Quantum Information and Computation, Vol. 11, No. 11&12 (2011) 0937–0947

SECURITY OF QUANTUM KEY DISTRIBUTION WITH STATE-DEPENDENT IMPERFECTIONS

HONG-WEI LI[a]
Key Laboratory of Quantum Information, University of Science and Technology of China
Hefei, 230026, China
Zhengzhou Information Science and Technology Institute
Zhengzhou, 450004, China

ZHEN-QIANG YIN[b] SHUANG WANG
Key Laboratory of Quantum Information, University of Science and Technology of China
Hefei, 230026, China

WAN-SU BAO
Zhengzhou Information Science and Technology Institute
Zhengzhou, 450004, China

GUANG-CAN GUO ZHENG-FU HAN[c]
Key Laboratory of Quantum Information, University of Science and Technology of China
Hefei, 230026, China

Received March 8, 2011
Revised August 18, 2011

In practical quantum key distribution system, the state preparation and measurement have state-dependent imperfections comparing with the ideal BB84 protocol. If the state-dependent imperfection can not be regarded as an unitary transformation, it should not be considered as part of quantum channel noise introduced by the eavesdropper, the commonly used secret key rate formula GLLP can not be applied correspondingly. In this paper, the unconditional security of quantum key distribution with state-dependent imperfections will be analyzed by estimating upper bound of the phase error rate in the quantum channel and the imperfect measurement. Interestingly, since Eve can not control all phase error in the quantum key distribution system, the final secret key rate under constant quantum bit error rate can be improved comparing with the perfect quantum key distribution protocol.

Keywords: SECURITY, QUANTUM KEY DISTRIBUTION, STATE-DEPENDENT IMPERFECTIONS
Communicated by: S Braunstein & H Zbinden

1 Introduction

Quantum key distribution (QKD) is the art of sharing secret keys between the transmitter Alice and receiver Bob. It has unconditional security, even if unlimited computational power

---

[a]The author Hong-Wei Li and Zhen-Qiang Yin contributed equally to this work.
[b]yinzheqi@mail.ustc.edu.cn
[c]zfhan@ustc.edu.cn

and storage capacity are controlled by the eavesdropper Eve. Since the QKD protocol has been proposed by Bennett and Brassard in 1984 [1], the unconditional security attracts a lot of attentions both in theory and experimental sides [2]. Theoretical physicists have analyzed unconditional security of QKD in many respects. Initially, Lo and Chau [3] proposed the security analysis with the help of quantum computer. Then, Shor and Preskill [4] proved security of prepare-and-measure protocol is equival to entanglement-based protocol, thus unconditional security of QKD has been proved combining with the CSS code and entanglement distillation and purification (EDP) technology. Without applying the EDP technology, Renner [5] has analyzed security of QKD with information theory method. More recently, Horodecki et al. [6] have analyzed security of QKD based on Private-entanglement states. Inspired by Horodecki's mind, Renes and Smith [7] have analyzed noisy processing allows some phase errors to be left uncorrected without compromising unconditional security of the key. However, all of the security analysis are based on perfect states preparation and measurement. The first unconditional security of QKD based on imperfect devices was proposed by Gottesman, Lo, Lukenhaus, and Preskill [8] (GLLP formula), they proved that only the single photon state transmitted in the quantum channel can be used to generate the final secret key. Applying the GLLP formula and decoy state method [9], security of the decoy state QKD has been analyzed by Lo [10] and Wang [11] respectively. Correspondingly, the secret key transmission distance can be improved greatly with decoy state method [12, 13]. More recently, Berta et al. [14, 15] have given a method for proving Bob's device independent QKD protocol by using the uncertainty relation, which is related to the earlier work by Koashi [16], but it also requires that the state preparation in Alice's side should be well characterized.

Obviously, if the imperfection is basis-dependent, we can consider a slightly changed protocol, where the state preparation and measurement are perfect, while there is an virtual unitary transformation controlled by Eve introduces the basis-dependent imperfection in the quantum channel. Since security of the original protocol is no less than the slightly changed protocol, the final secret key rate can be estimated utilizing the GLLP formula. However, most of the imperfection in states preparation and measurement are state-dependent [17, 18], which can not be controlled by Eve in the security analysis. For instance, the wave plate may be inaccurate in polarization based QKD system, while the phase modulator may be modulated by inaccurate voltage in phase-coding QKD system. If the imperfection can not be illustrated as an unitary transformation, it can no be considered as part of the quantum channel controlled by Eve.

In this paper, security of practical QKD system with state-dependent imperfections will be analyzed by considering imperfect states preparation in Alice's side and imperfect states measurement in Bob's side respectively. We apply the EDP technology by considering the most general imperfection, and a much better secret key rate under constant imperfect parameters has been analyzed in comparation with previous works. Comparing with the security analysis given by Marøy et al. [17] and Lydersen et al. [18], we apply a much simpler method and get a much higher secret key rate. We consider that states prepared by Alice and measured by Bob both have individual imperfections. The whole security analysis can be divided into two steps based on an virtual protocol. Firstly, we consider that Alice prepares perfect entangled quantum state pairs, and she keeps half of the perfect entangled quantum state, sends half of the imperfect modulated quantum state to Bob, which illustrate the imperfect states preparation.

Meanwhile, Bob applies perfect Hadamard transformation in the receiver's side, thus Alice and Bob can share the maximally entangled quantum state utilizing the EDP technology. Secondly, Alice applies perfect measurement with her maximally entangled quantum states, and Bob applies imperfect measurement with his entangled quantum states correspondingly, finally they can establish the raw key. Similar to Shor and Preskill's [4] security analysis, security of the practical QKD is equal to the virtual protocol with the EDP technology and imperfect measurement. Since the phase error introduced by Bob's imperfect measurement should not be controlled by Eve, we can get a much higher secret key rate correspondingly. The similar result has also been given by Renner et al. [19, 20, 21], they proved that adding noise in the classical post processing can improve the secret key rate by considering that phase errors introduced in the post processing can not be controlled by the eavesdropper Eve [7]. Comparing with the security analysis given by Renner et al., the noise introduced by the imperfect device are precisely known by Eve, since the random encoding choice, the imperfection can not be corrected or controlled by Eve. Thus, the exactly known but can not be controlled imperfection is similar to adding noise as the security analysis model given by Kraus et al. [19, 20].

2 Security of quantum key distribution with perfect states preparation and measurement

Before introducing the method to analyze security of QKD with imperfect devices, security of QKD with perfect devices will be analyzed in this section. Suppose that Alice and Bob choose the polarization encoding QKD system in our security analysis, the standard prepare-and-measure QKD protocol will be introduced in the following section. In Alice's side, the classical bit 0 is randomly encoded by quantum states $|0^o\rangle$ or $|45^o\rangle$, the classical bit 1 is randomly encoded by quantum states $|90^o\rangle$ or $|-45^o\rangle$. In Bob's side, he randomly choose rectilinear basis $\{|0^o\rangle, |90^o\rangle\}$ or diagonal basis $\{|45^o\rangle, |-45^o\rangle\}$ to measure the quantum state transmitted through the quantum channel. After Bob's perfect measurement and some classical steps of QKD (sifting, parameter estimation, error correction and privacy amplification), secret key bits can be shared between Alice and Bob.

Following the technique obtained by Shor and Preskill [4], security of prepare-and-measure QKD protocol is equal to security of entanglement-based QKD protocol, which can be constructed by considering the corresponding prepare-and-measure encoding scheme as shown in Fig.1.

Alice prepares maximally entangled pairs $|\phi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$. After applying the Hadamard operation randomly to the second part of the pair, she sends Bob half of the pair. Bob acknowledges the reception of his state and applies the Hadamard operation randomly. In the security analysis, the most generally noisy channels we need to consider are Pauli channels. By considering Eve's eavesdropping in the Pauli channel, the quantum state about Alice, Bob and Eve is given by

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

where $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the perfect Hadamard operator, which means the transforma-

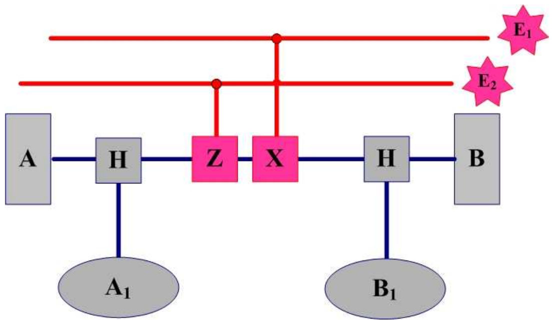

Fig. 1. Entanglement-based protocol with Pauli channel and eavesdropper Eve. Z is Eve's phase error operation, X is Eve's bit error operation. A_1 is part of Alice's system, B_1 is part of Bob's system.

tion between different bases in practical QKD system. $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the X operator, which means the bit error introduced by Eve. $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ is the Z operator, which means the phase error introduced by Eve. Correspondingly, XZ means the bit phase error introduced by Eve in the quantum channel. $P_{uv},\ u,v \in \{0,1\}$ means the probability of the $X^u Z^v$ operator introduced by Eve, which should be normalized by the following equation

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

$Q_{ij},\ i,j \in \{0,1\}$means the probability of H^i and H^j matrix introduced by Alice and Bob respectively, which satisfies $Q_{ij} = \frac{1}{4}$ for Alice and Bob's randomly choice.

After the sifting step, the case of $i \neq j$ will be discarded. We trace out A_1, B_1 and Eve's systems to get the following equation

$$\begin{aligned} &\rho_{AB} = \sum_{u,v} P_{uv}(\tfrac{1}{2} I_A \bigotimes X^u_{E_1} Z^v_{E_2} |\phi_1\rangle\langle\phi_1| Z^v_{E_2} X^u_{E_1} \bigotimes I_A \\ &+\tfrac{1}{2} I_A \bigotimes H_{B_1} X^u_{E_1} Z^v_{E_2} H_{A_1} |\phi_1\rangle\langle\phi_1| H_{A_1} Z^v_{E_2} X^u_{E_1} H_{B_1}) \bigotimes I_A. \end{aligned} \tag{3}$$

There are bit errors and phase errors in the Pauli channel, all of errors are considered to be introduced by Eve in the security analysis. After transmitting through the quantum channel, the initially shared maximally entangled state can be transformed into Bell states as the following equation

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

If the maximally entangled pairs $|\phi_1\rangle$ is transformed into Bell state $|\phi_1\rangle$, there is no error can be introduced in the quantum channel. However, if the maximally entangled pairs $|\phi_1\rangle$ is transformed into Bell states $|\phi_2\rangle$, $|\phi_3\rangle$ and $|\phi_4\rangle$ respectively, the bit error, phase error and bit phase error will be introduced by Eve correspondingly. Thus, the bit error rate and phase error rate can be given by

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

The bit error rate and phase error rate should be calculated when we analyze unconditional security of QKD. In practical QKD system, quantum bit error rate can be estimated after the parameter estimation step in the classical part of QKD protocol. The main difficulty in security analysis is how to estimate upper bound of the phase error rate.

Combining equations (3), (4) with (5), the phase error rate minus the bit error rate is

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

Thus, the phase error can be estimated by the bit error rate accurately in the perfect device case. Correspondingly, the final secret key rate can be given by

$$R = 1 - h(e_{phase}) - h(e_{bit}) = 1 - 2h(e_{bit}). \tag{7}$$

where, h is the binary entropy function. The maximal tolerated bit error rate in the quantum channel is 0.11 with equation (7), which has also been given by Shor and Preskill.

3 Security of quantum key distribution with state-dependent imperfections

Since practical QKD devices always have some flaws, the photon state preparation and measurement are always imperfect in practical QKD realizations. In the most general case, the imperfection is state-dependent. For example, the deflection angle has slight differences between different wave plates in polarization based QKD system. Similar to the security analysis of QKD with perfect devices, we will give the security analysis of QKD with imperfect devices in this section by utilizing the EDP technology and imperfect measurement. We firstly give the model description about the imperfect states preparation and measurement, then we will prove that the imperfect measurement is equal to the perfect measurement adding the noisy processing in our security analysis, finally security of the virtual protocol will be analyzed combining with the imperfect measurement and EDP technology.

3.1 Device-independent imperfections description

Angular deviation of the practical device can be used for illustrating the state-dependent imperfection. In Alice's side, the classical bit 0 is randomly encoded by quantum states $|\alpha_1{}^o\rangle$ or $|45+\alpha_2{}^o\rangle$, while the classical bit 1 is randomly encoded by quantum states $|90+\alpha_3{}^o\rangle$ or $|-45+\alpha_4{}^o\rangle$, where α_1, α_2, α_3 and α_4 are security parameters for illustrating Alice's angular deviations. In Bob's side, he randomly choose the imperfect rectilinear basis $\{|\beta_1{}^o\rangle, |90+\beta_3{}^o\rangle\}$ or the imperfect diagonal basis $\{|45+\beta_2{}^o\rangle, |-45+\beta_4{}^o\rangle\}$ to measure the quantum state transmitted in the quantum channel, where β_1, β_2, β_3 and β_4 are security parameters for illustrating Bob's angular deviation. Since the random encoding and decoding choice, all of the imperfection can not be controlled or corrected by the eavesdropper, detailed illustration of the imperfect parameter can be given as in Fig. 2. If the security parameter can be satisfied with $\alpha_1 = \alpha_3$, $\alpha_2 = \alpha_4$, $\beta_1 = \beta_3$ and $\beta_2 = \beta_4$, it will be the basis-dependent imperfection correspondingly.

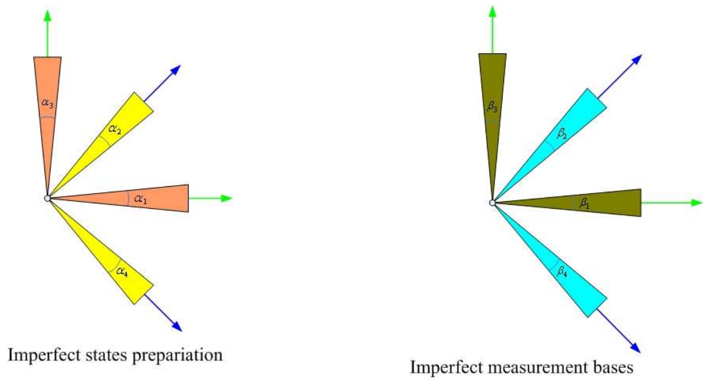

Fig. 2. The most general imperfect states preparation and measurement in practical QKD experimental realization, where α_1, α_2, α_3 and α_4 illustrates the imperfect states preparation, β_1, β_2, β_3 and β_4 illustrates the imperfect measurement.

3.2 Imperfect measurement

In practical QKD system with imperfect devices as illustrated in the previous subsection, Bob gets the classical bit 0 with the projective measurement operator $|\beta_1{}^{o}\rangle\langle\beta_1{}^{o}|$ and $|45+\beta_2{}^{o}\rangle\langle 45+\beta_2{}^{o}|$, gets the classical bit 1 with the projective measurement $|90+\beta_3{}^{o}\rangle\langle 90+\beta_3{}^{o}|$ and $|-45+\beta_4{}^{o}\rangle\langle -45+\beta_4{}^{o}|$ respectively. Since the rectilinear basis and diagonal basis will be selected randomly, the quantum bit error rate introduced by the imperfect measurement can be given by

$$
\begin{aligned}
& e_{bit1} \\
&= \tfrac{1}{2}\Big[\tfrac{1}{2}\Big(\frac{\langle 90+\beta_3{}^{o}|0^{o}\rangle\langle 0^{o}|90+\beta_3{}^{o}\rangle}{\langle 90+\beta_3{}^{o}|0^{o}\rangle\langle 0^{o}|90+\beta_3{}^{o}\rangle+\langle\beta_1{}^{o}|0^{o}\rangle\langle 0^{o}|\beta_1{}^{o}\rangle}+\frac{\langle\beta_1{}^{o}|90^{o}\rangle\langle 90^{o}|\beta_1{}^{o}\rangle}{\langle\beta_1{}^{o}|90^{o}\rangle\langle 90^{o}|\beta_1{}^{o}\rangle+\langle 90+\beta_3{}^{o}|90^{o}\rangle\langle 90^{o}|90+\beta_3{}^{o}\rangle}\Big)+ \\
&\quad \tfrac{1}{2}\Big(\frac{\langle -45+\beta_4{}^{o}|45^{o}\rangle\langle 45^{o}|-45+\beta_4{}^{o}\rangle}{\langle -45+\beta_4{}^{o}|45^{o}\rangle\langle 45^{o}|-45+\beta_4{}^{o}\rangle+\langle 45+\beta_2{}^{o}|45^{o}\rangle\langle 45^{o}|45+\beta_2{}^{o}\rangle} \\
&\quad +\frac{\langle 45+\beta_2{}^{o}|-45^{o}\rangle\langle -45^{o}|45+\beta_2{}^{o}\rangle}{\langle 45+\beta_2{}^{o}|-45^{o}\rangle\langle -45^{o}|45+\beta_2{}^{o}\rangle+\langle -45+\beta_4{}^{o}|-45^{o}\rangle\langle -45^{o}|-45+\beta_4{}^{o}\rangle}\Big)\Big] \\
&= \tfrac{1}{2}\Big[\tfrac{1}{2}\Big(\frac{sin^2\beta_1}{sin^2\beta_1+cos^2\beta_3}+\frac{sin^2\beta_3}{sin^2\beta_3+cos^2\beta_1}\Big)+\tfrac{1}{2}\Big(\frac{sin^2\beta_2}{sin^2\beta_2+cos^2\beta_4}+\frac{sin^2\beta_4}{sin^2\beta_4+cos^2\beta_2}\Big)\Big].
\end{aligned}
\tag{8}
$$

From this calculation, we can get the result that the imperfect measurement will introduce bit flipping with the probability e_{bit1}. Comparing with the imperfect measurement, the perfect measurement will introduce the bit flipping with zero probability. In our security analysis, Alice and Bob should establish the maximally entangled pairs before applying the measurement, which means that the eavesdropper can only get the error bit information about the secret key through the imperfect measurement in Bob's side. Thus, we can simplify the imperfect measurement as the perfect measurement adding a noisy processing protocol, where the bit 0(1) will be transformed into 1(0) with the probability e_{bit1}.

3.3 Virtual EDP protocol

We propose the virtual protocol based on the EDP technology as in Fig. 3. The new protocol mainly contain two steps: the first step is considering the maximally entangled state $|\phi_1\rangle$ to be shared between Alice and Bob. In the rectilinear basis case, the classical bit 0 is prepared by the quantum state $cos(\alpha_1)|0^{o}\rangle + sin(\alpha_1)|1^{o}\rangle$, while the classical bit 1 is prepared by the

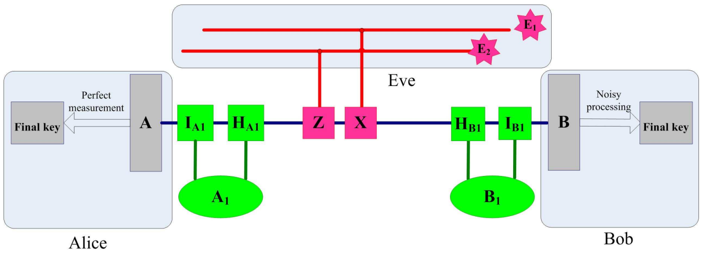

Fig. 3. Entanglement-based quantum key distribution protocol with imperfect devices. We introduce the third party A_1, B_1 in the new protocol, which can not be controlled by Alice, Bob and Eve respectively. In the first step, Alice and Bob share the maximally entangled pairs. In the second step, Alice applies the perfect measurement, Bob applies the perfect measurement and a noisy processing protocol to get the raw key.

quantum state $-sin(\alpha_3)|0^o\rangle+cos(\alpha_3)|1^o\rangle$. In the diagonal basis, the classical bit 0 is prepared by the quantum state $cos(\alpha_2+\frac{\pi}{4})|0^o\rangle+sin(\alpha_2+\frac{\pi}{4})|1^o\rangle$, while the classical bit 1 is prepared by the quantum state $cos(\alpha_4-\frac{\pi}{4})|0^o\rangle+sin(\alpha_4-\frac{\pi}{4})|1^o\rangle$. For simplicity, the state preparation can also be illustrated as the following case, Alice prepares the quantum state $\frac{1}{\sqrt{2}}(|0^o\rangle I_{A_1}|0^o\rangle + |1^o\rangle I_{A_1}|1^o\rangle)|e_0\rangle + \frac{1}{\sqrt{2}}(|0^o\rangle H_{A_1}|0^o\rangle + |1^o\rangle H_{A_1}|1^o\rangle)|e_1\rangle$ and transmits half of the perfect state to Bob, where $H_{A_1} = \begin{pmatrix} cos(\alpha_2+\frac{\pi}{4}) & cos(\alpha_4-\frac{\pi}{4}) \\ sin(\alpha_2+\frac{\pi}{4}) & sin(\alpha_4-\frac{\pi}{4}) \end{pmatrix}$, $I_{A_1} = \begin{pmatrix} cos(\alpha_1) & -sin(\alpha_3) \\ sin(\alpha_1) & cos(\alpha_3) \end{pmatrix}$, $|e_0\rangle$ and $|e_1\rangle$ are Alice's auxiliary quantum states. If Alice want to transmit the state $|0^o\rangle$ to Bob, the auxiliary quantum state $|e_0\rangle$ will be selected, and the practical quantum state $I_{A_1}|0^o\rangle = cos(\alpha_1)|0^o\rangle + sin(\alpha_1)|1^o\rangle$ will be transmitted in the quantum channel. Since all of the imperfect state can be analyzed similarly, the non-unitary matrix H_{A_1} and I_{A_1} can be used for illustrating the imperfect state preparation. In the receiver's side, Bob applies the unitary transformation H_{B_1} or I_{B_1} randomly, where $H_{B_1} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the perfect Hadamard transformation, $I_{B_1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the perfect identity transformation. Since Alice and Bob can apply the EDP technology, they will share the maximally entangled quantum pairs before the imperfect measurement.

The second step is applying the perfect and imperfect measurement in Alice's side and Bob's side respectively. More precisely, Alice measure the entangled quantum state with perfect rectilinear basis $\{0^o\rangle, |90^o\rangle\}$ or diagonal basis $\{45^o\rangle, |-45^o\rangle\}$. Bob measure the entangled quantum state with the imperfect rectilinear basis $\{|\beta_1{}^o\rangle, |90+\beta_3{}^o\rangle\}$ or imperfect diagonal basis $\{|45+\beta_2{}^o\rangle, |-45+\beta_4{}^o\rangle\}$ correspondingly, then Alice and Bob will share the raw key.

Similar to the security analysis based on the prefect device, A_1 and B_1 can not be changed by Alice and Bob in our security analysis, it can not be changed by Eve simultaneously. However, A_1 and B_1 are permitted to share the imperfection information with Alice, Bob and Eve. In the virtual protocol, the state preparation and measurement is the same as the original practical QKD system. If the unconditional security of the virtual protocol can be proved, security of the practical QKD system can be proved naturally. By considering Eve's eavesdropping in the Pauli channel, the quantum state about Alice and Bob before the measurement can be given by

$$\sum_{u,v,i,j}\sqrt{P_{uv}Q_{ij}}(I_A\bigotimes I_{B_1}^{i+1}H_{B_1}^{i}X_{E_1}^{u}Z_{E_2}^{v}H_{A_1}^{j}I_{A_1}^{j+1}|\phi_1\rangle|u\rangle_{E_1}|v\rangle_{E_2}|i\rangle_{B_1}|j\rangle_{A_1}). \tag{9}$$

After the sifting step, the case of $i \neq j$ will be discarded. We trace out Eve, A_1 and $B_1's$ systems, the density matrix about Alice and Bob can be given by

$$\begin{array}{l}\rho'_{AB}=\sum\limits_{u,v}P_{uv}(\frac{1}{2}I_A\bigotimes I_{B_1}X_{E_1}^{u}Z_{E_2}^{v}I_{A_1}|\phi_1\rangle\langle\phi_1|I_{A_1}Z_{E_2}^{v}X_{E_1}^{u}I_{B_1}\bigotimes I_A+\\ \frac{1}{2}I_A\bigotimes H_{B_1}X_{E_1}^{u}Z_{E_2}^{v}H_{A_1}|\phi_1\rangle\langle\phi_1|H_{A_1}Z_{E_2}^{v}X_{E_1}^{u}H_{B_1}\bigotimes I_A).\end{array} \tag{10}$$

Suppose that Alice prepare maximally entangled quantum states $|\phi_1\rangle^{\bigotimes N}$ in her side. After the EDP protocol, Alice and Bob will share maximally entangled quantum states $|\phi_1\rangle^{\bigotimes M}$, which can be illustrated as the following equation

$$\begin{array}{l}M=N(1-h(e_{bit})-h(e_{phase})),\\ e_{bit}=\langle\phi_2|\rho'_{AB}|\phi_2\rangle+\langle\phi_4|\rho'_{AB}|\phi_4\rangle,\\ e_{phase}=\langle\phi_3|\rho'_{AB}|\phi_3\rangle+\langle\phi_4|\rho'_{AB}|\phi_4\rangle,\end{array} \tag{11}$$

where e_{bit} and e_{phase} are the quantum bit error rate and phase error rate between Alice and Bob by considering the EDP technology. Since the calculation of e_{bit} and e_{phase} are much difficulty, we will get the calculation result based on some special imperfect parameters and the Mathematic software. Additionally, Bob will apply the imperfect measurement with the perfect entanglement quantum state as illustrated in the imperfect measurement subsection, Alice will apply the perfect measurement with the perfect entanglement quantum state correspondingly. Considering the virtual protocol, the practical quantum bit error rate between Alice and Bob can be estimated by

$$Q=1-(1-e_{bit1})(1-e_{bit})-e_{bit}e_{bit1}, \tag{12}$$

this equation means that the practical quantum bit error rate can be divided into two cases (considering the EDP protocol and the perfect measurement in Alice's side and imperfect measurement in Bob's side respectively). The first case is considering the EDP protocol has the right bit, the measurement protocol has the error bit. The second case is considering the EDP protocol has the error bit, the measurement has the right bit respectively. We can estimate Eve's information through the whole bit error rate and the phase error rate in the first step. Finally, the secret key rate can be given by

$$\begin{array}{l}R\geq lim_{N\to\infty}\frac{M(1-h(e_{bit1}))}{N}\\ =(1-h(e_{phase})-h(e_{bit}))(1-h(e_{bit1})).\end{array} \tag{13}$$

the calculation of which is much complicated for the formula has too many security parameters, we will give some examples to illustrate how to use this secret key rate formula in practical QKD system.

We give a simple example in the following, we suppose that the imperfect parameters in our security analysis are $\alpha_1=\alpha_3=\beta_1=\beta_3=0,\alpha_2=\beta_2=\frac{-\pi}{4},\alpha_4=\beta_4=\frac{3\pi}{4}$. Thus, we can get $H_{A_1}=I_{A_1}=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, this case means that Alice only send the rectilinear basis $\{|0^o\rangle,|90^o\rangle\}$, and Bob will only measure in the rectilinear basis correspondingly. The quantum bit error rate and phase error rate in the EDP protocol can be calculated respectively as the following equation

$$\begin{aligned} e_{bit} &= \tfrac{1}{4}(p_{00} + p_{01} + 3p_{10} + 3p_{11}), \\ e_{phase} &= \tfrac{1}{4}(p_{00} + 3p_{01} + p_{10} + 3p_{11}). \end{aligned} \tag{14}$$

Correspondingly, upper bound of the phase error rate can be estimated by

$$e_{phase} \leq e_{bit} + \tfrac{1}{2} \mid p_{10} - p_{01} \mid \leq e_{bit} + \tfrac{1}{2}. \tag{15}$$

Finally, we can only get zero secret key rate utilizing equation (13). In practical experimental realization, Eve can measure Alice's states in the same rectilinear basis with 0 bit error, and she will introduce the perfect man-in-the-middle attack without being discovered.

4 Calculation

To compare our security analysis with GLLP's security analysis, we will give the calculation result by considering the case which can not be analyzed by the GLLP formula in this section. We consider that the device has individual imperfections both in the transmitter's side and receiver's side respectively, which means quantum states in the same basis maybe have the different angular deviation. Precisely, we assume that the security parameters can be satisfied with $\alpha_1 = \beta_1 = \beta_2 = a, \alpha_2 = \alpha_3 = \alpha_4 = \beta_3 = \beta_4 = 0$. After some lengthy but not very interesting algebra, the bit error rate and phase error rate in the first step (Alice and Bob establish the maximally entangled quantum pairs with the EDP technology) can be calculated respectively as following equations,

$$\begin{aligned} e_{bit} = &\tfrac{1}{8}[cos^2(a)(p_{11}+p_{10}) + sin^2(a)(p_{00}+p_{01}) + cos(a)(2p_{10}-2p_{11}) + 4p_{01} + p_{10} + p_{11}] \\ &+ \tfrac{1}{8}[cos^2(a)(p_{11}+p_{10}) + sin^2(a)(p_{00}+p_{01}) + cos(a)(-2p_{10}+2p_{11}) + p_{10} + 5p_{11}], \end{aligned} \tag{16}$$

$$\begin{aligned} e_{phase} = &\tfrac{1}{8}[cos^2(a)(p_{00}+p_{01}) + sin^2(a)(p_{10}+p_{11}) + cos(a)(2p_{01}-2p_{00}) + 4p_{10} + p_{01} + p_{00}] \\ &+ \tfrac{1}{8}[cos^2(a)(p_{11}+p_{10}) + sin^2(a)(p_{00}+p_{01}) + cos(a)(-2p_{10}+2p_{11}) + p_{10} + 5p_{11}]. \end{aligned} \tag{17}$$

Equations (16) and (17) can be directly calculated combining equation (11) with practical imperfect parameters. From this calculation, we can find that the phase error rate is equal to the bit error rate in case of all imperfect parameters are equal to zero.

From this calculation result, upper bound of the phase error rate can be estimated by considering the following inequation

$$\begin{aligned} &|e_{phase} - e_{bit}| \\ &\leq \tfrac{1}{8}|[cos^2(a)(p_{11}+p_{10}-p_{00}-p_{01}) + sin^2(a)(p_{01}+p_{00}-p_{11}-p_{10}) \\ &\quad + 2cos(a)(p_{10}-p_{11}+p_{00}-p_{01}) + 3p_{01} - 3p_{10} + p_{11} - p_{00}]| \\ &= \tfrac{1}{4}|[cos^2(a)(p_{11}+p_{10}-p_{00}-p_{01}) + cos(a)(p_{10}-p_{11}+p_{00}-p_{01}) + 2p_{01} - 2p_{10}]| \\ &= \tfrac{1}{4}|[(cos^2(a)-1)(p_{11}+p_{10}-p_{00}-p_{01}) + (cos(a)-1)(p_{10}-p_{11}+p_{00}-p_{01})]| \\ &\leq \tfrac{1}{4}(1 + sin^2(a) - cos(a)) \end{aligned} \tag{18}$$

$$e_{phase} \leq \tfrac{1}{2}(1 + sin^2(a) - cos(a)) + e_{bit}. \tag{19}$$

Utilizing equation (8), we can get the bit error rate e_{bit1} as the following equation

$$e_{bit1} = \tfrac{1}{2}\tfrac{sin^2(a)}{sin^2(a)+1}. \tag{20}$$

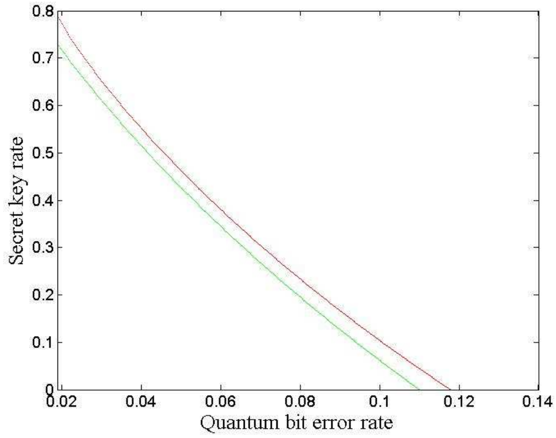

Fig. 4. Final secret key rate with perfect and imperfect devices. The blue line means the perfect devices case, which can be satisfied with equation (7). The red line means security of imperfect devices by considering parameters $\alpha_1 = \beta_1 = \beta_2 = 0.2, \alpha_2 = \alpha_3 = \alpha_4 = \beta_3 = \beta_4 = 0$.

Combining equations (12), (13) with (20), we can get the final secret key rate formula as the following equation

$$R \geq (1 - h(\tfrac{Q-e_{bit1}}{1-2e_{bit1}} + \tfrac{1}{2}(1 + sin^2(a) - cos(a))) - h(\tfrac{Q-e_{bit1}}{1-2e_{bit1}}))(1 - h(e_{bit1})), \quad (21)$$

combining wit this formula, we give the simulation result of the final secret key rate by considering practical imperfect security parameters as in Fig. 4.

Since the detection setup has the individual imperfection in our security analysis, the GLLP security analysis result can not be applied in this case. Comparing with the perfect QKD protocol, the final secret key rate has been improved in our calculation result, the reason for which is that Eve can not control the phase error introduced by Bob's imperfect measurement, and it should no be corrected by Alice and Bob correspondingly.

5 conclusions

In practical quantum key distribution realizations, the state-dependent imperfection in Alice and Bob's side can not be satisfied with the GLLP formula. A simple security proof of QKD with state-dependent imperfect states preparation and measurement have been analyzed in this paper. Our security analysis result shows that the imperfect QKD system maybe tolerate much higher quantum bit error rate comparing with the previous security analysis.

Acknowledgements

The author Hong-Wei Li would like to thank Lars Lydersen for his helpful discussion and comments. The author would like to thank the anonymous referees, they had put a real great effort into reviewing this article, and they had provided lots of useful feedback that helped to improve the presentation of this article. This work was supported by National Fundamental Research Program of China (2006CB921900), National Natural Science Foundation of China (60537020, 60621064) and the Innovation Funds of Chinese Academy of Sciences.

References

1. C. H. Bennett, G. Brassard, in *Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175-179.
2. Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dusek, Norbert Lutkenhaus, Momtchil Peev , Rev.Mod. Phys. 81, 1301 (2009).
3. Hoi-Kwong Lo, H. F. Chau, Science **283**, 5410 (1999).
4. W. Shor, J. Preskill, Phys. Rev. Lett. **85**, p. 441, (2000).
5. R. Renner, *Security of Quantum Key Distribution*, PhD thesis, Diss. ETH No 16242, quant-ph/0512258.
6. K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, J. Oppenheim, IEEE Transactions on Information Theory Vol 54 Issue 6 p2604-2620 (2008)
7. Joseph M. Renes, Graeme Smith, Phys. Rev. Lett. 98, 020502 (2007).
8. D. Gottesman, H.-K. Lo, Norbert Lukenhaus, and John Preskill , Quantum Inf. Comput**4**, 325 (2004)
9. W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
10. H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
11. X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
12. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian Phys. Rev. Lett. 96, 070502 (2006).
13. D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt Phys. Rev. Lett. 98, 010503 (2007).
14. M. Berta, M. Christandl, R. Colbeck, J. M. Renes, R. Renner. Nature Physics **,** 1734 (2010).
15. M. Tomamichel, R. Renner. Phys. Rev. Lett. 106, 110506 (2011).
16. M. Koashi. J. Phys. Conf. Ser. 36, 98-102 (2006).
17. Ø. Marøy, L. Lydersen, J. Skaar. Phys. Rev. A 82, 032337 (2010).
18. L. Lydersen, J. Skaar. Quant. Inf. Comp. 10, 0060 (2010).
19. B. Kraus, N. Gisin, R. Renner. Phys. Rev. Lett. 95, 080501 (2005).
20. R. Renner, N. Gisin, B. Kraus. Phys. Rev. A 72, 012332 (2005).
21. R. Garca-Patrn, N. J. Cerf. Phys. Rev. Lett. 102, 130501 (2009).