SCIENTIFIC REPORTS

OPEN

Randomness determines practical security of BB84 quantum key distribution

Received: 14 August 2015
Accepted: 12 October 2015
Published: 10 November 2015

Hong-Wei Li[1,2,3], Zhen-Qiang Yin[1,3], Shuang Wang[1,3], Yong-Jun Qian[1,3], Wei Chen[1,3], Guang-Can Guo[1,3] & Zheng-Fu Han[1,3]

Unconditional security of the BB84 quantum key distribution protocol has been proved by exploiting the fundamental laws of quantum mechanics, but the practical quantum key distribution system maybe hacked by considering the imperfect state preparation and measurement respectively. Until now, different attacking schemes have been proposed by utilizing imperfect devices, but the general security analysis model against all of the practical attacking schemes has not been proposed. Here, we demonstrate that the general practical attacking schemes can be divided into the Trojan horse attack, strong randomness attack and weak randomness attack respectively. We prove security of BB84 protocol under randomness attacking models, and these results can be applied to guarantee the security of the practical quantum key distribution system.

Quantum key distribution (QKD)[1] is the art of sharing secret keys between two remote parties Alice and Bob, unconditional security of which is based on the fundamental laws of quantum mechanics. The detailed security analysis has been proved by applying the entanglement distillation and purification (EDP) technology[2,3] and the von Neumann entropy theory[4–6] respectively. However, unconditional security of the QKD protocol has an important assumption, which requires Alice and Bob have random input numbers to control the classical bit encoding and measurement bases selection, and it can be easily proved that the measurement outcomes will become unsafe if the input random numbers are controlled or known by the eavesdropper Eve. A pair of important elements in practical QKD system is the random preparation and measurement of quantum states. If these procedures are imperfect, which can be perceived as a kind of incomplete randomness, the deviation may be used to perform quantum attacking[7]. More generally, practical attacking schemes can be divided into three different types from the view point of system randomness.

The first type is the Trojan horse attack[8], where the signal state combining with the Trojan horse state can be assumed to be high dimensional state modulation. Thus, Eve can measure one dimension of the modulated high dimensional state to get all of the secret key information without being discovered.

The second type is the strong randomness attack, where part of the input random numbers are totally controlled or known by the eavesdropper Eve. For example, the multi photon pulses generated by the practical weak coherent light source can be utilized by Eve to perform photon number splitting (PNS) attack[9,10], if the multi photon encoding quantum states are assumed to be known by Eve. Another example is the detector blinding attack[11,12], where Eve can easily mount the man-in-the-middle (MITM) attack by converting the avalanche photodiodes (APDs) into linear mode. The single photon detector has the count iff Bob's bases selection is equal to Eve, thus the bases selection in Bob's side are controlled by Eve. More recently, we proposed the probabilistic blinding attack model[13], where Eve partly applies the blinding attack to avoid being catched by detecting the current parameter, thus part of the bases selection can be assumed to be controlled by Eve correspondingly. In the strong randomness attack model, the final secret key should

[1]Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, China. [2]Zhengzhou Information Science and Technology Institute, Zhengzhou, 450004, China. [3]Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei 230026, China. Correspondence and requests for materials should be addressed to Z.-Q.Y. (email: yinzheqi@mail.ustc.edu.cn) or Z.-F.H. (email: zfhan@ustc.edu.cn)

shrink Eve's information from the multi-photon pulses to an arbitrary small value. To avoid the PNS attack, Gottesman-Lo-Lutkenhaus-Preskill (GLLP)[14] To avoid the PNS attack, Gottesman-Lo-Lutkenhaus-Preskill (GLLP)[14] formula combining with the decoy state method[15–17] is used in practical QKD systems to eliminate all of the multi photon pulse counting result, and ensure that only the single photon counting events can generate the final secret key. To avoid the probabilistic blinding attack, all blinding counting results should be eliminated, and only the non-blinding counting events can generate the final secret key. In the strong randomness attack model, the secret key rate[18] formula should be modified to

$$R \geq pS(a|E) - fh(Q), \tag{1}$$

where p is the probability of getting valid counting result, which can't be controlled by Eve. a is Alice's measurement outcome, E is Eve's auxiliary quantum system, $S(a|E) = S(a, E) - S(E)$ is the conditional von Neumann entropy, Q is the practical quantum bit error rate, $h(Q) = -Q\log_2 Q - (1 - Q)\log_2(1 - Q)$ is the classical Shannon entropy function, $f \geq 1$ is the error correction efficiency. If we prove security of BB84 QKD protocol under the PNS attack, p and $S(a|E)$ should be estimated by the single photon counting rate and the single photon error rate respectively[14–17].

The third type is the weak randomness attack, where the input random numbers are partly controlled by Eve[19]. Such as the wavelength dependence of the beam splitter will introduce the wavelength attack[20], where Eve can apply different wavelengths to control Bob's bases selection. Since the practical beam splitter maybe has partial wavelength correlation, that is the coupling ratio can't reach 0 and 1 with two different wavelengths, thus Eve can only partly control Bob's bases selection. Another example is the time shift attack[21], where Eve controls the APDs detection efficiency by controlling the photon arriving time, thus Eve has the advantage to guess the measurement outcomes. Since the practical time shift attack will introduce nonzero error rate, the classical bit encoding can be assumed to be partly known by Eve correspondingly.

Now, the Trojan horse attack can be avoided by applying the dimension filter (such as the wavelength filter) before the state modulation and measurement, which can be utilized to prevent Eve's Trojan horse light. The strong randomness attacking model has also been analyzed by applying the strict post processing technology, where we only need to precisely estimate p and $S(a|E)$. However, the weak randomness attacking model has not been analyzed until now. In this work, we prove security of the practical QKD system with weak input random numbers, which can affect the classical bit encoding and bases selection respectively. We give two security analysis models, the first model is based on the one-step post processing, where all of the measurement outcomes should integrally apply error correction and privacy amplification. While the second model is based on the two-step post processing, where the measurement outcomes can be divided into two sets with different measurement bases, then the two sets should apply error correction and privacy amplification individually. If we only consider the bit encoding weak randomness, two distinct methods can get the same secret key rate. But, if we consider the bases selection weak randomness, the analysis result shows that the two post processing method can generate much more secret key. Our analysis model can be applied in numerous attacking schemes, such as the wavelength attack and the time shift attack. Combining with the previous three attacking models, security of the practical QKD system can be evaluated.

BB84 QKD Protocol with Weak Randomness

In the BB84 protocol, there are two binary input bits x_1 and x_0 in Alice's side, which can be used to select the state preparation bases and encoding classical bits respectively. While the state measurement side Bob needs one binary input bit y to select the measurement basis. After the quantum state preparation and measurement, Alice and Bob should apply the bases sifting process to save the same bases case ($x_1 = y$). Thus, in the security analysis model, the input randomness can be divided into two sets, the first set can be used to decide the encoding classical bit selection x_0, while the second set can be used to decide the encoding and decoding bases selection x_1 (or y). Since Alice and Bob should publicly compare x_1 and y to save the same value, we can only consider Eve has partial knowledge about the bases selection x_1 before the state measurement, the security analysis model can be simplified correspondingly. Thus we can only assume weak random numbers x_0 and x_1 to control the encoding classical bit and bases selection respectively, the detailed analysis model is given in Fig. 1.

In the weak randomness model, the weak random numbers x_0 and x_1 can be controlled by two different sets of hidden variables λ_0 and λ_1 as the following equations,

$$\begin{aligned} p(x_0) &= \sum_i p_{\lambda_0=i}\, p(x_0|\lambda_0 = i), \\ p(x_1) &= \sum_j p_{\lambda_1=j}\, p(x_1|\lambda_1 = j), \end{aligned} \tag{2}$$

where λ_0 and λ_1 are hidden variables controlled by Eve, $p(x_0 = 0)$ is the probability that Alice encodes classical bit 0, while $p(x_0 = 1) = 1 - p(x_0 = 0)$ is the probability that Alice encodes classical bit 1. Similarly, $p(x_1 = 0)$ is the probability that Alice applies the rectilinear encoding basis, $p(x_1 = 1) = 1 - p(x_1 = 0)$ is the probability that Alice applies the diagonal encoding basis. Note that two sets of hidden variables λ_0 and λ_1 should satisfy $\sum_i p_{\lambda_0=i} = \sum_j p_{\lambda_1=j} = 1$. However, even if the practical experimental realization

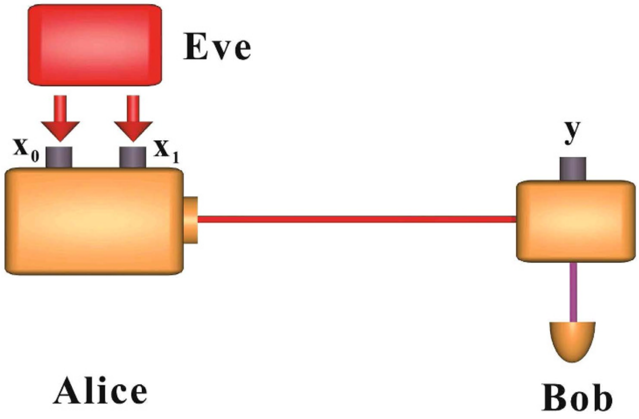

Figure 1. Weak randomness QKD model, where x_0 decides the encoding classical bit, x_1 decides the encoding bases selection, y decides the measurement bases selection. In the weak randomness QKD model, Eve has the advantage to guess the classical bit encoding x_0 and the basis selection x_1.

can observe $p(x_0) = \frac{1}{2}$ and $p(x_1) = \frac{1}{2}$ respectively, we still can't guarantee $p(x_0|\lambda_0 = i) = p(x_1|\lambda_1 = j) = \frac{1}{2}$ for arbitrary hidden variables $\lambda_0 = i$ and $\lambda_1 = j$. Thus, the aforementioned security analysis model based on perfect random input numbers can't be satisfied directly, we need to estimate the randomness deviation for arbitrary hidden variables. The practical weak randomness model is given by

$$\left|p(x_0|\lambda_0 = i) - \frac{1}{2}\right| \le \varepsilon_0,$$
$$\left|p(x_1|\lambda_1 = j) - \frac{1}{2}\right| \le \varepsilon_1, \tag{3}$$

where $0 \le \varepsilon_0, \varepsilon_1 \le \frac{1}{2}$, $\varepsilon_0 = 0$ ($\varepsilon_1 = 0$) is the perfect random number case, which means that Eve has no prior knowledge about the classical bit selection (bases selection). While $\varepsilon_0 = \frac{1}{2}\left(\varepsilon_1 = \frac{1}{2}\right)$ means Eve previously knows the classical bit selection (bases selection), in which case Alice and Bob can't generate any secret key even if they can observe $p(x_0) = \frac{1}{2}\left(p(x_1) = \frac{1}{2}\right)$.

One-Step Post Processing Method

By considering the given hidden variable $\lambda_0 = i$, we apply the EDP technology to illustrate the practical state preparation as the following equation,

$$|\varphi\rangle_{\lambda_0 = i} = \sqrt{p(x_0 = 0|\lambda_0 = i)}\,|00\rangle + \sqrt{p(x_0 = 1|\lambda_0 = i)}\,|11\rangle, \tag{4}$$

where Alice encoding the classical bit 0 with probability $p(x_0 = 0|\lambda_0 = i)$, and encoding the classical bit 1 with probability $p(x_0 = 1|\lambda_0 = i) = 1 - p(x_0 = 0|\lambda_0 = i)$. By considering the given hidden variable $\lambda_1 = j$, Alice prepares the quantum state in the rectilinear basis with probability $p(x_1 = 0|\lambda_1 = j)$, and prepares the quantum state in the diagonal basis with probability $p(x_1 = 1|\lambda_1 = j) = 1 - p(x_1 = 0|\lambda_1 = j)$, thus the final quantum state preparation under the Pauli quantum channel is

$$\begin{aligned}\rho_{AB_{ij}} = \sum_{u,v} q_{u,v}\Big\{& p(x_1 = 0|\lambda_1 = j)\, I \otimes X^u Z^v |\varphi\rangle\langle\varphi|_{\lambda_0 = i} Z^v X^u \otimes I \\ &+ p(x_1 = 1|\lambda_1 = j)\, I \otimes H X^u Z^v H |\varphi\rangle\langle\varphi|_{\lambda_0 = i} H Z^v X^u H \otimes I\Big\},\end{aligned} \tag{5}$$

where $u, v \in \{0, 1\}$, $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the Hadmard matrix, $\sum_{u,v} q_{u,v} = 1$, $q_{0,0}$ is the probability that Eve applies identity operation $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $q_{0,1}$ is the probability that Eve applies phase error operation $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $q_{1,0}$ is the probability that Eve applies bit error operation $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $q_{1,1}$ is the probability that Eve applies bit phase error operation XZ. Since Alice's state preparation is restricted in the two dimensional Hilbert space, we can prove the final secret key rate under the Pauli quantum channel. Thus, the quantum bit error rate and phase error rate introduced by Eve can be respectively given by

$$\begin{aligned} e^{i,j}_{bit} &= \langle \phi_2 | \rho_{AB_{ij}} | \phi_2 \rangle + \langle \phi_4 | \rho_{AB_{ij}} | \phi_4 \rangle, \\ e^{i,j}_{phase} &= \langle \phi_3 | \rho_{AB_{ij}} | \phi_3 \rangle + \langle \phi_4 | \rho_{AB_{ij}} | \phi_4 \rangle, \end{aligned} \tag{6}$$

where

$$\begin{aligned} |\phi_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ |\phi_2\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\phi_3\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\phi_4\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{7}$$

For arbitrary hidden variable $\lambda_0 = i$ and $\lambda_1 = j$, upper bound of the phase error rate $e^{i,j}_{phase}$ can be estimated by applying the bit error rate $e^{i,j}_{bit}$ and the randomness deviation parameters,

$$\begin{aligned} e^{i,j}_{phase} - e^{i,j}_{bit} = &\left(\frac{1}{2} - \sqrt{-\left(p(x_0 = 0|\lambda_0 = i) - \frac{1}{2}\right)^2 + \frac{1}{4}}\right) q_{00} \\ &- \left(\frac{1}{2} - \sqrt{-\left(p(x_0 = 0|\lambda_0 = i) - \frac{1}{2}\right)^2 + \frac{1}{4}}\right) q_{11} \\ &+ (2p(x_1 = 0|\lambda_1 = j) - 1)\left(\frac{1}{2} + \sqrt{-\left(p(x_0 = 0|\lambda_0 = i) - \frac{1}{2}\right)^2 + \frac{1}{4}}\right) q_{01} \\ &- (2p(x_1 = 0|\lambda_1 = j) - 1)\left(\frac{1}{2} + \sqrt{-\left(p(x_0 = 0|\lambda_0 = i) - \frac{1}{2}\right)^2 + \frac{1}{4}}\right) q_{10} \\ &\le \left(\frac{1}{2} - \sqrt{-\epsilon_0^2 + \frac{1}{4}}\right) q_{00} + \left(\frac{1}{2} - \sqrt{-\epsilon_0^2 + \frac{1}{4}}\right) q_{11} \\ &+ 2\epsilon_1 q_{01} + 2\epsilon_1 q_{10} \le max\left(\left(\frac{1}{2} - \sqrt{-\epsilon_0^2 + \frac{1}{4}}\right),\ 2\epsilon_1\right) \equiv \delta, \end{aligned} \tag{8}$$

where we apply $q_{00} + q_{11} \le 1$, $q_{01} + q_{10} \le 1$ and $\sum_{u,v} q_{u,v} = 1$ in the previous calculation. By applying the EDP technology, the final secret key rate with given hidden variables $\lambda_0 = i$ and $\lambda_1 = j$ is

$$R^{i,j} \ge 1 - h\left(e^{i,j}_{phase}\right) - h(e^{i,j}_{bit}) \ge 1 - h(e^{i,j}_{bit} + \delta) - h(e^{i,j}_{bit}). \tag{9}$$

In the practical experimental realization, we can only observe the practical quantum bit error rate $e_{bit} = \sum_{i,j} p_{\lambda_0 = i} p_{\lambda_1 = j} e^{i,j}_{bit}$, the final secret key rate with given quantum bit error rate e_{bit} can be given by

$$\begin{aligned} R &\ge \sum_{i,j} p_{\lambda_0 = i} p_{\lambda_1 = j} R^{i,j} \\ &\ge \sum_{i,j} p_{\lambda_0 = i} p_{\lambda_1 = j} (1 - h(e^{i,j}_{phase}) - h(e^{i,j}_{bit})) \\ &\ge \sum_{i,j} p_{\lambda_0 = i} p_{\lambda_1 = j} (1 - h(e^{i,j}_{bit} + \delta) - h(e^{i,j}_{bit})) \\ &\ge 1 - h\left(\sum_{i,j} p_{\lambda_0 = i} p_{\lambda_1 = j} e^{i,j}_{bit} + \delta\right) - h\left(\sum_{i,j} p_{\lambda_0 = i} p_{\lambda_1 = j} e^{i,j}_{bit}\right) \\ &= 1 - h(e_{bit} + \delta) - h(e_{bit}), \end{aligned} \tag{10}$$

where we apply the concavity property of the Shannon entropy function in the previous calculation. By implementing the security analysis result, we calculate the secret key rate R with given randomness deviation parameters ϵ_0 and ϵ_1 in Fig. 2. The calculation result demonstrates that the bases selection weak

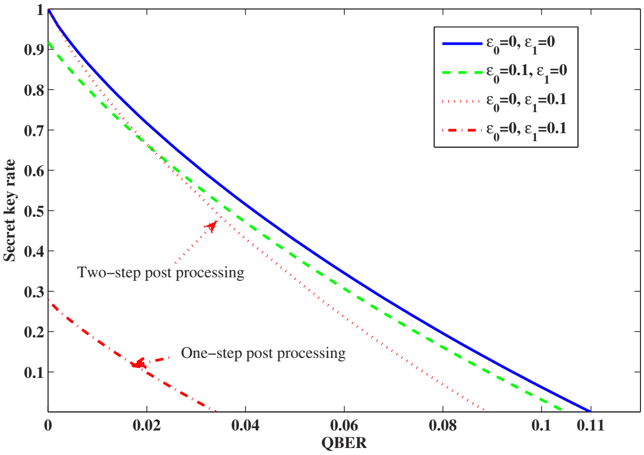

Figure 2. Secret key rate with different quantum bit error rate value, where the blue solid line is no randomness deviation case, the green dash line is considering $\epsilon_0 = 0.1$ and $\epsilon_1 = 0$, the red dotted line is considering $\epsilon_0 = 0$ and $\epsilon_1 = 0.1$ with two-step post processing method, the red dash dotted line is considering $\epsilon_0 = 0$ and $\epsilon_1 = 0.1$ with one-step post processing method. Comparing with the one-step post processing method, two-step post processing method can generate much more secret key with given basis selection randomness deviation, this is because we can get more precious phase error estimation in the two-step post processing method.

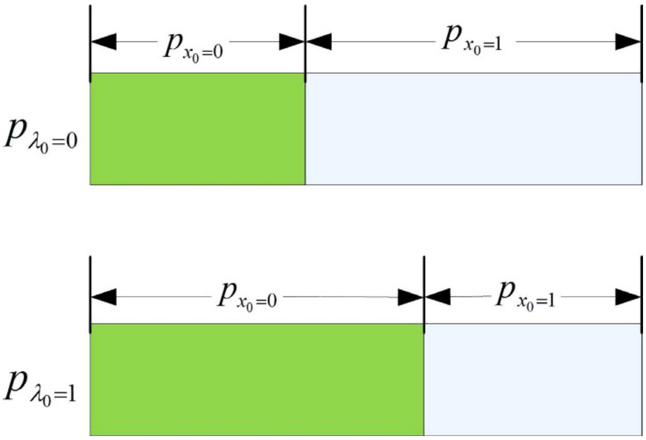

Figure 3. The classical bit encoding x_0 is controlled by the hidden variable λ_0, different λ_0 values have different classical bit encoding probability $p(x_0|\lambda_0)$.

randomness decrease the final secret key rate more obviously comparing with the classical bit encoding weak randomness.

Two-Step Post Processing Method

In the previous weak randomness model, the input random numbers maybe controlled by the hidden variables λ_0 and λ_1. Since there are two different bases selection (diagonal basis and rectilinear basis) and two different classical bit encoding (0 and 1), we can simply assume λ_0 and λ_1 have two different values {0, 1} respectively.

In the practical experimental realization, we can only observe the classical bit encoding probability $p(x_0) = p_{\lambda_0=0}p(x_0|\lambda_0 = 0) + p_{\lambda_0=1}p(x_0|\lambda_0 = 1)$, but $p(x_0) = \frac{1}{2}$ can't guarantee $p(x_0|\lambda_0 = 0)= p(x_0|\lambda_0 = 1) = \frac{1}{2}$, the detailed classical bit deviation model is given in Fig. 3.

Similarly, we can also only observe the bases selection probability $p(x_1) = p_{\lambda_1=0}p(x_1|\lambda_1 = 0)+ p_{\lambda_1=1}p(x_1|\lambda_1 = 1)$, but the observed probability $p(x_1) = \frac{1}{2}$ can't guarantee $p(x_1|\lambda_1 = 0) = p(x_1|\lambda_1 = 1) = \frac{1}{2}$, the detailed bases selection deviation model is given in Fig. 4.

The practical quantum state preparation is given by

$$\rho_{AB} = \sum_{\lambda_1} p_{\lambda_1} p(x_1 = 0|\lambda_1) \sum_{\lambda_0} p_{\lambda_0} \rho_{AB_{Z\lambda_0}} + \sum_{\lambda_1} p_{\lambda_1} p(x_1 = 1|\lambda_1) \sum_{\lambda_0} p_{\lambda_0} \rho_{AB_{X\lambda_0}}, \tag{11}$$

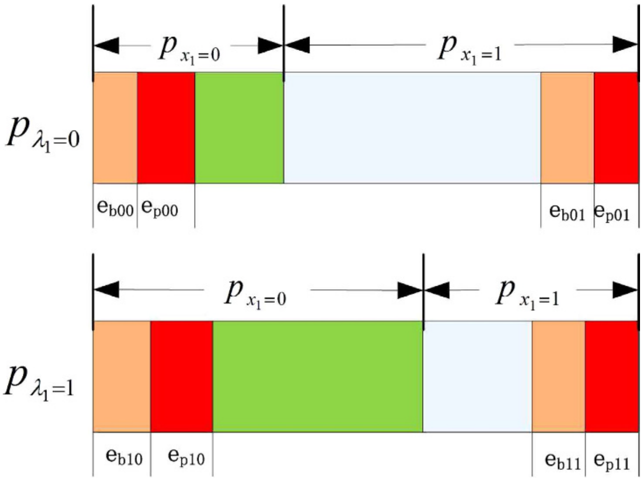

Figure 4. The basis selection deviation is controlled by the hidden variable λ_1, different λ_1 value has different basis selection probability $p(x_1|\lambda_1)$. For given hidden variable $\lambda_1 = 0$, e_{b00} and e_{b01} are bit error rates introduced in the rectilinear basis and diagonal basis, while e_{p00} and e_{p01} are phase error rates introduced in the rectilinear basis and diagonal basis respectively. For given hidden variable $\lambda_1 = 1$, e_{b10} and e_{b11} are bit error rates introduced in the rectilinear basis and diagonal basis, while e_{p10} and e_{p11} are phase error rates introduced in the rectilinear basis and diagonal basis respectively.

where

$$\begin{aligned}\rho_{AB_{Z\lambda_0}} &= \sum_{u,v} q_{u,v} I \otimes X^u Z^v |\varphi\rangle\langle\varphi|_{\lambda_0} Z^v X^u \otimes I,\\ \rho_{AB_{X\lambda_0}} &= \sum_{u,v} q_{u,v} I \otimes HX^u Z^v H |\varphi\rangle\langle\varphi|_{\lambda_0} HZ^v X^u H \otimes I.\end{aligned} \tag{12}$$

For given hidden variables λ_0 and λ_1, the difference between the phase error rate in the rectilinear basis and bit error rate in the diagonal basis can be given by

$$\left|e_{p\lambda_0\lambda_1 0} - e_{b\lambda_0\lambda_1 1}\right| \le \frac{1}{2} - \sqrt{-\epsilon_0^2 + \frac{1}{4}}. \tag{13}$$

where $e_{p\lambda_0\lambda_1 0} = \langle\phi_3|\rho_{AB_{Z\lambda_0}}|\phi_3\rangle + \langle\phi_4|\rho_{AB_{Z\lambda_0}}|\phi_4\rangle$, $e_{b\lambda_0\lambda_1 1} = \langle\phi_2|\rho_{AB_{X\lambda_0}}|\phi_2\rangle + \langle\phi_4|\rho_{AB_{X\lambda_0}}|\phi_4\rangle$. Similarly, The difference between the phase error rate in the diagonal basis and bit error rate in the rectilinear basis can be given by

$$\left|e_{p\lambda_0\lambda_1 1} - e_{b\lambda_0\lambda_1 0}\right| \le \frac{1}{2} - \sqrt{-\epsilon_0^2 + \frac{1}{4}}, \tag{14}$$

where $e_{p\lambda_0\lambda_1 1} = \langle\phi_3|\rho_{AB_{X\lambda_0}}|\phi_3\rangle + \langle\phi_4|\rho_{AB_{X\lambda_0}}|\phi_4\rangle$, $e_{b\lambda_0\lambda_1 0} = \langle\phi_2|\rho_{AB_{Z\lambda_0}}|\phi_2\rangle + \langle\phi_4|\rho_{AB_{Z\lambda_0}}|\phi_4\rangle$. By considering $e_{p\lambda_1 0} = \langle\phi_3|\sum_{\lambda_0} p_{\lambda_0}\rho_{AB_{Z\lambda_0}}|\phi_3\rangle + \langle\phi_4|\sum_{\lambda_0} p_{\lambda_0}\rho_{AB_{Z\lambda_0}}|\phi_4\rangle = \sum_{\lambda_0} p_{\lambda_0} e_{p\lambda_0\lambda_1 0}$ and $e_{b\lambda_1 1} = \langle\phi_2|\sum_{\lambda_0} p_{\lambda_0}\rho_{AB_{X\lambda_0}}|\phi_2\rangle + \langle\phi_4|\sum_{\lambda_0} p_{\lambda_0}\rho_{AB_{X\lambda_0}}|\phi_4\rangle = \sum_{\lambda_0} p_{\lambda_0} e_{b\lambda_0\lambda_1 1}$, we calculate the difference between the phase error rate $e_{p\lambda_1 0}$ and the bit error rate $e_{b\lambda_1 1}$

$$\begin{aligned}|e_{p\lambda_1 0} - e_{b\lambda_1 1}| &= \left|\sum_{\lambda_0} p_{\lambda_0}(e_{p\lambda_0\lambda_1 0} - e_{b\lambda_0\lambda_1 1})\right|\\ &\le \sum_{\lambda_0} p_{\lambda_0}|e_{p\lambda_0\lambda_1 0} - e_{b\lambda_0\lambda_1 1}|\\ &\le \sum_{\lambda_0} p_{\lambda_0}\left(\frac{1}{2} - \sqrt{-\epsilon_0^2 + \frac{1}{4}}\right)\\ &= \frac{1}{2} - \sqrt{-\epsilon_0^2 + \frac{1}{4}}.\end{aligned} \tag{15}$$

Similarly, the difference between $e_{p\lambda_1 1}$ and $e_{b\lambda_1 0}$ is

$$\left|e_{p\lambda_1 1} - e_{b\lambda_1 0}\right| \le \frac{1}{2} - \sqrt{-\epsilon_0^2 + \frac{1}{4}}. \tag{16}$$

The probability of getting the rectilinear basis and diagonal basis measurement outcomes in Bob's side can be respectively given by

$$p_{rec} = p_{rec1} + p_{rec2}, \; p_{dia} = p_{dia1} + p_{dia2}, \tag{17}$$

where $p_{rec1} = p_{\lambda_1=0}p(x_1 = 0|\lambda_1 = 0)$, $p_{rec2} = p_{\lambda_1=1}p(x_1 = 0|\lambda_1 = 1)$, $p_{dia1} = p_{\lambda_1=0}p(x_1 = 1|\lambda_1 = 0)$, $p_{dia2} = p_{\lambda_1=1}p(x_1 = 1|\lambda_1 = 1)$. The phase error rate in the rectilinear basis and diagonal basis can be respectively given by

$$\begin{aligned} e_{recpha} &= \frac{p_{rec1}e_{p00} + p_{rec2}e_{p10}}{p_{rec}} \le \frac{p_{rec1}e_{b01} + p_{rec2}e_{b11}}{p_{rec}} + \frac{1}{2} - \sqrt{-\epsilon_0^2 + \frac{1}{4}}, \\ e_{diapha} &= \frac{p_{dia1}e_{p01} + p_{dia2}e_{p11}}{p_{dia}} \le \frac{p_{dia1}e_{b00} + p_{dia2}e_{b10}}{p_{dia}} + \frac{1}{2} - \sqrt{-\epsilon_0^2 + \frac{1}{4}}. \end{aligned} \tag{18}$$

The bit error rate in the rectilinear basis and diagonal basis can be respectively given by

$$e_{recbit} = \frac{p_{rec1}e_{b00} + p_{rec2}e_{b10}}{p_{rec}}, \; e_{diabit} = \frac{p_{dia1}e_{b01} + p_{dia2}e_{b11}}{p_{dia}}. \tag{19}$$

By applying the two-step post processing method with the two different bases measurement outcomes, the final secret key rate can be given by

$$R \ge p_{rec}\left(1 - h(e_{recbit}) - h(e_{recpha})\right) + p_{dia}\left(1 - h(e_{diabit}) - h(e_{diapha})\right), \tag{20}$$

where the first part is the secret key generated by the rectilinear basis, while the second part is the secret key generated by the diagonal basis. The corresponding secret key rate *R* with different quantum bit error rate values is given in Fig. 2, the calculation is based on the nonlinear optimization method with given quantum bit error rate, the detailed explanation is in the methods. To explain our analysis result, we compare the two analysis methods by considering the wavelength attack has the coupling ratio 0.4 and 0.6 with different wavelengths. If the observed quantum bit error rate is 0.02, one-step post processing method can generate the secret key rate 0.0984, while the two-step post processing method can generate the secret key rate 0.6642.

Methods

By considering Eve's arbitrary attacking scheme, the final secret key rate with two different bases can be calculated with the following optimization method

$$\begin{aligned} \textit{Minimize}:\; & p_{rec}\left(1 - h(e_{recbit}) - h(e_{recpha})\right) + p_{dia}\left(1 - h(e_{diabit}) - h(e_{diapha})\right) \\ \textit{Subject to}:\; & p_{\lambda_0=0} + p_{\lambda_0=1} = p_{\lambda_1=0} + p_{\lambda_1=1} = 1 \\ & p(x_0 = 0|\lambda_0) + p(x_0 = 1|\lambda_0) = p(x_1 = 0|\lambda_1) + p(x_1 = 1|\lambda_1) = 1 \\ & 0 \le e_{b00}, e_{b01}, e_{b10}, e_{b11}, p_{\lambda_0=0}, p_{\lambda_1=0} \le 1 \\ & \left|p(x_0|\lambda_0 = i) - \frac{1}{2}\right| \le \varepsilon_0 \\ & \left|p(x_1|\lambda_1 = j) - \frac{1}{2}\right| \le \varepsilon_1 \\ & \left|e_{p\lambda_1 0} - e_{b\lambda_1 1}\right| \le \frac{1}{2} - \sqrt{-\epsilon_0^2 + \frac{1}{4}} \\ & \left|e_{p\lambda_1 1} - e_{b\lambda_1 0}\right| \le \frac{1}{2} - \sqrt{-\epsilon_0^2 + \frac{1}{4}} \\ & p_{rec} = p_{dia} = \frac{1}{2} \\ & p_{rec}e_{recbit} + p_{dia}e_{diabit} = Q, \end{aligned} \tag{21}$$

where Q is the quantum bit error rate estimated in the practical experimental realization, $p_{rec} = p_{dia} = \frac{1}{2}$ are the bases selection probability observed in the practical experimental realization.

Conclusion

In this work, security of BB84 QKD protocol against the strong randomness attack and the weak randomness attack have been analyzed, which satisfies several practical attacking schemes, such as the photon number splitting attack, detector blinding attack, wavelength attack and time shift attack. We demonstrate that security of the practical QKD system can be evaluated by respectively considering the Trojan horse attack, the strong randomness attack and the weak randomness attack, and the three attacking models can be employed to build the practical QKD system security standardization in the future.

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public-key distribution and coin tossing, Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179 (IEEE, New York, 1984).
2. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283,** 5410 (1999).
3. Shor, P. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441–444 (2000).
4. Renner, R. Security of Quantum Key Distribution. PhD thesis, Diss. ETH No 16242, quant-ph/0512258 (2005).
5. Kraus, B., Gisin, N. & Renner, R. Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication. *Phys. Rev. Lett.* **95,** 080501 (2005).
6. Renner, R., Gisin, N. & Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **72,** 012332 (2005).
7. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
8. Gisin, N., Fasel, S., Kraus, B., Zbinden, H. & Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A*. **73,** 022320 (2006).
9. Lutkenhaus, N. Estimates for practical quantum cryptography. *Phys. Rev. A*. **59,** 3301 (1999).
10. Lutkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*. **61,** 052304 (2000).
11. Lydersen, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*. **4,** 686–689 (2010).
12. Yuan, Z. L., Dynes J. F. & Shields, A. J., Avoiding the blinding attack in QKD. *Nature Photonics*. **4,** 800 (2010).
13. Qian, Y. J. *et al.* Countermeasure against probabilistic blinding attack in practical quantum key distribution systems. *Chin. Phys. B*. Vol. **24,** No. 9, 090305 (2015).
14. Gottesman, D., Lo, H. K., Lutkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput*. **5,** 325–360 (2004).
15. Hwang, W. Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
16. Wang, X. B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94,** 230503 (2005).
17. Lo, H. K., Ma, X. & Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **94,** 230504 (2005).
18. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. Lond. A* **461** (2005).
19. Bouda, J., Pivoluska, M., Plesch, M. & Wilmott. C, Weak randomness seriously limits the security of quantum key distribution. *Phys. Rev. A*. **86,** 062308 (2012).
20. Li, H. W. *et al.* Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A*. **84,** 062308 (2011).
21. Qi, B., Fung, C. H. F., Lo, H. K. & Ma, X. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.* **7,** 73–82 (2007).

Acknowledgements

The authors are supported by the National Natural Science Foundation of China (Grant Nos. 11304397, 61201239, 61205118 and 61475148), China Postdoctoral Science Foundation (Grant No. 2013M540514) and Anhui Provincial Natural Science Foundation (Grant No. 1408085QF102).

Author Contributions

H.-W.L., Z.-Q.Y., Z.-F.H. and G.-C.G. conceived the project. H.-W.L., S.W., Y.-J.Q. and W.C. performed the optimization calculation and analysis. H.-W.L. wrote the paper.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Li, H.-W. *et al.* Randomness determines practical security of BB84 quantum key distribution. *Sci. Rep.* **5**, 16200; doi: 10.1038/srep16200 (2015).