Tight finite-key analysis for RRDPS protocol

Hang Liu[1,2,3] , Zhen-Qiang Yin[1,2,3,*], Rong Wang[1,2,3], Ze-Hao Wang[1,2,3], Shuang Wang[1,2,3], Wei Chen[1,2,3], Guang-Can Guo[1,2,3], and Zheng-Fu Han[1,2,3]

1. CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China.
2. CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China.
3. State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China.
Email: yinzq@ustc.edu.cn

1 Introduction

As the maturest field of quantum information sciences, quantum key distribution (QKD) is well-known for its information-theoretic security. In QKD, round-robin-differential-phase-shift (RRDPS) can upper bound Eve's information without using any parameter of signal disturbance. In 2018, Yin et al. put forward a phase randomized method to improve it by constructing the optimal collective attack model [1]. Here we give a tight finite-key analysis for RRDPS with widely used phase randomized weak coherent source. The essential idea is observing that the randomized phases of each pulse of the train lead the composite system of Alice, Bob and Eve into becoming a mixture state, in which different components may have different information leakage. Next one can apply the entropic uncertainty relation [2] to estimate phase error rates and min-entropies for each mixture components. Moreover, by introducing Azuma's inequality [3], the effects of coherent attacks are well-considered.

2 Virtual protocols

virtual protocol 1 **virtual protocol 2**

The security of RRDPS protocol is essentially regarded as virtual protocol 1. As a matter of fact, the virtual protocols 1 and 2 generates same sifted key bits, and Eve cannot distinguish Alice is performing virtual protocol 1 or virtual protocol 2. Therefore, from the view of security proof, the smooth min-entropy of the actual protocol can be lower bounded by the larger one of min-entropies calculated in virtual protocols 1 and 2. This consideration is the first reason that our analysis can converge to the optimal key rate given in ref. [1].

3.1 The bound for smooth min-entropy

In single photon case, assuming that Bob announces (a, b) in the l-th trial, we obtain the tripartite quantum state shared by Alice, Bob and Eve,

$$\rho_{\mathrm{ABE}} = \wp\left\{\tilde{C}^l_{aa}|-\rangle_{\mathrm{A}^l_a}|+\rangle_{\mathrm{A}^l_b} + \tilde{C}^l_{ba}|+\rangle_{\mathrm{A}^l_a}|-\rangle_{\mathrm{A}^l_b}\right\} + \sum_{i^l\neq a,b}\wp\left\{\tilde{C}^l_{i^l a}|+\rangle_{\mathrm{A}^l_a}|+\rangle_{\mathrm{A}^l_b}\right\}$$

where $\wp\{|x\rangle\} \coloneqq |x\rangle\langle x|$. Note that $\tilde{C}^l_{i^l j^l}$ is the quantum system of $\mathrm{A}^{\neq l}$, $\mathrm{B}^{\neq l}$ and E. The first part is coupled with Eve, which means Eve may learn sifted key bit from this mixture component. Conversely, the second part is decoupled with Eve, which will result in perfect secret key evidently. We call the former coupled case and the latter decoupled case, whose probabilities are:

$$P^l_{\mathrm{co}} = \frac{\sum_b |\tilde{C}^l_{aa}|^2 + |\tilde{C}^l_{ba}|^2}{\sum_b \sum_{i^l} |\tilde{C}^l_{i^l a}|^2} \quad P^l_{\mathrm{deco}} = \frac{\sum_b \sum_{i^l\neq a,b} |\tilde{C}^l_{i^l a}|^2}{\sum_b \sum_{i^l} |\tilde{C}^l_{i^l a}|^2}$$

respectively. The probability of finding A^l_a in $|-\rangle$ and the probability of finding A^l_b in $|-\rangle$, just corresponding to the virtual protocols 1 and 2 respectively, are:

$$P^l_a = \frac{\sum_b |\tilde{C}^l_{aa}|^2}{\sum_b \sum_{i^l} |\tilde{C}^l_{i^l a}|^2} \qquad P^l_b = \frac{\sum_b |\tilde{C}^l_{ba}|^2}{\sum_b \sum_{i^l} |\tilde{C}^l_{i^l a}|^2}$$

And the theoretic phase error rate is:

$$P^l \coloneqq \min\{P^l_a, P^l_b\}$$

3.2 The bound for smooth min-entropy

Above formulae are just for the l-th bit of $\tilde{\mathbf{Z}}$. We resort to Azuma's inequality to complete estimation the smooth min-entropy. In the l-th round, Alice's local qubits A^l_a and A^l_b can be classified into decoupled cases or coupled cases, while coupled ones can be classified into with phase error and no phase error. For every kind of cases, we could construct a martingale respectively, which justifies the application of Azuma's inequality. The same logic can be seen in ref. [4].

According to Azuma's inequality, for all $N \geq 0$ and any $\alpha \geq 0$, we get:

$$\Pr\left[\frac{h_N - \sum_{l=1}^N p^l}{N} \geq \alpha\right] \leq 2\mathrm{e}^{-N\alpha^2/2}$$

where h_N can be the actual decoupled(coupled) number $N_{\mathrm{deco}}(N_{\mathrm{co}})$ or phase error rate e_{ph}. And p^l can be the $P^l_{\mathrm{deco}}(P^l_{\mathrm{co}})$ or P^l.

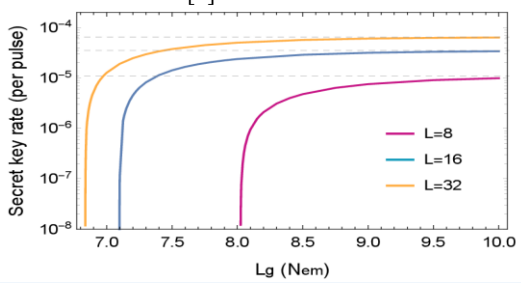
Finally, the smooth min-entropy of $\tilde{\mathbf{Z}}$ is:

$$H^{\epsilon}_{\min}(\tilde{\mathrm{Z}}|\mathrm{E}) \geq N - N_{\mathrm{co}} H_2(e_{ph}) - \log\frac{2}{\epsilon'^2_0}$$

where ϵ and ϵ'_0 represent the failure probability.

4. Results

Secret key rate R versus N. The dashed lines represent the asymptotic results of ref. [1].



5. Conclusion

As far as we know, our results are optimal for RRDPS in finite-key region, which implies that QKD without monitoring signal disturbance can be realized in present QKD systems. Besides, from the view of security proofs, this may shed lights on the developments of techniques for security proofs of applying the uncertainty relation and Azuma's to high-dimensional protocols.

Reference

[1] Yin, Z.-Q. et al. Nat. Commun. 9, 457 (2018).
[2] Tomamichel, M. et al. Phys. Rev. Lett. 106, 110506 (2011)
[3] Azuma, K. Tohoku Math. J. 19, 357–367 (1967).
[4] Boileau, J.-C. et al. Phys. Rev. Lett. 94, 040503 (2005).