Finite-size key security of Phoenix-Barnett-Chefles 2000 quantum-key-distribution protocol

Mhlambululi Mafu[1], **Kevin Garapo**[1] **and Francesco Petruccione** [1,2]

[1] Centre for Quantum Technology, School of Chemistry and Physics, University of KwaZulu-Natal, P/Bag X54001 Durban 4000, South Africa

[2] National Institute for Theoretical Physics (NITheP), KwaZulu-Natal, South Africa

E-mail: mafum@ukzn.ac.za

Abstract. A post-selection technique was introduced by Christandl, König and Renner [*Phys Rev. Lett.* 102, 020504 (2009)] in order to simplify the security of quantum key distribution schemes, yet it has not been worked out in detail for any specific and realistic protocol. Here, we demonstrate how it can be applied to study the security of the Phoenix-Barnett-Chefles 2000 trine state (PBC00) protocol, a symmetric version of the Bennett 1992 (B92) protocol.

1. Introduction

Quantum key distribution (QKD) enables secure real-time distribution of a cryptographic key between two parties, Alice and Bob, who are connected by a quantum channel and an authenticated classical channel in the presence of a competent malicious party, an eavesdropper called Eve [1]. This technique is based on two laws of quantum mechanics, namely the uncertainty principle and the no-cloning theorem [1]. The first, and most established, operable QKD protocol, BB84, was proposed by Bennett and Brassard [2] in 1984, basing on Wiesner's idea of conjugate coding [3]. In 1991, Ekert [4] extended the idea by introducing quantum entanglement and the violation of Bell's theorem [1]. Ever since, several protocols have been invented by both theorists and experimentalists. These include: Bennett 1992 (B92) [5], six state [6], the Scarani-Acín-Ribordy-Gisin 2004 (SARG04) [7], the differential-phase shift (DPS) [8], the coherent-one-way (COW) [9] and the Phoenix, Barnett and Chefles 2000 (PBC00) protocol [10]. The PBC00 protocol is based on the B92 protocol and the main difference between the two is that the latter uses two states whilst the former uses three states. Consequently, the PBC00 protocol is more symmetrical (in the sense that either Alice or Bob, but not both, can declare unused observables) and shows lower qubit losses than the B92 protocol.

Since the first unconditional security proof by Mayers [11], various techniques for proving the security of QKD protocols have been developed [12]. An unconditional security proof is a proof that considers an unbounded adversary. The construction of security proofs generally depend on the steps of the protocol and also on their practical implementation. For example, the unconditional security proof for the BB84 based protocols have long since been introduced [13]. This is because they share a common property of being symmetrical. However, the security proofs for the class of distributed-phase-reference (which consist of DPS and COW) protocols

still remain unknown [12], mainly because their construction and encoding deviates from the usual symmetry that exists in BB84-type protocols [8]. The study of security proofs of QKD protocols in the asymptotic key length has been studied in several papers [14, 15, 16, 17, 18, 19].

The unconditional security proof of the PBC00 protocol independent of the channel's qubit loss rate loss has been given in Ref [20]. The security proof was done by transforming the protocol to a secure QKD protocol based on the entanglement distillation protocol initiated by state rotations and a local filtering operation, followed by error correction. In this paper we compute the secret key rates against coherent attacks for the PBC00 protocol by using the post-selection technique when given a finite amount of resources.

In order to prove security against coherent attacks, one can use either the de Finetti theorem [21] or the post-selection technique [22]. The former technique was developed by Renner where one uses the fact that a permutation invariant state is close to an independent and identically distributed (i.i.d) state [23]. The latter technique gives a way to bound the diamond distance between two maps from a quantity evaluated for a very specific quantum state, called a "de Finetti state". The two techniques are independent, therefore one can use either of them to prove security of a protocol provided the protocol is permutation invariant [22]. However, it has been shown that the post-selection technique gives better bounds than the de Finetti theorem [16], so one can always proceed by using the post-selection technique. Moreover, the symmetry, hence permutation invariance that exists in the PBC00 protocol enables us to directly apply the post-selection technique.

2. PBC00 QKD protocol

The PBC00 protocol proceeds as follows:

Preparation and Measurement. Alice prepares randomly with equal probability each qubit in one of the mutually non-orthogonal states $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ and encodes her bit on the states as in the original B92 protocol [24]. These states are defined as $|\psi_1\rangle \equiv \frac{1}{2}|0_x\rangle + \frac{\sqrt{3}}{2}|1_x\rangle, |\psi_2\rangle \equiv \frac{1}{2}|0_x\rangle - \frac{\sqrt{3}}{2}|1_x\rangle$ and $|\psi_3\rangle \equiv |0_x\rangle$, where $\{|0_x\rangle, |1_x\rangle\}$ is the X basis of a qubit state. The Z basis is defined by $\{|j_z\rangle \equiv [|0_x\rangle + (-1)^j|1_x\rangle]/\sqrt{2}\}$ where $(j = 0, 1)$. She creates a large trit string r and a large bit string b of the same length N. For each r_i, the ith trit value of the trit string r, she chooses the set $\{|\psi_1\rangle, |\psi_2\rangle\}$ (if r_i=0), $\{|\psi_2\rangle, |\psi_3\rangle\}$ (if r_i=1), and $\{|\psi_3\rangle, |\psi_1\rangle\}$ (if r_i=2). If the ith bit value b_i is 0, she prepares the first state of the chosen pair, however if the bit is 1, she prepares the second state. Alice sends all the prepared states to Bob.

On the receiving side, Bob performs measurements on each qubit he receives. These measurements are described by the POVM

$$\{\frac{2}{3}|\bar{\psi_1}\rangle\langle\bar{\psi_1}|, \frac{2}{3}|\bar{\psi_2}\rangle\langle\bar{\psi_2}|, \frac{2}{3}|\bar{\psi_3}\rangle\langle\bar{\psi_3}|\}. \tag{1}$$

These states can be defined as $|\bar{\psi_1}\rangle = \frac{\sqrt{3}}{2}|0_x\rangle - \frac{1}{2}|1_x\rangle, |\bar{\psi_2}\rangle = \frac{\sqrt{3}}{2}|0_x\rangle + \frac{1}{2}|1_x\rangle$ and $|\bar{\psi_3}\rangle = |1_x\rangle$ and are orthogonal to $|\psi_1\rangle, |\psi_2\rangle$ and $|\psi_3\rangle$ respectively.

Sifting. In this sifting step, both parties agree which signals to discard. Bob announces when all his measurements are done, and Alice in turn announces the trit string r. Bob regards the i^{th} measurement outcome $|\bar{\psi_1}\rangle$ (if $r_i = 0$), $|\bar{\psi_2}\rangle$ (if $r_i = 1$), and $|\bar{\psi_3}\rangle$ (if $r_i = 2$) as the bit value 0. Bob also considers $|\bar{\psi_2}\rangle$ (if $r_i = 0$), $|\bar{\psi_3}\rangle$ (if $r_i = 1$), and $|\bar{\psi_1}\rangle$ (if $r_i = 2$) as the bit value 1. All other events are considered as inconclusive and they discard the data. Bob announces whether his measurement outcome is inconclusive or not. Alice and Bob keep the data when Bob's outcome is conclusive, discarding the rest.

Parameter estimation. The role of parameter estimation is to decide whether the input given to the protocol can be used to distill a secret key. On the conclusive measurements, Alice randomly chooses chooses $m < N$ samples as test bits in order to estimate the Quantum Bit Error Rate (QBER) on the code bits, and announces her selection to Bob. If the error rate is small, they use the post-processing methods to extract the key otherwise if the error rate is too high Alice and Bob abort the protocol. If the statistics λ_m are obtained by measuring m samples of ρ_{AB} according to a POVM with d possible outcomes and if $\lambda_\infty(\rho_{AB})$ denotes the perfect statistics in the limit of infinite measurements, then for any state ρ_{AB}

$$\Gamma_\xi := \{\rho_{AB} : ||\lambda_m - \lambda_\infty(\rho_{AB})|| \leq \xi(\varepsilon_{\mathrm{PE},m_i})\}. \tag{2}$$

Γ_ξ is a set of states from which a key is extracted with a non-negligible probability. By the law of large numbers [23]

$$\xi(\varepsilon_{\mathrm{PE},m_i}) := \sqrt{\frac{\ln(1/\varepsilon_{\mathrm{PE}}) + 2\ln(m+1)}{2m}}. \tag{3}$$

where $\varepsilon_{\mathrm{PE},m_i}$ is the measured QBER in the direction $|\psi_1\rangle, |\psi_2\rangle$ and $|\psi_3\rangle$.

Error correction. In this step Alice and Bob apply a one-way error correction protocol by using authenticated classical communication channel to correct their strings. As result they will exchange L_{EC} bits on the channel and is given as

$$L_{\mathrm{EC}} = f_{\mathrm{EC}} n h(Q) + \log_2\left(\frac{2}{\varepsilon_{\mathrm{EC}}}\right), \tag{4}$$

where n is the length of the raw key, f_{EC} is a constant larger than 1 which represents a deviation of the real protocol from the asymptotic one, $h(Q) = -Q\log_2 Q - (1-Q)\log_2(1-Q)$ is the binary Shannon entropy and Q is the QBER and $\varepsilon_{\mathrm{EC}}$ is the error in error correction step.

Privacy amplification. In this step, the quantity of the correct information which the eavesdropper may have obtained about Alice's and Bob's reference raw key is minimized by the use of a two-universal hash function resulting in a string called a key [23].

3. Security against collective attacks

The PBC00 protocol belongs to the class of prepare and measure schemes. It employs polarization-encoded qubits to transmit information. This simply involves a sequential exchange of n signals. Based on that, Alice and Bob's systems can be described by an n-partite density operator which is permutation invariant. This allows us to analyze the protocol based on the fact that it consists of states which are independent and identical copies of each other. More formally, the states $|\psi_1\rangle$, $|\psi_2\rangle$ and $|\psi_3\rangle$ all occur with the same probability.

The aim of the eavesdropper is to extract as much classical information as possible from the strings that are held by Alice and Bob. In the PBC00 protocol, the probability that Eve maximizes her probability of correctly distinguishing between the exchanged states is expressed as $P_D = \sum_i \mathcal{X}_i P_{(i,i)}$, where P_D is the discrimination probability, $\mathcal{X}_i$ represents the a priori probability of the state $|i\rangle$ and $P_{(i,i)}$ denotes the probability that the state $|i\rangle$ is sent and that the Eve's measurement reveals the result i. For symmetric states, the maximum discrimination probability is equal to $P_D^{\max} = 2/3$. Based on this probability, without losing generality the number of states that can be unambiguously discriminated satisfies the inequality $N \leq \frac{2}{3}\binom{n+d-1}{n}$, where d is the photon Hilbert space i.e., d=2 for the PBC00 protocol. This gives us the necessary condition for unambiguous discrimination between N states each spanning a d-dimensional space when given n-copies of the state. The dimension of the symmetric subspace, $g_{n,d}$ can be expressed

as $g_{n,d} = \frac{2}{3}\binom{n+d-1}{n} \leq \frac{2}{3}(n+1)^{d-1}$. Since the PBC00 protocol uses symmetric encoding as in the BB84 protocol, it is then possible to parametrize the most general attacks. This leads to the unconditional security. The expression for the secret key rate $r_{N,\mathrm{col}}$ against collective attacks is written as

$$r_N = r_{N,\mathrm{col}} - \frac{2(d^4-1)\log_2(N+1)}{N}. \tag{5}$$

The bound for collective attacks for the PBC00 protocol is expressed as

$$\varepsilon \leq \frac{2}{3} \cdot 2^{-c\delta^2 N + (d^4-1)\log_2(N+1)} \tag{6}$$

and is calculated via the total security parameter ε defined later in (13), where c for $(c \geq 0)$ is the cost of reducing the key size by fraction δ [22].

4. Finite key analysis

Scarani and Renner have provided a general security formula to calculate the lower bound on the secure key rate of the BB84 protocol [14]. This has been followed by the derivation of many bounds for different protocols based on the BB84 encoding. In the same spirit, we use this intuition of finite size key analysis to derive the upper bound for the secure key rate against collective attacks for the PBC00 protocol.

Let ρ_{KE} be the quantum state that describes the classical key K of length ℓ distilled at the end of the run of the QKD protocol. Then for any $\varepsilon \geq 0$, a final key K is said to be ε-secure with respect to an adversary Eve if the key ρ_{KE} satisfies

$$\min_{\rho_E} ||\rho_{KE} - \tau_K \otimes \rho_E||_1 \leq \varepsilon, \tag{7}$$

where $||\cdot||_1$ is the trace distance, $\rho_{KE} = \sum_{k\in\mathcal{K}} P_k(k)|k\rangle\langle k| \otimes \rho_E^k$ where P_k is the probability distribution of the key K and $\{|k\rangle\}_{k\in\mathcal{K}}$ is an orthonormal basis of some Hilbert space $\mathcal{H}_k$, $\tau_K = \sum_{k\in\mathcal{K}} P_k \frac{1}{|K|}|k\rangle\langle k|$ is a fully mixed state on $\mathcal{H}_k$, ρ_E is the state held by an eavesdropper [23]. The parameter ε represents the maximum failure probability of the key extraction procedure. Therefore, the classical key K is indistinguishable from a random and uniform key with probability $1-\varepsilon$.

In order to arrive at our security bounds for the PBC00 protocol, we follow closely the definitions found in Ref. [23] and the formalism in Ref. [14]. If $\mathcal{H}$ denotes a finite-dimensional Hilbert space and $\mathcal{P}(\mathcal{H})$ is the set of positive semidefinite operators on $\mathcal{H}$ then the set $\mathcal{S}(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) : \mathrm{tr}\rho = 1\}$ represents normalized states and the set $\mathcal{S}_{\leq}(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) : \mathrm{tr}\rho \leq 1\}$ represents the set of sub-normalized states on the Hilbert space. Let $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$ and $\sigma_B \in \mathcal{S}(\mathcal{H}_B)$, then the min-entropy of A conditioned on B of the state ρ_{AB} relative to σ_B is defined as

$$H_{\min}(A|B)_{\rho|\sigma} := \max_{\sigma} \sup\{\lambda \in \mathbb{R} : \rho_{AB} \leq 2^{-\lambda}\mathbb{1}_A \otimes \sigma_B\}, \tag{8}$$

where the maximum is taken over the states $\sigma_B \in \mathcal{S}(\mathcal{H}_B)$. Furthermore we define,

$$H_{\min}(A|B)_{\rho} := \max_{\sigma_B \in \mathcal{S}(\mathcal{H}_B)} H_{\min}(A|B)_{\rho|\sigma}. \tag{9}$$

For some $\varepsilon \geq 0$, it has been found that the achievable length of secret key can be expressed as [25]

$$\ell \leq H_{\min}^{\bar{\varepsilon}}(X^n|E^n) - L_{\mathrm{EC}} - 2\log_2(1/\varepsilon), \tag{10}$$

where $\bar{\varepsilon} = (\varepsilon/8)^2$ is the smoothing parameter. In above expression, $H_{\min}^{\bar{\varepsilon}}(X^n|E^n)$ gives the amount of a key that can be extracted from a string X when given E, the uncertainty of the

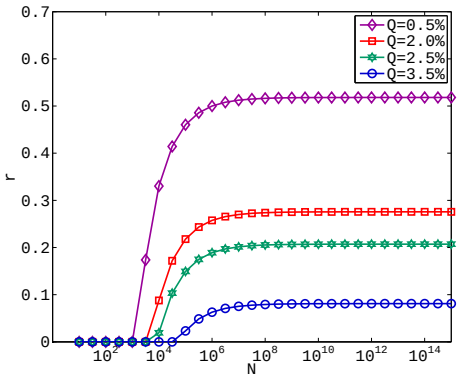

Figure 1. (Color online) Upper bound on the secret key fraction, r, for the finite PBC00 protocol as a function of the exchanged quantum signals N for bit error rates Q= 0.5%, 2%, 2.5%, 3.5%, $\varepsilon = 10^{-5}$ and $\varepsilon_{\rm EC} = 10^{-10}$.

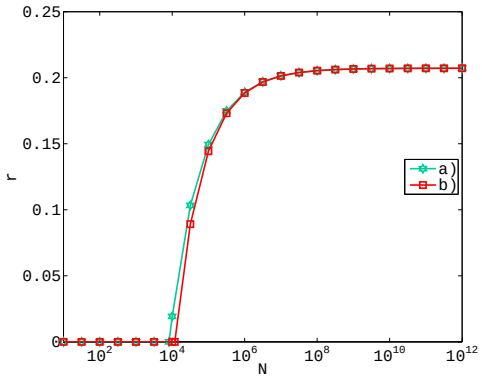

Figure 2. (Color online) Upper bound on the secret key fraction, r, for the finite PBC00 protocol as a function of the exchanged quantum signals N for bit error rate Q= 2.5%, $\varepsilon = 10^{-5}$, $\varepsilon_{\rm EC} = 10^{-10}$ for (a) collective attacks (b) post-selection technique.

adversary about X measured by using the smooth min-entropies. The smooth min-entropy of the state shared between Alice and the eavesdropper is lower bounded as

$$H_{\min}^{\bar{\varepsilon}}(X^n|E^n) \geq n(\min_{\sigma_{XE}\in\Gamma} H(X|E) - \triangle), \tag{11}$$

where $\triangle = (2\log_2 d + 3)\sqrt{[\log_2(2/\bar{\varepsilon})]/n}$. For a finite number of signals, the achievable secure key rate was derived to be [14]

$$r = \frac{n}{N}\left[\min_{\sigma_{XE}\in\Gamma} H(X|E) + \triangle(n) - L_{\rm EC}\right] + \frac{2}{N}\log_2(2\varepsilon_{\rm PA}). \tag{12}$$

The total security parameter, ε of a QKD scheme depends on the sum of probabilities of failures of the classical post-processing protocols which can be written as

$$\varepsilon = \bar{\varepsilon} + \varepsilon_{\rm PA} + \varepsilon_{\rm EC} + \varepsilon_{\rm PE}, \tag{13}$$

where $\bar{\varepsilon}$ denotes the error in the smooth min-entropy. In the PBC00 protocol, the secret key rate is obtained by measuring both the bit (e_1) and phase error (e_2) rates. The secret key rate for the bit error rate and the phase error rate is expressed as $p_c[1 - h(e_1) - h(e_2)]$, where p_c is the probability of the conclusive outcome. It has been found that the protocol is secure for a bit error rate of up to 9.81%. For an asymptotic formula $e_1 = e_2 = Q$, the lower bound for the protocol can be expressed as

$$H(X|E) = p_c[1 - h(Q) - h(\frac{5}{4}Q)], \tag{14}$$

where $H(X|E)$ is evaluated by using the QBER from the parameter estimation step.

In figure 1, we show the variation of the secret key rate r, with the number of signals N, which Alice sends to Bob when given a finite amount of resources. We found that the minimum number of signals required in order to extract a reasonable amount of secret key compares with

those of the BB84 protocol [14]. In figure 2, we show the variation of the secret key rate r, with the number of signals N for bit error $Q = 2.5\%$. In this figure, it can be observed that the post-selection technique gives optimal bounds when a finite amount of signals are used. Therefore, for a large number of signals the optimal attack is close to a collective attack. This shows that this technique is a powerful tool which can be considered in simplifying security proofs and also leads to improved key rates.

5. Conclusion

We have shown how one can apply the finite-key analysis formalism and the results of the post-selection technique in order to find the secret key rates for finite amount of resources. We have shown that the secret key rate largely depends on the number of signals sent. In particular, reasonable key rates are obtained for $N \approx 10^5$-10^6 signals. We have also shown that the post-selection technique leads to optimal security bounds for the PBC00 protocol. These results also appear in the longer version of our paper in Ref [26]. Therefore, in the absence of bounds for collective attacks one can appeal to the bounds given by the post-selection technique. These results can be applied to other protocols which are symmetric as well. This study has demonstrated the feasibility of applying the post-selection technique to the PBC00 QKD protocol, which is a specific and realistic protocol.

Acknowledgments

This work is based on research supported by the South African Research Chair Initiative of the Department of Science and Technology and National Research Foundation.

References

[1] Scarani V, Bechmann-Pasquinucci H, Cerf N, Dušek M, Lütkenhaus N and Peev M 2009 *Reviews of Modern Physics* **81** 1301–1350 ISSN 1539-0756

[2] Bennett C, Brassard G *et al.* 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* vol 175 (Bangalore, India)

[3] Wiesner S 1983 *ACM Sigact News* **15** 78–88

[4] Ekert A 1991 *Physical Review Letters* **67** 661–663

[5] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121–3124

[6] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018–3021

[7] Scarani V, Acín A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901

[8] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902

[9] Stucki D, Fasel S, Gisin N, Thoma Y and Zbinden H 2007 *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series* vol 6583 p 18

[10] Phoenix S J, Barnett S M and Chefles A 2000 *Journal of Modern Optics* **47** 507–516

[11] Mayers D 2001 *J. ACM* **48** 351–406 ISSN 0004-5411

[12] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301–1350

[13] Shor P and Preskill J 2000 *Physical Review Letters* **85** 441–444

[14] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100**(20) 200501

[15] Cai R and Scarani V 2009 *New Journal of Physics* **11** 045024

[16] Sheridan L, Le T P and Scarani V 2010 *New Journal of Physics* **12** 123019

[17] Abruzzo S, Kampermann H, Mertz M and Bruß D 2011 *Physical Review A* **84** 032321

[18] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nature communications* **3** 634

[19] Mafu M, Garapo K and Petruccione F 2013 *Physical Review A* **88** 062306

[20] Boileau J, Tamaki K, Batuwantudawe J, Laflamme R and Renes J 2005 *Physical Review Letters* **94** 40503

[21] Renner R and Cirac J 2009 *Phys. Rev. Lett.* **102** 110504

[22] Christandl M, König R and Renner R 2009 *Physical Review Letters* **102** 20504

[23] Renner R 2008 *International Journal of Quantum Information* **6** 1–127

[24] Bennett C 1992 *Physical Review Letters* **68** 3121–3124

[25] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501

[26] Mafu M, Garapo K and Petruccione F 2014 *Phys. Rev. A* **90**(3) 032308