Quantum Information Processing (2018) 17:228
https://doi.org/10.1007/s11128-018-1998-3

Unconditional security of a *K*-state quantum key distribution protocol

Dariusz Kurzyk[1] · **Łukasz Pawela**[1] · **Zbigniew Puchała**[1,2]

Received: 3 April 2018 / Accepted: 19 July 2018 / Published online: 26 July 2018

Abstract
Quantum key distribution protocols constitute an important part of quantum cryptography, where the security of sensitive information arises from the laws of physics. In this paper, we introduce a family of key distribution protocols which generalize the PBC00 protcol. We compare its key with the well-known protocols such as BB84, PBC00 and generation rate to the well-known protocols such as BB84, PBC0 and R04. We also state the security analysis of these protocols based on the entanglement distillation and CSS codes techniques.

Keywords Quantum key distribution · Quantum cryptography · Cryptographic protocols

1 Introduction

Quantum cryptography is a blooming field of scientific research, where quantum phenomena are applied to securing sensitive information. Usually, cryptographic systems are based on the key distribution mechanisms and security of the systems depends on computational complexity. The security of quantum cryptography arises from the laws of quantum physics. Scenarios of quantum key distribution (QKD) protocols are based on the assumption that secret key is shared by Alice and Bob. The first QKD protocol, BB84 [1], became a motivation for expanding research in this area. As a con-

✉ Łukasz Pawela
lpawela@iitis.pl

Dariusz Kurzyk
dkurzyk@iitis.pl

Zbigniew Puchała
zpuchala@iitis.pl

[1] Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, Bałtycka 5, 44-100 Gliwice, Poland

[2] Faculty of Physics, Astronomy and Applied Computer Science, Jagiellonian University, Łojasiewicza 11, 30-348 Kraków, Poland

sequence, Mayers in [2] proved the unconditional security of this protocol on a noisy channel against a general attack. Quantum entanglement and the violation of Bell's theorem were introduced to the BB84 protocol by Ekert [3]. Next, Bennett proposed a simple protocol B92 [4] based on two nonorthogonal states. Unconditional security analysis of this protocol was performed by Tamaki et al. in [5,6] and by Quan et al. in [7]. Subsequently, Phoenix et al. [8] introduced PBC00 protocol and they showed that key bits can be generated more efficiently by the usage of three mutually nonorthogonal states. Renes developed the key creation protocols R04 [9] for two-qubit-based spherical codes, which is a modified version of the PBC00 protocol. The R04 protocol allows one to use all conclusive events for key extraction. In [10], Boileau et al. proved the unconditional security of the trine spherical code QKD protocol, which concerns also to PBC00 and R04 protocols. The experimental realization of PBC00 and R04 protocols was proposed in [11] and [12]. New results referring to asymptotic analysis of three-state protocol can be found in [13].

In this paper, we propose a class of QKD protocols which generalize the PBC00 protocols. We perform the security analysis of this class using of techniques similar as in [5,10]. It means that the proposed protocol was considered as entanglement distillation protocol (EDP) [14,15]. Subsequently, similarly as in case of BB84 [16], CSS codes [17,18] were used to the security proof.

2 Defined state protocol

Our aim is to generalize the PBC00 protocol. We will achieve this in two steps. First generalize the well-known PBC00 protocol to an arbitrary number of states. Next, we will introduce modifications to the measurements used by both parties which allow us to obtain better key rates.

Let us introduce a class of QKD protocols, which generalize the PBC00 protocol [8]. Assume that Alice and Bob would like to share N secret bits b_i. Then, the protocol is as follows.

Protocol 1 (P1)

1. Alice and Bob share N pairs of maximally entangled two-qubit states $\rho_{AB} = |\phi^-\rangle\langle\phi^-|$, where $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.
2. She chooses K states $|\psi_k\rangle = \cos(a+\theta_k)|0\rangle + \sin(a+\theta_k)|1\rangle$, where $a \in [0, 2\pi)$ is a constant and $\theta_k = \frac{2k\pi}{K}$ for $k \in \{0, \ldots, K-1\}$. The states $|\psi_k\rangle$ are grouped into pairs $S_k = \{|\psi_k\rangle, |\psi_{k+1 \mod K}\rangle\}$.
3. Subsequently, Alice measures her parts of the states ρ_{AB} using the positive operator-valued measure (POVM) $\{\frac{2}{K}|\psi_k^\perp\rangle\langle\psi_k^\perp|\}_k$, where $|\psi_k^\perp\rangle$ is orthogonal to $|\psi_k\rangle$. Detection of the state $|\psi_{m_i}^\perp\rangle$ after measurement in the ith step is equivalent to sending a state $|\psi_{m_i}\rangle$ to Bob.
4. Alice chooses each key bit b_i randomly and calculates $r_i \in \{0, \ldots, K-1\}$ as $r_i = m_i + b_i \mod K$. This r_i determines the encoding base S_{r_i}.
5. Alice publicly announces when all of her measurements are done.

6. Bob prepares measurements described by the POVM $\{\frac{2}{K}|\psi_k^{\perp}\rangle\langle\psi_k^{\perp}|\}_k$ and measures his parts of the states ρ_{AB}. He announces when the measurements are done.
7. Alice sends sequences of values r_i to Bob.
8. Bob detects the state $|\psi_{j_i}^{\perp}\rangle$. If $j_i = r_i$, he decodes $b_i = 0$. If $j_i = r_i - 1 \mod K$, he decodes $b_i = 1$. In other cases, the events are regarded as inconclusive. These results are discarded.
9. Half of randomly chosen conclusive events are used in the estimation of a bit error rate. If the bit error rate is to high, then they abort the protocol.
10. In the end, they use a classical error correction and privacy amplification protocols.

Notice that for $K = 3$ and an appropriate choice of constant a, the above scenario is equivalent to the PBC00 protocol [8]. It can also be shown that protocols of this class achieve the highest key rate for $K = 3$. Note that for $K = 4$ the protocol becomes trivial as there are only two unique operators $|\psi_k\rangle\langle\psi_k|$. Hence, the potential eavesdropper knows exactly which measurements to perform.

3 An enhancement

Now we consider a modification of the above protocol. Steps 1–4 are the same as in the previous protocol.

Protocol 2 (P2)

5′. Alice publicly announces when all her measurements are done and she sends sequences of values r_i to Bob.
6′. For each r_i, Bob prepares an unambiguous measurement described by the POVM

$$\{\Pi_{r_i-1}, \Pi_{r_i}, \Pi_{\text{fill}}\} = \left\{ \frac{1}{\lambda}|\psi_{r_i}^{\perp}\rangle\langle\psi_{r_i}^{\perp}|, \frac{1}{\lambda}|\psi_{r_i+1 \bmod K}^{\perp}\rangle\langle\psi_{r_i+1 \bmod K}^{\perp}| \right. \\ \left. \mathbb{1}_2 - \frac{1}{\lambda}\left(|\psi_{r_i}^{\perp}\rangle\langle\psi_{r_i}^{\perp}| + |\psi_{r_i+1 \bmod K}^{\perp}\rangle\langle\psi_{r_i+1 \bmod K}^{\perp}|\right)\right\} \tag{1}$$

where $\lambda = \frac{\sqrt{2}}{2}\sqrt{\cos\frac{4\pi}{K} + 1} + 1 = 1 + |\cos(\frac{2\pi}{K})|$. The value λ is determined as a maximal eigenvalue of

$$|\tilde{\psi}_{r_i}\rangle\langle\tilde{\psi}_{r_i}| + |\tilde{\psi}_{r_i+1 \bmod K}\rangle\langle\tilde{\psi}_{r_i+1 \bmod K}|. \tag{2}$$

7′. This point is now redundant and can be omitted.

Steps 8, 9 and 10 are again the same as in the previous protocol. For $K = 3$, the characteristics of the protocols P1 and P2 are the same and are equivalent to the characteristics of the PBC00 protocol. In next section, we will show that we get higher key rate in the case of protocol P2 with $K = 5$ than the case of PBC00 protocol.

4 Security analysis

Similarly to [5,10,16], we consider an entanglement distillation protocol (EDP) [15] related to quantum error-correcting codes [16], which can be reduced to a QKD protocol equivalent to the above scheme. Lo and Chau shown similarities between QKD and EDP [15]. Notice that Alice and Bob share Bell state, which provides security from an eavesdropper. Lo and Chau proved that existence of eavesdropping or noise does not spoil of security of QKD protocol based on EDP [15]. Shor and Preskill used approach proposed by Lo and Chau for analysis of security proof based on CSS codes [16]. In contrast to classical linear error-correcting codes, quantum codes refer not only with bit errors, but also with phase errors. It can be supposed that in Lo-Chau protocol, Alice and Bob can use CSS codes able to correcting bit and phase errors. One of the advantage of CSS codes is fact that bit errors and phase errors are correctable separately. Similarly to [10], we prepare phase error estimation utilizing the Azuma's inequality [19].

Firstly, we transform the vectors $|\psi_i\rangle$ by the rotation operator $R(-\eta)$, where $R_y(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ and $\eta = \arccos(\langle\psi_1|\psi_0\rangle)/2 + \arctan\left(\frac{\langle\psi_0|1\rangle}{\langle\psi_0|0\rangle}\right)$. After this transformation, we get states $|\tilde{\psi}_i\rangle = R(-\eta)|\psi_i\rangle$, where $|\tilde{\psi}_0\rangle = \cos(\frac{\pi}{K})|0\rangle + \sin(\frac{\pi}{K})|1\rangle$ and $|\tilde{\psi}_1\rangle = \cos(-\frac{\pi}{K})|0\rangle + \sin(-\frac{\pi}{K})|1\rangle$. This transformation has no impact on the protocol, but is important in the security analysis. Assume that Alice prepares many pairs of qubits in the entangled state $|\psi\rangle = \frac{1}{\sqrt{2}}(|+\rangle|\tilde{\psi}_0\rangle + |-\rangle|\tilde{\psi}_1\rangle)$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and the basis $\{|+\rangle, |-\rangle\}$ will be denoted by $\pm$-basis. Next, she randomly chooses a string $r_i, r_i \in \{0, \ldots, K-1\}$ of length N and applies $R_y(\theta_{r_i})$ on the second qubit of every pair. After that, she sends qubits to Bob through a quantum channel. Alice announces the values of r_i. Next, Bob performs *local filtering operations* [20–22] $F = \frac{1}{\sqrt{2\lambda}}\Big((|\tilde{\psi}_0^{\perp}\rangle + |\tilde{\psi}_1^{\perp}\rangle)\langle 0| + (|\tilde{\psi}_0^{\perp}\rangle - |\tilde{\psi}_1^{\perp}\rangle)\langle 1|\Big)$ and operation $R_y(-\theta_{r_i})$ on the received qubits. Next, half of the states are used to determine the number of bit errors after application of $\pm$-basis measurements by Alice and Bob. If the number of errors is too high, then the protocol is aborted. Remaining qubits are used to distill Bell states by an EDP based on CSS codes. Alice and Bob perform $\pm$-basis measurements on Bell states to obtain a secret key.

Notice that $R_y(\theta_{r_i})|\tilde{\psi}_j\rangle = |\tilde{\psi}_{r_i+j \mod K}\rangle$ and Alice's operation related to measurement $\{\frac{1}{\lambda}|\tilde{\psi}_i^{\perp}\rangle\langle\tilde{\psi}_i^{\perp}|\}_i$ on her state are equivalent to $\pm$-basis measurement on the state $\big(\mathbb{1}_2 \otimes R_y(\theta_{r_i})\big)|\psi\rangle$. The filtering operations F, rotation operation $R_y(-\theta_{r_i})$ and $\pm$-basis measurement performed by Bob can by described by the following POVM

$$\begin{aligned} &\{R_y(\theta_{r_i})F^{\dagger}|+\rangle\langle+|FR_y(\theta_{r_i})^{\dagger}, \\ &R_y(\theta_{r_i})F^{\dagger}|-\rangle\langle-|FR_y(\theta_{r_i})^{\dagger}, \\ &R_y(\theta_{r_i})(\mathbb{1}_2 - F^{\dagger}F)R_y(\theta_{r_i})^{\dagger}\}. \end{aligned} \tag{3}$$

This measurement is equivalent to the POVM

$$\{\tilde{\Pi}_{r_i-1}, \tilde{\Pi}_{r_i}, \tilde{\Pi}_{\text{fill}}\} = \left\{ \frac{1}{\lambda}|\tilde{\psi}_{r_i}^{\perp}\rangle\langle\tilde{\psi}_{r_i}^{\perp}|, \frac{1}{\lambda}|\tilde{\psi}_{r_i+1 \bmod K}^{\perp}\rangle\langle\tilde{\psi}_{r_i+1 \bmod K}^{\perp}|, \right. \\ \left. \mathbb{1}_2 - \frac{1}{\lambda}(|\tilde{\psi}_{r_i}^{\perp}\rangle\langle\tilde{\psi}_{r_i}^{\perp}| + |\tilde{\psi}_{r_i+1 \bmod K}^{\perp}\rangle\langle\tilde{\psi}_{r_i+1 \bmod K}^{\perp}|) \right\}. \tag{4}$$

In [16], Shor and Preskill have shown that if the bound of estimations of bit and phase error decreases exponentially as N increases, then Eve's information on secret key is exponentially small. This approach was used to prove the unconditional security of the Bennet 1992 protocol, by Tamaki et al. [5], and the PBC00 and R04 protocols, by Boileau et al. [10]. These proofs were based on the usage of reduction to an entanglement distillation protocol initiated by a local filtering process. Subsequently, we will prove the security of the above entanglement distillation protocol in the same manner as in [5,10,16].

Assume that $\{p_b^{(i)}\}_{i=1}^N$ and $\{p_p^{(i)}\}_{i=1}^N$ are sets of probabilities of a bit error and a phase error, respectively, on the ith pair after Alice and Bob have done the same measurements on $i-1$ previous pairs. Thus, $p_b^{(i)}$ and $p_p^{(i)}$ depend on previous results. Moreover, we introduce e_b and e_p as rates of bit error and phase error in all conclusive results, respectively.

Estimations of bit and phase error rates will be performed by the use of Azuma's inequality [19] as in [10].

Theorem 1 ([19]) *Let* $\{X_i : i = 0, 1, \dots\}$ *be a martingale sequence and for each* k *it holds that* $|X_k - X_{k-1}| \leq c_k$. *Then for all integers* $N \geq 0$ *and real numbers* $\gamma \geq 0$

$$P(|X_N - X_0| \geq \gamma) \leq 2^{-\frac{\gamma^2}{2\sum_{k=1}^N c_k^2}}. \tag{5}$$

Notice that for $c_k = 1$ we get

$$P(|X_N - X_0| \geq \gamma) \leq 2^{-\frac{\gamma^2}{2N}}. \tag{6}$$

As a result of the Azuma's inequality, Ce_b is exponentially close to e_p ($Ce_b = e_p$) for particular constant C, if $Cp_b^{(i)} = p_p^{(i)}$ is satisfied for all i. Assume that Eve can perform any coherent attack $E^{(i)}$ on qubits sent by Alice such that $\sum_i E^{(i)\dagger}E^{(i)} \leq \mathbb{1}$. The general equation for the ith state can be described by a mixed state

$$\rho^{(i)} = \frac{1}{K}\sum_{k=0}^{K} |\phi_k^{(i)}\rangle\langle\phi_k^{(i)}|, \tag{7}$$

where

$$|\phi_k^{(i)}\rangle = \mathbb{1}_A \otimes \left(FR(-\theta_k)E^{(i)}R(\theta_k)\right)|\psi\rangle. \tag{8}$$

Let us introduce the notation $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|+\rangle|+\rangle \pm |-\rangle|-\rangle)$ and $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|+\rangle|-\rangle \pm |-\rangle|+\rangle)$. Since the probability of sharing by Alice and Bob a Bell state $|\Phi^{+}\rangle$ is equal to the probabilities of a bit error $p_b^{(i)}$ and phase error $p_p^{(i)}$ on the ith, respectively, thus

$$\begin{aligned} p_b^{(i)} &= \frac{1}{Z^{(i)}}\left(\langle\Psi^{+}|\rho^{(i)}|\Psi^{+}\rangle + \langle\Psi_Z^{-}|\rho^{(i)}|\Psi^{-}\rangle\right) \\ p_p^{(i)} &= \frac{1}{Z^{(i)}}\left(\langle\Phi^{-}|\rho^{(i)}|\Phi^{-}\rangle + \langle\Psi^{-}|\rho^{(i)}|\Psi^{-}\rangle\right), \end{aligned} \tag{9}$$

where

$$\begin{aligned} Z^{(i)} = \Big(&\langle\Psi^{+}|\rho^{(i)}|\Psi^{+}\rangle + \langle\Psi^{-}|\rho^{(i)}|\Psi^{-}\rangle \\ &+ \langle\Phi^{+}|\rho^{(i)}|\Phi^{+}\rangle + \langle\Phi^{-}|\rho^{(i)}|\Phi^{-}\rangle\Big). \end{aligned} \tag{10}$$

It can be checked that

$$C = \frac{p_p^{(i)}}{p_b^{(i)}} = 1 + |\langle\psi_1|\psi_0\rangle|^2 = 1 + \cos^2\left(\frac{2\pi}{K}\right). \tag{11}$$

Similarly as in [10], we calculate the key rate S from the following formula

$$S = p_c(e_b)\left(1 - h(e_b) - h(e_p)\right), \tag{12}$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ and $p_c(e_b)$ is the probability of a conclusive result. Since $Ce_b = e_p$, we get

$$S = p_c(e_b)\big(1 - h(e_b) - h(Ce_b)\big). \tag{13}$$

Notice that for a bit value $b = 0$ we get outcome probabilities
$\{0, \frac{1}{\lambda}|\langle\tilde{\psi}^{\perp}_{r_i+1 \bmod K}|\tilde{\psi}_{r_i}\rangle|^2, 1 - \frac{1}{\lambda}|\langle\tilde{\psi}^{\perp}_{r_i+1 \bmod K}|\tilde{\psi}_{r_i}\rangle|^2\}$, and for $b = 1$, we get
$\{\frac{1}{\lambda}|\langle\tilde{\psi}^{\perp}_{r_i}|\tilde{\psi}_{r_i+1 \bmod K}\rangle|^2, 0, 1 - \frac{1}{\lambda}|\langle\tilde{\psi}^{\perp}_{r_i}|\tilde{\psi}_{r_i+1 \bmod K}\rangle|^2\}$. Hence, it can be checked that $|\langle\tilde{\psi}^{\perp}_{r_i+1 \bmod K}|\tilde{\psi}_{r_i}\rangle|^2 = |\langle\tilde{\psi}^{\perp}_{r_i}|\tilde{\psi}_{r_i+1 \bmod K}\rangle|^2 = \sin^2\left(\frac{2\pi}{K}\right)$. Thus, the probability of a conclusive result, with the assumption that $e_b = 0$, is equal to

$$p_c(0) = \frac{\sin^2\left(\frac{2\pi}{K}\right)}{1 + \left|\cos\left(\frac{2\pi}{K}\right)\right|}, \tag{14}$$

which can be simplified to $p_c(0) = 2\sin^2(\frac{\pi}{K})$ for $K > 3$. Note that $K = 4$ we have $p_c(0) = 1$. This is to be expected for a trivial protocol as this corresponds to sending the key over a public channel.

Generally, p_c can be expressed as

$$p_c(e_b) = \frac{\sin^2\left(\frac{2\pi}{K}\right)}{\lambda\left(1 - 2e_b\cos^2\left(\frac{2\pi}{K}\right)\right)}, \tag{15}$$

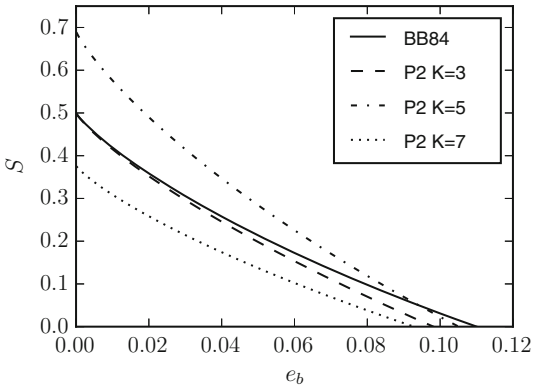

Fig. 1 Comparison of key rates depending on e_b for different setups of the P2 protocol. Notice that for $K = 5$ we get the best key rates. For $K = 7$, these drop below the values of obtained for $K = 3$. We also show the key rates of the BB84 protocol for comparison

which was derived in "Appendix A." Notice that for $K = 3$ Eq. (15) is reduced to $p_c(e_b) = \frac{1}{2-e_b}$, which corresponds to probability of conclusive results in PBC00 protocol.

In the case of BB84 protocol, bit error rate is equal to phase error rate. Thus, $C = 1$ and $p_c(e_b) = \frac{1}{2}$. In the case of PBC00, $C = \frac{5}{4}$ and $p_c(e_b) = \frac{1}{2-e_b}$. From Eq. (13), we get that $e_b \approx 11.0\%$ for BB84 protocol and $e_b \approx 9.81\%$ for PBC00 protocol. It can be checked that an interesting case is for $K = 5$, where $C = \frac{1}{8}(11 - \sqrt{5})$ and $e_b \approx 10.5\%$. Comparison of proposed protocol with BB84 and PBC00 protocols is shown in Fig. 1. As we can see, the best key rate is for $K = 5$. We plot the key rates for K up to 7. For higher K, the key rates decrease with K and are bounded from above by $2\sin^2\left(\frac{\pi}{K}\right)$.

The fact that the highest key rate is obtained for $K = 5$ can be explained as follows. The POVM elements are projection operators corresponding to vectors evenly distributed on a circle. For $K = 3$, we get that the angle between the vectors is $\frac{2}{3}\pi$, and for $K = 5$, we get angle of $\frac{2}{5}\pi$. The latter is closer to $\frac{\pi}{2}$; hence, the probability of distinguishing the vectors is higher which yields a higher key rate. As discussed earlier, the case $K = 4$ reduces to a trivial protocol.

5 Conclusion

In this paper, we have introduced a new class of quantum key distribution protocols. We have also provided unconditional security analysis of this protocol. We have shown that there exists 5-state protocol with reasonably high key rate for small bit-flip error rates.

Acknowledgements The authors acknowledge the support by the Polish National Science Center under the Project Number 2015/17/B/ST6/01872.

Appendix A: Probability of conclusive events

Notice that if Alice performs $|\psi_i^{\perp}\rangle$, where $|\psi_i\rangle \in S_r$, $i = r$ or $i = r + b \mod K$ and Bob chooses $|\psi_i^{\perp}\rangle$, then it corresponds to an error. In the case when Bob chooses a state which corresponds to S_r but is not orthogonal to Alice's state, then Bob can correctly conclude the state $|\psi_i\rangle$.

Let n_g, n_e, n_i denote the numbers of good conclusive, error conclusive and inconclusive events, respectively. Besides that, let $n_t = n_g + n_e + n_i$ and thus $1 = \frac{n_g}{n_t} + \frac{n_e}{n_t} + \frac{n_i}{n_t}$. Assume that after Alice sent r to Bob, Bob performs measurement described by POVM

$$\begin{aligned}\{\Pi_r, \Pi_{r+1}, \Pi_{\text{fill}}\} \quad &= \left\{\tfrac{1}{\lambda}|\psi_r^{\perp}\rangle\langle\psi_r^{\perp}|, \tfrac{1}{\lambda}|\psi_{r+1 \bmod K}^{\perp}\rangle\langle\psi_{r+1 \bmod K}^{\perp}|,\right.\\ &\left. \mathbb{1}_2 - \tfrac{1}{\lambda}(|\psi_r^{\perp}\rangle\langle\psi_r^{\perp}| + |\psi_{r+1 \bmod K}^{\perp}\rangle\langle\psi_{r+1 \bmod K}^{\perp}|)\right\}. \quad (16)\end{aligned}$$

Now, we suppose that $b = 0$ and Eve simulates a noisy channel, where state $|\psi_r\rangle\langle\psi_r|$ evolves as $\rho_B = (1-p)|\psi_r\rangle\langle\psi_r| + \frac{p}{2}\mathbb{1}_2$. Next, Bob performs measurement and receives measurement outcomes with probabilities $\{\mathrm{Tr}\Pi_r\rho_B = \frac{p}{2\lambda}, \mathrm{Tr}\Pi_{r+1}\rho_B = \frac{p}{2\lambda} + \frac{1-p}{\lambda}\sin^2(\frac{2\pi}{K}), \mathrm{Tr}\Pi_{\text{fill}}\rho_b = 1 - \frac{p}{\lambda} - \frac{1-p}{\lambda}\sin^2(\frac{2\pi}{K}\}$.

A bit error rate e_b is defined as the rate of error in conclusive results. Hence

$$e_b = \frac{n_e}{n_e + n_g} \quad \text{and} \quad n_e = \frac{e_b}{1-e_b} n_g. \tag{17}$$

Notice that error e_b can be estimated as

$$e_b = \frac{\mathrm{Tr}\Pi_{r+1}\rho_B}{\mathrm{Tr}\Pi_{r+1}\rho_B + \Pi_{\text{fill}}\rho_b} = \frac{p}{2(1-p)\sin^2\left(\frac{2\pi}{K}\right) + 2p}. \tag{18}$$

Now, let us determine a ratio

$$\begin{aligned} D = \frac{\mathrm{Tr}\Pi_{r+1}\rho_B}{\mathrm{Tr}\Pi_{\text{fill}}\rho_B} &= \frac{2(1-p)\sin^2\left(\frac{2\pi}{K}\right) + p}{2\lambda - 2(1-p)\sin^2\left(\frac{2\pi}{K}\right) - 2p} \\ &= \frac{2(1-e_b)\sin^2\left(\frac{2\pi}{K}\right)}{2\lambda\left(1 - 2e_b\cos^2\left(\frac{2\pi}{K}\right)\right) - 2\sin^2\left(\frac{2\pi}{K}\right)}. \end{aligned} \tag{19}$$

From the central limit theorem and the above calculation we get

$$\frac{n_g}{n_t} = \frac{Dn_i}{n_t} + O(\epsilon). \tag{20}$$

Continuing we obtain

$$\begin{aligned} 1 &= \frac{n_g}{n_t} + \frac{n_e}{n_t} + \frac{n_i}{n_t} = \frac{n_g}{n_t} + \frac{e_b}{1-e_b}\frac{n_g}{n_t} + \frac{n_i}{n_t} \\ &\approx \frac{Dn_i}{n_t} + \frac{e_b}{1-e_b}\frac{Dn_i}{n_t} + \frac{n_i}{n_t} \\ &\approx \frac{D+1-e_b}{1-e_b}\frac{n_i}{n_t} \end{aligned} \tag{21}$$

and

$$p_c = 1 - \frac{n_i}{n_t} = \frac{D}{D+1-e_b} = \frac{\sin^2\left(\frac{2\pi}{K}\right)}{\lambda\left(1-2e_b\cos^2\left(\frac{2\pi}{K}\right)\right)}. \tag{22}$$

References

1. Bennett, C.H., Brassard, G.: An update on quantum cryptography. In: Crypto, vol. 84, pp. 475–480 Springer (1984)
2. Mayers, D.: Quantum key distribution and string oblivious transfer in noisy channels. In: Advances in Cryptology—Proceedings of Crypto96, pp. 343–357. Springer (1996)
3. Ekert, A.K.: Quantum cryptography based on bell's theorem. Phys. Rev. Lett. **67**(6), 661 (1991)
4. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121 (1992)
5. Tamaki, K., Koashi, M., Imoto, N.: Unconditionally secure key distribution based on two nonorthogonal states. Phys. Rev. Lett. **90**(16), 167904 (2003)
6. Tamaki, K., Lütkenhaus, N.: Unconditional security of the bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. Phys. Rev. A **69**(3), 032316 (2004)
7. Quan, Z., Chaojing, T.: Simple proof of the unconditional security of the bennett 1992 quantum key distribution protocol. Phys. Rev. A **65**(6), 062301 (2002)
8. Phoenix, S.J.D., Barnett, S.M., Chefles, A.: Three-state quantum cryptography. J. Mod. Opt. **47**(2–3), 507–516 (2000)
9. Renes, J.M.: Spherical-code key-distribution protocols for qubits. Phys. Rev. A **70**(5), 052314 (2004)
10. Boileau, J.-C., Tamaki, K., Batuwantudawe, J., Laflamme, R., Renes, J.M.: Unconditional security of a three state quantum key distribution protocol. Phys. Rev. Lett. **94**(4), 040503 (2005)
11. Senekane, M., Mafu, M., Petruccione, F.: Six-state symmetric quantum key distribution protocol. J. Quantum Inf. Sci. **5**(02), 33 (2015)
12. Schiavon, M., Vallone, G., Villoresi, P.: Experimental realization of equiangular three-state quantum key distribution. Sci. Rep. **6**, 30089 (2016)
13. Krawec, W.O.: Asymptotic analysis of a three state quantum cryptographic protocol. In: 2016 IEEE International Symposium on Information Theory (ISIT), pp. 2489–2493. IEEE (2016)
14. Bennett, C.H., DiVincenzo, D.P., Smolin, J.A., Wootters, W.K.: Mixed-state entanglement and quantum error correction. Phys. Rev. A **54**(5), 3824 (1996)
15. Lo, H.-K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050–2056 (1999)
16. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441 (2000)
17. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. Phys. Rev. A **54**(2), 1098 (1996)
18. Steane, A.: Multiple-particle interference and quantum error correction. Proc. R. Soc. Lond. Math. Phys. Eng. Sci. **452**, 2551–2577 (1996)
19. Azuma, K.: Weighted sums of certain dependent random variables. Tohoku Math. J. Second Ser. **19**(3), 357–367 (1967)

20. Gisin, N.: Hidden quantum nonlocality revealed by local filters. Phys. Lett. A **210**(3), 151–156 (1996)
21. Bennett, C.H., Bernstein, H.J., Popescu, S., Schumacher, B.: Concentrating partial entanglement by local operations. Phys. Rev. A **53**(4), 2046 (1996)
22. Horodecki, M., Horodecki, P., Horodecki, R.: Inseparable two spin-$\frac{1}{2}$ density matrices can be distilled to a singlet form. Phys. Rev. Lett. **78**(4), 574 (1997)