Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution

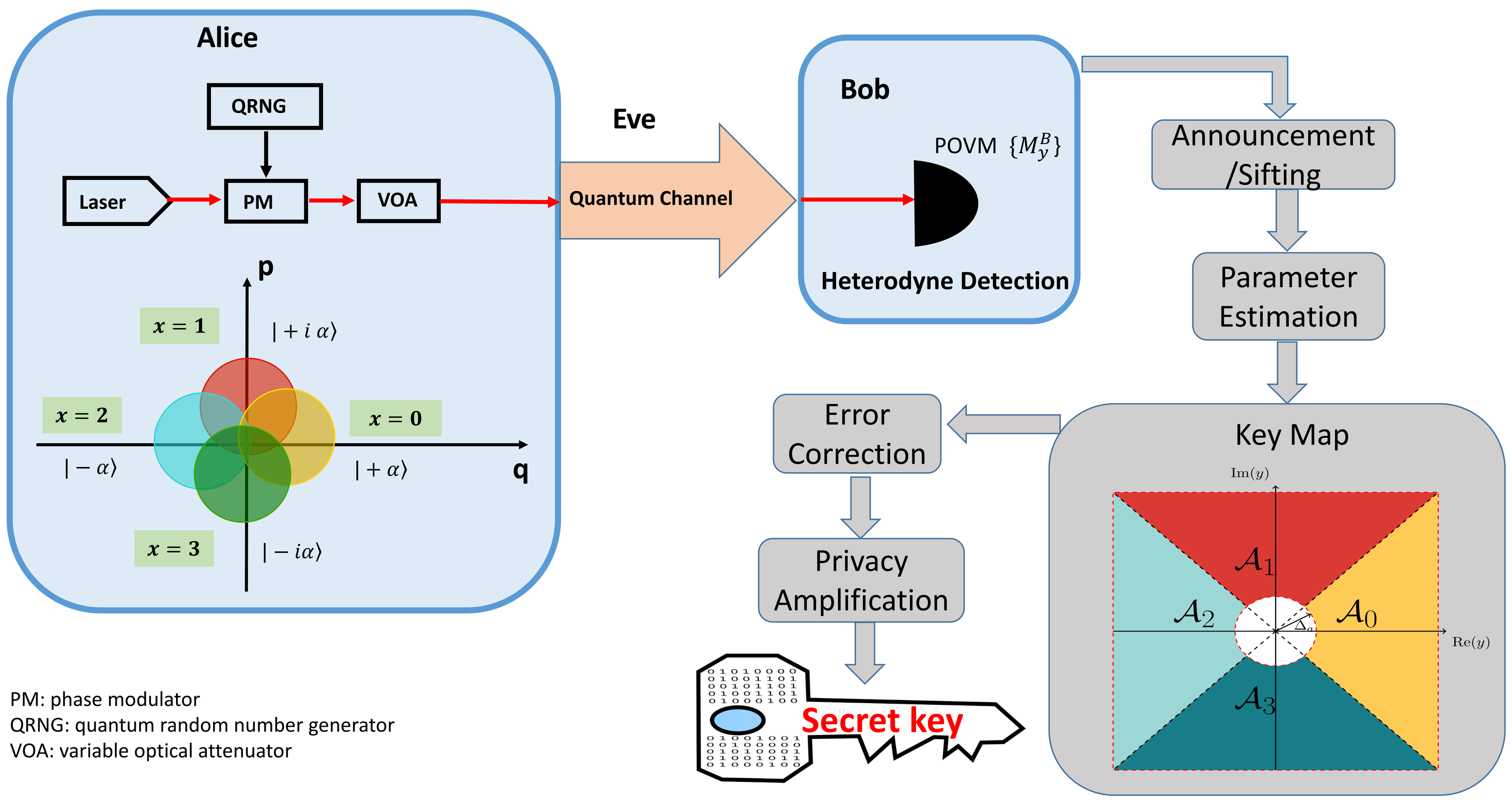
Jie Lin, Twesh Upadhyaya and Norbert Lütkenhaus
Institute for Quantum Computing and Department of Physics & Astronomy, University of Waterloo, Waterloo, ON, Canada

See Refs. [1, 2] for details.

INTRODUCTION

Discrete-modulated continuous-variable (CV) quantum key distribution (QKD) can be a cost-effective solution to distributing secret keys in the quantum-secured networks since it uses a setup nearly identical to modern telecommunication equipment.

PROTOCOL DESCRIPTION



PM: phase modulator
QRNG: quantum random number generator
VOA: variable optical attenuator

SECURITY PROOF METHOD

Source-replacement scheme: $|\Psi\rangle_{AA'} = \sum_x \sqrt{p_x}|x\rangle_A |\alpha_x\rangle_{A'}$

where Alice prepares $|\alpha_x\rangle$ with *a priori* probability p_x, and $\{|x\rangle\}$ is an orthonormal basis for the register A.

$\rho_{AB} = (id_A \otimes \mathcal{E}_{A'\to B})(|\Psi\rangle\langle\Psi|_{AA'})$, where $\mathcal{E}_{A'\to B}$ is a completely positive trace preserving (CPTP) map.

Asymptotic key rate (reverse reconciliation):

$$R^\infty = p_{\text{pass}}(\beta\, I(\mathbf{X};\mathbf{Z}) - \max_{\rho\in S}\chi(\mathbf{Z}:\mathbf{E}))$$ ← Devetak-Winter formula [3]

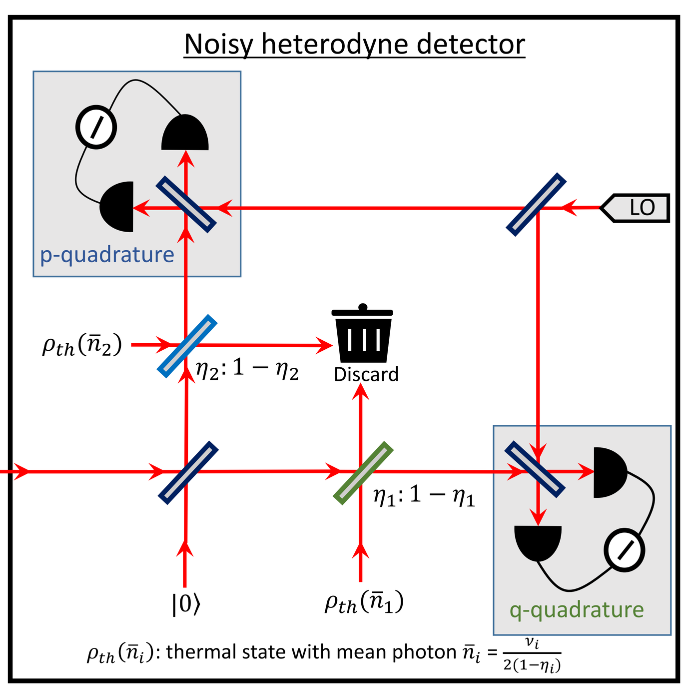
$$= p_{\text{pass}}(\min_{\rho\in S} H(\mathbf{Z}|\mathbf{E}) - H(\mathbf{Z}) + \beta\, I(\mathbf{X};\mathbf{Z}))$$ ← Rewriting $\chi(\mathbf{Z}:\mathbf{E})$

$$= \min_{\rho_{AB}\in S} D(\mathcal{G}(\rho_{AB})||\mathcal{Z}(\mathcal{G}(\rho_{AB}))) - p_{\text{pass}} H(\mathbf{Z}) + p_{\text{pass}}\,\beta\, I(\mathbf{X};\mathbf{Z})$$ ← Ref. [4]

where the cost of error correction per signal is $H(\mathbf{Z}) - \beta\, I(\mathbf{X};\mathbf{Z})$.

DETECTOR MODEL

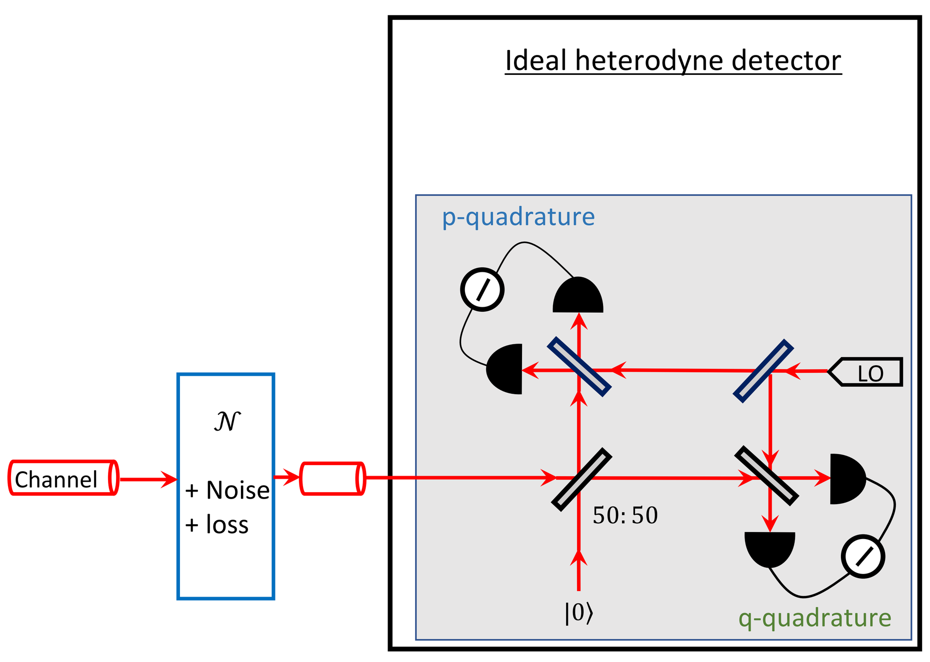
Trusted Detector Noise



Each homodyne detector has two imperfections:
detector efficiency: η_i; electronic noise: ν_i.

POVM:
a (scaled) projection onto displaced squeezed thermal states

Untrusted Detector Noise



POVM:
a (scaled) projection onto coherent states

KEY RATE OPTIMIZATION PROBLEM

Constraint formulation:

$P(y|x) = \text{Tr}(\rho_x M_y^B)$ → Data processing → $\int f(y,y^*)P(y|x)d^2y$ ⟷ General observables: $\hat{O} = \int f(y,y^*)M_y^B d^2y$

where $f(y,y^*)$ is a real-valued function such that the integral converges.

Nonlinear semidefinite program:

minimize $D(\mathcal{G}(\rho_{AB})||\mathcal{Z}(\mathcal{G}(\rho_{AB})))$
subject to:

$Tr[\rho_{AB}\,(|x\rangle\langle x|_A \otimes \hat{O}_i)] = p_x\,\langle O_i\rangle_x$

$\text{Tr}_B[\rho_{AB}] = \sum_{i,j=0}^{3}\sqrt{p_i p_j}\langle\alpha_j|\alpha_i\rangle|i\rangle\langle j|_A$

$\rho_{AB} \geq 0$, $\text{Tr}[\rho_{AB}] = 1$

for $x \in \{0,1,2,3\}$ and some choices of $\hat{O}_i$

Examples of $f(y,y^*)$:
$\text{Re}(y)$, $\text{Im}(y)$, yy^*-1

Examples of $\hat{O}_i$:
Quadrature operators $\hat{q}$ and $\hat{p}$
Photon-number operator $\hat{n}$

Region operators: $R_j = \int_{y\in\mathcal{A}_j} M_y^B d^2y$.

$\mathcal{G}(\sigma) = K\,\sigma\,K^\dagger$, where K is defined as $K = \sum_{z=0}^{3}|z\rangle_R \otimes 1_A \otimes (\sqrt{R_z})_B$

$\mathcal{Z}(\sigma) = \sum_{j=0}^{3} Z_j\,\sigma\,Z_j$, where $Z_j = |j\rangle\langle j|_R \otimes 1_{AB}$ for $j \in \{0,1,2,3\}$.

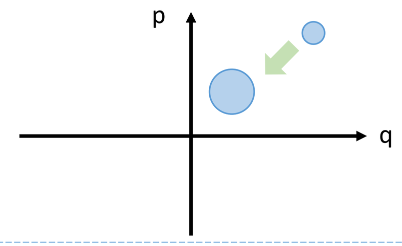
OUR CONTRIBUTION

- Asymptotic security proofs against collective attacks
- Both untrusted and trusted detector noise scenarios
- Allowing postselection of data
- Can handle different variants of the protocol:
  - homodyne/ heterodyne
  - general discrete modulation schemes (not restricted to four)

SIMULATION METHOD

Channel simulation

A phase-invariant Gaussian channel with
- **transmittance η_t**
- **excess noise ξ** referred to input of the channel



Detector simulation

Two homodyne detectors have the same imperfections:
detector efficiency: $\eta_d := \eta_1 = \eta_2$;
electronic noise: $\nu_{el} := \nu_1 = \nu_2$.

SIMULATION RESULTS

Ideal detector scenario

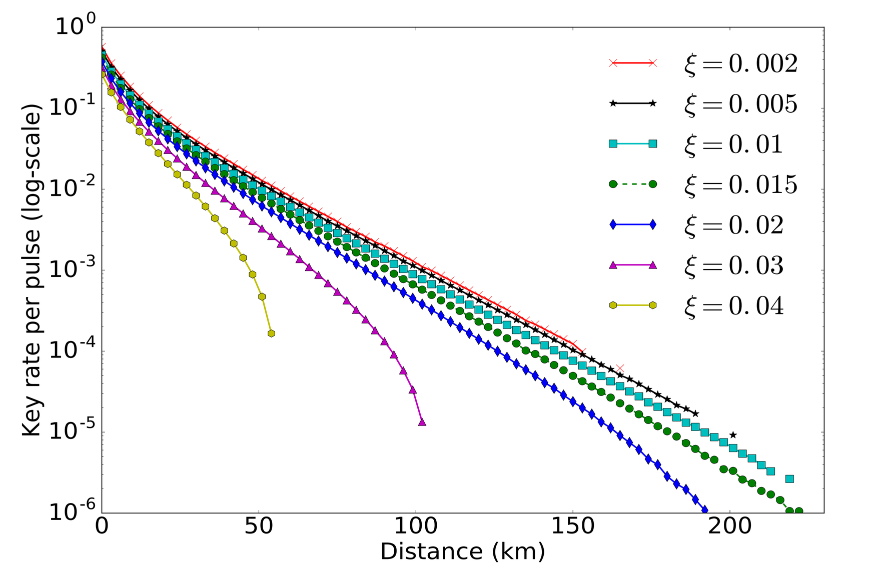


Fig. 7 of Ref. [1]. Key rate vs. transmission distance for different values of excess noise, from top to bottom, ξ = 0.002, 0.005, 0.01, 0.015, 0.02, 0.03, 0.04. Error correction efficiency β = 95%. Coherent state amplitude α is optimized via a coarse-grained search. (η_d=1, ν_{el}=0)

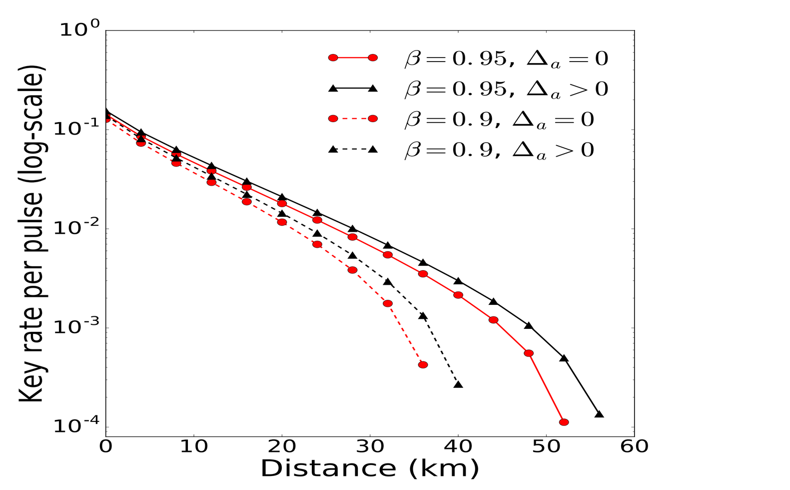


Fig. 10 (b) of Ref. [1]. Key rate vs. transmission distance for postselection. The relevant postselection parameter Δ_a is optimized via a coarse-grained search in the interval [0.4, 0.7] where the optimal value falls. α = 0.6, ξ = 0.04. (η_d=1, ν_{el}=0)

Trusted detector scenario

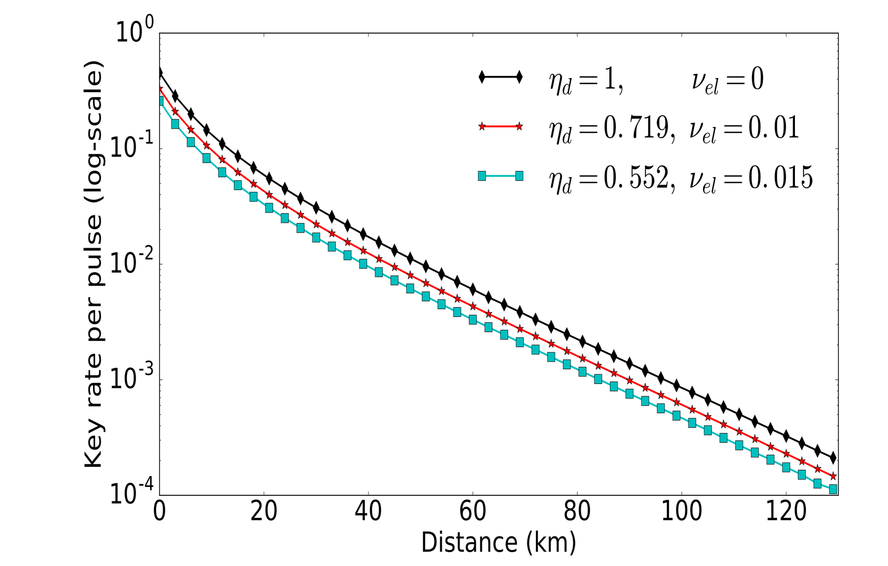


Fig. 4 of Ref. [2]. Key rate vs. transmission distance for different detector imperfections. The excess noise is ξ = 0.01. Error correction efficiency β = 95%. Coherent state amplitude α is optimized via a coarse-grained search.

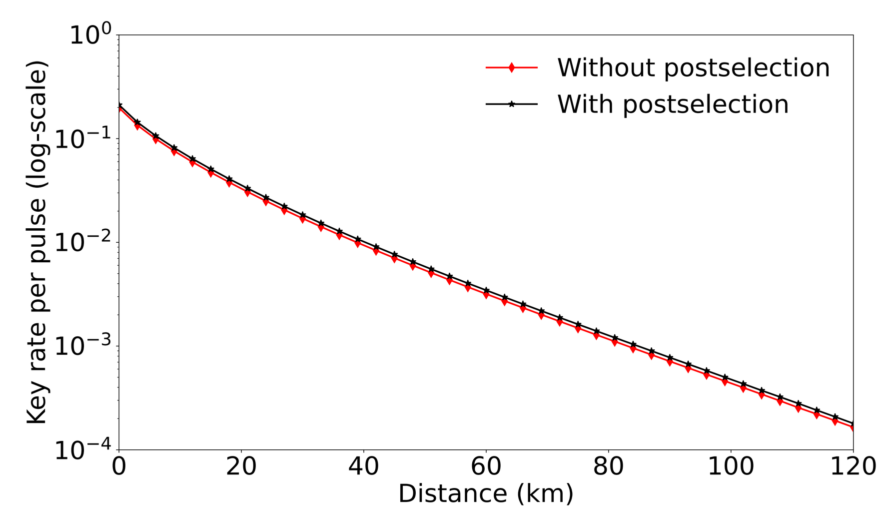


Fig. 8 of Ref. [2]. Key rate vs. transmission distance for postselection. Detector parameters are η_d=0.552, ν_{el}=0.015. The relevant postselection parameter Δ_a is optimized via a coarse-grained search in the interval [0.45, 0.7]. α = 0.75, ξ = 0.01. Error correction efficiency β = 95%.

Comparison between **trusted** and **untrusted** detector noise scenarios

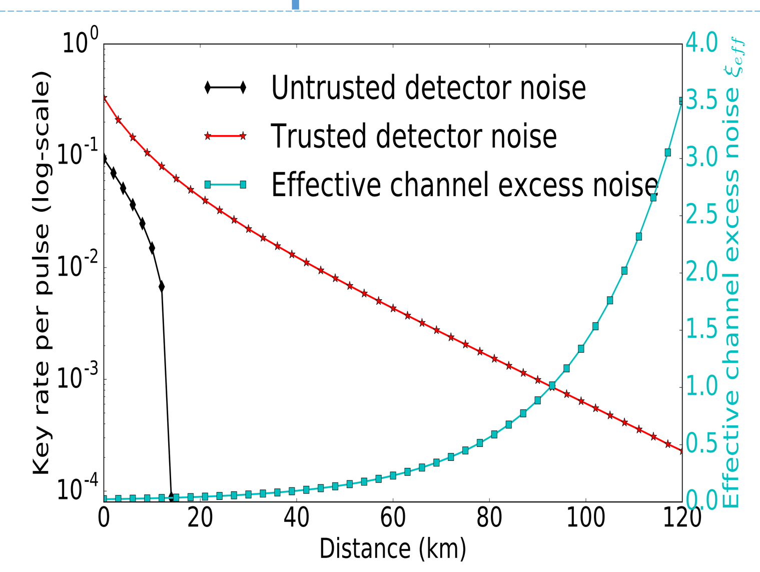


Fig. 3 of Ref. [2]

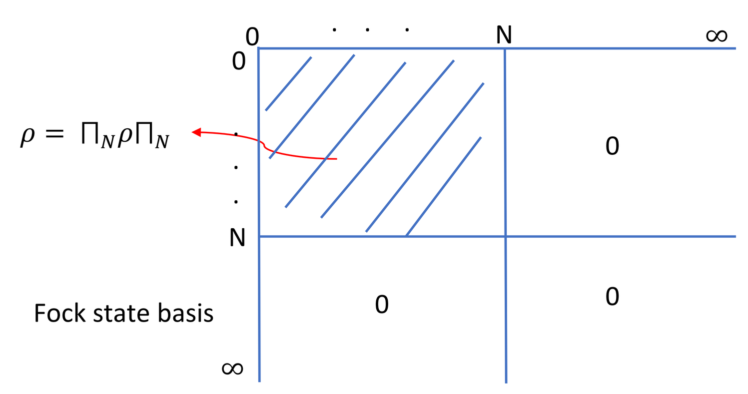
Parameters:
The excess noise: ξ = 0.01
Detector efficiency: η_d = 0.719
Electronic noise: ν_{el} = 0.01
Error correction efficiency β = 95%

Two scenarios with the same observed statistics

Coherent state amplitude α is optimized.

PHOTON-NUMBER CUTOFF ASSUMPTION

Assume $\rho_{AB} = (1_A \otimes \Pi_N)\rho_{AB}(1_A \otimes \Pi_N)$ for a sufficiently large integer N.



See poster by Twesh Upadhyaya for removing this assumption

Intuition of the cutoff assumption:
When mean photon number n << N, essential information is captured in ≤ N subspace

OUTLOOK

Refs. [1, 2] or the work by T. Upadhyaya et. al + Ref. [5] + Ref. [6] ? → Finite key analysis

REFERENCES

[1] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Phys. Rev. X 9, 041064 (2019), arXiv: 1905.10896
[2] J. Lin and N. Lütkenhaus, arXiv: 2006.06166
[3] I. Devetak and A. Winter, Proc. R. Soc. A 461, 207 (2005), arXiv: quant-ph/0306078
[4] A. Winick, N. Lütkenhaus, and P. J. Coles, Quantum 2, 77 (2018), arXiv: 1710.05511
[5] I. George, J. Lin and N. Lütkenhaus, arXiv: 2004.11865
[6] R. Renner and J. I. Cirac, Phys. Rev. Lett. 102, 110504 (2009), arXiv: 0809.2243
Related work: [7] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Phys. Rev. X 9, 021059 (2019), arXiv: 1902.01317

Discovery Grants Program: Grant No. 341495
Collaborative Research and Development Program, Grant No. CRDP J 522308-17
Financial support for this work has been partially provided by Huawei Technologies Canada Co., LTD.