Security of QKD with detection-efficiency mismatch in the multiphoton case

Anton Trushechkin

Steklov Mathematical Institute of Russian Academy of Sciences, Moscow
Russian Quantum Center, Moscow

e-mail: trushechkin@mi-ras.ru,

arXiv: 2004.07809

1. Main results

- We prove the security of the BB84 protocol with detection-efficiency mismatch for the case when both Alice's output and Bob's input are multiphoton
- In particular, we rigorously prove bounds for the number of multiphoton detection events
- We adapt the decoy state method to the case of detection-efficiency mismatch and, thus, generalize the results to the case when Alice sends weak coherent pulses instead of true single photons

2. Problem of detection-efficiency mismatch

- BB84 with active basis choice uses two single-photon detectors: One for the signals encoding bit 0 and one for the signals encoding bit 1, respectively.
- Detection-efficiency mismatch: two detectors have different quantum efficiencies, $\eta_0 \neq \eta_1$
- This should be taken into account: In the extreme case $\eta_1 = 0$, $\eta_0 > 0$ the protocol is insecure (the sifted key consists of only zeros).
- We consider the case of constant and known mismatch: η_0 and η_1 are constant and known. But the generalization to the mode-dependent mismatch is possible.

3. Multiphoton Bob's input

- Additional (the main) difficulty: Bob's input is not necessarily single photon. Eve may add photons.
- Mathematically: Bob's Hilbert space is not two-dimensional, but an infinite-dimensional Fock space
- Due to this reason, simple random discarding of some detections from the detector with a higher efficiency, does not work. Sending many photons by Eve violates the balance again.

4. Previous security proofs for QKD with detection-efficiency mismatch

Under the assumptions that: (i) the Bob's input is single photon (Eve cannot add more photons), (ii) the source is single-photon:

- C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Quant. Inf. Comput. **9**, 131 (2009)
- A. Winick, N. Lütkenhaus, and P. J. Coles, Quantum **2**, 77 (2018)
- J. Ma, Y. Zhou, X. Yuan, and X. Ma, Phys. Rev. A **99**, 062325 (2019)

Tight analytic bounds for the case of the single-photon Bob's input and adaptation of the decoy state method:

- M. K. Bochkov and A. T., Phys. Rev. A **99**, 032308 (2019)

Under the assumption of the single-photon source and with a numerical conjecture for the estimation of the number of multiphoton detection events

- Y. Zhang, P. J. Coles, A. Winick, J. Lin, N. Lütkenhaus, arXiv: 2004.04383

5. Our result

- We use analytic bound for the single-photon case on the Bob's side and analytic bound for the number of multiphoton detection events based on the entropic uncertainty relations.
- Adapt decoy state method to include the case of weak coherent light source

6. Model: the case of the single-photon source

- Let only z basis be used for key generation
- Without loss of generality we assume that $\eta_0 = 1$ and $\eta_1 = \eta$, $0 < \eta \leqslant 1$ (Y. Zhang and N. Lütkenhaus, Phys. Rev. A **95**, 042319 (2017))
- Equivalent entanglement-based formulation
- Collective attacks, iid setting, ρ_{ABE} – tripartite state chosen by Eve
- $\tilde{\rho}'_{ABE}$ – the post-selected state conditioned on the detection event in the z basis

7. Secret key rate: problem of basis-dependent detection rate

- Devetak–Winter formula for the secret key rate:

$$K \sim H(Z|E)_{\tilde{\rho}'} - H(Z|B)_{\tilde{\rho}'} \geqslant 1 - H(X|B)_{\tilde{\rho}'} - h(Q_z)$$

  $h(x)$ – binary entropy, Q_z – QBER in the z basis
- $H(X|B)_{\tilde{\rho}'}$ – entropy of the Alice's result of the x-measurement conditioned on the Bob's quantum state BUT for the state $\tilde{\rho}'$, i.e., after the attenuation corresponding to the measurement in the z basis (detection rate is basis-dependent)
- The same thing in other words: phase error rate is not equal to bit error rate in the x basis

8. Convex optimization problem

Worst-case: minimization of K over $\rho_{AB} \in \mathbf{S}$, where $\mathbf{S}$ are linear restrictions :

- Probability of detection (for the z basis)
- Weighted mean erroneous detection rate in the x basis
- Probability of a single click of the detector 1 for the measurement in the z basis
- Mean probability of a double click

Similar to the numerical approach (reduction to the convex optimization)

P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Nat. Commun. **7**, 11712 (2016); A. Winick, N. Lütkenhaus, and P. J. Coles, Quantum **2**, 77 (2018)

Theorem

The secret key rate is lower bounded by

$$K \geqslant \min_{p^{(2)}_{\mathrm{det}}} p^{(1),\mathrm{L}}_{\mathrm{det}} \left[1 - h\left(\frac{1-\delta^{\mathrm{L}}_x}{2}\right)\right] - p_{\mathrm{det}} h(Q_z), \quad (1)$$

where $\delta^{\mathrm{L}}_x = \sqrt{\eta}(t^{\mathrm{L}}_1 - 2q^{\mathrm{U}}_1)/p^{(1),\mathrm{L}}_{\mathrm{det}}$. The minimization is performed over the segment $p^{(2)}_{\mathrm{det}} \in \left[0, p^{(2),\mathrm{U}}_{\mathrm{det}}\right]$. The expression under minimization in Ineq. (1) is a convex function of $p^{(2)}_{\mathrm{det}}$.

9. Comments to the theorem

Estimations obtained from the linear restrictions:

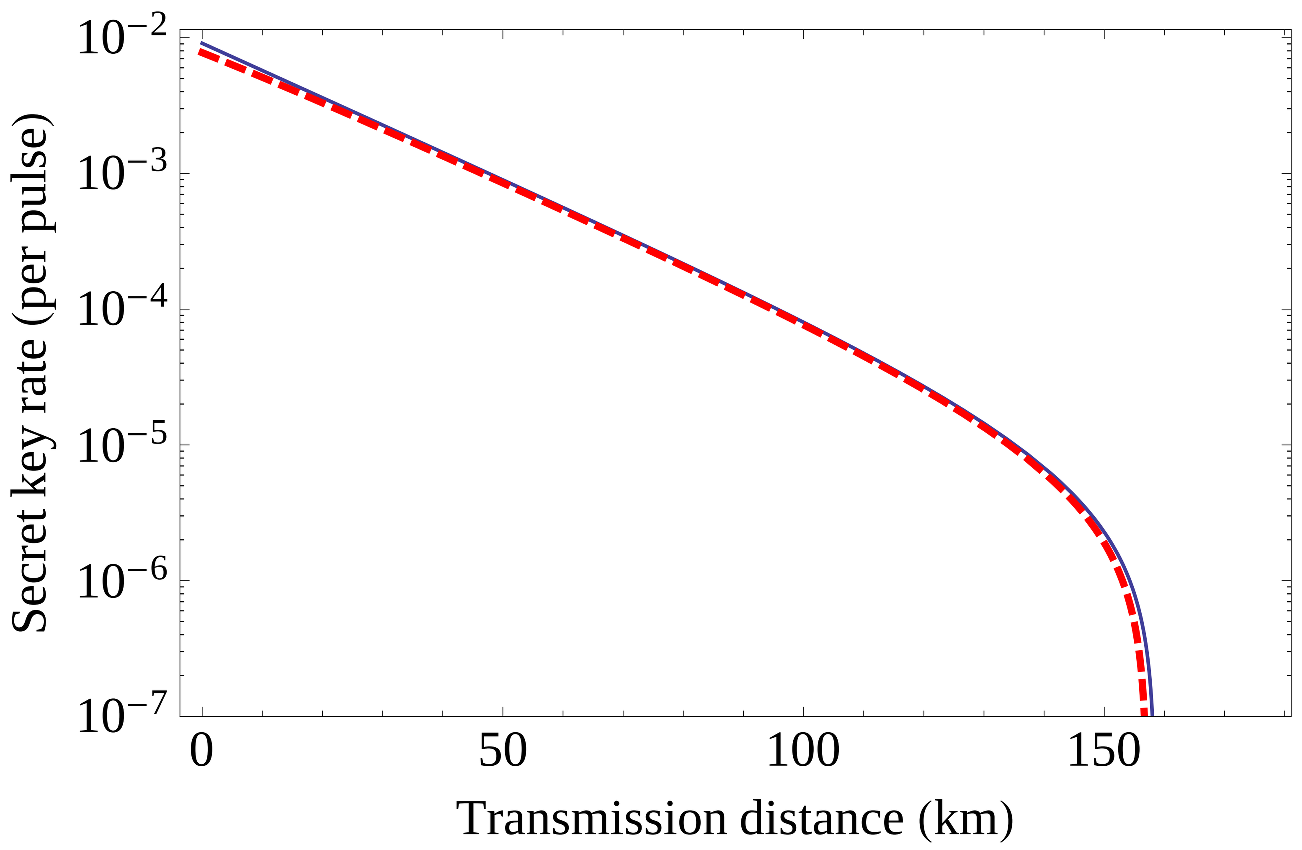
- $p^{(1),\mathrm{L}}_{\mathrm{det}}$ and $p^{(2),\mathrm{U}}_{\mathrm{det}}$ are lower and upper bounds for single-photon and double-photon detections.
- t^{L}_1 is the lower bound for the probability of the single-photon input
- q^{U}_1 is related to the bit error rate in the x basis

Method of proof: Two cornerstones

- Analytic bound for the case of the single-photon Bob's input
- Estimation of the number of multiphoton detection events based on the entropic uncertainty relations and monogamy of entanglement

10. Decoy states for the case of detection-efficiency mismatch

- The decoy state method itself does not assume anything about the detectors.
- The only difference with the usual decoy state is more detailed data are required (not averaged over the bases and outcomes).



Red dashed line: detection-efficiency mismatch
Blue line: no mismatch but the same average detection efficiency $(\eta_0 + \eta_1)/2$

Thank you for reading