Physics Open 7 (2021) 100075

Contents lists available at ScienceDirect

Physics Open

journal homepage: www.journals.elsevier.com/physics-open

Security of quantum-key-distribution protocol by using the post-selection technique

Comfort Sekga *, Mhlambululi Mafu

Department of Physics and Astronomy, Botswana International University of Science and Technology, P/Bag 16, Palapye, Botswana

ARTICLE INFO

Keywords:
Quantum key distribution
SARG04 protocol
Post-selection technique
Finite resources

ABSTRACT

The post-selection technique was proposed by Christandl, König, and Renner [Phys. Rev. Lett. 102, 020504 (2009)] to simplify the security of quantum-key-distribution schemes. This work applies this technique to derive the security bounds for the six-state Scarani-Acin-Rigbordy-Gisin 2004 quantum key distribution protocol. This protocol can extract secure keys from a source emitting multi-photons due to its robustness from photon number splitting attacks, making it a good candidate for practical implementations. We also compare the security bounds for this protocol under collective attacks to the security bounds obtained after applying the post-selection technique when using finite resources. Our results demonstrate that the bounds for optimal attack are close to the bound for collective attack for many signals. Notably, the six-state SARG04 protocol proves to be more robust to the PNS attacks when compared to the original four-state SARG04 protocol. This demonstrates the power of the post-selection technique in deriving the security bounds for the six-state protocol when finite resources are used.

1. Introduction

Quantum key distribution (QKD) is one of the most advanced applications of quantum cryptography which permits two legitimate parties, Alice and Bob, to securely share a random secret key in the presence of an eavesdropper, Eve [1]. QKD, in principle, promises information-theoretic security guaranteed by the laws of quantum physics [2]. However, in practice, some theoretical and experimental challenges remain unresolved. For instance, the matching of the theoretical security proofs to real devices and implementing QKD over large scale networks [3–5]. Other challenges include obtaining reasonable key rates over large distances, high costs associated with deploying QKD technologies and combining QKD with information-theoretic cryptographic protocols or algorithms, for instance, AES encryption [6–8]. Thus, these challenges make QKD technologies not a viable immediate alternative to conventional cryptography. Impressively, regardless of these challenges, commendable progress has been realised as higher transmission distances have recently been achieved [9–12] and quantum technology-based systems have become available on the market [13]. Also, QKD has been practically implemented in various countries, for example, during the 2010 World Cup in South Africa [14]. Furthermore, it has been installed in fibre networks at metropolitan areas [15–19] as well as in satellite QKD communications [20–23]. Thus, these examples demonstrate that QKD will be vital in securing the next generation of digital communications.

In 1984 following Wiesner's ideas, Bennett and Brassard proposed the first complete QKD protocol, now known as the BB84 protocol [24]. The BB84 protocol has become one of the best-studied QKD schemes and has been demonstrated experimentally. It was designed to distribute a secret key between two legitimate parties securely, and this key is used in one-time-pad (OTP) encryption [25]. In 1991 Ekert augmented the idea and considered a protocol for which the security is based on the violation of Bell's inequality, thus leading to the realization of E91 protocol [26]. In 1992, by applying the idea of E91 to the BB84 protocol, Bennett, Brassard and Mermin developed the BBM92 protocol, which also relies on the principle of entanglement for security [27]. Based on the detection technique required to recover the key information encoded in the properties of light, QKD protocols can be divided into three classes. The BB84, E91, BBM92, B92 [28], SARG04 [29] and decoy-state protocols [30–32] belong to a class called discrete-variable (DV) protocols. In this class, information is encoded in the polarization pulses, which simulate true single-photon states and require single-photon detectors for their implementation. Owing to the difficulty in realizing true single-photon sources and detectors, another class of continuous-variable (CV) protocols was proposed. In this class, information is encoded in the quadratures of the quantized electromagnetic field, for instance, those of

* Corresponding author.
E-mail addresses: comfort.sekga@gmail.com, comfort.sekga@studentmail.biust.ac.bw (C. Sekga).

https://doi.org/10.1016/j.physo.2021.100075
Received 16 February 2021; Received in revised form 26 April 2021; Accepted 8 May 2021
Available online 25 May 2021

coherent or squeezed states [33–39]. Due to other practical requirements, the class of distributed-phase-reference (DPR) protocols in which the coherence of sequential pulses play an important role in security was proposed. In the DPR class, information is encoded in photon arrival times or the phase between adjacent weak coherent pulses. Members of this family are the differential-phase-shift (DPS) protocol [40] and coherent-one-way (COW) protocol [41] and these protocols are tolerant to photon number splitting (PNS) attacks. Regarding detection, the DV and DPR protocols employ the single-photon detection technique while the CV protocols use homodyne or heterodyne detection technique [42–44].

While noticeable progress has also been realised on the practical side, as previously mentioned, significant effort has been dedicated to developing new QKD security proofs and improving existing ones [2]. Since the first unconditional security proof by Mayers in 1996 [45], many security tools and proofs have been developed [46–58]. Most of these QKD security proofs are based on the assumption that the communicating parties have a perfect single-photon source and perfect detectors [2,48, 59–61]. However, in practical QKD the imperfections in the physical devices used for implementing the protocol are inevitable [62,63]. In order to circumvent these challenges, several protocols such as device-independent QKD [64,65], measurement-device-independent QKD [66–68], DPR protocols and decoy state protocols [32] were proposed. In these works, security bounds were computed on the assumption that an infinite number of signals are available to generate a reasonable secret key. However, the tools for computing unconditional security in the finite-key regime have become available and proofs of security for finite length keys have been studied mostly under the assumptions of collective and coherent attacks for DV protocols [55,69–75], decoy state protocols [76–80] CV protocols [81–83] and for DPR protocols [84]. Other efforts have been undertaken to improve the bounds on the secret key rates, for instance, by using a technique involving the uncertainty relations for smooth-entropies [72,85,86]. This approach has demonstrated to be elegant since it provides bounds for general kinds of attacks rather than collective attacks. However, this strategy works perfectly for protocols implemented with two mutually unbiased bases; thus, we cannot employ this strategy in six state SARG04 protocol because of the additional Y basis.

The non-orthogonal state coding proposed in the SARG04 QKD protocol is an important feature that can allow the user to implement quantum cryptography with a multiphoton source. Due to its interesting property of uncertainty in discrimination of quantum states, it has been applied to prove security against forgery attack in quantum digital signature schemes [87,88]. Furthermore, it has been widely investigated both theoretically [89–92] and experimentally [93,94] to demonstrate security of QKD. All these works considered asymptotic key size regime to obtain security bounds. Therefore, in this work, we apply the post-selection technique to derive the security bounds for the six-state SARG04 QKD protocol using finite resources. This protocol is robust against the zero-error type of attacks such as PNS attacks, and this allows us to demonstrate the unconditional security against the optimal coherent attacks under practical conditions where a source emits multiple photons. Although the DPR protocols are also resistant to PNS attacks, they are not symmetric, and this makes it not immediate to derive their bounds using the post-selection technique. Therefore, our results provide an insight about the size of secret key generation rates one can obtain when the six-state protocol is practically implemented.

This paper is arranged according to the following. In section I, we provide an introduction where we make a brief review of QKD security developments and the motivation of our work. In section II, a review of the six-state SARG04 protocol is undertaken. This is followed by section III, where we show the details of the security proof for the six-state SARG04 protocol based on collective attacks. In section IV, we provide security bounds for the coherent attacks along the lines sketched in Ref. [95]. Finally, we compare the security bounds for the four-state protocol, the six-state SARG04 protocol under collective attacks, and the security bounds obtained after applying the post-selection technique.

2. Review of the six-state SARG04 protocol

The SARG04 protocol [96] was developed in an attempt to combat the photon number splitting (PNS) attacks [97,98]. This protocol uses the same four quantum states as the BB84 protocol. Thus, the quantum state transmission and measurements phases are similar to that in the BB84 protocol, and therefore their experimental implementations are similar. The main difference lies in the classical post-processing phase. Furthermore, a secure key can be generated from both a single photon and a two-photon part in SARG04 instead of a single photon part in the BB84 protocol. Therefore, this makes the SARG04 protocol resistant to PNS attacks. Specifically, this is achieved by encoding classical bit into pairs of non-orthogonal states. This is because non-orthogonal states cannot be discriminated deterministically. In the SARG04 protocol, Alice randomly sends to Bob one of the four states either in $|\pm x\rangle$ or $|\pm z\rangle$. Bob then executes measurements on the received signals either on the σ_x or σ_z. In the classical sifting stage, Alice publicly announces one of the four pairs of non-orthogonal states $\mathcal{A}_{w,w'} = \{|wx\rangle, |w'z\rangle\}$, with $w, w' \in \{+, -\}$. The states $|\pm x\rangle$ and $|\pm z\rangle$ code for '0' and '1' respectively. Thus, this kind of encoding presents an effective method that leads to the imperfect discrimination of states by an adversary.

A protocol using N states for encoding can lead to unambiguous discrimination of states only if at least $N-1$ copies of state are in possession of an eavesdropper [99]. For instance, in a four-state SARG04 protocol, Eve can determine with a certain probability the state sent by Alice from the pulses that contain at least three photons. Thus, the protocols utilising more states for encoding are more robust to PNS attacks, as an eavesdropper needs more photons to discriminate the states unambiguously.

The six-state SARG04 protocol was proposed in Refs. [92,99] and can distil a secure key from a source that is capable of emitting at most four photons.

The protocol can be described using the entanglement distillation procedure as follows. Similar to the four-state SARG04 protocol, the basis $\{|0_x\rangle, |1_x\rangle\}, \{|0_z\rangle, |1_z\rangle\}$ are used for preparation and measurements of the qubits. The rotation operations performed by Alice and Bob on their pairs of qubits are defined as: $R = \cos\left(\frac{\pi}{4}\right)1 + \sin\left(\frac{\pi}{4}\right)(|1_x\rangle\langle 0_x| - |0_x\rangle\langle 1_x|)$; $\Gamma_0 = 1$ $\Gamma_1 = \cos(\frac{\pi}{4})1 - i\sin(\frac{\pi}{4})\frac{Z+X}{\sqrt{2}}$ and $\Gamma_2 = \cos(\frac{\pi}{4})1 - i\sin(\frac{\pi}{4})\frac{Z-X}{\sqrt{2}}$.

The protocol starts with Alice preparing the qubit pairs in the following state

$$|\psi\rangle_{AB}^{\otimes\nu} = \left(|0_z\rangle_A|\phi_0\rangle_B^{\otimes\nu} + |1_z\rangle_A|\phi_1\rangle_B^{\otimes\nu}\right)\Big/\sqrt{2}, \tag{1}$$

where $|\phi_i\rangle = \cos(\frac{\pi}{8})|0_x\rangle + (-1)^i\sin(\frac{\pi}{8})|1_x\rangle, i \in (0,1)$. Next Alice applies the rotation operation $\Gamma_l R^k$ and sends the other qubit to Bob. Here, $l \in \{0, 1, 2\}$ and $k \in \{0, 1, 2, 3\}$. Following the receipt of qubits Bob executes the reverse operation $R^{-k'}\Gamma_l^{-1}$ followed by a filtering operation described by Kraus operator $F = \sin\left(\frac{\pi}{8}\right)|0_x\rangle\langle 0_x| + \cos\left(\frac{\pi}{8}\right)|1_x\rangle\langle 1_x|$. Finally, Alice and Bob keeps only the qubits where they used the same rotation operations to obtain a raw key.

3. Security against collective attacks

The asymptotic secure key rate for the six-state SARG04 protocol using one way classical communication is given by Ref. [100].

$$r = 1 - h(e_{\text{bit}}) - \sum_{k=1}^{4} h(e_{\text{ph}}^k|e_{\text{bit}}), \tag{2}$$

where $h(e_{\text{bit}})$ represent the fraction of bits which has leaked to Eve during error correction. The parameter $h(e_{\text{ph}}^k|e_{\text{bit}})$ is the bits which are sacrificed

to remove Eve's knowledge on the final key during privacy amplification for each k-photon contributions. The function $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ represents the Shannon binary entropy function.

Due to symmetry of the protocol and assumptions based on collective attacks by Eve, Alice and Bob's systems are described by a Bell diagonal density matrix, ρ_{AB} which can be expressed in terms of four orthogonal Bell states given by

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \text{ and } |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).$$

If the initial state prepared by Alice is $|\Phi^+\rangle$, after applying projective measurements represented by Pauli operators, X, Y and Z, then the probability of getting only a bit flip error is $\Pr_X = \mathrm{Tr}(\rho_{AB}|\Psi^+\rangle\langle\Psi^+|)$ and the probability of getting only a phase flip error corresponds to $\mathrm{Tr}(\rho_{AB}|\Phi^-\rangle\langle\Phi^-|)$. Finally, the probability of both the phase and bit flip errors is given by $\mathrm{Tr}(\rho_{AB}|\Psi^-\rangle\langle\Psi^-|)$. The bit error rate is therefore given by

$$e_{\mathrm{bit}} = \Pr_X + \Pr_Y,$$

and the phase error rate is expressed as

$$e_{\mathrm{ph}} = \Pr_Z + \Pr_Y.$$

Let $\delta = \Pr_Y$ be the probability that both phase and bit flip errors occur. This probability quantifies the mutual information between phase flip errors and bit flip errors and it can be used to estimate the phase error rate from the bit error rate [92]. The relationship between phase error rate and bit flip error rate for one-photon part is given by

$$e^1_{\mathrm{ph}} = \frac{3}{2}e_{\mathrm{bit}}, \ \delta = \frac{3}{4}e_{\mathrm{bit}}. \tag{3}$$

For two-photon part, the relationship between the error rates is expressed as

$$e^2_{\mathrm{ph}} = \frac{2-\sqrt{2}}{4} + \frac{3}{2\sqrt{2}}e_{\mathrm{bit}}, \ \delta = \frac{4+\sqrt{2}}{8}e_{\mathrm{bit}}. \tag{4}$$

In the case of three-photons emitted by the source, the error rates are given by

$$e^3_{\mathrm{ph}} = \frac{1}{4} + \frac{3}{4}e_{\mathrm{bit}}, \ \frac{1}{2} \le \delta \le \frac{3}{4}e_{\mathrm{bit}}. \tag{5}$$

Finally, for the four-photon part the error rates are expressed as

$$\begin{aligned} e^4_{\mathrm{ph}} &= \min_x\{xe_{\mathrm{bit}} + f(x)\} \ \forall x, \\ \frac{2-2\sqrt{2}}{4}e_{\mathrm{bit}} &\le \delta < \frac{4+\sqrt{2}}{8}e_{\mathrm{bit}} \end{aligned} \tag{6}$$

$$\text{where } f(x) = \frac{6-4x+\sqrt{6-12\sqrt{2}x+16x^2}}{12}.$$

The conditional entropy $h(e^k_{\mathrm{ph}}|e_{\mathrm{bit}})$ quantifies the amount of information that Eve has on the error corrected key. It is given by

$$h(e^k_{\mathrm{ph}}|e_{\mathrm{bit}}) = -\sum p(e_{\mathrm{bit}}, e^k_{\mathrm{ph}})\log_2\left(\frac{p(e_{\mathrm{bit}}, e^k_{\mathrm{ph}})}{p(e_{\mathrm{bit}})}\right) \tag{7}$$

which can be explicitly expressed as

$$\begin{aligned} h(e^k_{\mathrm{ph}}|e_{\mathrm{bit}}) = \ & -(1+\delta-e_{\mathrm{bit}}-e^k_{\mathrm{ph}})\log_2\left(\frac{1+\delta-e_{\mathrm{bit}}-e^k_{\mathrm{ph}}}{1-e_{\mathrm{bit}}}\right) \\ & -(e^k_{\mathrm{ph}}-\delta)\log_2\left(\frac{e^k_{\mathrm{ph}}-\delta}{1-e_{\mathrm{bit}}}\right) - (e_{\mathrm{bit}}-\delta)\log_2\left(\frac{e_{\mathrm{bit}}-\delta}{e_{\mathrm{bit}}}\right) \\ & -\delta\log_2\left(\frac{\delta}{e_{\mathrm{bit}}}\right) \end{aligned} \tag{8}$$

3.1. Bound on the finite secret key rate

We derive the formula for secret key fraction r by considering finite security analysis, where Alice and Bob perform a total number of N measurements. After the parameter estimation and sifting phase, the parties remain with n raw bits in which the final key of length ℓ is distilled through error correction and privacy amplification. The finite key rate for the six-state SARG04 protocol under collective attack sketched along the lines in Ref. [71] is given by

$$\begin{aligned} r_{\mathrm{col}} \ = q\Bigg[& \min_{\sigma_{ABE}\in\Gamma_\xi} H(A|E) - H(A|B) - \frac{1}{n}\log\frac{2}{\epsilon_{\mathrm{EC}}} - \frac{2}{n}\log\frac{1}{\epsilon_{\mathrm{PA}}} \\ & - \left(2\log d + 3\right)\sqrt{\frac{\log\left(\frac{2}{\epsilon}\right)}{n}} \Bigg], \end{aligned} \tag{9}$$

where the first term $q = \frac{n}{N}$ means that n out N signals form the raw key, the value d represents the dimension of the quantum systems used in the protocol. The function, $\min_{\sigma_{ABE}\in\Gamma_\xi} H(A|E)$ is equivalent to summation of conditional entropies, $\sum_{k=1}^{4} h(e^k_{\mathrm{ph}}|e_{\mathrm{bit}})$ from each k-photon contribution. This corresponds to the bits sacrificed to remove Eve's knowledge of the final key during privacy amplification. The function is minimized by states σ_{ABE} in the set Γ_ξ compatible with parameter estimation statistics. The minimization is done mainly to account for fluctuations in the error rates due to finite-size effects. In particular, if the statistics λ_m are obtained by measuring m samples (the number of signals used for parameter estimation) of ρ_{AB} (i.e., the entangled state shared by Alice and Bob) according to a positive operator-valued measurement (POVM) with j possible outcomes then for any state ρ_{AB}

$$\Gamma_\xi := \{\rho_{AB} : \|\lambda_m - \lambda_\infty(\rho_{AB})\|_1 \le \xi\}, \tag{10}$$

where $\lambda_\infty(\rho_{AB})$ denotes the statistics obtained in the limit of infinite measurements, and by the law of large numbers [101]

$$\xi := \frac{1}{2}\sqrt{\frac{2\ln(1/\epsilon_{\mathrm{PE}}) + j\ln(m+1)}{m}}. \tag{11}$$

Specifically, λ corresponds to parameters that are used to measure Eve's information (for instance, error rate e^k_{ph}) and for the error rate, the number of POVM outcomes equals 2 since the outcomes are 'Alice's bit = Bob's bit' and 'Alice's bit ≠ Bob's bit'. Therefore, the upper bound on phase error rate, $e^{k,U}_{\mathrm{ph}}$ compatible with fluctuations is estimated as

$$e^{k,U}_{\mathrm{ph}} = e^k_{\mathrm{ph}} + \xi. \tag{12}$$

In Equation (9), the parameter $H(A|B)$ corresponding to $h(e_{\mathrm{bit}})$ represents the fraction of bits which has leaked to Eve during error correction. Finally, the term ϵ_{PE} is the failure probability of the parameter estimation step and ϵ is the smoothing parameter which gives the accuracy of parameter estimation. The parameter ϵ_{EC} is the probability that error correction procedure fails while ϵ_{PA} corresponds to a bound in which privacy amplification procedure fails to distil a secure key. These probabilities are subject to the following constraint,

$$\epsilon = \epsilon_{\mathrm{PE}} + \epsilon_{\mathrm{EC}} + \epsilon + \epsilon_{\mathrm{PA}}. \tag{13}$$

Here, ϵ is the overall security parameter that corresponds to the most considerable failure probability allowed to distil a secure key from the protocol.

4. Post-selection technique: SARG04 protocol on multi-photons

In this section, we derive the secret key rate of six state SARG04 protocol when implemented with multi-photons i.e., in the case of weak coherent pulses by applying the post selection technique proposed in

Ref. [95]. This is important because it allows us to spell out the bounds for distillation of the secret key in a real scenario. In the composable framework of security, the operation of the six state SARG04 protocol can be represented by a completely positive (CP) map $\mathcal{E}$ that takes the joint state $\rho_{A_1B_1\ldots A_nB_n}$ of the particle pairs (A_i, B_i) as inputs and outputs the state ρ_{SC} of the key. The transcript C represents the communication exchanged over the classical channel. Let presume $\mathcal{S}$ is a map which takes as input the bit strings of the keys $\{S^A, S^B, C\}$ produced by the map $\mathcal{E}$ and output perfect keys $\{S'^A, S'^B, C\}$. In order to find the security, we compare this mapping for six state SARG04 protocol with the ideal mapping $\mathcal{F}$ of a protocol which outputs a perfect key. The ideal CP map $\mathcal{F}$ can be constructed by concatenating the map $\mathcal{S}$ with the map $\mathcal{E}$ i.e., $\mathcal{F} = \mathcal{S}\circ\mathcal{E}$.

Based on the security definition and the post-selection theorem [95], it can be argued that $\mathcal{E}$ is ϵ-secure for any attack by an adversary if

$$\|\mathcal{E}-\mathcal{F}\|_{\diamond} \leq \epsilon. \tag{14}$$

The threshold on ϵ is given by the distance between two CP maps which computed by considering the map $\mathcal{E}$ which as takes input the de Finetti Hilbert Schmidt states and evaluating the deviation of its output key from a perfect key produced by the map $\mathcal{F}$. The de Finetti states correspond to the mixture of states which has product form $\rho_{AB}^{\otimes N}$ prepared from a source that generate identical and independent copies of density operator ρ_{AB}. These particular states are expressed as

$$\tau_{A^NB^N} = \int \rho_{AB}^{\otimes N}\mu(\rho_{AB}), \tag{15}$$

where $\mu(\rho_{AB})$ is the measure on the space of ρ_{AB} brought about by the Hilbert Schmidt metric.

The result obtained from the comparison of the distance between the two permutations invariant CP maps $\mathcal{E}$ and $\mathcal{F}$ under the assumption of collective attacks can be translated into security against the optimal coherent attacks as stated initially in Ref. [102]. By applying Theorem 1 in Ref. [95] to our scenario implies that $\mathcal{E}$ is ϵ secure if

$$\triangle(\mathcal{E},\mathcal{F})_{\rho_{A^NB^N}} \leq (N+1)^{(D^2-1)} \triangle(\mathcal{E},\mathcal{F})_{\tau_{A^NB^N}}, \tag{16}$$

where $\triangle(\mathcal{E},\mathcal{F})\rho_{A^NB^N}$ is the diamond norm distance for the protocol taking as inputs arbitrary states $\rho_{A^NB^N}$. $\triangle(\mathcal{E},\mathcal{F})\tau_{A^NB^N}$ correspond to the diamond-norm distance for the protocol using de Finetti states. The N qubit pairs shared by Alice and Bob span the Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ which has dimension $D = d^2$. The security parameter ϵ_{coh} for optimal coherent attacks is therefore given by

$$\epsilon_{\text{coh}} = \epsilon(N+1)^{(d^4-1)}. \tag{17}$$

In order to compute the finite key rate under coherent attacks, it is essential to remark that Eve holds the purification of Alice and Bob's density operator $\rho_{A^NB^N}$. This can be conveniently described under collective attacks where Eve hold purification of each subsystem ρ_{AB}. The joint state of N subsystems of unknown density operators ρ_{AB} which is correlated with Eve's system $\rho_E \in \{\mathcal{H}_E\}$ is described by de Finetti state

$$\tau'_{A^NB^NE^N} = \int \rho_{ABE}^{\otimes N}\mu(\rho_{ABE}). \tag{18}$$

Since Eve's attack is not restricted, she may also gain more information on the key as a consequence of holding the purification of the joint state of N systems $\tau_{A^NB^N}$. Let $\mathcal{H}_{E'}$ denote the Hilbert space in which the purification of the joint state resides. Then to bound Eve's knowledge on the key considering optimal coherent attacks we have to minimise the conditional entropy $H_{\min}^{\epsilon_{\text{coh}}}(A^N|E^NE')$. The entropy is given by

$$H_{\min}^{\epsilon_{\text{coh}}}(A^N|E^NE') \geq H_{\min}^{\epsilon_{\text{coh}}}(A^N|E^N) - 2H(E'). \tag{19}$$

Due to restriction from the security parameter ϵ_{coh} the dimension of the Hilbert space $\mathcal{H}_{E'}$ is bounded by $(N+1)^{d^4-1}$. This implies that $\mathcal{H}_{E'}$ can hold at most $\log_2(N+1)^{d^4-1}$ bits of information. Consequently, the conditional entropy $H_{\min}^{\epsilon_{\text{coh}}}(A^N|E^NE')$ can be rewritten as

$$H_{\min}^{\epsilon_{\text{coh}}}(A^N|E^NE') \geq H_{\min}^{\epsilon_{\text{coh}}}(A^N|E^N) - 2(d^4-1)\log_2(N+1). \tag{20}$$

The first term in the right hand side of Eqn. (20) is the conditional entropy for the collective attacks hence the key rate for coherent attacks can be formulated as

$$r_{\text{coh}} = r_{\text{col}} - \frac{2(d^4-1)\log_2(N+1)}{N}. \tag{21}$$

4.1. Simulation

Our simulation results demonstrate the performance of the six-state SARG04 protocol under collective attacks and coherent attacks when we apply the post-selection technique. It can be observed that the six-state SARG04 protocol under collective attacks provides better key generation rates when compared to the same protocol under coherent attacks.Based on Fig. 1 the protocol for collective attacks (*i*) requires fewer signals to achieve the positive key rate as compared to the one which uses post-selection technique (*ii*). However, the difference is not that substantial considering that the bounds obtained with the post-selection technique do not impose any restrictions on adversary attacks. As a result, this protocol provides a better alternative for proving the security of realistic QKD implementations.

We also compare our results for the six-state SARG04 protocol with the original four-state SARG04 protocol. This is shown in Fig. 2. We observe that the original SARG04 protocol yields better key rates with fewer signals in contrast to the six-state SARG04 protocol. These key rates are obtained with approximately 2×10^5 signals for the four-state SARG04 protocol when the post-selection technique is applied, whereas the six-state SARG04 protocol requires a minimum of 6×10^7 signals to achieve reasonable secret key rates. Nevertheless, in a realistic QKD scenario with an attenuated laser source, the six-state SARG04 protocol is more robust to the PNS attacks when compared to the original four-state SARG04 protocol. With the four-state SARG04 protocol, a secure key can be distilled from a source that emits at most two photons per pulse, whilst the six-state SARG04 protocol allows the secret key to be obtained even when a source produces pulses that contain four photons.

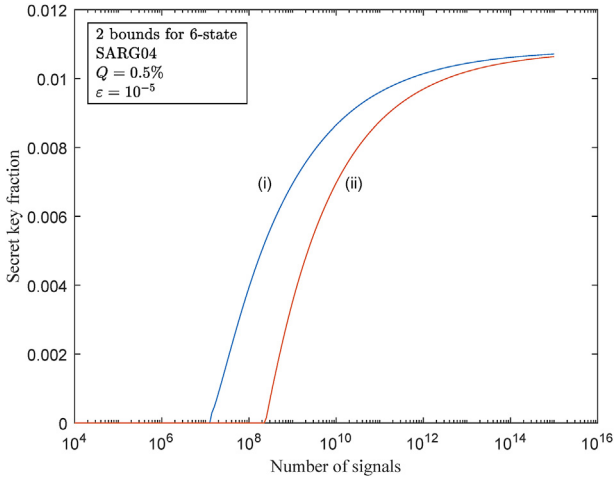

Fig. 1. The plot of secret key fraction versus the number of signals N, for (i) six-state SARG04 protocol under collective attacks with four-photon source, (ii) six-state SARG04 protocol with four-photon source following post-selection technique.

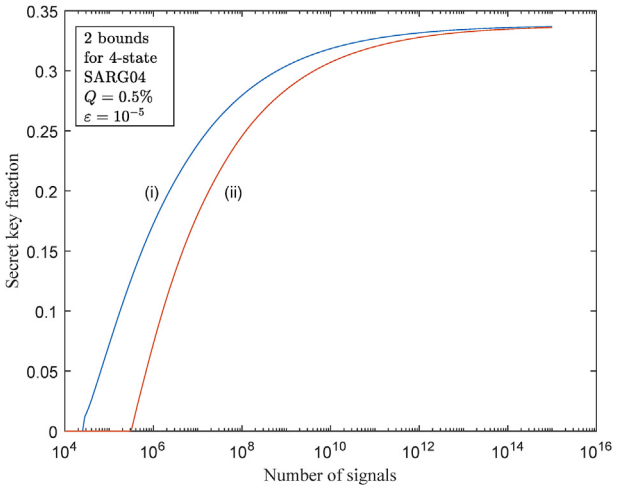

Fig. 2. The plot of secret key fraction versus the number of signals N, for (i) four-state SARG04 protocol under collective attacks with two-photon source, (ii) four-state SARG04 protocol with two-photon source following post-selection technique.

5. Conclusion

We have analysed the security of the six-state SARG04 protocol by applying the post-selection technique in the case of a finite number of resources. The technique translates security bounds restricted to collective attacks to the optimal coherent attacks by an adversary. Most security proofs have been derived based on the assumption of the availability of a perfect source and have been restricted to collective attacks. In contrast, our approach considers a multi-photon source and optimal coherent attacks as posited by the post-selection technique, enabling us to spell out the security bounds under realistic conditions. Furthermore, we compare the security bounds for the four-state protocol and six-state SARG04 protocol under collective attacks to the security bounds obtained after applying the post-selection technique when a finite number of resources are used. Our results demonstrate that the bounds for optimal attack are close to the bound for collective attack for a large number of signals. In fact, the six-state SARG04 protocol proves to be more robust to the PNS attacks when compared to the original four-state SARG04 protocol. When the four-state SARG04 protocol is implemented, a secure key can be distilled from a source that emits at most two photons per pulse, whilst the six-state SARG04 protocol allows the secret key to be obtained even when a source produces pulses that contain four photons. Thus, this demonstrates the power of the post-selection technique in deriving the security bounds for the six-state protocol when finite resources are used. This means that it is possible to distil a secure reasonable secret key from a reasonably good number of signals even when considering the optimal attack by an adversary.

CRediT authorship contribution statement

Comfort Sekga: Methodology, Software, Validation, Writing – original draft. **Mhlambululi Mafu:** Conceptualization, Writing – review & editing, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors would like to acknowledge with thanks the funding from Botswana International University of Science and Technology Research Initiation Grants R00015 and S00100.

References

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74 (1) (2002) 145.
[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 (3) (2009) 1301–1350.
[3] V. Scarani, C. Kurtsiefer, The black paper of quantum cryptography: real implementation problems, Theoret, Comput. Sci. 560 (2014) 27–32.
[4] M. Curty, K. Tamaki, F. Xu, A. Mizutani, C.C.W. Lim, B. Qi, H.-K. Lo, Bridging the gap between theory and practice in quantum cryptography, in: Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology, vol. 9648, International Society for Optics and Photonics, 2015, p. 96480X.
[5] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, J.-W. Pan, Large scale quantum key distribution: challenges and solutions, Opt Express 26 (18) (2018) 24260–24273.
[6] H.-K. Lo, M. Curty, K. Tamaki, Secure quantum key distribution, Nat. Photonics 8 (8) (2014) 595.
[7] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, et al., Using quantum key distribution for cryptographic purposes: a survey, Theoret, Comput. Sci. 560 (2014) 62–81.
[8] E. Diamanti, H.-K. Lo, B. Qi, Z. Yuan, Practical challenges in quantum key distribution, NPJ Quantum Inf 2 (2016) 16025.
[9] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, et al., Measurement-device-independent quantum key distribution over a 404 km optical fiber, Phys. Rev. Lett. 117 (19) (2016) 190501.
[10] M. Lucamarini, Z.L. Yuan, J.F. Dynes, A.J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature 557 (7705) (2018) 400.
[11] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, et al., Secure quantum key distribution over 421 km of optical fiber, Phys. Rev. Lett. 121 (19) (2018) 190502.
[12] C. Sekga, M. Mafu, Reference frame independent twin field quantum key distribution with source flaws, J. Phys. Commun. 5 (4) (2021), 045008.
[13] M. Mohseni, P. Read, H. Neven, S. Boixo, V. Denchev, R. Babbush, A. Fowler, V. Smelyanskiy, J. Martinis, Commercialize quantum technologies in five years, Nat. News 543 (7644) (2017) 171.
[14] A. Mirza, F. Petruccione, Realizing long-term quantum cryptography, J. Opt. Soc. Am. B 27 (6) (2010) A185–A188.
[15] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes, et al., The secoqc quantum key distribution network in vienna, New J. Phys. 11 (7) (2009), 075001.
[16] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, et al., Field test of quantum key distribution in the tokyo qkd network, Opt Express 19 (11) (2011) 10387–10409.
[17] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, et al., Field and long-term demonstration of a wide area quantum key distribution network, Opt Express 22 (18) (2014) 21739–21756.
[18] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, et al., Measurement-device-independent quantum key distribution over untrustful metropolitan network, Phys. Rev. X 6 (1) (2016), 011024.
[19] R. Courtland, China's 2,000-km quantum link is almost complete [news], IEEE Spectr 53 (11) (2016) 11–12.
[20] R. Bedington, J.M. Arrazola, A. Ling, Progress in satellite quantum key distribution, NPJ Quantum Inf 3 (1) (2017) 30.
[21] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, et al., Satellite-to-ground quantum key distribution, Nature 549 (7670) (2017) 43.
[22] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, et al., Satellite-based entanglement distribution over 1200 kilometers, Science 356 (6343) (2017) 1140–1144.
[23] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, et al., Satellite-relayed intercontinental quantum network, Phys. Rev. Lett. 120 (3) (2018), 030501.
[24] C. Bennett, G. Brassard, et al., Quantum cryptography: public key distribution and coin tossing, in: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, 1984. Bangalore, India.
[25] G.S. Vernam, Cipher printing telegraph systems: for secret wire and radio telegraphic communications, J. AIEE 45 (2) (1926) 109–115.
[26] A. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. 67 (6) (1991) 661–663.
[27] C.H. Bennett, G. Brassard, N.D. Mermin, Quantum cryptography without bell's theorem, Phys. Rev. Lett. 68 (5) (1992) 557.
[28] C. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. 68 (21) (1992) 3121–3124.
[29] V. Scarani, A. Acín, G. Ribordy, N. Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations, Phys. Rev. Lett. 92 (5) (2004), 057901.
[30] W.-Y. Hwang, Quantum key distribution with high loss: toward global secure communication, Phys. Rev. Lett. 91 (5) (2003), 057901.

[31] H.-K. Lo, Quantum key distribution with vacua or dim pulses as decoy states, in: International Symposium on Information Theory, 2004. ISIT 2004. Proceedings, IEEE, 2004, p. 137.
[32] H.-K. Lo, X. Ma, K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. 94 (23) (2005) 230504.
[33] T.C. Ralph, Continuous variable quantum cryptography, Phys. Rev. A 61 (1) (1999), 010303.
[34] M. Hillery, Quantum cryptography with squeezed states, Phys. Rev. A 61 (2) (2000), 022309.
[35] N.J. Cerf, M. Levy, G. Van Assche, Quantum distribution of Gaussian keys using squeezed states, Phys. Rev. A 63 (5) (2001), 052311.
[36] F. Grosshans, P. Grangier, Continuous variable quantum cryptography using coherent states, Phys. Rev. Lett. 88 (5) (2002), 057902.
[37] D. Gottesman, J. Preskill, Secure quantum key distribution using squeezed states, in: Quantum Information with Continuous Variables, Springer, 2003, pp. 317–356.
[38] P. Jouguet, S. Kunz-Jacques, A. Leverrier, Long-distance continuous-variable quantum key distribution with a Gaussian modulation, Phys. Rev. A 84 (6) (2011), 062317.
[39] C. Weedbrook, S. Pirandola, R. García-Patrón, N.J. Cerf, T.C. Ralph, J.H. Shapiro, S. Lloyd, Gaussian quantum information,, Rev. Mod. Phys. 84 (2) (2012) 621.
[40] K. Inoue, E. Waks, Y. Yamamoto, Differential phase shift quantum key distribution, Phys. Rev. Lett. 89 (3) (2002), 037902.
[41] D. Stucki, N. Brunner, N. Gisin, V. Scarani, H. Zbinden, Fast and simple one-way quantum key distribution, Appl. Phys. Lett. 87 (19) (2005) 194108.
[42] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf, P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, Nature 421 (6920) (2003) 238.
[43] J. Fiurášek, N.J. Cerf, Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution, Phys. Rev. A 86 (6) (2012), 060302.
[44] F. Laudenbach, C. Pacher, C.-H.F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, H. Hübel, Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations, Adv. Quantum Technol. 1 (1) (2018) 1800011.
[45] D. Mayers, Unconditional security in quantum cryptography, J. ACM 48 (3) (2001) 351–406.
[46] H.-K. Lo, H.F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science 283 (5410) (1999) 2050–2056.
[47] H. Lo, Proof of unconditional security of six-state quatum key distribution scheme, P Soc Photo-opt Ins 1 (2) (2001) 81–94.
[48] P.W. Shor, J. Preskill, Simple proof of security of the bb84 quantum key distribution protocol, Phys. Rev. Lett. 85 (2) (2000) 441.
[49] D. Gottesman, H. Lo, Proof of security of quantum key distribution with two-way classical communications, IEEE Trans. Inf. Theor. 49 (2) (2003) 457–475.
[50] R. Renner, N. Gisin, B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Phys. Rev. A 72 (1) (2005) 12332.
[51] J. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, J. Renes, Unconditional security of a three state quantum key distribution protocol, Phys. Rev. Lett. 94 (4) (2005) 40503.
[52] E. Biham, M. Boyer, P.O. Boykin, T. Mor, V. Roychowdhury, A proof of the security of quantum key distribution, J. Cryptol. 19 (4) (2006) 381–439.
[53] K. Tamaki, H.-K. Lo, Unconditionally secure key distillation from multiphotons, Phys. Rev. A 73 (1) (2006), 010302.
[54] H. Inamori, N. Lütkenhaus, D. Mayers, Unconditional security of practical quantum key distribution, Eur. Phys. J. D 41 (3) (2007) 599–627.
[55] R. Renner, Security of quantum key distribution, Int. J. Quant. Inf. 6 (2008) 1–127, 01.
[56] N.J. Beaudry, T. Moroder, N. Lütkenhaus, Squashing models for optical measurements in quantum communication, Phys. Rev. Lett. 101 (9) (2008), 093601.
[57] T. Tsurumaru, K. Tamaki, Security proof for quantum-key-distribution systems with threshold detectors, Phys. Rev. A 78 (3) (2008), 032302.
[58] M. Mafu, et al., A simple security proof for entanglement-based quantum key distribution, J. Quant. Inf. Sci. 6 (2016) 296, 04.
[59] B. Kraus, N. Gisin, R. Renner, Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication, Phys. Rev. Lett. 95 (8) (2005) 80501.
[60] C. Branciard, N. Gisin, B. Kraus, V. Scarani, Security of two quantum cryptography protocols using the same four qubit states, Phys. Rev. A 72 (3) (2005) 32301.
[61] K. Tamaki, N. Lütkenhaus, M. Koashi, J. Batuwantudawe, Unconditional security of the bennett 1992 quantum-key-distribution scheme with a strong reference pulse, Phys. Rev. A 80 (3) (2009), 032302.
[62] D. Gottesman, H.-K. Lo, N. Lutkenhaus, J. Preskill, Security of quantum key distribution with imperfect devices, in: International Symposium on Information Theory, 2004. ISIT 2004. Proceedings, IEEE, 2004, p. 136.
[63] M. Pereira, M. Curty, K. Tamaki, Quantum Key Distribution with Flawed and Leaky Sources, arXiv Preprint arXiv:1902.02126.
[64] E. Hänggi, Device-independent Quantum Key Distribution, arXiv Preprint arXiv: 1012.3878.
[65] L. Masanes, S. Pironio, A. Acín, Secure device-independent quantum key distribution with causally independent measurement devices, Nat. Commun. 2 (2011) 238.
[66] H.-K. Lo, M. Curty, B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. 108 (13) (2012) 130503.
[67] X. Ma, C.-H.F. Fung, M. Razavi, Statistical fluctuation analysis for measurement-device-independent quantum key distribution, Phys. Rev. A 86 (5) (2012), 052305.
[68] C. Zhou, P. Xu, W.-S. Bao, Y. Wang, Y. Zhang, M.-S. Jiang, H.-W. Li, Finite-key bound for semi-device-independent quantum key distribution, Opt Express 25 (15) (2017) 16971–16980.
[69] T. Meyer, H. Kampermann, M. Kleinmann, D. Bruß, Finite key analysis for symmetric attacks in quantum key distribution, Phys. Rev. A 74 (4) (2006), 042340.
[70] V. Scarani, R. Renner, Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing, Phys. Rev. Lett. 100 (20) (2008) 200501.
[71] L. Sheridan, T. Le, V. Scarani, Finite-key security against coherent attacks in quantum key distribution, New J. Phys. 12 (2010) 123019.
[72] M. Tomamichel, C.C.W. Lim, N. Gisin, R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. 3 (2012) 634.
[73] M. Mafu, K. Garapo, F. Petruccione, Finite-size key in the bennett 1992 quantum-key-distribution protocol for rényi entropies, Phys. Rev. A 88 (6) (2013), 062306.
[74] M. Curty, F. Xu, W. Cui, C.C.W. Lim, K. Tamaki, H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. 5 (2014) 3732.
[75] 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.
[76] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, A. Shields, Efficient decoy-state quantum key distribution with quantified security, Opt Express 21 (21) (2013) 24550–24565.
[77] C.C.W. Lim, M. Curty, N. Walenta, F. Xu, H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A 89 (2) (2014), 022307.
[78] C. Zhou, W.-S. Bao, H.-W. Li, Y. Wang, Y. Li, Z.-Q. Yin, W. Chen, Z.-F. Han, Tight finite-key analysis for passive decoy-state quantum key distribution under general attacks, Phys. Rev. A 89 (5) (2014), 052328.
[79] Y. Wang, W.-S. Bao, C. Zhou, M.-S. Jiang, H.-W. Li, Tight finite-key analysis of a practical decoy-state quantum key distribution with unstable sources, Phys. Rev. A 94 (3) (2016), 032335.
[80] Y. Wang, W.-S. Bao, C. Zhou, M.-S. Jiang, H.-W. Li, Finite-key analysis of practical decoy-state measurement-device-independent quantum key distribution with unstable sources, J. Opt. Soc. Am. B 36 (3) (2019) B83–B91.
[81] A. Leverrier, F. Grosshans, P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, Phys. Rev. A 81 (6) (2010), 062343.
[82] F. Furrer, T. Franz, M. Berta, A. Leverrier, V.B. Scholz, M. Tomamichel, R.F. Werner, Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks, Phys. Rev. Lett. 109 (10) (2012) 100502.
[83] A. Leverrier, R. García-Patrón, R. Renner, N.J. Cerf, Security of continuous-variable quantum key distribution against general attacks, Phys. Rev. Lett. 110 (3) (2013), 030502.
[84] T. Moroder, M. Curty, C.C.W. Lim, H. Zbinden, N. Gisin, et al., Security of distributed-phase-reference quantum key distribution, Phys. Rev. Lett. 109 (26) (2012) 260501.
[85] M. Tomamichel, R. Renner, Uncertainty relation for smooth entropies, Phys. Rev. Lett. 106 (11) (2011) 110506.
[86] P.J. Coles, M. Berta, M. Tomamichel, S. Wehner, Entropic uncertainty relations and their applications, Rev. Mod. Phys. 89 (1) (2017), 015002.
[87] H.-L. Yin, Y. Fu, Z.-B. Chen, Practical quantum digital signature, Phys. Rev. A 93 (3) (2016), 032316.
[88] H.-L. Yin, Y. Fu, H. Liu, Q.-J. Tang, J. Wang, L.-X. You, W.-J. Zhang, S.-J. Chen, Z. Wang, Q. Zhang, et al., Experimental quantum digital signature over 102 km, Phys. Rev. A 95 (3) (2017), 032334.
[89] X. Fang-Xing, W. Shuang, H. Zheng-Fu, G. Guang-Can, Passive decoy state sarg04 quantum-key-distribution with practical photon-number resolving detectors, Chin. Phys. B 19 (10) (2010) 100312.
[90] L. Jing-Bo, F. Xi-Ming, Nonorthogonal decoy-state quantum key distribution, Chin. Phys. Lett. 23 (4) (2006) 775.
[91] H.-P. Hu, J.-D. Wang, Y.-X. Huang, S.-H. Liu, W. Lu, Nonorthogonal decoy-state quantum key distribution based on conditionally prepared down-conversion source, Acta Phys. Sin. 59 (1) (2010) 287–292.
[92] H.-L. Yin, Y. Fu, Y. Mao, Z.-B. Chen, Security of quantum key distribution with multiphoton components, Sci. Rep. 6 (2016) 29482.
[93] Y.-C. Jeong, Y.-S. Kim, Y.-H. Kim, Effects of depolarizing quantum channels on bb84 and sarg04 quantum cryptography protocols, Laser Phys. 21 (8) (2011) 1438–1442.
[94] Y.-C. Jeong, Y.-S. Kim, Y.-H. Kim, An experimental comparison of bb84 and sarg04 quantum key distribution protocols, Laser Phys. Lett. 11 (9) (2014), 095201.
[95] M. Christandl, R. König, R. Renner, Postselection technique for quantum channels with applications to quantum cryptography, Phys. Rev. Lett. 102 (2) (2009) 20504.
[96] 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 (5) (2004) 57901.
[97] G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders, Limitations on practical quantum cryptography, Phys. Rev. Lett. 85 (6) (2000) 1330.
[98] N. Lütkenhaus, M. Jahma, Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack, New J. Phys. 4 (1) (2002) 44.

[99] K. Tamaki, H. Lo, Unconditionally secure key distillation from multi-photons in a single-photon polarization based Quantum Key Distribution, Phys. Rev. A (2006), 010302(R).
[100] C. Fung, K. Tamaki, H. Lo, On the performance of two protocols: SARG04 and BB84, Phys. Rev. A 73 (2006), 012337.
[101] R. Cai, V. Scarani, Finite-key analysis for practical implementations of quantum key distribution, New J. Phys. 11 (2009), 045024.
[102] R. Renner, Symmetry of large physical systems implies independence of subsystems, Nat. Phys. 3 (9) (2007) 645.