons in the transmitted signal. Various proposals and implementations of QND have been reported in the literature, and have very high single-photon detections [26–30]. In our proposed scheme, Alice and Bob perform a QND measurement on the number of photons sent by the source in the proposed scheme. The positive operator-valued measurement (POVM) of the QND measurement consists of two elements $\{|1\rangle\langle 1|, 1 - |1\rangle\langle 1|\}$, where $\{|n\rangle\}$ is the Fock state basis. Therefore, after each QND measurement step, only the time-slots containing single photons are used in the next stage of the protocol's execution. In the time-slot where there are vacuum components and multi-photon pulses, a zero is recorded. The discarding of multi-photon pulses also prevent Eve from performing PNS attacks. This is so because, in this scenario, the legitimate users of the system can post-select only those events where Alice sends single-photon state. Also, if one assumes that Eve cannot influence the correct operation of Bob's QND measurements once the QND measurement has been performed, the sifted pulse will pass through a standard QKD measurement set-up, where one measurement basis is chosen at random out

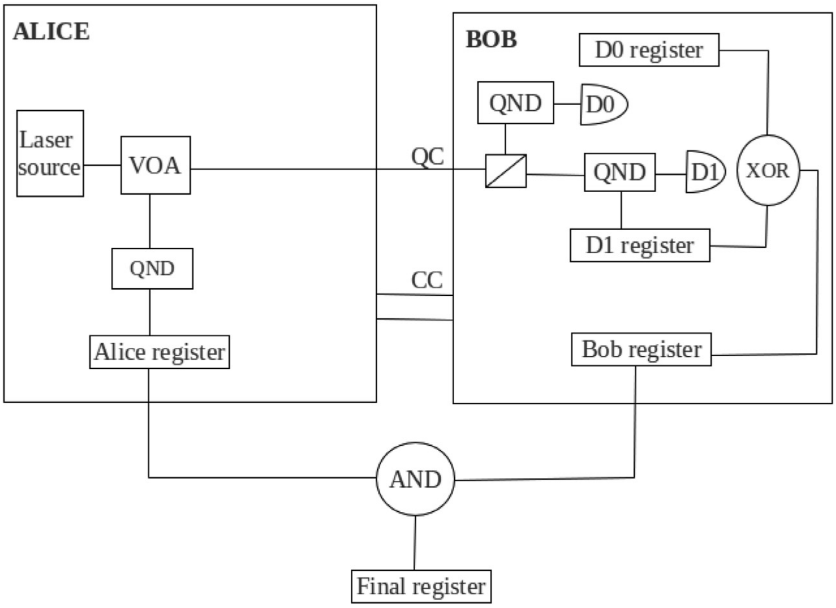

Fig. 1. The schematic diagram for the LTBB84 QKD protocol. In the diagram, CC: classical communication channel, QC: quantum channel, VOA: variable optical attenuator, XOR and AND gates, QND: quantum non-demolition measurement apparatus, D0, and D1: detectors.

of the X- and Y-bases. This step's significance is to allow only the use of time-slots with single photons that carry useful information, thereby improving efficiency and secret key generation rates.

Operation of the protocol

Ideally, QKD protocols should use single-photon sources. However, in practical QKD implementations, weak coherent pulses (given as $|\sqrt{\mu e^{i\theta}}\rangle$, where μ is the mean photon number and the random angle) are used instead [1]. These laser pulses are attenuated to single-photon levels in order to mimic true single-photon sources. Unfortunately, such lasers sources obey Poissonian distribution given as

$$P_n = \frac{e^{-\mu}\mu^n}{n!}, \tag{1}$$

where P_n is the probability of containing n photons. In such cases, some of the pulses will have more than one photon or no photon at all. Multi-photon pulses expose QKD systems to photon number splitting (PNS) attacks and detector blinding attacks, while zero-photon pulses increase the channel loss.

An analysis on the effect using imperfect photon sources and inefficient detectors on the BB84 protocol was done by Gottesman et al. [32], which rendered the BB84 protocol inoperable over long distances. To improve the performance of the BB84 by using imperfect devices, the decoy-state method was developed [18,33]. A series of decoy-state QKD experiments have been performed and proved successful. For example, it was demonstrated that the decoy-state QKD was effective against PNS attacks [34] and could distribute secret keys over a distance above 200 km [35]. However, even though this decoy method is provably secure, it is very inefficient since some of the signals are used as decoy states, and these decoy states do not form part of the secret key.

In the light of the above, we propose a QKD protocol that makes use of QND measurements to counter similar challenges. This protocol does not rely on the optimization of the mean photon number. Additionally, the proposed protocol can be realized over a relatively longer distance than the decoy-state QKD. The notion of QND measurement is already used in QKD security proofs, and it is normally assumed that Eve has QND apparatus [32]. In this proposal, legitimate parties (Alice and Bob) also have access to the QND apparatus. In the set-up, we assume that standard measurements are performed for the preparation devices and the detectors. In particular, the latter is assumed to be of finite efficiency. For simplicity, we assume ideal QND measurements at both Alice's and Bob's sides. However, we point out that we are under no illusion that ideal QND measurements are easy to implement.

Fig. 1 shows a schematic diagram of the proposed protocol. The scheme is a modification of the BB84 protocol [4] but it can equally be applied to the B92 protocol [36] and other prepare-and-measure protocols. It works as follows:

1. A QND measurement is performed for each pulse on Alice's side after the attenuation stage. Then, the result of the measurement is recorded in Alice's register. If a zero-photon pulse or a multi-photon pulse is detected, a value '0' is

entered into the register. On the other hand, if a single photon is detected, a value ‘1’ is entered into the register. We can call this result_a.

2. A QND measurement is then performed on each detector on Bob’s side. Like Alice’s case, the value ‘1’ is recorded if the single-photon was measured, while ‘0’ is recorded for zero-photon emissions. Then the XOR operation is applied to each detector’s register with the other, resulting in result_b.
3. In the case where a multi-photon pulse is detected in at least one of Bob’s QND set-ups, a value of zero is directly entered into the result b register. This, as will be discussed later, will effectively render any detector blinding attack impossible since all detector clicks corresponding to multi-photon pulses would be discarded.
4. Alice and Bob then exchange their results (registers the result_a and result_b) through the classical channel. Each then applies AND gate to their two registers, resulting in result_final on each side. If the entry of result_final is ‘1’, then the frame corresponding to that pulse is used for sifting; otherwise, it is discarded.

Alice’s system

As shown in Fig. 1, Alice’s equipment consists of a conventional apparatus, with an addition of a QND set-up. The QND apparatus is placed after the attenuator to detect a photon’s presence in a pulse that would propagate through a quantum channel. Since QND measurement equipment could detect a zero-photon pulse and a multi-photon pulse, the scheme can use the procedure above for zero-photon pulses and enable the decoy-state use method for multi-photon pulses [18]. This implies that with our set-up, we can also realize decoy-state QKD.

Bob’s system

According to Fig. 1, on Bob’s side, the QND measurement apparatus is placed before each detector to sense the photon’s presence from the quantum channel before detection. This set-up is also used to mitigate double-clicks. Typically, squash models are used to mitigate the effect of double-clicks though these models are limited [37,38]. Therefore, our proposed set-up on Bob’s side is similar to the one proposed in Ref. [23,37].

Post-processing

The post-processing stages of the proposed LTBB84 protocol are similar to the standard BB84 protocol except that there is a new stage added before sifting, and this stage is called the pre-sifting stage. This stage’s primary objective is to determine which pulses will be used for sifting and which ones are discarded (either because the pulses correspond to zero-photon emissions, multi-photon emissions, or detector double-clicks). This stage is responsible for the protocol’s loss-tolerant nature since not all the losses would be attributed to Eve. After the pre-sifting stage, all the stages are similar to the conventional BB84 protocol post-processing stages.

Security analysis

In this section, we analyze the security of the LTBB84 QKD protocol. When evaluating the security of a QKD protocol, several parameters are considered [2,39,40]. One of the most important figures of merit is the secret key rate or the maximal achievable distance [1]. Thus, we evaluate the achievable key rate or secret key generation rate over a transmission distance. The distance or length provides a constraint over which secure key material can be generated due to scattering and absorption of polarized photons and other factors, and this limits the ability of quantum channels to a certain distance [31]. An ideal scenario has a QKD protocol with a higher key rate over long distances. In the past decade, steadily increasing secret key rates have been obtained with improved optical components and better electronics, mainly in the detectors [8]. It has been established from the security proofs that a secure final key can be extracted from the sifted key at a non-zero asymptotic rate in the case of low bit-error rates. If the error-correction and privacy amplification are carried out by using only one-way communication from Alice to Bob, the ratio of length ℓ of the final key (after error correction and privacy amplification) to the length n of the sifted key is expressed as

$$\begin{aligned} r &= \lim_{n\to\infty} \frac{\ell}{n} \\ &\geq p(1-2h(Q)), \end{aligned} \tag{2}$$

where p is the probability that Alice generates a single-photon state and this photon is detected by Bob, $h(Q) = -Q\log_2 Q - (1-Q)\log_2(1-Q)$, is the binary Shannon entropy and Q is the quantum bit-error rate (QBER) of the single-photon events (that is, of those events where Alice “sees” precisely one photon in her QND measurement). It can be found that a secure key exchange can be achieved for any $Q < 11\%$ [32].

Furthermore, we investigate the finite-length key of the LTBB84 protocol. However, the finite-key analysis has also been investigated in several papers [41–46]. In our security analysis, we follow closely the tools invented by Renner [41] and the formalism in Ref. [42] to derive the lower bound for the secure key rate for the LTBB84 QKD protocol. Therefore, let ρ_{KE} be a classical-quantum state that describes the classical key K of length ℓ distilled at the end of the run of the QKD protocol.

Then, for any $\varepsilon \geq 0$, a final key K is said to be ε-secure with respect to an adversary Eve ρ_E if the joint state ρ_{KE} satisfies [41]

$$\min_{\rho_E} ||\rho_{KE} - \tau_K \otimes \rho_E||_1 \leq \varepsilon, \tag{3}$$

where τ_K is a completely mixed state on a key space S_K. The parameter ε represents the maximum failure probability of the key extraction procedure. Therefore, the classical key K is indistinguishable from a random and uniform key with probability $1-\varepsilon$. The total security parameter of a QKD scheme depends on the sum of probabilities of failures of the classical post-processing protocols. This can be written as

$$\varepsilon = \bar{\varepsilon} + \varepsilon_{\mathrm{PA}} + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PE}}, \tag{4}$$

where $\bar{\varepsilon}$ denotes the error in the smooth-min entropy, $\varepsilon_{\mathrm{PA}}$ is the error in the privacy amplification step, $\varepsilon_{\mathrm{EC}}$ denotes error in the error correctional step and $\varepsilon_{\mathrm{PE}}$ is the error in the parameter estimation step.

For parameter estimation, we let Γ_ξ be a set of compatible states from which a key is extracted with a non-negligible probability. If the statistics λ_m are obtained from measuring m samples of ρ_{AB} (i.e., the entangled state shared by Alice and Bob) according to a POVM measurement with d possible outcomes and $\lambda_\infty(\rho_{AB})$ denotes the perfect statistics in the limit of infinitely measurements, then for any state ρ_{AB} [42]

$$\Gamma_\xi := \{\rho_{AB} : ||\lambda_m - \lambda_\infty(\rho_{AB})||_1 \leq \xi\}, \tag{5}$$

where by the law of large numbers [41]

$$\xi := \sqrt{\frac{\ln(1/\varepsilon_{\mathrm{PE}}) + 2\ln(m+1)}{2m}}. \tag{6}$$

During the error correction procedure, the number of bits leaked during the classical communication to an eavesdropper is given by Scarani and Renner [42,43]

$$\mathrm{leak}_{\mathrm{EC}} = f_{\mathrm{EC}} n h(Q) + \log_2(\frac{2}{\varepsilon_{\mathrm{EC}}}), \tag{7}$$

where f_{EC} is a constant larger than 1 (in practice $f \approx$1.05 - 1.2), n is the length of the raw key, $h(Q)$ is the binary Shannon entropy, Q is the QBER and $\varepsilon_{\mathrm{EC}}$ is the error probability in the error correction step. Let η_{QND} be the QND measurement efficiency, η_B be Bob's detector efficiency, and transmittance t be given by

$$t = 10^{-\frac{\alpha L + \gamma_A + \gamma_B}{10}}, \tag{8}$$

where α is transmission loss per kilometre, γ_A is loss in Alice's optical elements and γ_B is loss in Bob's optical elements. Then, the number of signals used for QKD, N, is given as

$$N = P_1 \eta_{QND}^2 t \eta_B N', \tag{9}$$

where N' is the number of generated pulse. For a finite-number of signals, the achievable secure key rate was initially derived in Ref. [42] but has been found to be

$$r = \frac{n}{N'}[S_\xi(X|E) + \triangle(n) - \mathrm{leak}_{\mathrm{EC}}] + \frac{2}{N'}\log_2(2\varepsilon_{\mathrm{PA}}), \tag{10}$$

where $S_\xi(X|E) = 1 - 2h(Q)$ and $\triangle(n) = -(2\log d + 3)\sqrt{[\log_2(2/\bar{\varepsilon})]/n}$.

Fig. 2 shows the finite key as a function of input signals N' for different values of quantum bit error rate Q (2.5% and 5.0%) and different values of mean photon number μ (0.2 and 1.0). It can be observed from the figure that varying the value of μ does not result in a significant increase in key generation rate. This implies the proposed protocol is less dependant on the optimization of μ than the standard decoy-state protocol. On the other hand, in Fig. 3 we demonstrate the variation of secret key generation rate as a function of optical fibre distance for different values of Q and μ. Most significantly, it can be observed that the proposed protocol has a more extended range than the decoy-state QKD. Thus, we consider this a scientific advance since, in current implementations, noise or losses in optical fibres limit the maximal achievable distance.

Resilience against PNS attacks

Using the attenuated laser sources, which are usually implemented in practical QKD, the protocols' performance is limited due to PNS attacks. In this type of attack, the source emits two or more photons in a pulse. This means Eve can perform a QND measurement on one photon, thereby obtaining information that correlates with Alice's and Bob's information without causing errors [19]. This protocol is secure against PNS attacks because all multi-photon pulses are discarded during QND measurement, and only single photons that encode information are exchanged. Furthermore, the proposed protocol is secure against detector blinding attacks because the scheme can detect multi-photon pulses on Bob's side. The blinding pulse would be a multi-photon; therefore, it would be detected. It should be noted that for the standard decoy method to compare with our proposed LTBB84 QKD protocol, the decoy method must be implemented both on Alice's and Bob's sides. As already mentioned, since the decoy method is very inefficient, implementing it on both sides of the communicating parties decreases the secret key generation rate. Therefore, our proposed scheme offers an advantage of a better key generation rate over the standard decoy-state method.

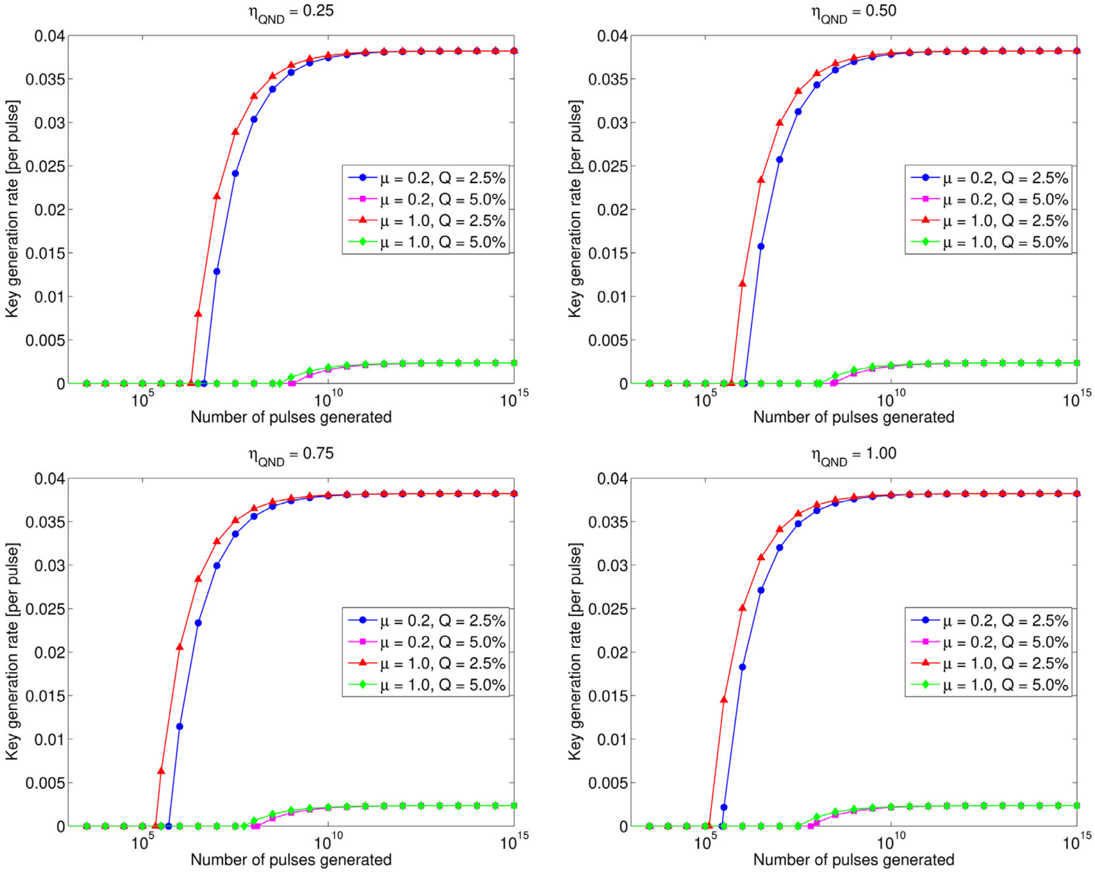

Fig. 2. Secret-key generation rate r is a function of the number pulses generated by Alice N' for different values of mean photon number μ, quantum bit error rate Q and QND measurement efficiency η_{QND}. The following parameters were used in the simulation: optical fibre attenuation coefficient $\alpha = 0.35$ dB/km, length of optical fibre $L = 100$km, losses due to Alice's and Bob's optical devices $\gamma_A = \gamma_B = 1.3$dB, detector efficiency $\eta_B = 0.2$, dark count probability $P_D = 3.3 \times 10^{-6}$, error correction efficiency $f_{EC} = 1.2$, failure probability of the protocol $\epsilon = 10^{-5}$ and error probability of the error correction step $\epsilon_{EC} = 10^{-10}$.

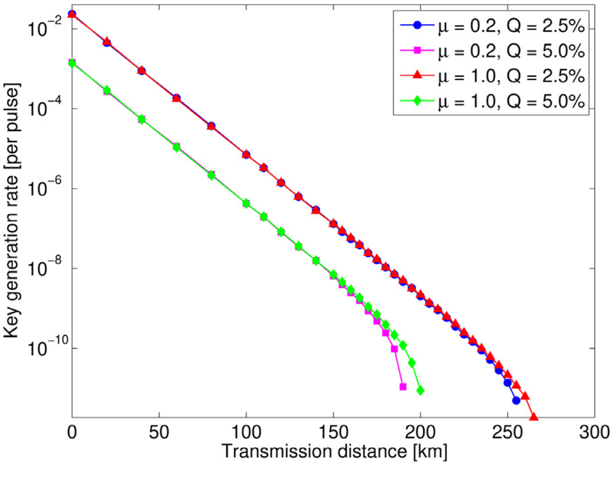

Fig. 3. Secret-key generation rate as a function of transmission distance for different values of the mean photon number μ and quantum bit error rate Q. The following parameters were used in the simulation: number of pulses generated $N' = 10^{15}$, optical fibre attenuation coefficient $\alpha = 0.35$ dB/km, losses due to Alice's and Bob's optical devices $\gamma_A = \gamma_B = 1.3$dB, detector efficiency $\eta_B = 0.2$, QND measurement efficiency $\eta_{QND} = 0.75$, dark count probability $P_D = 3.3 \times 10^{-6}$, error correction efficiency $f_{EC} = 1.2$, failure probability of the protocol $\epsilon = 10^{-5}$ and error probability of the error correction step $\epsilon_{EC} = 10^{-10}$.

Conclusion

We have demonstrated the operation of our proposed LTBB84 QKD scheme. We showed that performing QND measurements before the pulses go through the quantum channel (on Alice's side) and before they are detected (on Bob's side) leads to an increase in Alice and Bob's communication distance. Furthermore, we demonstrate that a minimum number of approximately $10^6 - 10^8$ signals are required to extract reasonable secret keys in realistic scenarios. Thus, it is possible to cover a longer distance in a lossy channel with the proposed protocol than a conventional decoy-state QKD. Additionally, our proposed protocol does not require optimizing the mean photon number ($\mu = (0, 1]$), unlike the decoy-state QKD, where μ must be optimized to ensure that yield is greater than the probability of multi-photon generation. Furthermore, we have shown that the LTBB84 QKD protocol is robust against PNS attacks. Therefore, the pre-sifting step and the QND measurement step prove functional processes that lead to increased secret-key generation rates over long distances, even when the channel is lossy.

Declaration of Competing Interest

The authors declare no conflict of interest.

CRediT authorship contribution statement

Mhlambululi Mafu: Conceptualization, Writing – original draft, Writing – review & editing, Project administration. **Comfort Sekga:** Writing – original draft, Writing – review & editing. **Makhamisa Senekane:** Conceptualization, Writing – original draft, Writing – review & editing.

Acknowledgments

This work is based on research supported by funding from Botswana International University of Science and Technology Research Initiation Grant (Grant number: R00015).

References

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74 (2002) 145–195.
[2] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. 81 (2009) 1301.
[3] M. Mafu, A simple security proof for entanglement-based quantum key distribution, J. Quantum Inf. Sci. 6 (2016) 296.
[4] C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. New York: Bangalore, India, 1984, pp. 175–179.
[5] D. Bruß, Optimal eavesdropping in quantum cryptography with six states, Phys. Rev. Lett. 81 (1998) 3018–3021.
[6] H.Q. Ma, K.J. Wei, J.H. Yang, Simple quantum key distribution scheme with excellent long-term stability, J. Opt. Soc. Am. B 30 (2013) 2560–2562.
[7] S. Hong, Security vulnerability and countermeasure on 5G networks: survey, J. Digit. Converg. 17 (2019) 197–202.
[8] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, M. Voznak, Quantum key distribution: a networking perspective, ACM Comput. Surv. (CSUR) 53 (2020) 1–41.
[9] M. Sasaki, Quantum key distribution and its applications, IEEE Secur. Priv. 16 (2018) 42–48.
[10] C. Elliott, D. Pearson, G. Troxel, Quantum cryptography in practice, in: Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'03), 2003, p. 227.
[11] T. Langer, The practical application of quantum key distribution, University of Lausanne, 2013 Ph.d. thesis.
[12] C. Sekga, M. Mafu, Quantum state sharing of an arbitrary m-particle state using einstein Podolsky Rosen pairs and application in quantum voting, Mod. Phys. Lett. A (2021) 2150151.
[13] Quantum-safe security solutions for banking and financial institutions. Retrieved from https://www.idquantique.com/quantum-safe-security/applications/banking-solutions/.
[14] A. Mirza, F. Petruccione, Realizing long-term quantum cryptography, J. Opt. Soc. Am. B 27 (2010) A185–A188.
[15] P. Morgen, Geneva vote will use quantum cryptography. Retrieved from https://spectrum.ieee.org/computing/networks/geneva-vote-will-use-quantum-cryptography.
[16] N.J. Van Rensburg, A. Telukdarie, P. Dhamija, Society 4.0 applied in Africa: advancing the social impact of technology, Technol. Soc. 59 (2019) 101125.
[17] T. Marwala, Closing the Gap: The Fourth Industrial Revolution in Africa, Macmillan, 2020.
[18] W.Y. Hwang, Quantum key distribution with high loss: toward global secure communication, Phys. Rev. Lett. 91 (2003) 057901.
[19] V. Scarani, A. Acin, G. Ribordy, N. Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations, Phys. Rev. Lett. 92 (2004) 57901.
[20] N. Lütkenhaus, Security against individual attacks for realistic quantum key distribution, Phys. Rev. A. 61 (5) (2000) 052304.
[21] S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin, V. Egorov, A. Kozubov, V. Makarov, An approach for security evaluation and certification of a complete quantum communication system, Sci. Rep. 11 (2021) 1–16.
[22] K. Tamaki, M. Curty, G. Kato, H.K. Lo, K. Azuma, Loss-tolerant cryptography with imperfect sources, Phys. Rev. A 90 (2014) 052314.
[23] C.-H.F. Fung, H.F. Chau, H.K. Lo, Universal squash model for optical communications using linear optics and threshold detectors, Phys. Rev. A 84 (2011) 020303.
[24] G. Vallone, A. Dall'Arche, M. Tomasin, P. Villoresi, Loss tolerant device-independent quantum key distribution: a proof of principle, New J. Phys. 16 (2014) 063064.
[25] M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press., 2000.
[26] H.A. Bachor, T.C. Ralph, A guide to experiments in quantum optics, 2004. 2nd, Revised and Enlarged Edition
[27] M. Curty, T. Moroder, Heralded-Qubit amplifiers for practical device-independent quantum key distribution, Phys. Rev. A. 84 (2011) 010304.
[28] N. Gisin, S. Pironio, N. Sangouard, Proposal for implementing device-independent quantum key distribution based on a Heralded Qubit amplifier, Phys. Rev. Lett. 105 (2010) 070501.

[29] T. Ralph, A. Lund, Nondeterministic noiseless linear amplification of quantum systems, in: Proceedings of the Ninth International Conference on Quantum Communication, Measurement and Computing (QCMC): QCMC (AIP Publishing)., 1110, 2009, pp. 155–160.

[30] A. Reiserer, S. Ritter, G. Rempe, Nondestructive detection of an optical photon, Science 342 (2013) 1349–1351.

[31] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, T. Länger, Security of trusted repeater quantum key distribution networks, J. Comput. Secur. 18 (2010) 61–87.

[32] D. Gottesman, H.K. Lo, N. Lütkenhaus, J. Preskill, Security of quantum key distribution with imperfect devices, Quant. Inf. Comput. 5 (2004) 325–360.

[33] H.K. Lo, X. Ma, K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. 94 (2005) 230504.

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

[35] Y. Liu, T.Y. Chen, J. Wang, W.Q. Cai, X. Wan, L.K. Chen, J.H. W, S.B. Liu, H. Liang, L. Yang, Decoy-state quantum key distribution with polarized photons over 200 km, Opt. Express 18 (2010) 8587–8594.

[36] C.H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. 68 (1992) 3121.

[37] T. Moroder, M. Curty, N. Lütkenhaus, Detector decoy quantum key distribution, New J. Phys. 11 (2009) 045008.

[38] V. Scarani, C. Kurtsiefer, The black paper of quantum cryptography: real implementation problems, Theor. Comput. Sci. 560 (2014) 27–32.

[39] M. Mafu, Security in quantum key distribution protocols, University of KwaZulu-Natal, 2013 Ph.d. thesis.

[40] M. Mafu, M. Senekane, Security of quantum key distribution protocols, in: Advanced Technologies of Quantum Key Distribution, IntechOpen, 2018, pp. 3–15.

[41] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. 6 (2008) 1–127.

[42] V. Scarani, R. Renner, Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way post-processing, Phys. Rev. Lett. 100 (2008) 200501.

[43] R.Y. Cai, V. Scarani, Finite-key analysis for practical implementations of quantum key distribution, New J. Phys. 11 (2009) 045024.

[44] M. Mafu, K. Garapo, F. Petruccione, Finite-size key in the Bennett 1992 quantum-key-distribution protocol for Rényi entropies, Phys. Rev. A 88 (2013) 062306.

[45] M. Mafu, K. Garapo, F. Petruccione, Finite-key-size security of the Phoenix-Barnett-Chefles 2000 quantum-key-distribution protocol, Phys. Rev. A 90 (3) (2014) 032308.

[46] M. Tomamichel, C.C.W. Lim, N. Gisin, R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. 3 (2012) 634.