OAK RIDGE National Laboratory

Discrete-variable quantum key distribution using conjugate homodyne detection

Bing Qi

Quantum information science group

Oak Ridge National Laboratory

ORNL is managed by UT-Battelle, LLC for the US Department of Energy

U.S. DEPARTMENT OF ENERGY

Qcrypt August 25 2021

Collaborators

Dr. Pavel Lougovski
Now at Amazon Web Services

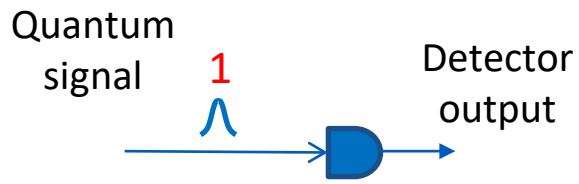
Dr. Brian Williams
Oak Ridge National Laboratory

- B. Qi, P. Lougovski, and B. P. Williams, "Characterizing photon number statistics using conjugate optical homodyne detection", Optics Express 28, 2276-2290 (2020)
- B. Qi, "Bennett-Brassard 1984 quantum key distribution using conjugate homodyne detection", Phys. Rev. A 103, 012606 (2021)

Detector in quantum key distribution

❑ Single-photon detector

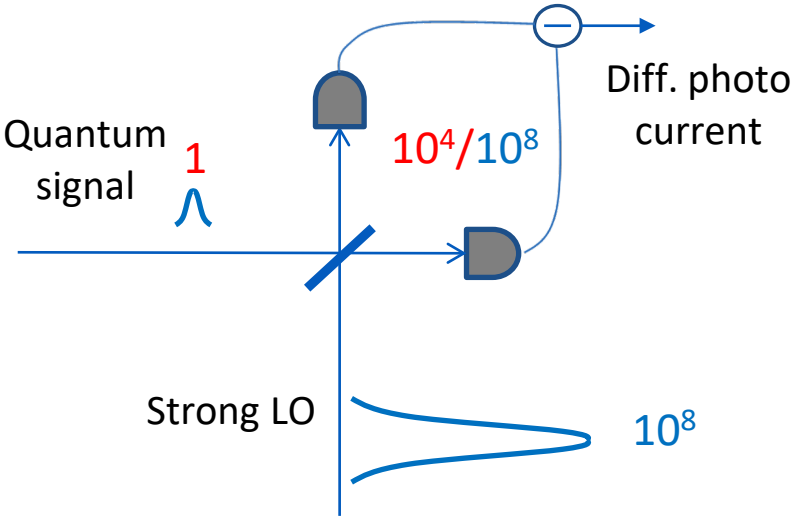
- ➢ Widely used in discrete-variable (DV) QKD
- ➢ Extremely low noise achievable
- ➢ Low temperature operation
- ➢ Limited detection rate due to dead-time



Direct detection

❑ Optical homodyne detection

- ➢ Widely used in continuous-variable (CV) QKD
- ➢ High efficiency, high speed, room temperature operation
- ➢ Immune to broadband background light
- ➢ Require a reliable phase reference.



Coherent detection

Motivation

Can we operate optical homodyne detectors in phase-insensitive, photon counting mode to implement DV QKD?

Such a scheme may inherit certain advantages of coherent detection without requiring a phase reference

Basic idea: conjugate homodyne as photon counter

Electric field

$$E(t) = E_x \cos \omega t + E_p \sin \omega t \Longrightarrow \text{Energy} \propto |E_x|^2 + |E_p|^2$$

$$\hat{X} \qquad \hat{P} \Longrightarrow \text{Photon number} \propto |X|^2 + |P|^2$$

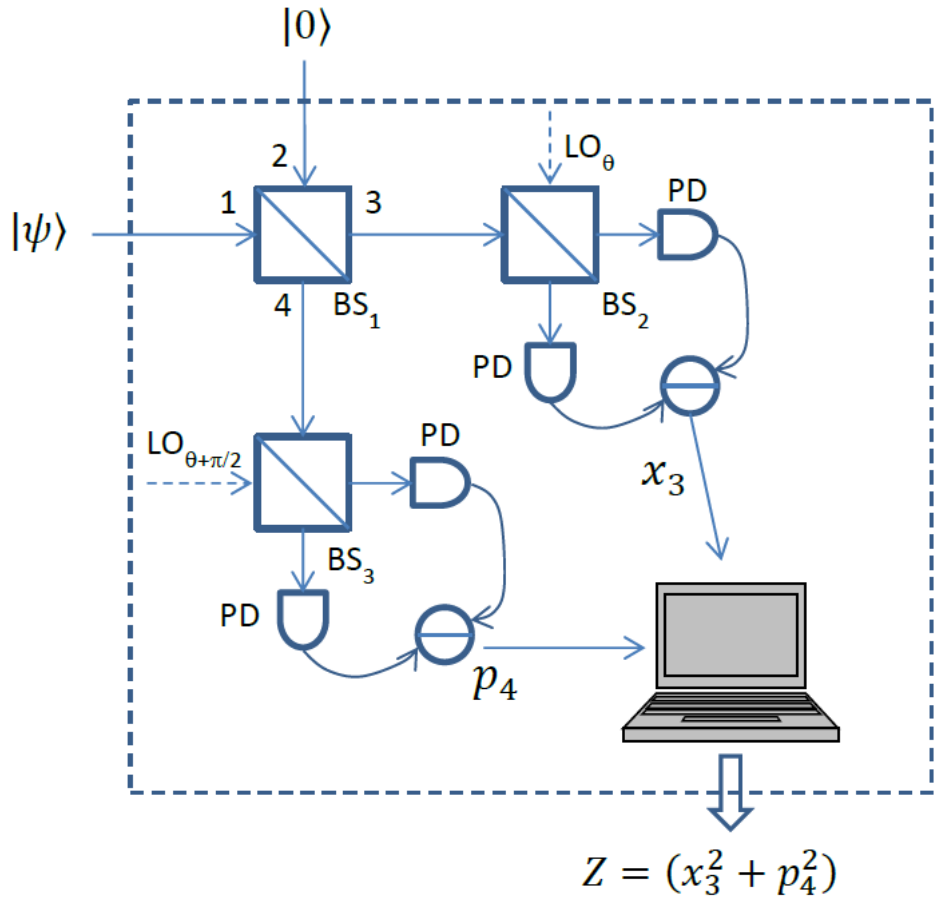
However

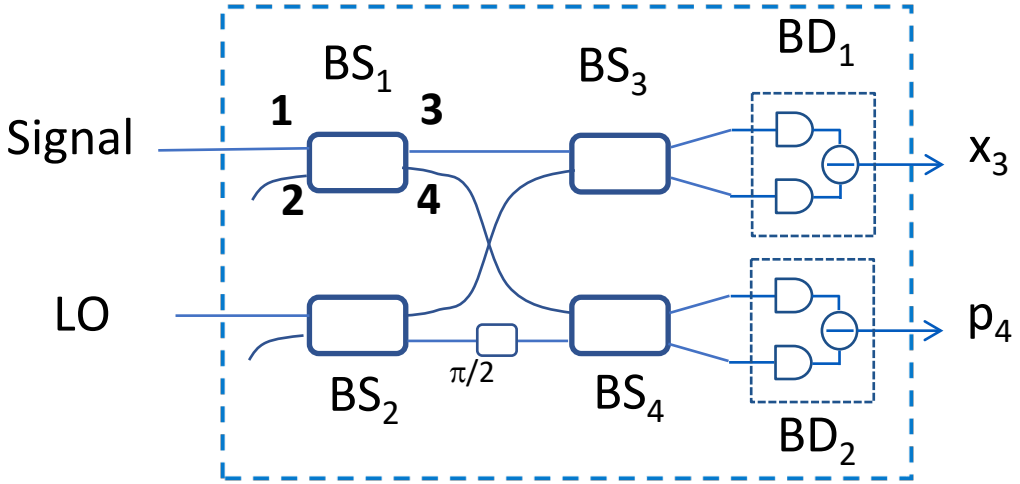
$$[\hat{X}, \hat{P}] \neq 0$$

Uncertainty principle ⟹

Intrinsically noisy measurement

Conjugate homodyne as single-photon detector





Commercial product from Optoplex

Single-shot measurement

Define $\hat{Z} = \hat{X}^2 + \hat{P}^2$

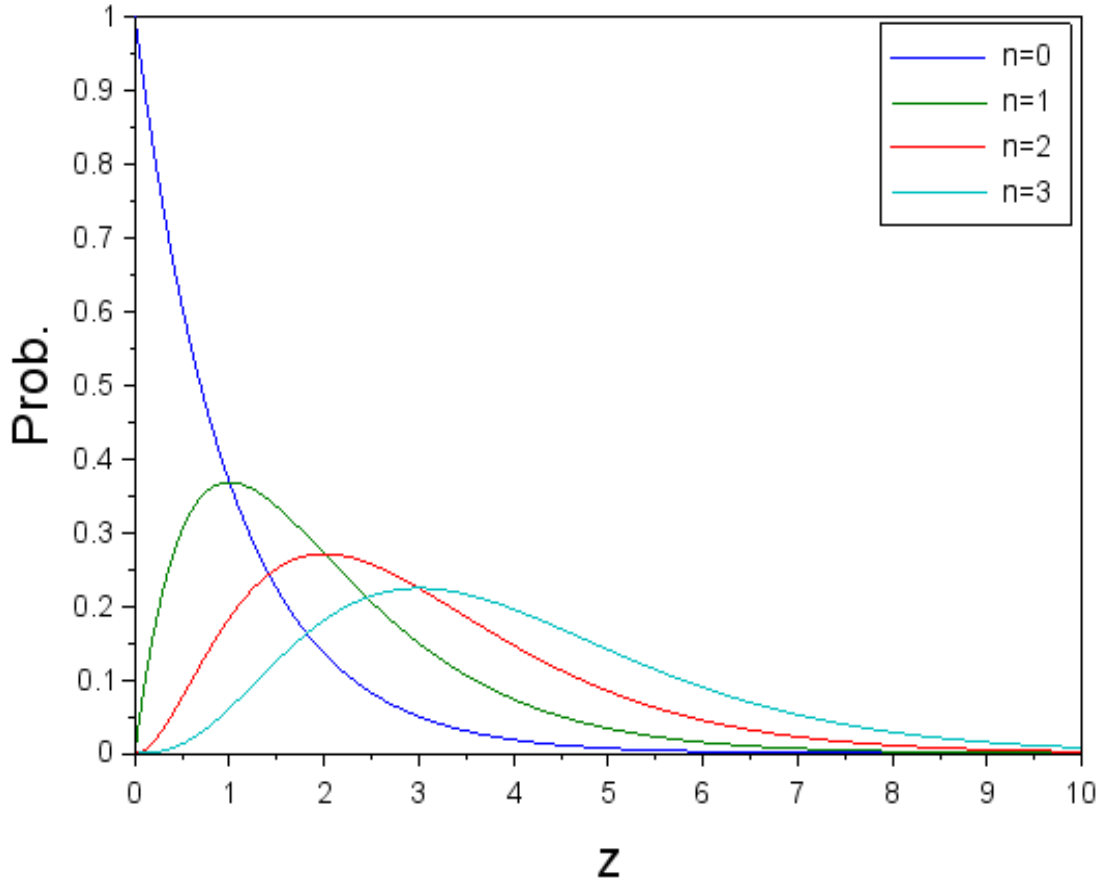
For an arbitrary input state ρ, the probability density of Z is

$$P(z) = e^{-z} \sum_{n=0}^{\infty} \frac{\rho_{nn}}{n!} z^n$$

Phase insensitive detector

For number state $|n\rangle$ input

$$P(z|n) = e^{-z} \frac{z^n}{n!}$$



B. Qi, P. Lougovski, and B. P. Williams, Optics Express 28, 2276-2290 (2020)

Threshold single-photon detector

Detection efficiency

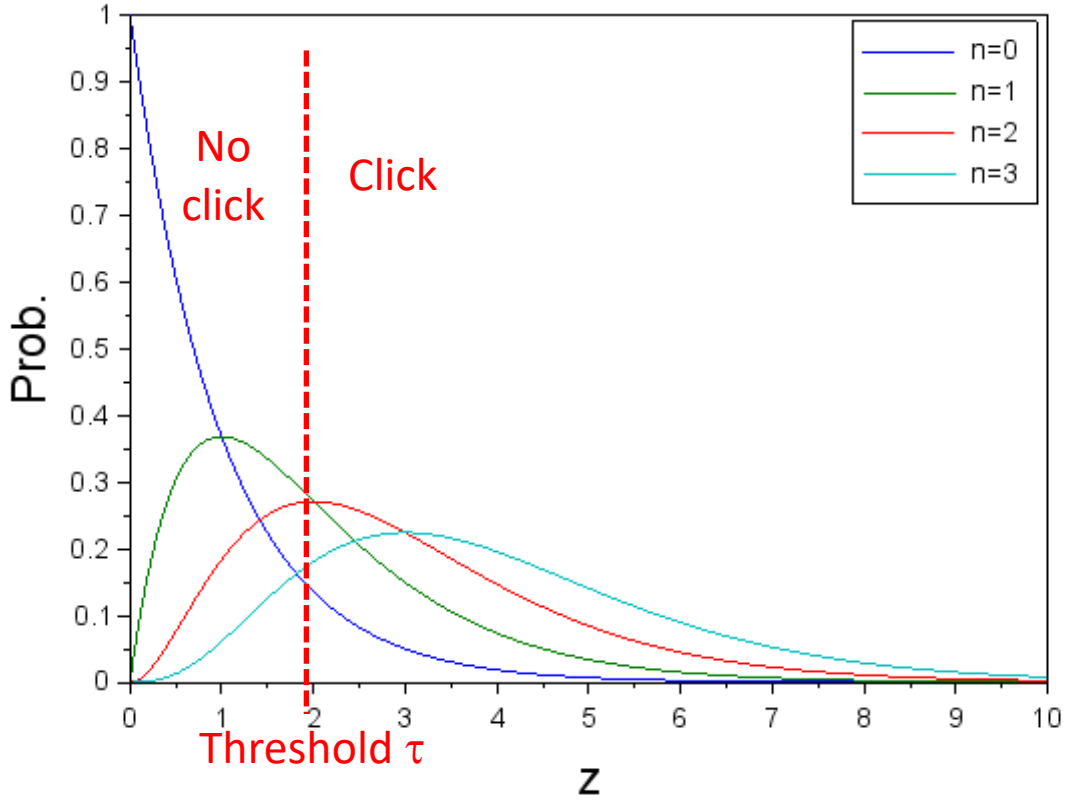
$$\eta = \int_{\tau}^{\infty} P(z|1)dz = e^{-\tau}(\tau + 1)$$

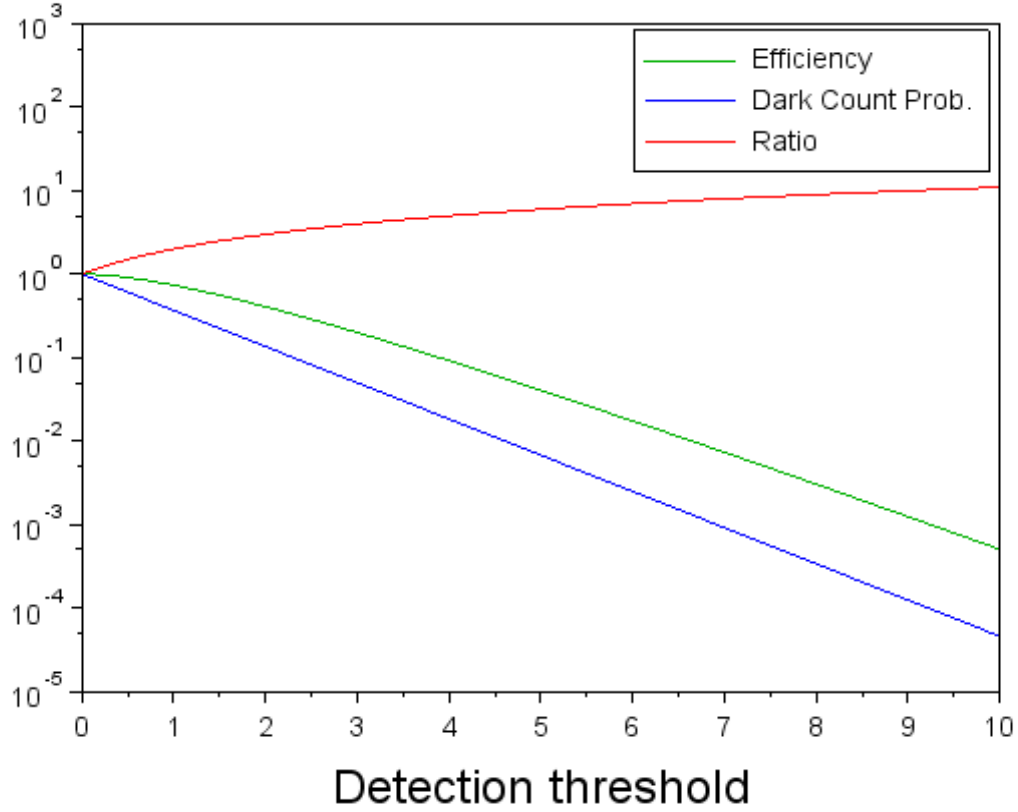
Dark count probability

$$\mathrm{D} = \int_{\tau}^{\infty} P(z|0)dz = e^{-\tau}$$

Ratio

$$R = {}^{\eta}/_{D} = \tau + 1$$

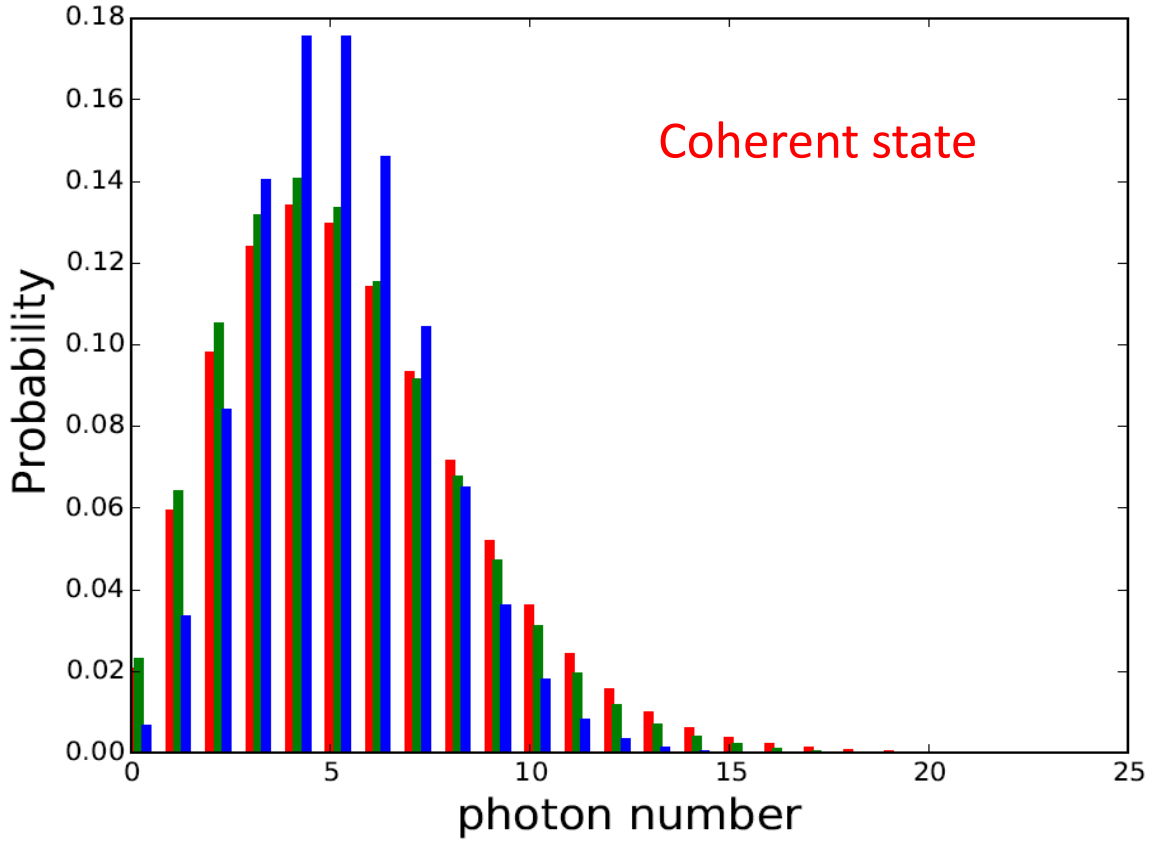


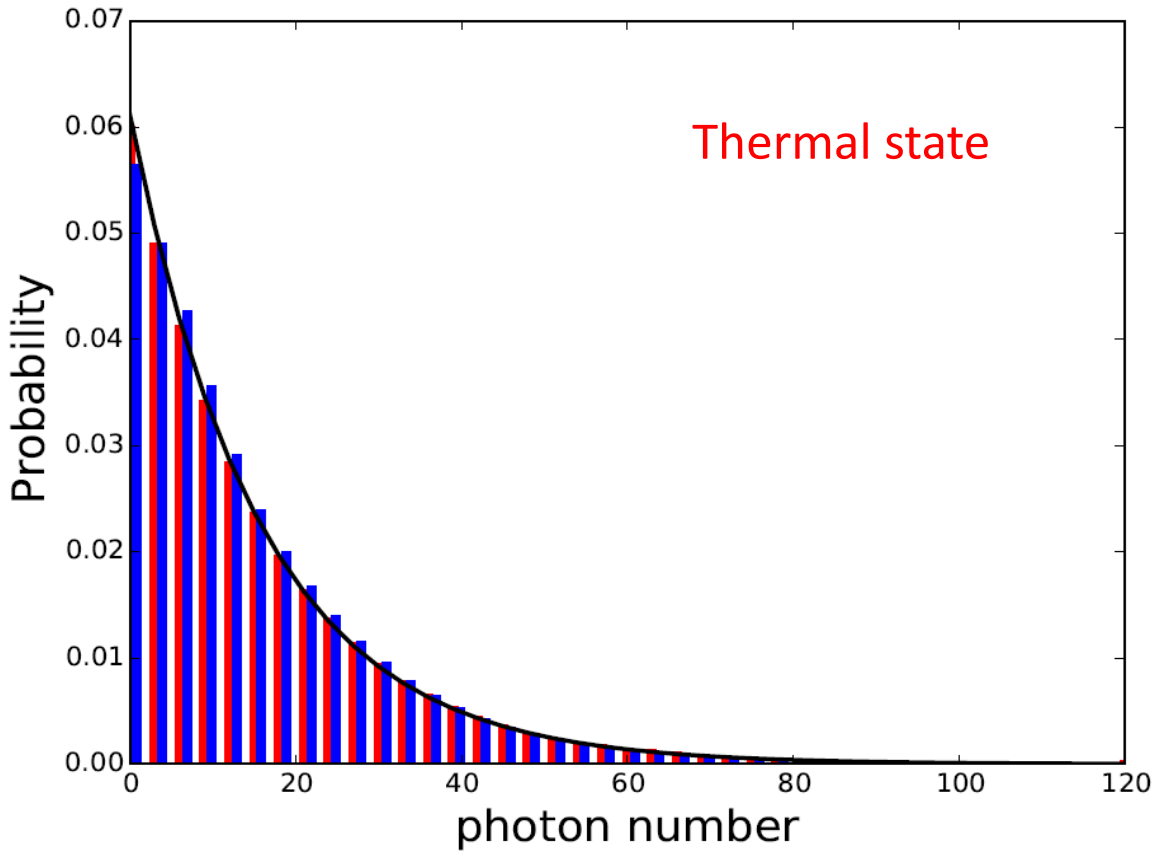


B. Qi, P. Lougovski, and B. P. Williams, Optics Express 28, 2276-2290 (2020)

Repeated measurement

From $P(z) = e^{-z} \sum_{n=0}^{\infty} \frac{\rho_{nn}}{n!} z^n$ ⇨ reconstruct photon number distribution



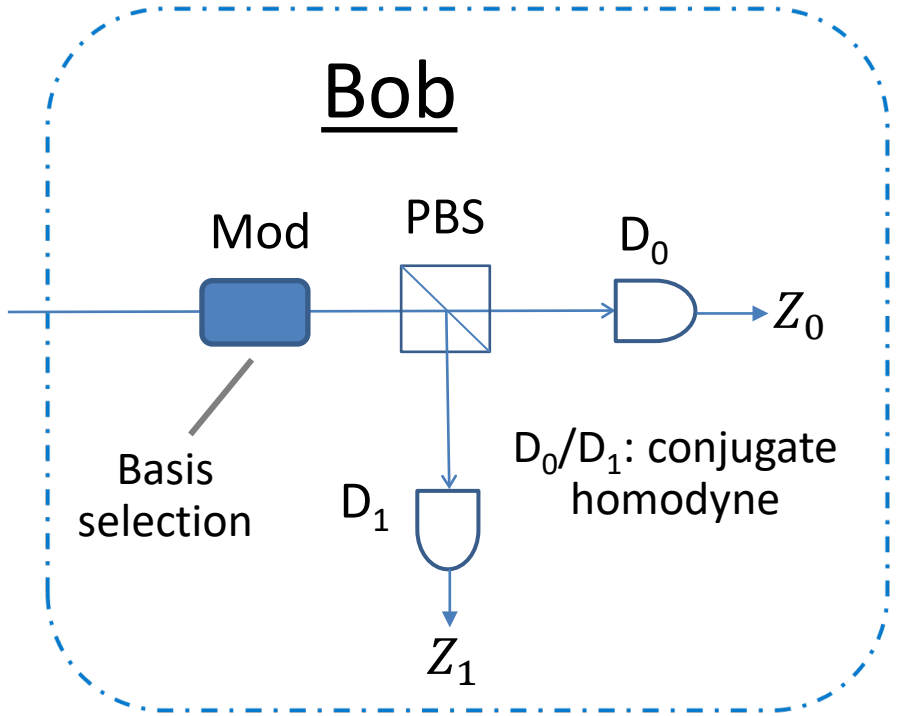


B. Qi, P. Lougovski, and B. P. Williams, Optics Express 28, 2276-2290 (2020)

BB84 QKD using conjugate homodyne detection

Protocol & assumptions

- Efficient BB84 QKD protocol—one basis is chosen more often than the other;
- Polarization encoding with a perfect single-photon source;
- No technical imperfection except channel loss;
- Perfect error correction approaching the Shannon limit
- Asymptotic case (neglect any finite data size effects)



Bob assigns the bit value as

0 (if $Z_0 > \tau$ and $Z_1 < \tau$);
Null (if $Z_0 < \tau$ and $Z_1 < \tau$);
1 (if $Z_0 < \tau$ and $Z_1 > \tau$);
Random (if $Z_0 > \tau$ and $Z_1 > \tau$).

Standard security analysis

Secret key rate

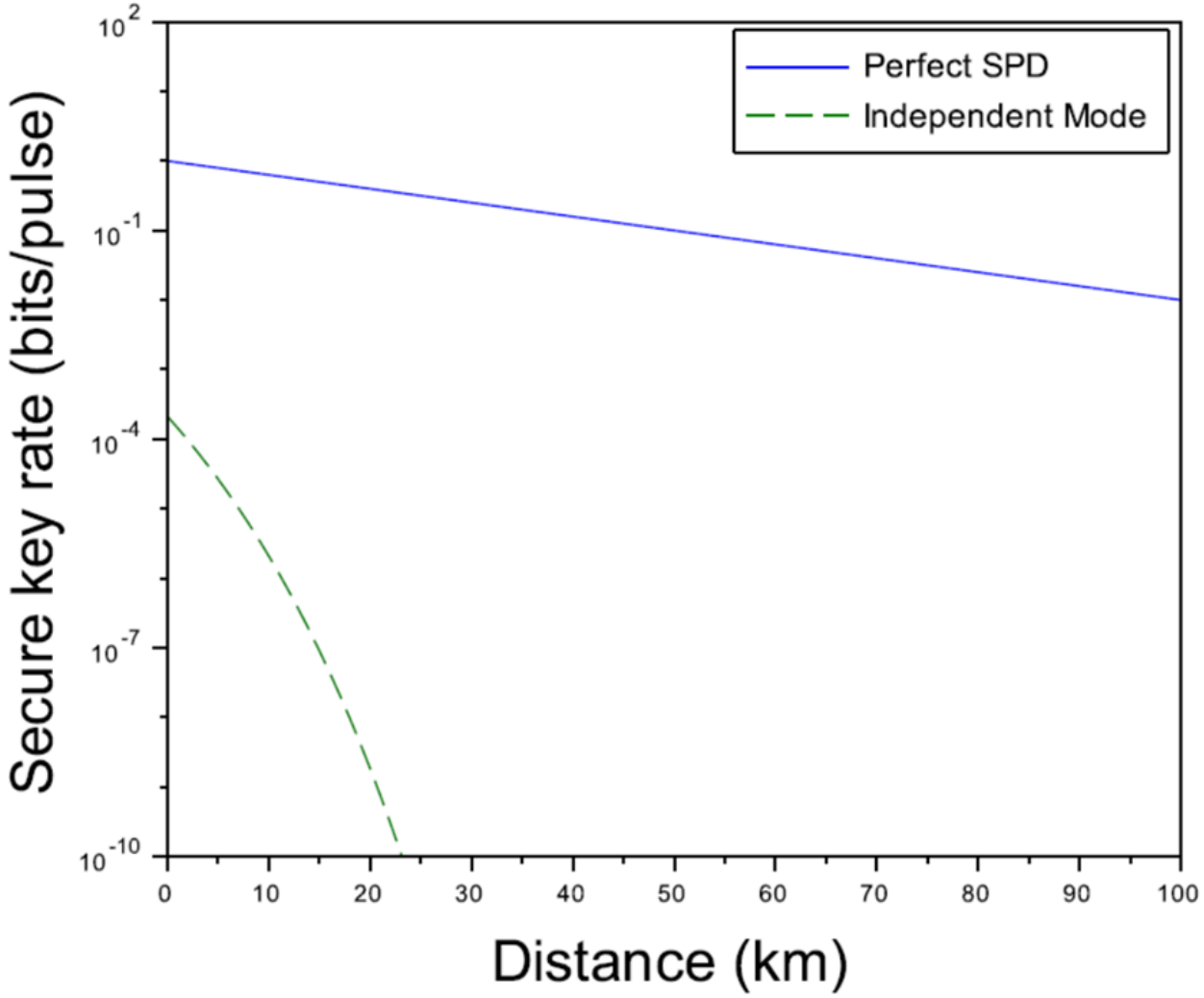
$$R = Q^{(Z)}\left[1 - H_2\left(E^{(X)}\right) - H_2\left(E^{(Z)}\right)\right]$$

$Q^{(Z)}$: Gain

$E^{(Z)}$ ($E^{(X)}$): Quantum bit error rate (QBER)

$$Q = 1 - P_{null}$$
$$= (\eta_{ch}\tau + 2)e^{-\tau} - (\eta_{ch}\tau + 1)e^{-2\tau}$$

$$E = \frac{P_{wrong} + 0.5P_{double}}{Q}$$
$$= \frac{e^{-\tau} - 0.5(\eta_{ch}\tau + 1)e^{-2\tau}}{Q}$$

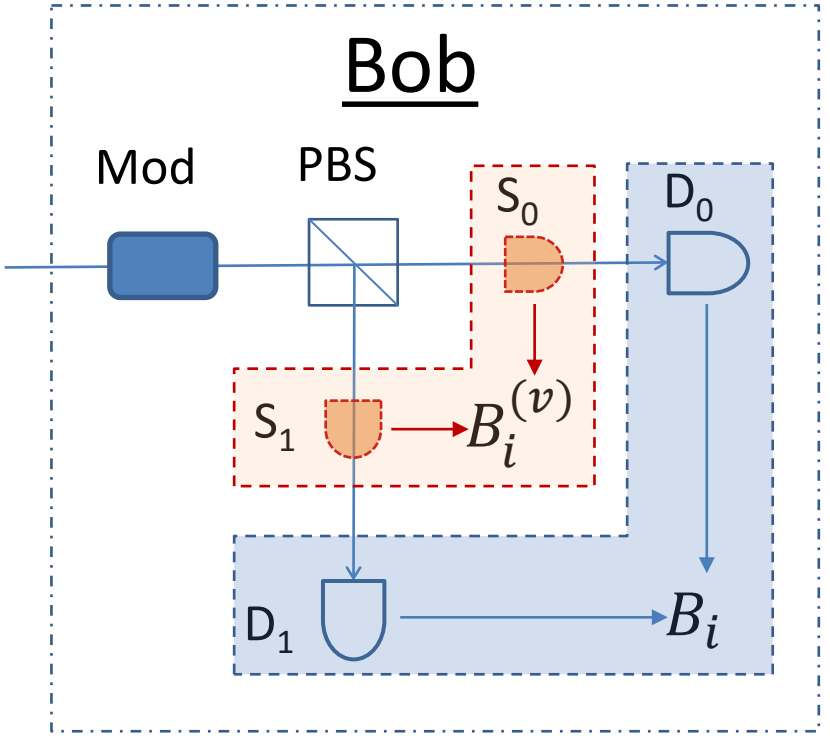


Two features of the detection scheme

- Trusted detector noise: fundamental detector noise cannot be controlled/accessed by Eve
- Photon number distribution at Bob can be reconstructed

Approach

- Introducing virtual ideal SPDs (S_0 and S_1)
- Secret key is generated from real detectors (D_0 and D_1)
- Detection statistics (QBER) of virtual detectors can be determined from the outputs of real detectors and will be used to upper bound Eve's information

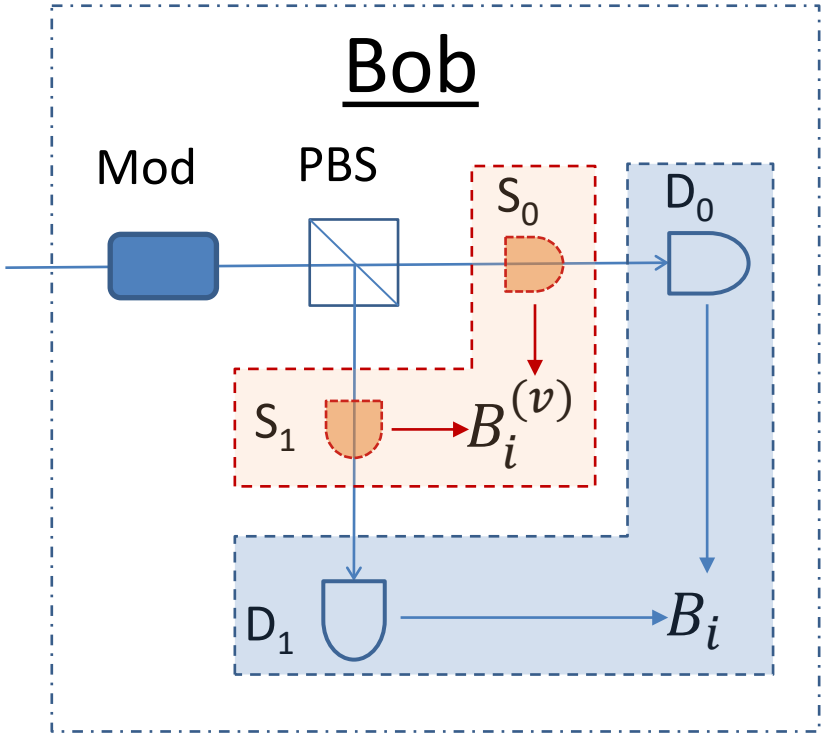


Improved security analysis

Secret key rate using reverse reconciliation

$$R = Q_{1,0}^{(Z)} + Q_{1,1}^{(Z)}\left[1 - H_2\left(E_{1,1}^{(X,V)}\right)\right] - fQ^{(Z)}H_2\left(E^{(Z)}\right)$$

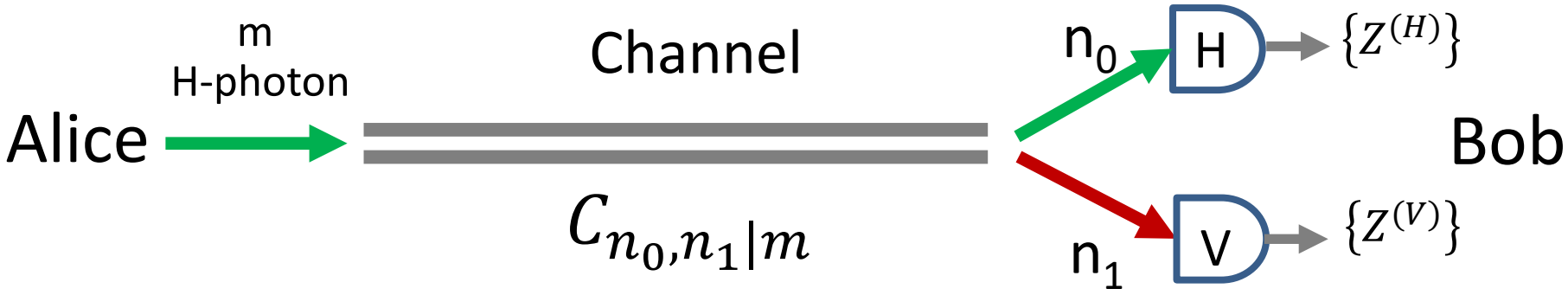
$Q^{(Z)}$	Overall gain in Z-basis (real detectors)
$E^{(Z)}$	Overall QBER in Z-basis (real detectors)
$Q_{\mathrm{i},j}^{(Z)}$	Gain in Z-basis from the cases when i photons are sent by Alice and j photons arrive at Bob
$E_{1,1}^{(X,V)}$	QBER in X-basis for the cases of when 1 photon is sent by Alice and 1 photon arrives at Bob (virtual detectors)
f	Reconciliation efficiency



B. Qi, Phys. Rev. A, 103, 012606 (2021)

Channel transformation

Alice sends m photon in H-polarization
Bob performs measurement in H/V basis



*Channel transformation $C_{n_0,n_1|m}$: the probability n_0 H-photons and n_1 V-photons outputted from the channel given m H-photons input

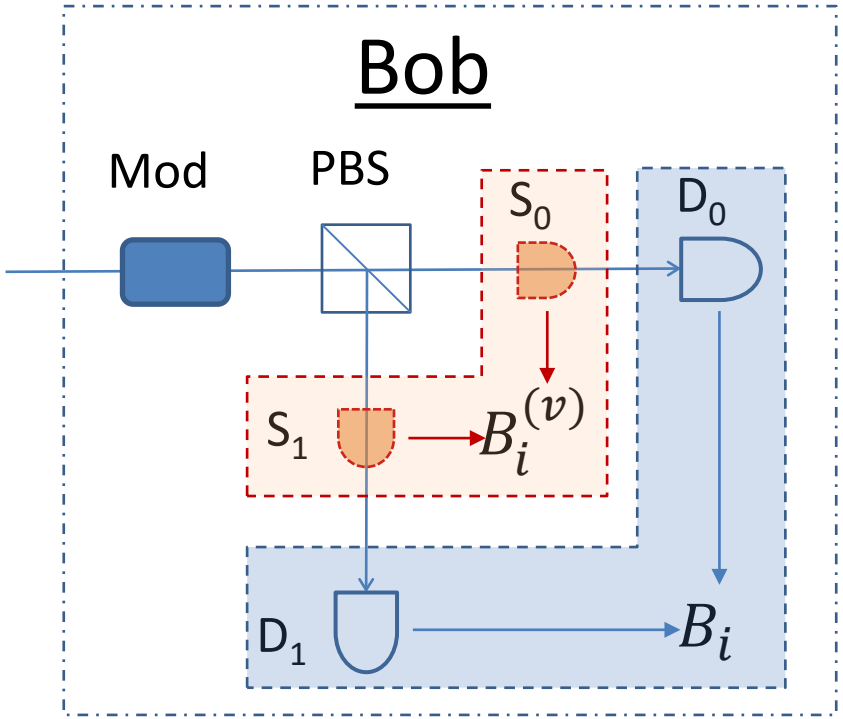
From the measurement results of real detectors $\{Z_i^{(H)}, Z_i^{(V)}, i = 1,2 \dots\}$, Bob can determine $C_{n_0,n_1|1}$, including $C_{0,0|1}$, $C_{1,0|1}$, and $C_{0,1|1}$

See also, E. Lavie, I. W. Primaatmaja, W. Y. Kon, C. Wang, C. Lim, arXiv preprint arXiv:2102.08419

Secret key rate

Detector outputs

- Raw keys
- Channel transformation $C_{n_0,n_1|1}$



Secret key rate

$$R = Q_{1,0}^{(Z)} + Q_{1,1}^{(Z)}\left[1 - H_2\left(E_{1,1}^{(X,V)}\right)\right] - fQ^{(Z)}H_2\left(E^{(Z)}\right)$$

$Q^{(Z)}$ and $E^{(Z)}$ can be determined from raw keys

$$Q_{1,0} = Q_{1,0,0} = C_{0,0|1}D_{0,0}$$

Detector response $D_{0,0}$ is given by

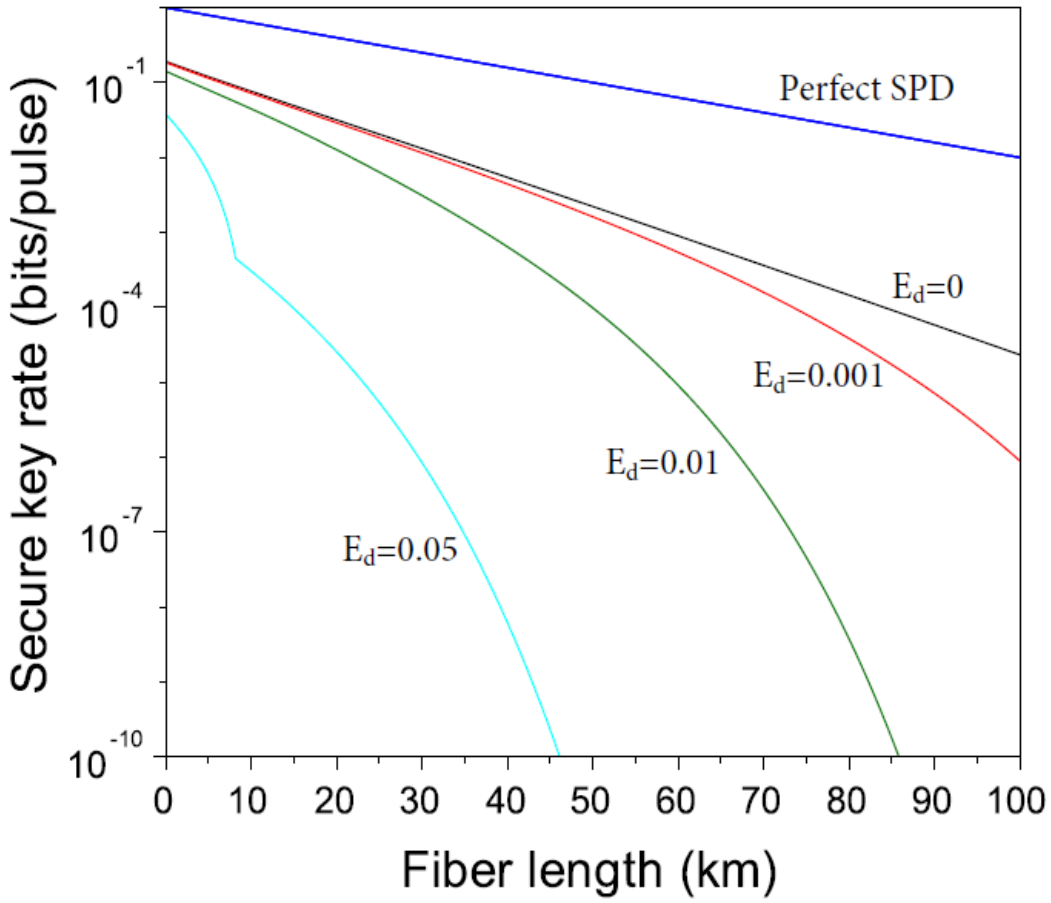
$$D_{0,0} = 2e^{-\tau}(1 - e^{-\tau})$$

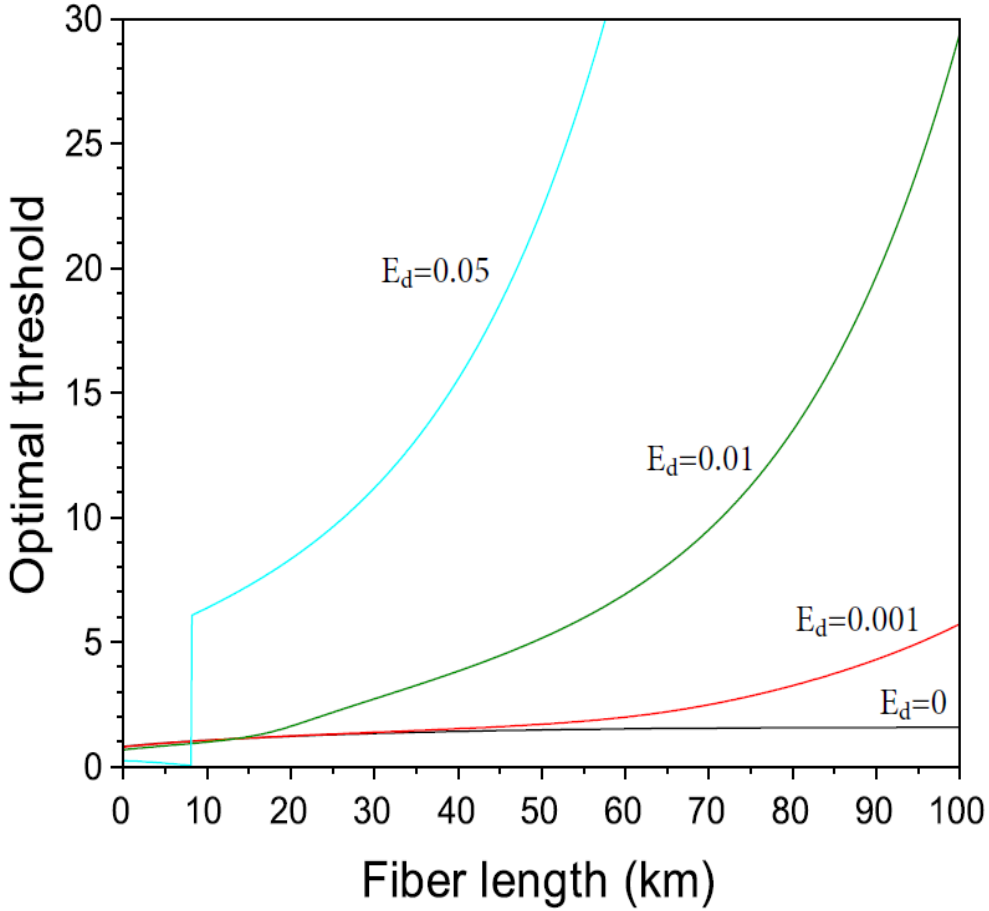
$$Q_{1,1} = Q_{1,1,0} + Q_{1,0,1} = C_{1,0|1}D_{1,0} + C_{0,1|1}D_{0,1}$$

$$D_{0,1} = D_{1,0} = (\tau + 2)e^{-\tau} - 2(\tau + 1)e^{-2\tau}$$

$$E_{1,1}^{(V)} = \frac{C_{0,1|1}}{C_{0,1|1} + C_{1,0|1}}$$

Simulation results





The proposed scheme could be useful for short-distance applications

B. Qi, Phys. Rev. A, 103, 012606 (2021)

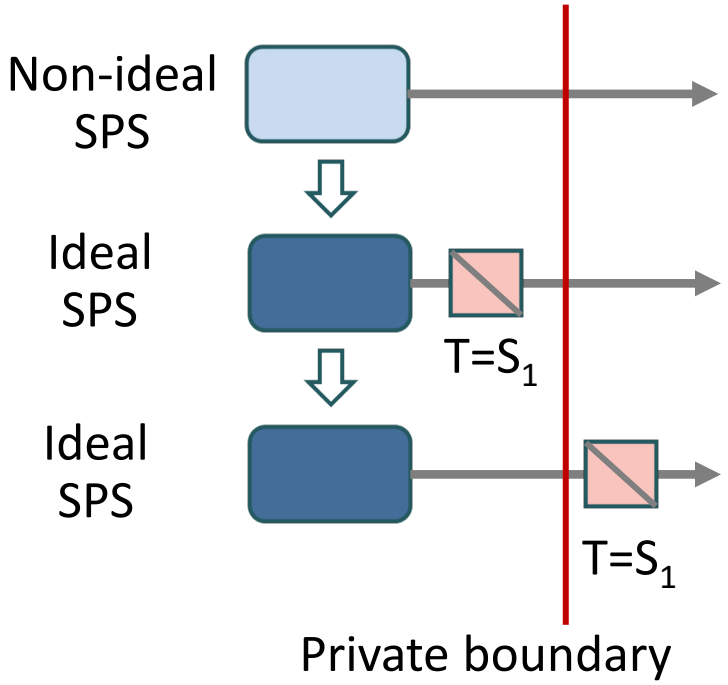
How about practical photon sources?

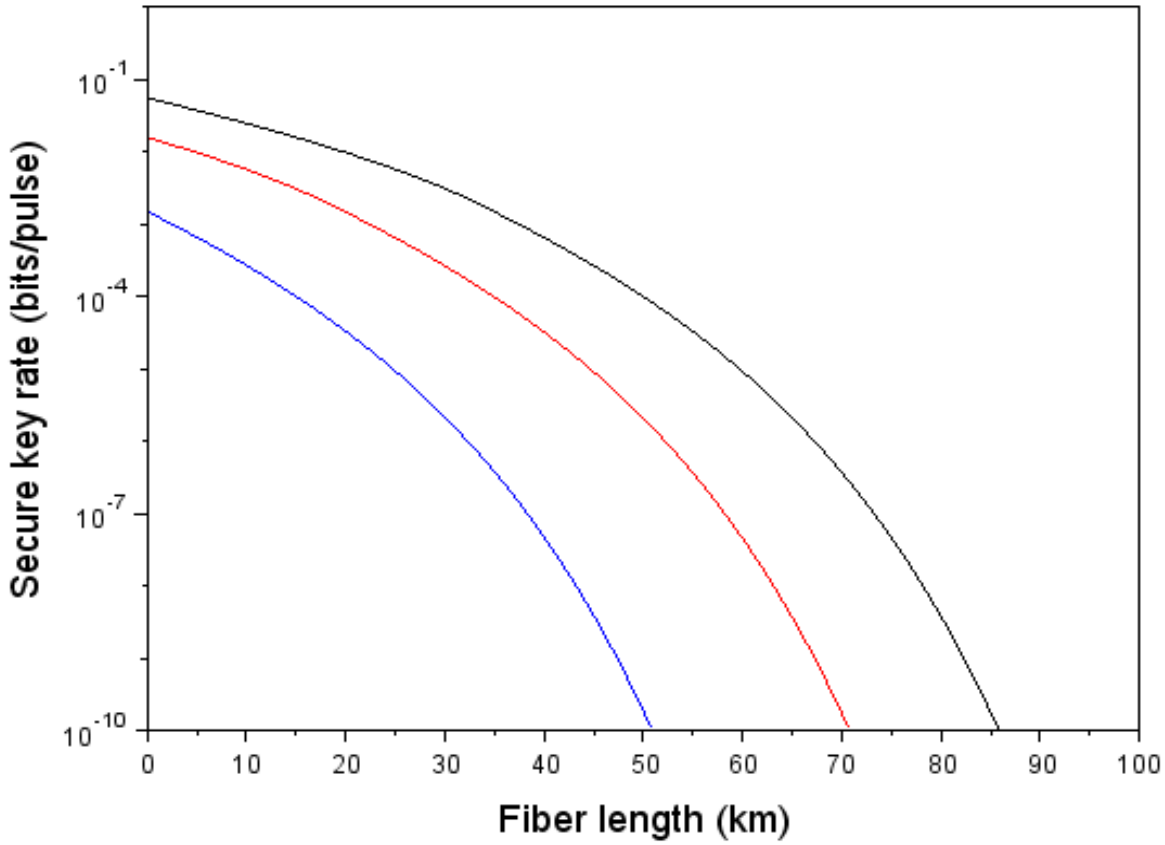
(Some very preliminary results)

Non-ideal single-photon source (SPS)

Assumption*

(a) Vacuum state probability S_0
(b) Single-photon probability S_1=1-S_0
(c) Multi-photon probability is negligible





The secret key rate of ideal SPS with channel transmittance η_{ch} replaced by $\eta = S_1\eta_{ch}$

Simulation results (S_1=1—black; 0.5—red; and 0.2—bule)
Intrinsic QBER= 0.01

*P. Chaiwongkhot, S. Hosseini, A. Ahmadi, et al, arXiv preprint arXiv:2009.11818 (2020)

Phase-randomized weak coherent source + decoy states

Infinite decoy-state protocol

- Each transmission, Alice randomly prepares either signal state (μ) or one of the decoy-states ($\nu_i, i = 1,2, \ldots.$)
- Decoy states are used to determine channel transformation $C_{n_0,n_1|m}$
- Signal state is used to generate secret key

Channel transformation of coherent state ν_i ($C_{n_0,n_1|\nu_i}$) can be determined experimentally

Channel transformation of number state ($C_{n_0,n_1|m}$) can be determined from $C_{n_0,n_1|\nu_i}$ ($i = 1,2, \ldots.$) using following linear equations

$$\sum_{m=0}^{\infty} S_m^{(\nu_i)} C_{n_0,n_1|m} = C_{n_0,n_1|\nu_i}$$

where $S_m^{(\nu_i)} = \frac{\nu_i^m}{m!} e^{-\nu_i}$ is the photon number distribution of coherent state

Phase-randomized weak coherent source + decoy states

Secret key rate

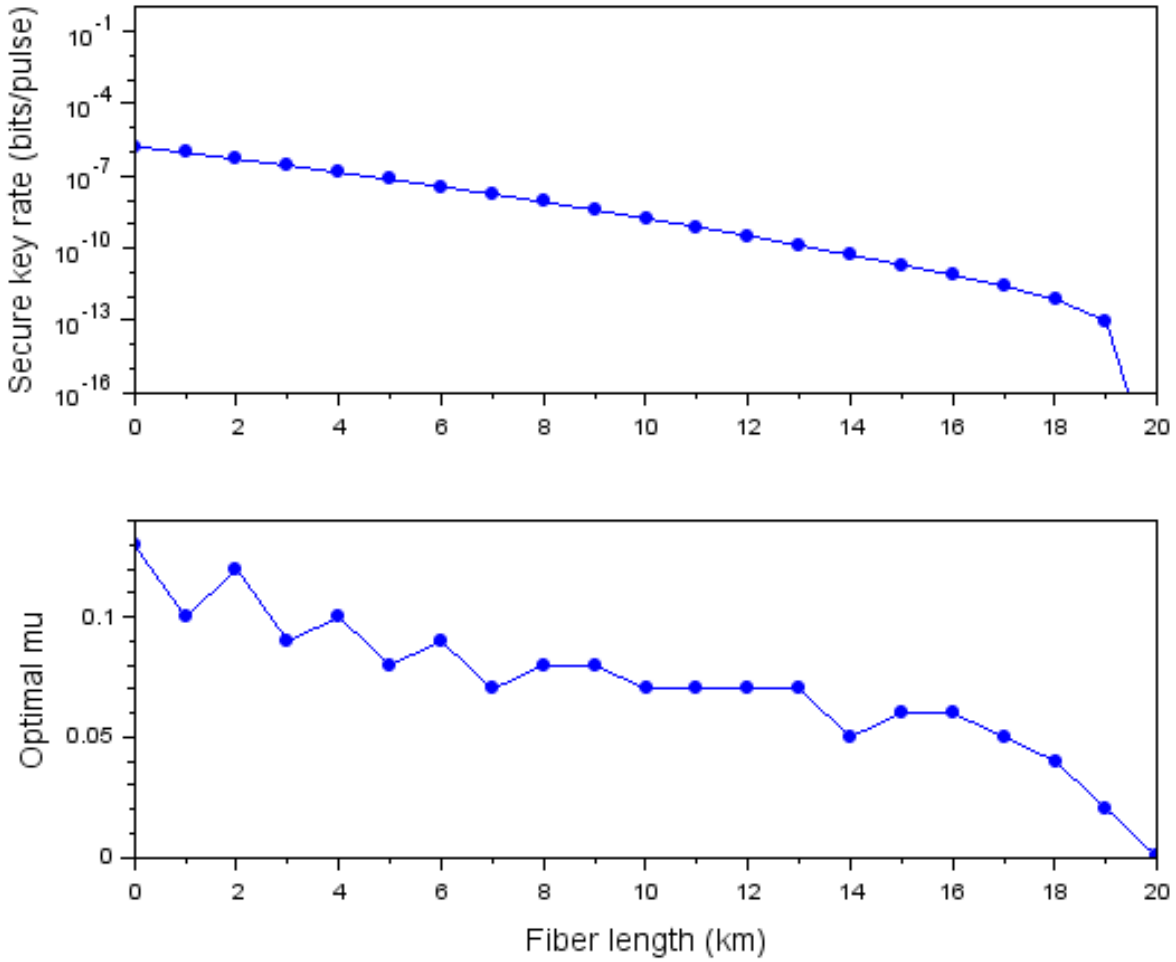
$$R = \sum_{m,n=0}^{\infty} Q_{\mathrm{m,n,n}}^{(\mu,Z)} + Q_{1,1}^{(\mu,Z)}\left[1 - H_2\left(E_{1,1}^{(X,V)}\right)\right] - f Q^{(\mu,Z)} H_2\left(E^{(\mu,Z)}\right)$$

$Q^{(\mu,Z)}$ and $E^{(\mu,Z)}$ determined from raw keys

$$Q_{m,n,n}^{(\mu)} = S_m^{(\mu)} C_{n,n|m} D_{n,n}$$

$$Q_{1,1}^{(\mu)} = S_1^{(\mu)}\left(C_{1,0|1} D_{1,0} + C_{0,1|1} D_{0,1}\right)$$

$$E_{1,1}^{(V)} = \frac{C_{0,1|1}}{C_{0,1|1} + C_{1,0|1}}$$



Simulation results with intrinsic QBER= 0

Multiphoton contributions (m=2 case)

Given Alice's signal pulse contains m=2 photons, under normal condition, the output of channel could be:

$\{n_0, n_1\} = \{0,0\},\ \{1,0\},\ \{0,1\},\ \{2,0\},\ \{1,1\},\ \{0,2\}$

Two observations

1. Given Eve knows $\{n_0, n_1\}$ photons arrive at Bob, she cannot predict Bob's measurement results with certainty (trusted noise assumption). Eve's uncertainty about Bob's key could be quantified by $H_2\left(BER_{n_0,n_1}\right)$, where $BER_{n_0,n_1} = \frac{P_w^{(n_0,n_1)}}{P_c^{(n_0,n_1)} + P_w^{(n_0,n_1)}}$
2. *Secret key could be generated from the case when Alice sends 2 photons and Bob receives 2 photons

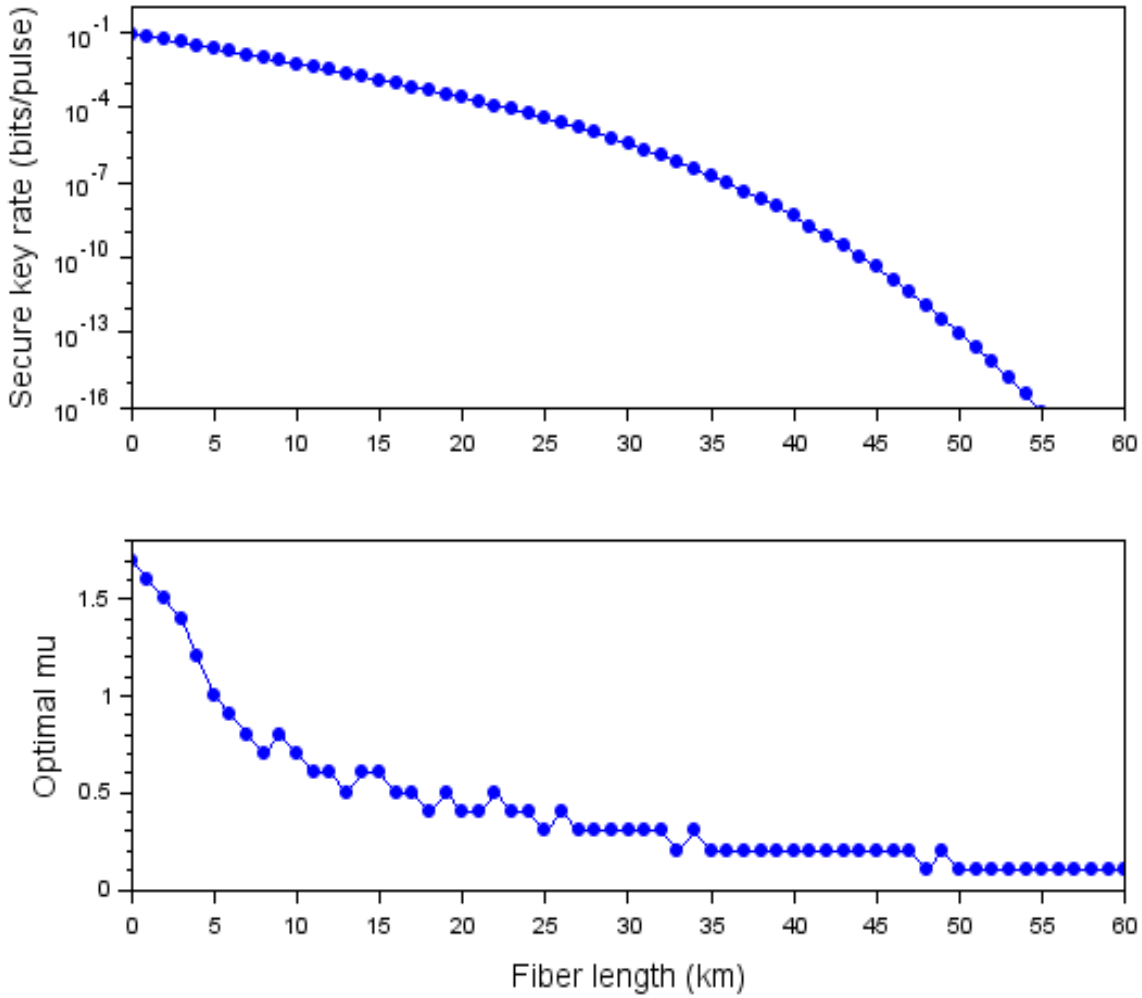
*This idea is from Ignatius William Primaatmaja and Charles Lim (private communication)

Potential improvement

Secret key rate
(with E_d=0)

$$R = \sum_{m,n=0}^{\infty} Q_{\mathrm{m,n},n}^{(\mu,Z)} + Q_{1,1}^{(\mu,Z)}\left[1 - H_2\left(E_{1,1}^{(X,V)}\right)\right]$$
$$-fQ^{(\mu,Z)}H_2\left(E^{(\mu,Z)}\right) + Q_{2,1.0}^{(\mu,Z)}H_2\left(BER_{1,0}\right) + Q_{2,2.0}^{(\mu,Z)}$$

$\{n_0, n_1\}$ = {0,0}, {1,0}, {0,1}, {2,0}, {1,1}, {0,2}



Simulation results with intrinsic QBER= 0

Summary

- We propose a scheme to implement BB84 QKD using conjugate homodyne detector operated in phase-insensitive, photon counting mode
- We refine the security analysis by exploring two features of the detector: trusted detector noise and the ability to construct photon number distribution
- This scheme can inherit certain advantages of coherent detection without requiring a phase reference, and might be useful for short distance application

This work is funded by

U.S. DOE Office of Cybersecurity Energy Security and Emergency Response (CESER) through the Cybersecurity for Energy Delivery Systems (CEDS) program

See more details in

Phys. Rev. A, 103, 012606 (2021)

Optics Express 28, 2276-2290 (2020)