Security of biased BB84 quantum key distribution with finite resource*

Zhao Liang-Yuan(赵良圆)[a)b)], Li Hong-Wei(李宏伟)[a)b)c)†], Yin Zhen-Qiang(银振强)[a)b)‡], Chen Wei(陈 巍)[a)b)], You Juan(尤 娟)[a)], and Han Zheng-Fu(韩正甫)[a)b)]

[a)] *Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei* 230026, *China*

[b)] *Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

[c)] *Zhengzhou Information Science and Technology Institute, Zhengzhou* 450004, *China*

(Received 17 April 2014; revised manuscript received 3 July 2014; published online 10 August 2014)

In the original BB84 quantum key distribution protocol, the states are prepared and measured randomly, which lose the unmatched detection results. To improve the sifting efficiency, biased bases selection BB84 protocol is proposed. Meanwhile, a practical quantum key distribution protocol can only transmit a finite number of signals, resulting in keys of finite length. The previous techniques for finite-key analysis focus mainly on the statistical fluctuations of the error rates and yields of the qubits. However, the prior choice probabilities of the two bases also have fluctuations by taking into account the finite-size effect. In this paper, we discuss the security of biased decoy state BB84 protocol with finite resources by considering all of the statistical fluctuations. The results can be directly used in the experimental realizations.

Keywords: biased basis selection, security bound, quantum key distribution

PACS: 03.67.Dd **DOI:** 10.1088/1674-1056/23/10/100304

1. Introduction

Quantum key distribution (QKD) provides a solution to the cryptographic task of distributing a secret key between the legitimate communicating parties usually called Alice and Bob. The first QKD protocol was proposed by Bennett and Brassard in 1984, known as BB84 protocol.[1] This fact was rediscovered in 1991 by Ekert and Artur.[2] The unconditional security of QKD has been first proved in Refs. [3]–[7]. Since then, QKD has grown into a mature field both in theory and practice.[8,9] Several reviews have been devoted to it.[10,11]

In the original BB84 protocol,[1] Alice and Bob exchanged infinite single-photon pulses. For each photon, they made a choice between two polarization bases, i.e. rectilinear basis (Z) and diagonal basis (X), each with an equal probability of $1/2$. In the sifting procedure, Alice and Bob disseminated their basis choices and discarded the unmatched detection results. For unbiased random selection of the bases, half of the detected photons were discarded and the efficiency was at most 50%. To improve the efficiency, Lo *et al.*[12] proposed a biased BB84 scheme. In the biased scheme, Alice and Bob chose the two bases with biased random selection. The secret key generation rate then increased to about 1 in the infinitely long key limit.

However, in practical QKD systems, the perfect single-photon source is beyond the level of current technology. A highly attenuated laser or a weak coherent-state source is used as a substitute, which contains multi-photons and can introduce photon-number-splitting (PNS) attack in the presence of high transmission loss.[6,13] To solve this problem, Hwang[14] proposed the decoy-state idea, where Alice sent pulses with different intensities instead of just one coherent state and randomized the phase of each state. Then Eve could not change the transmittance of a single-photon or multi-photon state freely without being noticed by Alice and Bob. Thus Alice and Bob could obtain a good lower bound on the yield of a single-photon and a good upper bound on the error rate of the single-photon. The security of this method was first studied in detail in Refs. [15] and [16]. To improve the decoy-state method, in Ref. [17], a biased bases selection idea was used and a new decoy-state scheme was proposed.

The other problem of the original BB84 protocol is that in practical QKD systems, Alice and Bob can use only finite resource for limited computational power and storage capacity. Thus only a finite number of pulses can be transmitted, resulting in keys of finite length. The security bounds in Refs. [3]–[7] hold true only if infinitely long keys are produced and processed. The pioneering proofs of security for a finite-length key are shown in Refs. [18] and [19], in which the noncomposable definition of security is used. The first composable security proofs with finite resources are given in Refs. [21] and [22]. The above proofs of security for a finite-length key focus mainly on the statistical fluctuations of the error rate. However, because the quantum channel is lossy, fluctuations

*Project supported by the the National Natural Science Foundation of China (Grant Nos. 61101137, 61201239, 61205118, and 11304397) and the China Postdoctoral Science Foundation. (Grant No. 2013M540514).

†Corresponding author. E-mail: lihw@mail.ustc.edu.cn

‡Corresponding author. E-mail: yinzheqi@mail.ustc.edu.cn

© 2014 Chinese Physical Society and IOP Publishing Ltd

still exist in the prior probabilities of bases selection, which will change the efficiency of the protocol. To improve the finite-key analysis, the statistical fluctuations of the probabilities should be considered.

In this paper, we derive a proof of finite-length key security for the biased BB84 protocol with and without decoy states. The statistical fluctuations of the prior probabilities of bases selection are also considered. The rest of this paper is organized as follows. In Section 2, we review the security proof of the original BB84 scheme combined with Shor and Preskill's work. In Section 3, we derive a proof of security for the biased BB84 with a finite resource. The security of biased decoy-state BB84 with a finite resource will be analyzed in Section 4. Finally, we draw some conclusions in Section 5.

2. Security proof of BB84 with balanced basis choice

Before introducing the method to analyze the security of biased BB84 protocol with finite resources, the security of BB84 with balanced basis choice is analyzed in this section.[20] In the original BB84 protocol, the bases are selected uniformly, i.e. each with a probability of $1/2$.

Following the technique obtained by Shor and Preskill,[4] security of prepare-and-measure QKD protocol is identical with the security of entanglement-based QKD protocol. Alice prepares a maximally entangled state $|\phi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$, and performs the Hadamard transform randomly to the second particle of the state. She then sends it to Bob. If Bob receives the qubit, it is announced and the Hadamard operation is used randomly. It is believed that Pauli channels are the universal noisy channels in the analysis of security. Considering Eve's attack in the Pauli channel, the quantum state among Alice, Bob and Eve can be described as

$$\sum_{u,v,i,j} \sqrt{P_{uv}Q_{ij}}(I_A \otimes H^i_{B_1}\sigma^u_{xE_1}\sigma^v_{zE_2}H^j_{A_1}) \times |\phi_1\rangle|u\rangle_{E_1}|v\rangle_{E_2}|i\rangle_{B_1}|j\rangle_{A_1}, \tag{1}$$

where A_1 is part of Alice's system and B_1 is part of Bob's system; $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)$ is the perfect Hadamard operator, which can turn Z basis into X basis and *vice versa* in practical QKD system; $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$ is the Pauli matrix σ_x operator, which means bit-flip error E_1 caused by Eve; $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ is the Pauli matrix σ_z operator, which means phase error E_2 caused by Eve. Then $\sigma_x\sigma_z$ operator means bit-flip phase error. $P_{uv}, u, v \in \{0,1\}$ is the probability that Eve introduces $\sigma^u_x\sigma^v_z$ operator, and satisfies

$$\sum_{u,v} P_{uv} = 1. \tag{2}$$

$Q_{ij}, i, j \in \{0,1\}$ is the probability that Alice performs H^i transform and Bob performs H^j transform simultaneously. In the case of balanced basis choice, $Q_{ij} = 1/4$. After comparing the bases they used, the case of $i \neq j$ is discarded. Computing the trace of the quantum system of particles A_1, B_1 and Eve, we can obtain the following equation:

$$\begin{aligned}\rho_{AB} = \sum_{u,v} P_{uv}\Big(&\frac{1}{2}I_A \otimes \sigma^u_{xE_1}\sigma^v_{zE_2}|\phi_1\rangle\langle\phi_1|\sigma^v_{zE_2}\sigma^u_{xE_1} \otimes I_A \\ &+ \frac{1}{2}I_A \otimes H_{B_1}\sigma^u_{xE_1}\sigma^v_{zE_2}H_{A_1}|\phi_1\rangle \\ &\times \langle\phi_1|H_{A_1}\sigma^v_{zE_2}\sigma^u_{xE_1}H_{B_1}\Big) \otimes I_A. \end{aligned} \tag{3}$$

Bit-flip errors and phase errors exist in the Pauli channel, and all of the errors are considered to be introduced by Eve in the security analysis. The initially shared maximally entangled state turns into one of the following four Bell states after transmitting through the quantum channel:

$$\begin{aligned}|\phi_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}),\\ |\phi_2\rangle &= \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB}),\\ |\phi_3\rangle &= \frac{1}{\sqrt{2}}(|00\rangle_{AB} - |11\rangle_{AB}),\\ |\phi_4\rangle &= \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}).\end{aligned} \tag{4}$$

If the previous state is still the Bell state $|\phi_1\rangle$, then there is no error in the process. However, once it becomes $|\phi_2\rangle$, $|\phi_3\rangle$ or $|\phi_4\rangle$, Alice and Bob think that Eve carries a bit-flip error, phase error or bit-flip phase error into the transmission correspondingly. By doing so, the bit error rate and phase error rate are given as

$$\begin{aligned}e_{\text{bit}} &= \langle\phi_2|\rho_{AB}|\phi_2\rangle + \langle\phi_4|\rho_{AB}|\phi_4\rangle,\\ e_{\text{phase}} &= \langle\phi_3|\rho_{AB}|\phi_3\rangle + \langle\phi_4|\rho_{AB}|\phi_4\rangle.\end{aligned} \tag{5}$$

In order to correct the error and distill the maximal entangled state, Alice and Bob must clear the e_{bit} and e_{phase}. In the practical QKD protocol, we can use a string of sample bits from the raw key to estimate e_{bit}. However, it is difficult to estimate e_{phase} which has no classical counterpart. Fortunately, in the balanced basis choice as we discuss here, from Eqs. (3)–(5), the bit-flip error minus phase error rate is

$$e_{\text{bit}} - e_{\text{phase}} = \langle\phi_2|\rho_{AB}|\phi_2\rangle - \langle\phi_3|\rho_{AB}|\phi_3\rangle = 0. \tag{6}$$

In this case, the phase error rate can be estimated by the bit error rate accurately in the balanced basis choice. Secret key generation rate is given as

$$R = \frac{1}{2}[1 - h(e_{\text{phase}}) - h(e_{\text{bit}})] = \frac{1}{2}[1 - 2h(e_{\text{bit}})], \tag{7}$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function and $1/2$ is the efficiency of original BB84. The maximal bit error rate is 11% given by Eq. (7).

3. Security proof of biased BB84 with finite resource

In the biased BB84 protocol,[12] the two bases are chosen with different probabilities. Consequently, Alice and Bob are now much more likely to use the same basis. Then the fraction of discarded photons is greatly reduced, thereby enhancing the efficiency greatly.

Now, let N be a large integer. Alice sends a sequence of N single-photons to Bob. For each single-photon, Alice makes a choice between the two bases, rectilinear Z and diagonal X, with probabilities p_a and $1-p_a$, respectively. Bob measures the polarization of each received single-photon independently along the Z and X bases with probabilities p_b and $1-p_b$, respectively. Note that $1/2 \leq p_a, p_b < 1$ and the values are made public.

In order to prove the security of biased BB84, we use a refined analysis of the sifted key, which is first put forward by Lo *et al.*[12] to generalize Shor and Preskill's[4] proof of security of BB84 to the biased scheme. The main idea is that Alice and Bob divide the sifted key into two subsets according to the basis employed, and estimate an error rate for each subset.

According to the relationship between the error rate in biased BB84 and that in the entanglement purification protocol (EPP), the phase error rate in the Z basis is the bit-flip error rate in the X basis and *vice versa*, i.e.

$$e_{\mathrm{p}}^{Z} = e_b^{X}, \quad e_{\mathrm{p}}^{X} = e_b^{Z}, \tag{8}$$

where e_b^Z and e_b^X are the bit-flip error rates of the Z basis and the X basis respectively, and e_{p}^Z and e_{p}^X are the phase error rates of the Z basis and the X basis, respectively.

Then, if a key is generated by making a fraction, that is, $p_a p_b/p_a p_b+(1-p_a)(1-p_b)$, of the measurements along the Z basis and a fraction, $(1-p_a)(1-p_b)/p_a p_b+(1-p_a)(1-p_b)$, along the X basis, then the bit-flip and phase error rates of the sifted key are given by weighted averages of the bit error rates of the two bases as follows:

$$\begin{aligned} e_b &= \frac{p_a p_b}{p_a p_b+(1-p_a)(1-p_b)} e_b^Z \\ &\quad + \frac{(1-p_a)(1-p_b)}{p_a p_b+(1-p_a)(1-p_b)} e_b^X, \\ e_{\mathrm{p}} &= \frac{p_a p_b}{p_a p_b+(1-p_a)(1-p_b)} e_{\mathrm{p}}^Z \\ &\quad + \frac{(1-p_a)(1-p_b)}{p_a p_b+(1-p_a)(1-p_b)} e_{\mathrm{p}}^X \\ &= \frac{p_a p_b}{p_a p_b+(1-p_a)(1-p_b)} e_b^X \\ &\quad + \frac{(1-p_a)(1-p_b)}{p_a p_b+(1-p_a)(1-p_b)} e_b^Z, \end{aligned} \tag{9}$$

where e_b and e_{p} are the bit-flip and phase error rates of the sifted key.

In a refined data analysis, Alice and Bob separate the sifted key from the two bases into two subsets and compute the error rates in the two subsets individually. This method gives them individual estimates on the bit error rates, e_b^Z and e_b^X, which demands that both error rates should be sufficiently small, for example,

$$0 \leq e_b^Z, \quad e_b^X < e_{\max} - \delta_e, \tag{10}$$

where δ_e is the small positive parameter. From the work of Shor and Preskill,[4] $e_{\max}$ is about 11%.

From Eq. (9) we can find that if equation (10) is satisfied, we have

$$0 \leq e_b, \quad e_{\mathrm{p}} < 11\%, \tag{11}$$

which says that both bit-flip and phase error rates of the EPP are small enough to allow the CSS code to be corrected. It means that Shor and Preskill's argument can be carried out directly to establish the security of the biased BB84 protocol, if Alice and Bob use a refined data analysis.

Here, following the refined data analysis proposed above, we give the secret key generation rate with the asymptotic limit as

$$\begin{aligned} R &= p_a p_b[1-h(e_b^Z)-h(e_{\mathrm{p}}^Z)] \\ &\quad + (1-p_a)(1-p_b)[1-h(e_b^X)-h(e_{\mathrm{p}}^X)] \\ &= [p_a p_b + (1-p_a)(1-p_b)] \\ &\quad \times [1-h(e_b^Z)-h(e_b^X)], \end{aligned} \tag{12}$$

in which equation (8) has been used. The explanation of this formula is as follows. If Alice and Bob want to distill final keys from Z basis, both the bit error rate and the phase error rate belong to Z basis. Similarly, if they want to distill the final keys from X basis, both the bit error rate and the phase error rate belong to X basis. The $p_a p_b$ and $(1-p_a)(1-p_b)$ are the efficiencies of the two bases, and $p_a p_b + (1-p_a)(1-p_b)$ is the efficiency of the protocol.

Also Alice and Bob can obtain the secret key generation rate directly by

$$R = [p_a p_b + (1-p_a)(1-p_b)][1-h(e_{\mathrm{p}})-h(e_b)] \tag{13}$$

with using Eq. (9). Comparing Eq. (12) with Eq. (13), we find that the difference between the two formulas is due to the fact that equation (12) needs post-processing twice and equation (13) only once: the rate of Eq. (12) is in principle higher because the bound on Eve's information is tighter. The strict mathematic proof is shown in Appendix A, in which the convexity of the binary entropy function $h(x)$ has been used.

3.1. Secret key generation rate with finite resource

In real QKD implementations, however, the number of emitted pulses is finite, resulting in keys of finite length. For this reason, statistical fluctuations exist for the error rates of the two bases. For p_a and p_b, statistical fluctuations also exist, i.e. the bias in the probabilities, even though Alice and Bob know p_a and p_b exactly at the beginning of the protocol. Like the security analysis of the QKD protocol with a finite resource,[22–25] for analyzing the security of biased BB84, the law of large numbers will be given in the following.[26]

If the statistics λ_m are obtained by measurements of m samples of σ according to a positive operator valued measure (POVM) with d outcomes, then for any $\varepsilon' > 0$, σ is contained in the set

$$\left\{\sigma : \|\lambda_m - \lambda_\infty\| \le \xi(m,\varepsilon'), \quad \text{where,} \quad \xi(m,\varepsilon') = \sqrt{\frac{2[\ln(1/\varepsilon') + d\ln(m+1)]}{m}}\right\}, \tag{14}$$

where λ_∞ denotes the probability distribution defined by the POVM applied to σ.

For analyzing the security of biased BB84 with finite resources, statistical fluctuations of p_a, $1-p_a$, p_b, $1-p_b$, e_b^Z, e_b^X, $e_{\rm p}^Z$, and $e_{\rm p}^X$ should be considered.

Single-photons encoded on Alice's side can be divided into Z-based ones and X-based ones, which means that the kind of single-photon transmitted by Alice has two outcomes. The upper and the lower bounds of the probabilities of the Z basis and X basis used by Alice in the finite resource case can be given as

$$\begin{aligned} p_a^{\rm U} &= \min\left(p_a + \frac{1}{2}\xi(N,\varepsilon_1), 1\right), \\ p_a^{\rm L} &= \max\left(p_a - \frac{1}{2}\xi(N,\varepsilon_1), 0\right), \end{aligned} \tag{15}$$

$$\begin{aligned} (1-p_a)^{\rm U} &= \min\left((1-p_a) + \frac{1}{2}\xi(N,\varepsilon_2), 1\right), \\ (1-p_a)^{\rm L} &= \max\left((1-p_a) - \frac{1}{2}\xi(N,\varepsilon_2), 0\right), \end{aligned} \tag{16}$$

where $d = 2$, N is the number of single-photon signals emitted by Alice, ε_1 and ε_2 are the security parameters of the statistical fluctuations of p_a and $1-p_a$, respectively.

Meanwhile, the upper and lower bounds of the probabilities of the two bases used by Bob in the finite resource case can be given as

$$\begin{aligned} p_b^{\rm U} &= \min\left(p_b + \frac{1}{2}\xi(N,\varepsilon_3), 1\right), \\ p_b^{\rm L} &= \max\left(p_b - \frac{1}{2}\xi(N,\varepsilon_3), 0\right), \end{aligned} \tag{17}$$

$$(1-p_b)^{\rm U} = \min\left((1-p_b) + \frac{1}{2}\xi(N,\varepsilon_4), 1\right),$$

$$(1-p_b)^{\rm L} = \max\left((1-p_b) - \frac{1}{2}\xi(N,\varepsilon_4), 0\right), \tag{18}$$

where $d = 2$, ε_3 and ε_4 are the security parameters of the statistical fluctuations of p_b and $1-p_b$, respectively.

Similarly, the outcomes of measurements by Bob contain the right and wrong ones in the Z and X bases, respectively. Then the upper and the lower bounds of the error rates of qubits in the finite resource case can be given as

$$\begin{aligned} e_b^{\rm UZ} &= \min\left(e_b^Z + \frac{1}{2}\xi(Np_a^{\rm L}p_b^{\rm L}, \varepsilon_5), 0.5\right), \\ e_b^{\rm LZ} &= \max\left(e_b^Z - \frac{1}{2}\xi(Np_a^{\rm L}p_b^{\rm L}, \varepsilon_5), 0\right), \end{aligned} \tag{19}$$

$$\begin{aligned} e_b^{\rm UX} &= \min\left(e_b^X + \frac{1}{2}\xi(N(1-P_a)^{\rm L}(1-p_b)^{\rm L}, \varepsilon_6), 0.5\right), \\ e_b^{\rm LX} &= \max\left(e_b^X - \frac{1}{2}\xi(N(1-P_a)^{\rm L}(1-p_b)^{\rm L}, \varepsilon_6), 0\right), \end{aligned} \tag{20}$$

where $d = 2$; N is the number of single-photon signals emitted by Alice; ε_5 and ε_6 are the security parameters of the statistical fluctuations of e_b^Z and e_b^X, respectively.

As for error rates with asymptotic limit,

$$e_{\rm p}^Z = e_b^X, \quad e_{\rm p}^X = e_b^Z. \tag{21}$$

exists.

Then, in the finite resource case where statistical fluctuations should be taken into account,[27,28] we have

$$e_{\rm p}^Z \approx e_b^X, \quad e_{\rm p}^X \approx e_b^Z. \tag{22}$$

Given e_b^X, we can have upper bound $e_{\rm p}^Z$ by randomly sampling argument. The details of proof are shown in the method of Ref. [17]. Then, the secret key generation rate with the finite resources is

$$\begin{aligned} R \ge\ & p_a^{\rm L}p_b^{\rm L}[1 - h(e_b^{\rm UZ}) - h(e_{\rm p}^{\rm UZ})] \\ & + (1-p_a)^{\rm L}(1-p_b)^{\rm L}[1 - h(e_b^{\rm UX}) - h(e_{\rm p}^{\rm UX})] \\ =\ & p_a^{\rm L}p_b^{\rm L}[1 - h(e_b^{\rm UZ}) - h(e_b^{\rm UX})] \\ & + (1-p_a)^{\rm L}(1-p_b)^{\rm L}[1 - h(e_b^{\rm UX}) - h(e_b^{\rm UZ})] \\ =\ & [p_a^{\rm L}p_b^{\rm L} + (1-p_a)^{\rm L}(1-p_b)^{\rm L}] \\ & \times [(1 - h(e_b^{\rm UZ}) - h(e_b^{\rm UX})]. \end{aligned} \tag{23}$$

Correspondingly, the secret parameter of the secret key is

$$\varepsilon = \varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 + \varepsilon_5 + \varepsilon_6. \tag{24}$$

3.2. Numerical simulation

In this section, we give numerical simulation results based on the analysis result in Subsection 3.1. All of the security parameters in this section are fixed to be 2^{-25}, then the secret parameter of the secret key can be given as

$$\varepsilon \le 2^{-22}. \tag{25}$$

For simplicity and without loss of generality, we assume that $p_a = p_b \equiv p$. For a prior estimation of our bounds, we have supposed as usual that parameter estimation should yield $e_b^Z = e_b^X \equiv Q$. The relationship between the optimal p and the number of emitted single-photon pulses is shown in Fig. 1. The corresponding secret key generation rate is shown in Fig. 2. For each number of single-photon pulses, we optimize the parameter p.

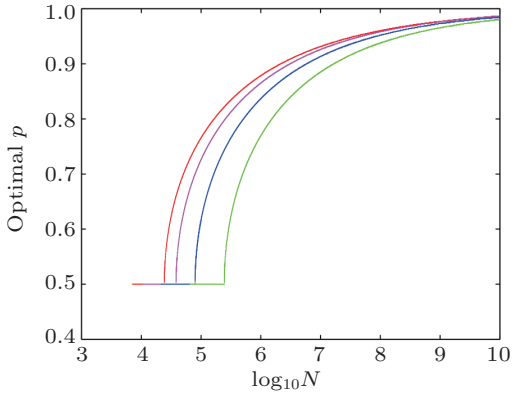


Fig. 1. (color online) Relationships between optimal p and the logarithm of the number of the emitted single-photon pulses, $\log_{10}N$, for the bit error rates of 0.5%, 2.5%, 5%, and 7.5% (from left to right).

From Fig. 1 it follows that when the number of emitted pulses is small, the value of optimal p will be kept at 0.5, which is the original BB84 scheme. Then the value of optimal p increases with the increasing number. In the limit of large numbers of photon transfer, the optimal $p \to 1^-$.

From Fig. 2, we can assess the influence of finite-key size on the secret key generation rate. We can see a progressive increase of the minimal number of the emitted single-photon pulses when the secret key generation rate becomes positive by increasing the bit error rate. We find that the minimal number of the emitted single-photon pulses is $N \sim 10^4$.

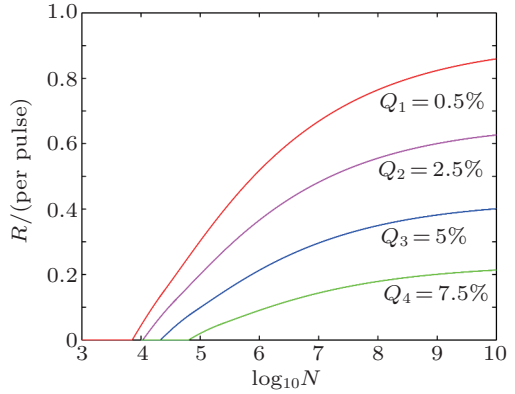


Fig. 2. (color online) Variarions of the secret key rate R with the logarithm of the number of the emitted single-photon pulses $\log_{10}N$ for different error rates, for the biased BB84 with finite resources. For each number of single-photon pulses, we optimize the parameter p.

4. Security proof of biased decoy-state BB84 with a finite resource

4.1. Model

To analyze the security of the biased BB84 decoy-state protocol, we follow the widely used decoy-state scheme, vacuum+weak decoy-state model established in Refs. [15] and [29] and also shown in Ref. [17]. The weak coherent state source is equivalent to a photon-number channel model and its photon number follows a Poisson distribution:

$$P(n) = \frac{\mu^n}{n!}\mathrm{e}^{-\mu}. \tag{26}$$

For an optical-fiber-based QKD system, the overall transmission and detection efficiency η between Alice and Bob is given as

$$\eta = t_{AB}\eta_{\mathrm{Bob}}, \tag{27}$$

where $t_{AB} = 10^{-\alpha l/10}$ is the l-length (km) channel transmittance between Alice and Bob; α is the loss coefficient in the quantum channel measured in dB/km; η_{Bob} denotes the transmittance on Bob's side, including the internal transmittance of the optical component and detector efficiency.

Denote Y_i as the yield of an i-photon state, and Y_0 as the background count rate, then in a normal channel when there is no intervention from Eve, Y_i will be given as

$$Y_i = 1 - (1 - Y_0)(1 - \eta)^i. \tag{28}$$

The gain of i-photon states Q_i is given as

$$Q_i = Y_i\frac{\mu^i}{i!}\mathrm{e}^{-\mu}. \tag{29}$$

The overall gain which means the probability for Bob to obtain a detection event in one pulse with intensity μ is

$$Q_\mu = \sum_{i=0}^{\infty} Q_i = \sum_{i=0}^{\infty} Y_i\frac{\mu^i}{i!}\mathrm{e}^{-\mu}. \tag{30}$$

The error rate of i-photon states e_i is given as

$$e_iY_i = e_0Y_0 + e_{\mathrm{d}}[1 - (1 - \eta)^i](1 - Y_0), \tag{31}$$

where e_{d} is the probability that a photon hits the erroneous detector and $e_0 = 1/2$. The overall quantum bit error rate (QBER) is given as

$$E_\mu Q_\mu = \sum_{i=0}^{\infty} e_iY_i\frac{\mu^i}{i!}\mathrm{e}^{-\mu}. \tag{32}$$

Without Eve changing Y_i and e_i, the gain and QBER are given as

$$\begin{aligned} Q_\mu &= 1 - \mathrm{e}^{-\eta\mu}(1 - Y_0), \\ E_\mu Q_\mu &= e_0Y_0 + e_d(1 - \mathrm{e}^{-\eta\mu})(1 - Y_0). \end{aligned} \tag{33}$$

4.2. Security proof of biased decoy-state BB84

Assume that Alice chooses the two bases Z and X with probabilities p_a and $1-p_a$ respectively, for signal states and decoy states. Bob measures the polarizations of each of the received pulses along the Z and X bases with probabilities p_b and $1-p_b$ respectively, without separating the signal states from the decoy states. Combining the model established above with the refined data analysis in Section 3 and the GLLP (Gottesman, Lo, Lütkenhaus and Preskill) formula,[6] the secret key generation rate in the asymptotic limit of infinitely long keys is

$$\begin{aligned} R \geq & -[p_a p_b + (1-p_a)(1-p_b)]Q_\mu f_\mu h(E_\mu) \\ & + p_a p_b Q_1^Z [1-h(e_{1p}^Z)] \\ & + (1-p_a)(1-p_b)Q_1^X [1-h(e_{1p}^X)] \\ = & -[p_a p_b + (1-p_a)(1-p_b)]Q_\mu f_\mu h(E_\mu) \\ & + p_a p_b Q_1^Z [1-h(e_{1b}^X)] \\ & + (1-p_a)(1-p_b)Q_1^X [1-h(e_{1b}^Z)], \end{aligned} \tag{34}$$

where μ is the intensity of the signal state, f_μ is the error correction inefficiency, Q_1^Z and Q_1^X are the gains of Z-based single-photon states and X-based single-photon states, respectively.

Since the single-photon state is basis-independent, the yields of single-photon states in different bases are equal to

$$Y_1^Z = Y_1^X = Y_1, \tag{35}$$

where Y_1^Z and Y_1^X are the yields of Z-based single-photon states and X-based single-photon states, respectively.

Then there is

$$Q_1^Z = Q_1^X = Q_1. \tag{36}$$

The secret key generation rate can be turned into

$$\begin{aligned} R \geq & -[p_a p_b + (1-p_a)(1-p_b)]Q_\mu f_\mu h(E_\mu) \\ & + p_a p_b Q_1^Z [1-h(e_{1p}^Z)] \\ & + (1-p_a)(1-p_b)Q_1^X [1-h(e_{1p}^X)] \\ = & -[p_a p_b + (1-p_a)(1-p_b)]Q_\mu f_\mu h(E_\mu) \\ & + Q_1\{p_a p_b [1-h(e_{1b}^X)] \\ & + (1-p_a)(1-p_b)[1-h(e_{1b}^Z)]\}. \end{aligned} \tag{37}$$

4.3. Secret key generation rate with a finite resource

For analyzing the security of biased decoy-state BB84 in the face of finite resources, statistical fluctuations of p_a, $1-p_a$, p_b, $1-p_b$, Y_1, P_1, e_{1b}^Z, e_{1b}^X, Q_μ, and E_μ should be considered. Photon pulses transmitted on Alice's side can be divided into single-photon pulses or multiple-photon pulses, which means that the proportion of the photon state transmitted by Alice has two outcomes, then the upper and the lower bounds of the proportion of single-photon states in the finite resource case can be given as

$$\begin{aligned} P_{1\mu}^{\mathrm{U}} &= \min(\mu \mathrm{e}^{-\mu} + \frac{1}{2}\xi(N_\mu, \varepsilon_7), 1), \\ P_{1\mu}^{\mathrm{L}} &= \max(\mu \mathrm{e}^{-\mu} - \frac{1}{2}\xi(N_\mu, \varepsilon_7), 0), \end{aligned} \tag{38}$$

where $d=2$, N_μ is the number of the exchanged signal states on Alice's side, and ε_7 is the security parameter of the statistical fluctuation of $P_{1\mu}$.

As for signal states, the yield on Bob's side contains the yield of single-photon states and the yield of multiple-photon states. Meanwhile, the single-photon yield contains the right case and the wrong case for each basis. Like the security analysis of the statistical fluctuation of $P_{1\mu}$, the upper and the lower bounds of the yield of single-photon states in the finite resource case can be given as

$$\begin{aligned} Y_1^{\mathrm{U}} &= \min\left(Y_1 + \frac{1}{2}\xi(N_\mu P_{1\mu}^{\mathrm{L}}, \varepsilon_8), 1\right), \\ Y_1^{\mathrm{L}} &= \max\left(Y_1 - \frac{1}{2}\xi(N_\mu P_{1\mu}^{\mathrm{L}}, \varepsilon_8), 0\right), \end{aligned} \tag{39}$$

and the upper and the lower bounds of error rates of single-photon states for each basis in the finite resource case can be given as

$$\begin{aligned} e_{1b}^{\mathrm{UZ}} &= \min\left(e_{1b}^Z + \frac{1}{2}\xi(N_\mu P_{1\mu}^{\mathrm{L}} Y_1^{\mathrm{L}} p_a^{\mathrm{L}} p_b^{\mathrm{L}}, \varepsilon_9), 0.5\right), \\ e_{1b}^{\mathrm{LZ}} &= \max\left(e_{1b}^Z - \frac{1}{2}\xi(N_\mu P_{1\mu}^{\mathrm{L}} Y_1^{\mathrm{L}} p_a^{\mathrm{L}} p_b^{\mathrm{L}}, \varepsilon_9), 0\right), \end{aligned} \tag{40}$$

$$\begin{aligned} e_{1b}^{\mathrm{UX}} &= \min\Big(e_{1b}^X + \frac{1}{2}\xi(N_\mu P_{1\mu}^{\mathrm{L}} Y_1^{\mathrm{L}} (1-p_a)^{\mathrm{L}} \\ &\quad \times (1-p_b)^{\mathrm{L}}, \varepsilon_{10}), 0.5\Big), \\ e_{1b}^{\mathrm{LX}} &= \max\Big(e_{1b}^X - \frac{1}{2}\xi(N_\mu P_{1\mu}^{\mathrm{L}} Y_1^{\mathrm{L}} (1-p_a)^{\mathrm{L}} \\ &\quad \times (1-p_b)^{\mathrm{L}}, \varepsilon_{10}), 0\Big), \end{aligned} \tag{41}$$

where $d=2$; ε_8, ε_9, and ε_{10} are the security parameters of the statistical fluctuations of Y_1^{U}, e_{1b}^Z, and e_{1b}^X, respectively. From Eqs. (38) and (39) we can obtain the upper and the lower bounds of the gain of the single-photon component of the signal states as

$$Q_1^{\mathrm{U}} = Y_1^{\mathrm{U}} P_1^{\mathrm{U}}, \quad Q_1^{\mathrm{L}} = Y_1^{\mathrm{L}} P_1^{\mathrm{L}}. \tag{42}$$

Likewise, the upper and the lower bounds of Q_μ and E_μ in the finite resource case can be given as

$$\begin{aligned} Q_\mu^{\mathrm{U}} &= \min\left(Q_\mu + \frac{1}{2}\xi(N_\mu, \varepsilon_{11}), 1\right), \\ Q_\mu^{\mathrm{L}} &= \max\left(Q_\mu - \frac{1}{2}\xi(N_\mu, \varepsilon_{11}), 0\right), \\ E_\mu^{\mathrm{U}} &= \min\left(E_\mu + \frac{1}{2}\xi(N_\mu Q_\mu^{\mathrm{L}}, \varepsilon_{12}), 0.5\right), \end{aligned} \tag{43}$$

$$E_\mu^{\mathrm{L}} = \max\left(E_\mu - \frac{1}{2}\xi(N_\mu Q_\mu^{\mathrm{L}}, \varepsilon_{12}), 0\right), \tag{44}$$

where $d = 2$, ε_{11} and ε_{12} are the security parameters of the statistical fluctuations of Q_μ, E_μ, respectively.

Equations (15)–(18), (38)–(44) together with Eq. (37) yield the secret key generation rate of biased decoy-state BB84 with finite resource

$$\begin{aligned} R \geq & -[p_a^{\mathrm{L}} p_b^{\mathrm{L}} + (1-p_a)^{\mathrm{L}}(1-p_b)^{\mathrm{L}}] Q_\mu^{\mathrm{L}} f_\mu h(E_\mu^{\mathrm{U}}) \\ & + Q_1^{\mathrm{L}}\{p_a^{\mathrm{L}} p_b^{\mathrm{L}}[1-h(e_{1b}^{UX})] \\ & + (1-p_a)^{\mathrm{L}}(1-p_b)^{\mathrm{L}}[1-h(e_{1b}^{\mathrm{UZ}})]\}. \end{aligned} \tag{45}$$

Correspondingly, the secret parameter of the secure key is

$$\begin{aligned} \varepsilon = & \varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 + \varepsilon_7 + \varepsilon_8 \\ & + \varepsilon_9 + \varepsilon_{10} + \varepsilon_{11} + \varepsilon_{12}. \end{aligned} \tag{46}$$

4.4. Numerical simulation

In this section, we give numerical simulation results based on the analysis result in Subsection 4.3. All the security parameters in this section are fixed to be 2^{-25}, then the secret parameter of the secure key can be given as

$$\varepsilon \leq 2^{-21}. \tag{47}$$

The parameters for simulation are cited from the experiment Gobby, Yuan and Shields (GYS) experiment[30] and shown in Table 1. We choose the average photon number $\mu = 0.48$ and the $f_\mu = 1.22$.[29] For simplicity and without loss of generality, we assume that $p_a = p_b = p$. For a prior estimation of our bounds, we have supposed as usual that parameter estimation should yield $e_{1b}^Z = e_{1b}^X = e_1$.

Table 1. Key parameters of GYS experiment for simulation.

α/(dB/km)	e_{Det}/(%)	Y_0	η_{Bob}
0.21	3.3	1.7×10^{-6}	0.045

The relationship between the optimal probability and the transmission distance is shown in Fig. 3. The corresponding secret key generation rate is shown in Fig. 4. For each transmission distance, we optimize the parameter p. From Fig. 3 we can see that the value of optimal probability p will decrease as transmission distance increases. At a smaller transmission loss, the optimal probability p approaches 1 when the finite key effect can be neglected. However, if the transmitted signals are lower, the optimal probability p decreases. At a larger transmission loss, no matter how many signals are transmitted, the optimal probability p is close to $1/2$, which approaches to the standard BB84 with the vacuum + weak decoy–state scheme. This is because the constraint on the biased parameter p is that there should be enough photons for performing the parameter estimation for both bases. Then Alice and Bob need large values of p and $1-p$ to estimate the error rates for error correction and privacy amplification, resulting in a trade-off between them.

From Fig. 4, we can assess the influence of finite-key size on the lower bound of the secret key generation rate. Given p_a, p_b, Y_1, e_{1b}^Z, and e_{1b}^X, the lower bound of the secret key generation rate is the worst case by considering their statistical fluctuations, which is demonstrated in Eq. (45). That means that Eve can obtain a maximum amount of information about the raw key. Using the law of large numbers in Eq. (14), we can find that the larger the N_μ, the smaller the statistical fluctuations will be. Therefore the lower bound of the secret key generation rate in Eq. (45) will increase, which is consistent with the simulation results in Fig. 4. Furthermore, we find that in practice if Alice can emit more than $N_\mu \sim 10^{12}$ signal pulses, they can be close to the asymptotic bound better.

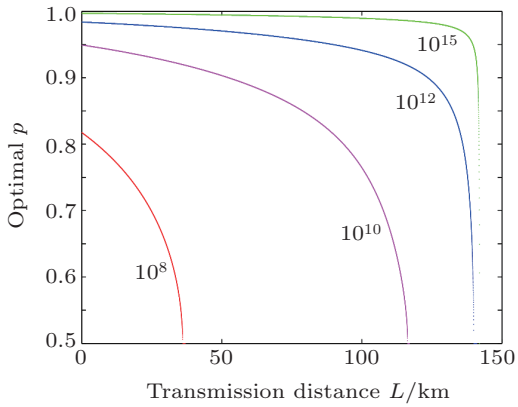


Fig. 3. (color online) Relationships between optimal probability p and transmission distance L for different values of N_μ.

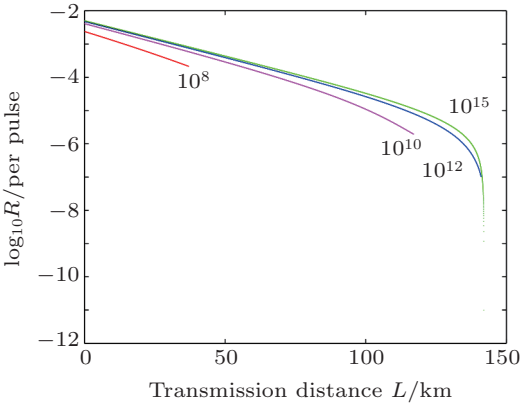


Fig. 4. (color online) Variations of logarithm of secret key generation rate with the transmission distance L for different values of N_μ. For each transmission distance, we optimize the parameter p.

5. Conclusion

In this paper, we derive the security proof of finite resource biased BB84 protocol with and without decoy states. We take into account the statistical fluctuations not only for the error rates and the yields of the signals, but also for the prior

probabilities of bases selection. We obtain the secret key generation rates and the optimal probabilities with and without decoy states. In the biased BB84 protocol with a finite resource, the optimal-biased parameter is susceptible to the length of the secret key. The optimal-biased parameter approaches 1 when the finite key effect can be neglected. However, the optimal-biased parameter is close to $1/2$ when the transmitted signal is low enough.

Appendix A: Proof for the comparison of the two formulas

To simplify the proof, let

$$e_b^Z = x, \quad e_b^X = y, \quad e_b = x', \quad e_{\rm p} = y',$$
$$\frac{p_a p_b}{p_a p_b + (1-p_a)(1-p_b)} = p,$$

then

$$\frac{(1-p_a)(1-p_b)}{p_a p_b + (1-p_a)(1-p_b)} = 1-p,$$

and

$$\begin{cases} x' = px + (1-p)y, \\ y' = (1-p)x + py. \end{cases} \tag{A1}$$

Therefore,

$$\begin{aligned} R_1 &= [p_a p_b + (1-p_a)(1-p_b)][1 - h(e_b^Z) - h(e_b^Z)] \\ &= [p_a p_b + (1-p_a)(1-p_b)][1 - h(x) - h(y)], \end{aligned} \tag{A2}$$

$$\begin{aligned} R_2 &= [p_a p_b + (1-p_a)(1-p_b)][1 - h(e_{\rm p}) - h(e_b)] \\ &= [p_a p_b + (1-p_a)(1-p_b)][1 - h(x') - h(y')]. \end{aligned} \tag{A3}$$

Consider that $\Delta = R_1 - R_2$, then we will have

$$\Delta = [p_a p_b + (1-p_a)(1-p_b)][h(x') + h(y') - h(x) - h(y)].$$

Using the convexity of $h(x)$ and Eq. (A1), we can obtain that

$$h(x') = h(px + (1-p)y) \geq ph(x) + (1-p)h(y), \tag{A4}$$

$$h(y') = h((1-p)x + py) \geq (1-p)h(x) + ph(y). \tag{A5}$$

With expression (A4) plus expression (A5), we arrive at

$$h(x') + h(y') \geq h(x) + h(y). \tag{A6}$$

Therefore $\Delta \geq 0$, which means that $R_1 \geq R_2$. If and only if $x = y$, the "=" holds.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore: IEEE) p. 175

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Lo H K and Chau H F 1999 *Science* **283** 2050

[4] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[5] Mayers D 2001 *J. ACM* **48** 351

[6] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 arXiv preprint quant-ph/0212066

[7] Renner R, Gisin N and Kraus B 2005 *Phys. Rev. A* **72** 012332

[8] Chen W, Han Z F, Zhang T, Wen H, Yin Z Q, Xu F X, Wu Q L, Liu Y, Zhang Y, Mo X F, Gui Y Z, Wei G and Guo G C 2009 *IEEE Photon. Technol. Lett.* **21** 575

[9] Wan S, Chen W, Yin Z Q, Zhang Y, Zhang T, Li H W, Xu F X, Zhou Z, Yang Y, Huang D J, Zhang L J, Li F Y, Liu D, Wang Y G, Guo G C and Han Z F 2010 *Opt. Lett.* **35** 2454

[10] Gisin N, Ribordy G, Tittel W and Zbinden H 2001 *Rev. Mod. Phys.* **74** 145

[11] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lutkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[12] Lo H K, Chau H F and Ardehali M 2005 *J. Cryptol.* **18** 133

[13] Lütkenhaus N and Jahma M 2002 *New J. Phys.* **4** 44

[14] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[15] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[16] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[17] Wei Z C, Wang W L, Zhang Z, Gao M, Ma Z and Ma X F 2013 *Sci. Rep.* **3** 2453

[18] Mayers D 1996 *Advances in Cryptology–CRYPTO'96* (Berlin: Springer) p. 343

[19] Inamori H, Lütkenhaus N and Mayers D 2007 *Eur. Phys. J. D* **41** 599

[20] Li H W, Chen W, Huang J Z, Yao Y, Liu D, Li F Y, Wang S, Yin Z Q, He D Y, Zhou Z, Li Y H, Yu N H and Han Z F 2012 *Sci. Sin.: Phys. Mech. Astron.* **42** 1237

[21] Hayashi M 2007 *Phys. Rev. A* **76** 012329

[22] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501

[23] Scarani V and Renner R 2008 *Theory of Quantum Computation, Communication, and Cryptography* (Berlin: Springer-Verlag) p. 83

[24] Cai R Y Q and Scarani V 2009 *New J. Phys.* **11** 045024

[25] Li H W, Zhao Y B, Yin Z Q, Wang S, Han Z F, Bao W S and Guo G C 2009 *Opt. Commun.* **282** 4162

[26] Cover T M and Thomas J A 2012 *Elements of Information Theory* (New York: John Wiley & Sons) p. 411

[27] Ma X F, Fung C H F, Boileau J C and Chau H F 2011 *Computers & Security* **30** 172

[28] Fung C H F, Ma X F and Chau H F 2010 *Phys. Rev. A* **81** 012318

[29] Ma X F, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326

[30] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762