Improving key rates of the unbalanced phase-encoded BB84 protocol using the flag-state squashing model

Nicky Kai Hong Li and Norbert Lütkenhaus

Institute for Quantum Computing & Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada

(arXiv:2007.08662 [quant-ph])   Email: kai.hong.li@uwaterloo.ca

Introduction

- Phase-encoded BB84 experiments have unbalanced signal amplitudes due to loss in phase modulators.
- Ref. [1, 2] turn the security proof into a standard BB84 proof using decoy states, signal tagging, and the qubit squashing model [3].
- The qubit approach pessimistically assumes that Eve has full access to the information carried by multiphoton signals.
  ➔ underestimate the secure key rate of this protocol.
- Here, our different proof technique achieves **higher key rates**.

Protocol Description

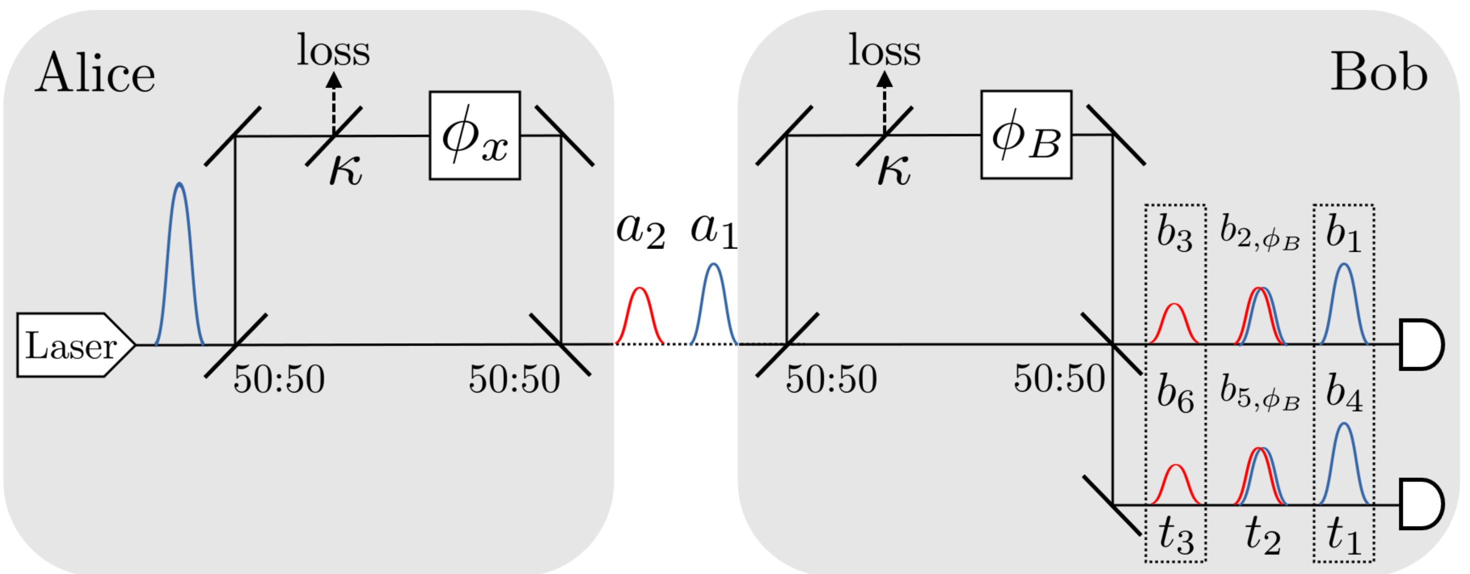


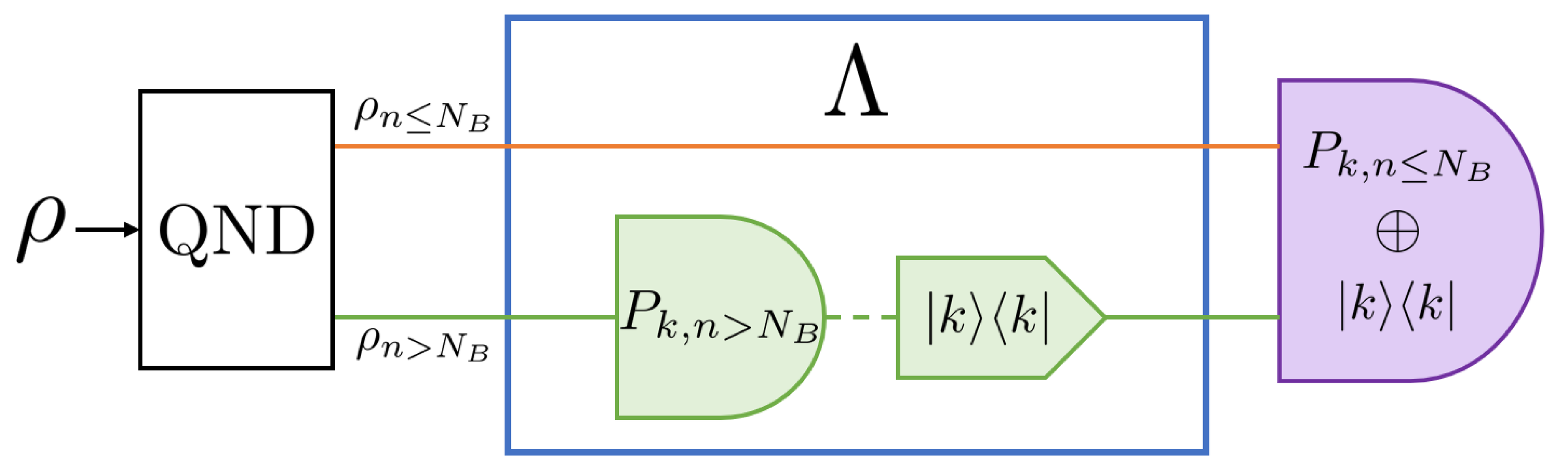
Fig. 1: Setup for the phase-encoded BB84 protocol with unbalanced signal intensities.

- Alice's output: $\sigma_x(\alpha) = \int_0^{2\pi} \frac{d\theta}{2\pi} |\psi_x^\theta(\alpha)\rangle\langle\psi_x^\theta(\alpha)|$, $|\psi_x^\theta(\alpha)\rangle = |\alpha e^{i\theta}, \sqrt{\kappa}\, \alpha e^{i(\theta-\phi_x)}\rangle$
- Phases: $\phi_x \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$, $\phi_B \in \{0, \frac{\pi}{2}\}$ (equally probable)

Methods

Differences between our approach and Refs. [1, 2]'s:

- We apply the numerical analysis formulated in [4] to obtain reliable lower bounds on the key rates.
- Source side: tag the photon number of the signals and extend our analysis to a higher tagged threshold photon number.
- Receiver side: use flag-state squashing model [5] (see Yanbao Zhang's talk)



to avoid extra qubit errors from the qubit squashing model.

- Need lower bound for $p(n \le N_B) := \mathrm{Tr}(\rho_{n\le N_B})$ ➔ preserve entanglement

➔ preserve some parts of the multi-photon generated private information

Summary of technical details:

- Lower bound $p(n \le N_B)$ with Markov's inequality + cross-click probability
- Infinite decoy + Eve's QND photon counting + signal tagging

➔ Decomposition of privacy amplification (PA) term in key rate formula

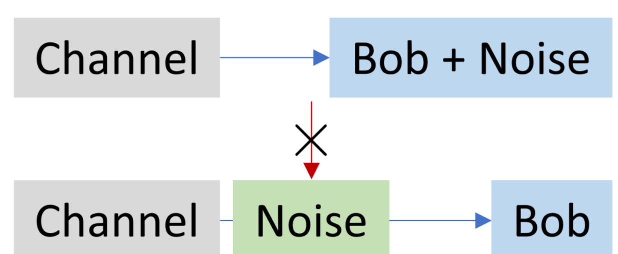
$$R_\infty \ge p_{\mathrm{pass}}^{\tilde{n}=0} + \sum_{\tilde{n}=1}^{N_A} p_{\tilde{n}} \min_{\rho_{AB}^{\tilde{n}} \in \mathbf{S}_{\tilde{n}}} D(\mathcal{G}(\rho_{AB}^{\tilde{n}}) || \mathcal{Z}(\mathcal{G}(\rho_{AB}^{\tilde{n}}))) - p_{\mathrm{pass}}\, \delta_{\mathrm{EC}}$$

- Each PA term independent of signal intensity α ➔ easy to optimise over

Simulation

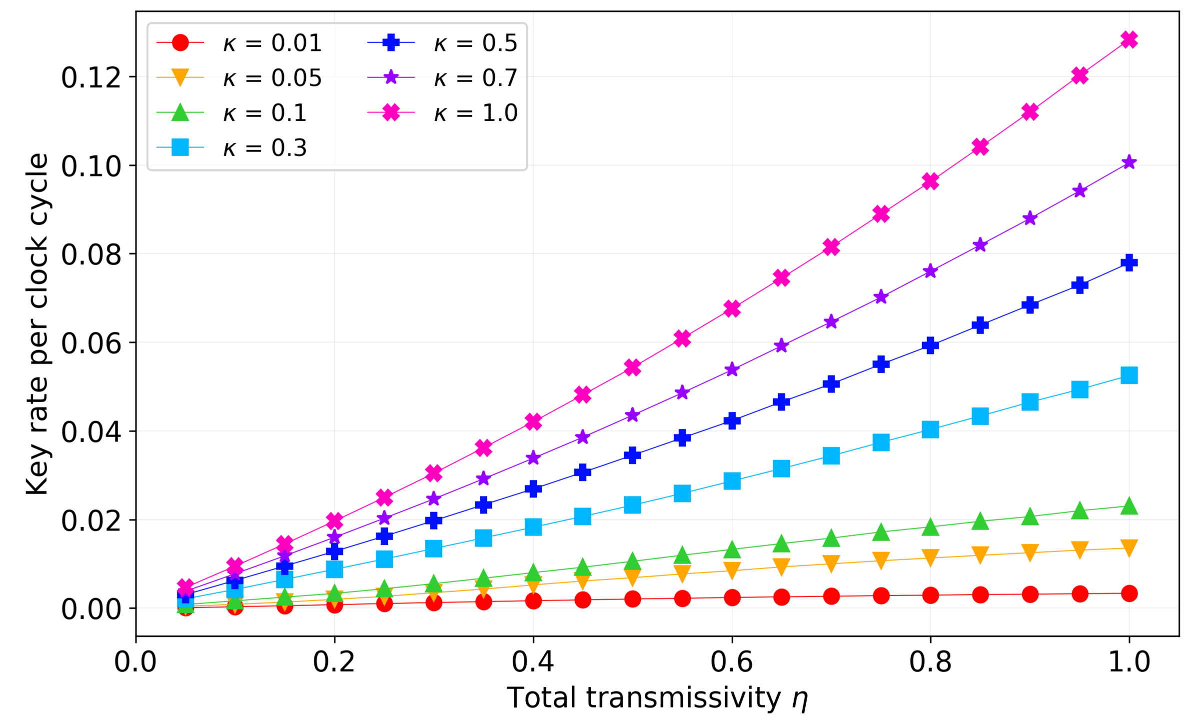
- Loss-only channel + detection inefficiency ➔ transmissivity η
- Two alternative **loss** scenarios:
  - Trusted loss: detector efficiency = η_{det}
  - Untrusted loss: detector efficiency = 1 (i.e. all loss due to Eve)
- Dark counts ➔ classical post-processing map
- Two alternative **noise** scenarios:
  - Trusted noise: each detector has the same dark count rate p_d
  - Untrusted noise: assume Bob's detectors "dark count free" (i.e. Eve causes the dark counts)

  ➔ may lead to unphysical constraints (∵ no replacement model for noise) ➔



Results

Parameters: Alice's tagged photon number cutoff $N_A = 3$, Bob's flag-state photon number cutoff $N_B = 4$, $p_d = 8.5 \times 10^{-7}$, $f_{EC} = 1.22$



Observation

- key rates increase with larger κ values

Fig. 2: Our optimal lower bounds for secure key rates per clock cycle for both trusted and untrusted dark counts versus total transmissivity η.

Compare key rates with previous results

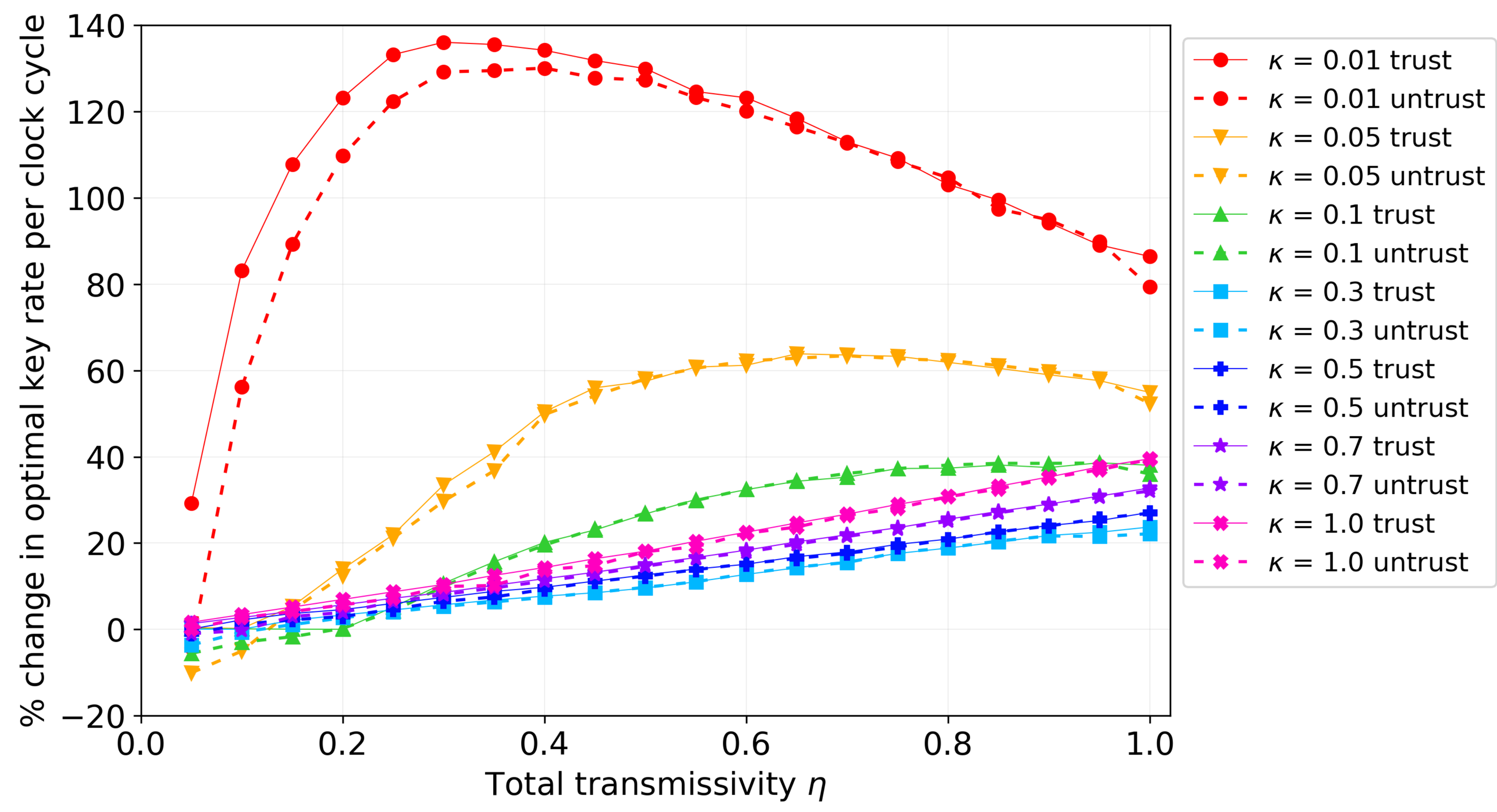
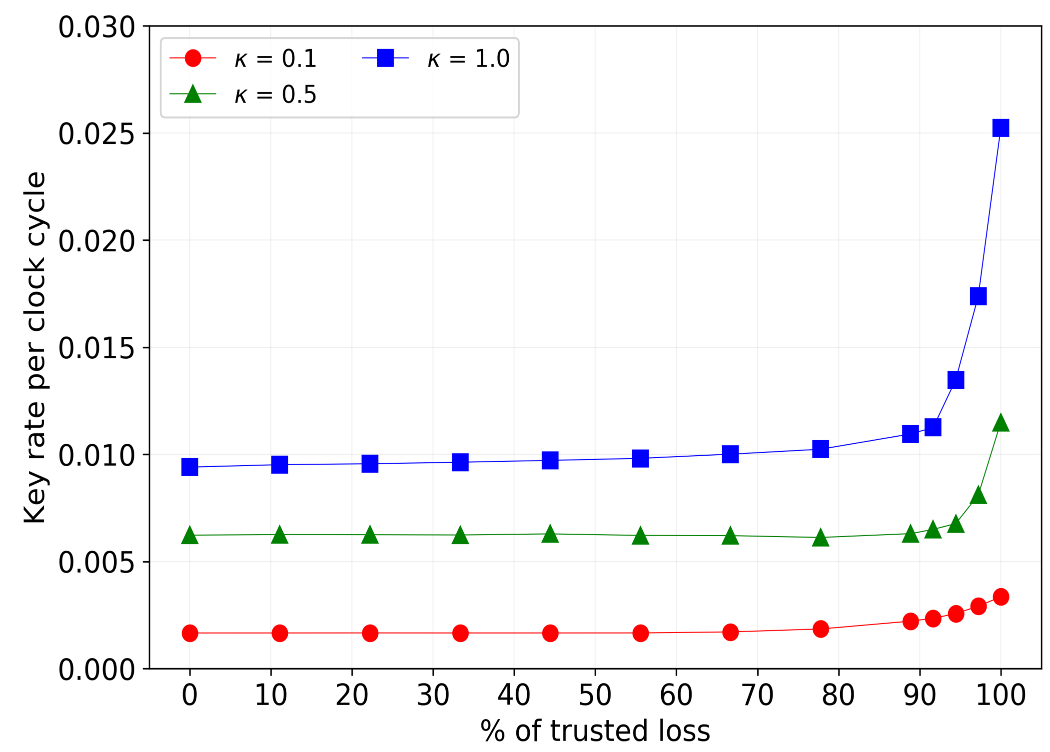


Fig. 3: Percentage change in key rates comparing our optimal lower bounds for key rates with [2]'s optimal key rates versus total transmissivity η. We label the changes for trusted (untrusted) dark counts with solid (dotted) lines. A positive change means that our key rate is higher.

- Our key rates are higher than [2]'s mainly in low-loss regime
- Encounter unphysical constraints for untrusted noise at $\eta < 0.2$

Effect of Trusted Loss



- Key rates increase with higher trusted loss ratio $\frac{1-\eta_{\mathrm{det}}}{1-\eta}$

Fig. 4: Assuming trusted dark counts, our lower bounds for key rates plotted against the proportion (in percentage) of the trusted loss coming from the detection inefficiency of Bob's detectors to a fixed total loss corresponding to total transmissivity η = 0.1.

Conclusion

New security proof:

Numerical Analysis [4]

\+

Flag-state squashing model [5]

\+

Higher tagging threshold

➔

- Higher key rates than [2]'s in low-loss regime
- Discover untrusted noise may lead to unphysical constraints
- Explored trusted loss scenario (not allowed in [1,2]'s proof)

References

[1] A. Ferenczi, V. Narasimhachar, and N. Lütkenhaus, Phys. Rev. A 86, 042327 (2012).
[2] S. Sunohara, K. Tamaki, and N. Imoto, (2013), arXiv:1302.1701 [quant-ph].
[3] V. Narasimhachar, Study of realistic devices for quantum key distribution (2011).
[4] A. Winick, N. Lütkenhaus, and P. J. Coles, Quantum 2, 77 (2018).
[5] Y. Zhang, P. J. Coles, A. Winick, J. Lin, and N. Lutkenhaus, (2020), arXiv:2004.04383 [quant-ph].

NSERC CRSNG
Industry Canada Industrie Canada
Canada
Financial support for this work has been partially provided by Huawei Technologies Canada Co., Ltd.