Finite-size key in QKD protocols for Rényi entropies

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, South Africa

[2] Centre for Quantum Technology, National Institute for Theoretical Physics, School of Chemistry and Physics, University of KwaZulu-Natal, P/Bag X54001 Durban, South Africa

E-mail: `209526077@stu.ukzn.ac.za, 209523532@stu.ukzn.ac.za, petruccione@ukzn.ac.za`

Abstract. A realistic quantum key distribution protocol necessarily runs with finite resources. This is in contrast to the existing quantum key distribution security proofs which are asymptotic, in the sense that they only work if certain parameters are exceedingly large as compared to practical realistic values. In this paper, we give the bounds and formalism to derive bounds on the secret key rates for the B92 protocol [Phys. Rev. Letter, 68. 3121 1992] which includes a preprocessing step. This is expressed as an optimization problem by using results on the uncertainty relations and the smooth Rényi entropies.

1. Introduction

Quantum Key Distribution (QKD) provides the only physically secure and proven method for the transmission of a secret key between two distant parties, Alice and Bob [1, 2, 3]. The goal of QKD is to guarantee that the possible eavesdropper known as Eve, with access to the communication channel is unable to obtain useful information about the message [3]. Since invention of the first complete QKD protocol by C. H. Bennet and G. Brassard in 1984 [1] and independently by A. Ekert in 1991 [4], various protocols and their unconditional security proofs against various attacks have been realized. In addition, various QKD products have been commercialized. Many efforts have been done for improving the bounds on the secret key rates for finite amount of resources. The tools for the possible study of unconditional security in the finite-key regime for all discrete variable protocols are now available in [5, 6]. Of recent, a technique using the uncertainty relations for the smooth entropies has been realized [7]. This approach has proved to be elegant because instead of providing bounds for coherent attacks, it provides bounds also for the general kind of attacks, even though its not trivial how you can apply to the six-state protocol. However to our knowledge, this technique has not been done for the B92 protocol [8]. Therefore, in this paper we show how we can derive the bounds for the B92 based on the uncertainty relations and the Rényi entropies.

The security bounds for the BB84 and the six-state protocols have been calculated using the smooth-min entropies in [6, 9]. The secret key rate for the six-state protocol via Rényi entropies has been presented in [10]. In this paper we are going to present bounds on the achievable key length for the B92 protocol [8] which involves a preprocessing step by using the Rényi entropies. In the B92 protocol, in the case of perfect transmission, the strings conditioned upon acceptance are identical and randomly distributed.

2. The B92 QKD Protocol

The B92 protocol [8] resembles symmetry like the BB84 protocol [1] and the six-state protocol [11]. In contrast to the BB84 protocol which uses two orthogonal bases, the B92 protocol utilizes two non-orthogonal bases. By encoding in the non-orthogonal states of the quantum system, it makes it neither impossible for the eavesdropper to make an exact copy of the system nor to gain partial information about the system without disturbing it.

State preparation In this protocol, Alice sends two non-orthogonal states which we denote by $|\psi_\pm\rangle$, to Bob. Bob chooses to measure randomly in one of the two von Neumann measurements. The first measurement $|\psi_+\rangle$ consists of the vectors $\{|\psi_-\rangle, |\tilde{\psi}_-\rangle\}$ where $|\tilde{\psi}_-\rangle$ is orthogonal to $|\psi_-\rangle$. The second measurement $|\psi_-\rangle$ is given as $\{|\psi_+\rangle, |\tilde{\psi}_+\rangle\}$ where $|\tilde{\psi}_+\rangle$ is orthogonal to $|\psi_+\rangle$. On the receiving side, Bob announces an acceptance if he gets an outcome which corresponds to $|\tilde{\psi}_\pm\rangle$, otherwise both parties discard the values that they recorded.

Sifting and Measurement Alice records the bit value 0 or 1 if she sends $|\psi_+\rangle$ or $|\psi_-\rangle$ and Bob records 0 or 1 if he obtains $|\tilde{\psi}_-\rangle$ or $|\tilde{\psi}_+\rangle$. Alice sends each quantum state with equal probability and Bob chooses randomly with equal probability between his two measurements.

Parameter estimation The role of the parameter estimation step is to minimize the set of compatible states Γ and the number sample points m while minimizing the failure probability ε_{PE}. Let $\Gamma_{\varepsilon_{\mathrm{PE}}}$ be a set of states from which a key is extracted with non-negligible probability where $\varepsilon_{\mathrm{PE}}$ is the failure probability in the parameter estimation step (i.e., the parameter estimation passes although the raw key does not contain sufficient secret information). In particular, if the statistics λ_m are obtained by measuring m samples of ρ_{AB} (i.e., the entangled state shared by Alice and Bob) according to a POVM measurement with d possible outcomes and $\lambda_\infty(\rho_{AB})$ denotes the perfect statistics in the limit of infinitely measurements then for any ρ_{AB} we can write

$$\Gamma_\xi := \{\rho_{AB} : ||\lambda_m - \lambda_\infty(\rho_{AB})||_1 \leq \xi\}, \tag{1}$$

where

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

Error correction The error correction step serves the purpose of correcting all the erroneously received bits and giving an estimate of the error rate. Alice and Bob hold correlated bits strings denoted as X^n and Y^n. The number of bits leaked during the classical communication to an eavesdropper is given by

$$\mathrm{leak}_{\mathrm{EC}} = f_{\mathrm{EC}} \mathrm{n} h(e) + \log_2(\frac{2}{\varepsilon_{\mathrm{EC}}}), \tag{3}$$

where f_{EC} is a constant larger than 1 (in practice f ≈1.05 - 1.2), $h(e)$ is the binary Shannon entropy and e is the QBER, $\varepsilon_{\mathrm{EC}}$ is the error probability in the error correction step.

Privacy amplification The objective of this step is to minimize the quantity of correct information which the eavesdropper may have obtained about Alice's and Bob's raw key. Let Alice and Bob hold a perfectly correlated bit string X^n on which Eve might have some information. Alice chooses at random a function $\mathcal{F}$ from a two universal hash functions and sends a description of $\mathcal{F}$ to Bob. Then Alice and Bob compute their keys $S_A = \mathcal{F}(X^n)$ and $S_B = \mathcal{F}(\hat{X}^n)$. By using an important result in [12], it has been found that the achievable length of the secret key rate that can be computed from X by the two universal hash function $\mathcal{F}$ can be expressed as,

$$\ell = H_{\max}^{\bar{\varepsilon}}(X|E) - H_{\min}^{\bar{\varepsilon}}(X|Y) - 2\log_2(1/\varepsilon), \tag{4}$$

where $\bar{\varepsilon} = (\varepsilon/8)^2$, if the key is required to be secure with respect to $\rho_E \otimes P_{|F\rangle}$.

3. Definitions

3.1. Rényi entropies

The Rényi entropies are a family of functions on the probability distributions. They quantify the uncertainty or randomness of a system. The Rényi entropy of order α is defined as [13]

$$H_\alpha(X) = \frac{1}{1-\alpha}\log\sum_{x\in\mathcal{X}} P(x)^\alpha, \quad \alpha \in (0,1)\cup(1,\infty). \tag{5}$$

for which $H_\infty(\alpha\to\infty)$, $H_0(\alpha\to 0)$ and the Shannon entropy $(\alpha\to 1)$ are defined as limits. For a finite-dimensional Hilbert space $\mathcal{H}$, we use $\mathcal{P}(\mathcal{H})$ to denote the set of positive semi-definite operators on $\mathcal{H}$. The set of normalized quantum states $\mathcal{S}(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) : \mathrm{tr}\rho = 1\}$ and the set of sub-normalized states $\mathcal{S}_\leq(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) : \mathrm{tr}\rho \leq 1\}$. We use indices to denote multi-partite Hilbert spaces for example, $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Definition 1. Let $\rho_{AB} \in S_\leq(\mathcal{H}_{AB})$ and $\sigma_{AB} \in \mathcal{S}(\mathcal{H}_B)$, then the min-entropy of A conditioned on B of the state ρ_{AB} relative to σ_B is defined as

$$H_{\min}(A|B)_{\rho|\sigma} := \sup\{\lambda \in \mathbb{R}|\exists\sigma_B \in \mathcal{S}(\mathcal{H}_B) : \rho_{AB} \leq 2^{-\lambda}\mathbb{1}_A \otimes \mathbb{1}_B\}. \tag{6}$$

Furthermore we define

$$H_{\min}(A|B)_\rho := \max_{\sigma_B\in\mathcal{S}(\mathcal{H}_B)} H_{\min}(A|B)_{\rho|\sigma}. \tag{7}$$

The smooth min-entropy, $H_{\min}(A|B)_\rho$ is finite if and only if $\mathrm{supp}\{\sigma_B\} \subseteq \mathrm{supp}\{\sigma_B\}$ and $-\infty$ otherwise. The max-entropy is its dual with regards to a purification ρ_{ABC} of ρ_{AB} on an auxiliary Hilbert space $\mathcal{H}_C$.

Definition 2. Let $\rho_{ABC} \in S_\leq(\mathcal{H}_{ABC})$ be pure, then the max-entropy of A conditioned on B of the state ρ_{AB} is defined as

$$H_{\max}(A|B)_\rho := -H_{\min}(A|C)_\rho. \tag{8}$$

The quantum entropies can be ordered as follows

$$H_{\min}(A|B)_\rho \leq H(A|B)_\rho \leq H_{\max}(A|B)_\rho. \tag{9}$$

In order to define smooth versions, we consider the set of states close to ρ in the following sense. For $\varepsilon > 0$, we define an ε-ball of states around $\rho \in \mathcal{S}(\mathcal{H})$ as

$$\mathcal{B}^\varepsilon(\rho) := \{\tilde{p} \in \mathcal{S}_\leq(\mathcal{H}) : C(\rho,\tilde{\rho}) \leq \varepsilon\}, \tag{10}$$

where $C(\rho,\tilde{\rho}) := \sqrt{1-F^2(\rho,\tilde{\rho})}$ is a distance measure (on normalized states) based on the fidelity $F(\rho,\tilde{\rho}) := \mathrm{tr}|\sqrt{\rho}\sqrt{\tilde{\rho}}|$. We use this choice of measure because it is invariant under purifications and is directly related to the trace distance for pure states. Smoothed versions of the min-entropy are then defined:

$$\begin{aligned} H_{\min}^\varepsilon(A|B)_{\rho|\sigma} &:= \max_{\tilde{\rho}\in\mathcal{B}^\varepsilon(\rho_{AB})} H_{\min}(A|B)\tilde{\rho}|\sigma \\ H_{\min}^\varepsilon(A|B)_\rho &:= \max_{\tilde{\rho}\in\mathcal{B}^\varepsilon(\rho_{AB})} H_{\min}(A|B)\tilde{\rho}. \end{aligned} \tag{11}$$

and similarly

$$H^{\varepsilon}_{\max}(A|B)_{\rho} := \min_{\tilde{\rho}\in\mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\max}(A|B)\tilde{\rho} \tag{12}$$

For a more in-depth treatment of smooth conditional entropies and their basic properties we refer to [14]. The Rényi entropies with $\alpha > 1$ are close to the smooth min-entropy in the sense that

$$H^{\varepsilon}_{\min}(X) \geq H_{\alpha}(X) - \frac{1}{\alpha-1}\log\frac{1}{\varepsilon}, \quad \alpha > 1. \tag{13}$$

while those with $\alpha < 1$ are close to the smooth max-entropy.

3.2. Bound on the secure key rate

According to [15], for any $\varepsilon \geq 0$, a final key S is said to be ε-secure with respect to an adversary Eve if the joint state ρ_{SE} satisfies

$$\min_{\rho_E}\frac{1}{2}||\rho_{SE} - \tau_S \otimes \rho_E||_1 \leq \varepsilon, \tag{14}$$

where $\rho_{SE} = \sum_{s\in\mathcal{S}} P_s(s)|s\rangle\langle s| \otimes \rho^s_E$ and $\{|s\rangle\}_{s\in\mathcal{S}}$ is an orthonormal basis of some Hilbert space $\mathcal{H}_s$ and ε is the total security parameter. The parameter τ_S is the completely mixed state on the key space, and $||\cdot||_1$ is the trace distance. The parameter ε represents the maximum failure probability in which an adversary may have gained some information on S, or it can be interpreted as the maximum failure probability in which the extracted key deviates from the ideal key. The secret key rate in the asymptotic regime is expressed as [9]

$$\lim_{N\to\infty} r = S(X|E) - H(X|Y), \tag{15}$$

where $S(X|E)$ and $H(X|Y)$ are the von Neumann and the Shannon entropies. However, in the non-asymptotic regime this equation becomes invalid as we have a finite number of bits that Alice sends to Bob.

In the non-asymptotic limit the secret key rate is found to be [5, 16]

$$r = \frac{n}{N}[\sup_{\substack{A'\leftarrow X\\ B\leftarrow A'}} \min_{\sigma_{AB}\in\Gamma_{\xi}} H(X|E) + \triangle(n) - \text{leak}_{\text{EC}}/n] + \frac{2}{N}\log(2\varepsilon_{PA}). \tag{16}$$

where the set Γ_{ξ} contains all states compatible with the statistics in parameter estimation and is defined by Equation (1), $\triangle(n) = -7\sqrt{[\log_2(2/\bar{\varepsilon})]/n}$ represents the security parameter of the privacy amplification step and provides a lower bound for the $\bar{\varepsilon}$-smooth min-entropy. The leakage term, $\text{leak}_{\text{EC}} = 1.2h(Q)$ for $\varepsilon_{\text{EC}} = 10^{-10}$ and $h(x)$ is the binary entropy. The total security parameter ε is bounded by

$$\varepsilon = \bar{\varepsilon} + \varepsilon_{\text{PA}} + \varepsilon_{\text{EC}} + \varepsilon_{\text{PE}}. \tag{17}$$

In order to determine the number ℓ^{ε}_n of ε-secure key bits that can be generated by this protocol we use the following recent results on the uncertainty relation [7]. The amount of key that can be extracted from a string X is given by the uncertainty of the adversary about X, measured in terms of the smooth Rényi entropies. The amount of information B needs to correct his errors, using optimal error correction, is given by his uncertainty about A's string again measured in terms of the smooth Rényi entropies. Combining these two results we have

$$H^{\bar{\varepsilon}}_{\min}(\mathbf{X}|E) + H^{\bar{\varepsilon}}_{\max}(\mathbf{Z}|B) \geq \log\frac{1}{c}, \tag{18}$$

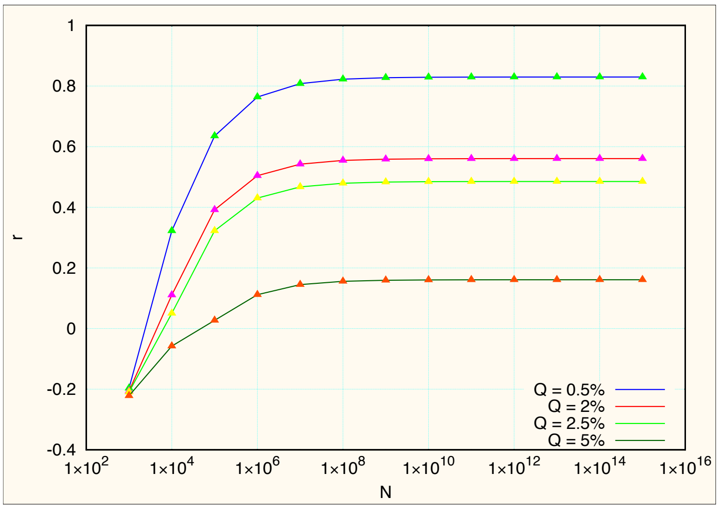

Figure 1. Lower bound on the secret key fraction, r for the finite B92 protocol as a function of the exchanged quantum signals N, values: $\varepsilon = 10^{-5}, \varepsilon_{EC} = 10^{-10}$.

where $\bar{\varepsilon} \geq 0$ is the smoothing parameter and c quantifies the 'incompatibility' between the measurements $\mathbf{Z} = Z^{\otimes n}$ and $\mathbf{X} = X^{\otimes n}$. The definitions of the smooth min and max-entropies have been given above. However, any decent measure of uncertainty $H_{\min}$ can only increase under information processing and in particular under Bob's measurement so that

$$H^{\bar{\varepsilon}}_{\max}(\mathbf{Z}|B) \leq H^{\bar{\varepsilon}}_{\max}(\mathbf{Z}|\mathbf{Z}'), \tag{19}$$

where the measurement $\mathbf{Z}' = Z'^{\otimes n}$ is made on Bob's system. The protocol does not need to prescribe the actual measurements of $\mathbf{Z}$ and $\mathbf{Z}'$. However, based on the observed parameters we can replace the measurement on $\mathbf{X}$ and $\mathbf{X}'$ in this hypothetical protocol by highly correlated measurements $\mathbf{Z}$ and $\mathbf{Z}'$ respectively. This means that the uncertainty in $H^{\bar{\varepsilon}}_{\max}(\mathbf{Z}|\mathbf{Z})$ is small and holds for the following bound on the smooth max-entropy

$$H^{\bar{\varepsilon}}_{\max}(\mathbf{Z}|\mathbf{Z}') \leq nq - \frac{(1-2\delta)\eta + 2\delta}{2}(\varepsilon - (1-\varepsilon)h(x)), \tag{20}$$

where q is the quality factor and $x = \frac{(1-5\delta)(1-\delta)\eta(1-\eta)}{(\delta+(1-2\delta)\eta)(1-\delta)-(1-5\delta)\eta)}$. The error rate conditioned on acceptance is given by $\varepsilon = \frac{\delta}{(1-2\delta)\eta+2\delta}$ with $\eta = (2\alpha\beta)^2$ [17].

3.3. Bound on the achievable key length

Let ρ_{XBE} be the state describing Alice's bit string X^n and Bob's string B^n as well as Eve's quantum information represented by ρ_{E^n}. Let $\bar{\varepsilon}, \varepsilon_{\rm PA} \geq$0. If the length of the key is such that

$$\ell \leq \max_{\bar{\varepsilon},\varepsilon_{\rm PA}} \left(H_{\min}(\mathbf{X}|E)_{\rho_{XBE}} - 2\log\frac{1}{2\bar{\varepsilon}} - \text{leak}_{\rm EC} - 2\log\frac{1}{2\varepsilon_{\rm PA}} \right), \tag{21}$$

then the protocol is $(2\bar{\varepsilon} + \varepsilon_{\rm PA})$-secure.

By using the data processing inequality and the uncertainty relation in (18) we have

$$\begin{aligned} H^{\varepsilon'}_{\min}(\mathbf{X}|E') &\geq H^{\varepsilon'}_{\min}(\mathbf{X}|E) - \text{leak}_{\rm EC} - 2\log\frac{1}{2\varepsilon_{PA}} \\ &\geq nq - H^{\bar{\varepsilon}}_{\max}(\mathbf{Z}|\mathbf{Z}') - \text{leak}_{\rm EC} - 2\log\frac{1}{2\varepsilon_{PA}} \\ &\geq nq - \frac{(1-2\delta)\eta+2\delta}{2}(\varepsilon - (1-\varepsilon)h(x)) - \text{leak}_{\rm EC} - 2\log\frac{1}{2\varepsilon_{PA}}. \end{aligned} \tag{22}$$

If we combine Equation (22) with the proposed bound on the achievable key length in (21) and also by using the Quantum Leftover Hash Lemma [18] we have

$$\triangle \leq \varepsilon' + \frac{1}{2}\sqrt{2^{\ell - H_{\min}^{\varepsilon'}}(X|E')} \leq 2\bar{\varepsilon} + \varepsilon_{PA}, \tag{23}$$

where E' summarizes all information Eve learned about $\mathbf{X}$ during the protocol including the classical communication sent by Alice and Bob over the authenticated channel. This completes the proof for security bound.

4. Conclusion

We have demonstrated how one can use results of the uncertainty relations and smooth Rényi entropies to derive security bounds for the B92 QKD protocol when a finite number of signals are used. The results show that a minimum number of approximately $10^4 - 10^6$ signals are required in order to extract a reasonable length of secret key in QKD protocols under realistic scenarios. This minimum number of signals has been also observed in other QKD protocols as well [5, 9, 19]. Therefore, the uncertainty relations and the smooth Rényi entropies prove to be a powerful technique for the derivation of the security bounds in QKD protocols in the finite size-key regime.

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

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

[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–195

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

[5] Scarani V and Renner R 2008 *Physical review letters* **100** 200501

[6] Renner R 2005 *arXiv:0512258v2*

[7] Tomamichel M and Renner R 2011 *Physical Review Letters* **106** 110506

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

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

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

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

[12] Kraus B, Gisin N and Renner R 2005 *Physical review letters* **95** 80501

[13] Rényi A 1961 *Fourth Berkeley Symposium on Mathematical Statistics and Probability* pp 547–561

[14] Konig R, Renner R and Schaffner C 2009 *Information Theory, IEEE Transactions on* **55** 4337–4347

[15] Müller-Quade J and Renner R 2009 *New Journal of Physics* **11** 085006

[16] Scarani V and Renner R 2008 *Arxiv preprint arXiv:0806.0120*

[17] Christandl M, Renner R and Ekert A 2004 *arXiv:0402131v2*

[18] Tomamichel M, Schaffner C, Smith A and Renner R 2011 *IEEE Transactions on Information Theory* **57** 5524 –5535 ISSN 0018-9448

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