Security proof of practical quantum key distribution with detection-efficiency mismatch

Yanbao Zhang

NTT Research Center for Theoretical Quantum Physics

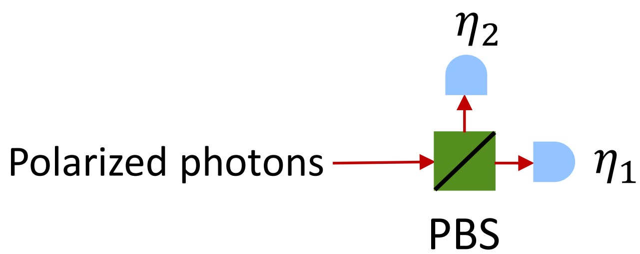
NTT Basic Research Lab, Japan

Based on the joint work arXiv:2004.04383 with

Patrick J. Coles, Adam Winick, Jie Lin, and Norbert Lütkenhaus

Why detection-efficiency mismatch matters？

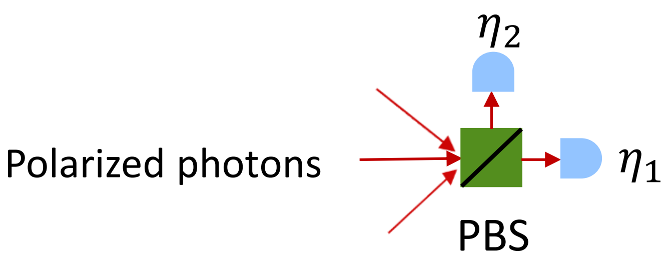
- Detection-efficiency mismatch due to manufacturing and setup



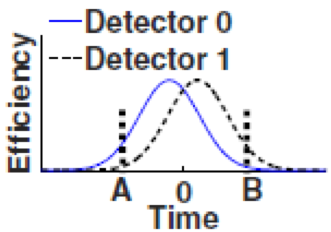
It is difficult to build two detectors with identical efficiency.

*Detectors considered in this work are threshold detectors.

- Detection-efficiency mismatch induced by Eve



spatial-mode-dependent



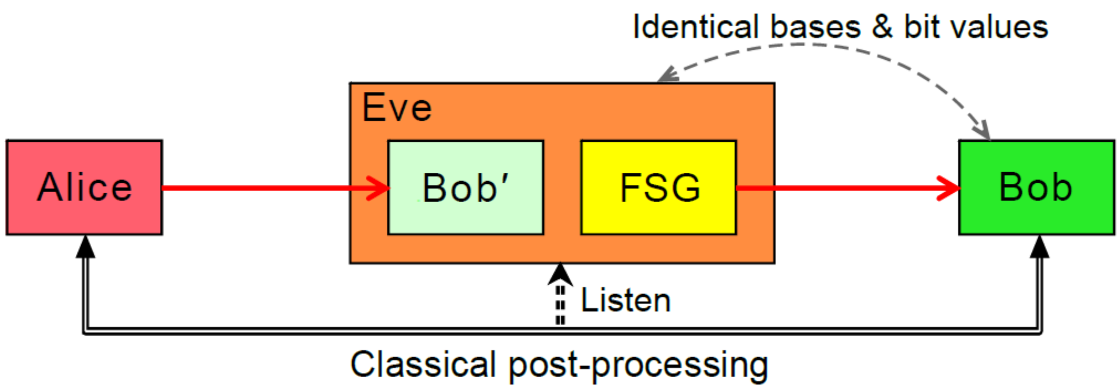
temporal-mode-dependent

Rau *et al.*, IEEE J. Quantum Electron. 21, 6600905 (2014)
Sajeed *et al.*, Phys. Rev. A 91, 062301 (2015)
Chaiwongkhot *et al.*, Phys. Rev. A 99, 062315 (2019)

Zhao *et al.*, Phys. Rev. A 78, 042333 (2008)

Problems caused by efficiency mismatch

- Efficiency mismatch helps Eve to attack QKD systems.



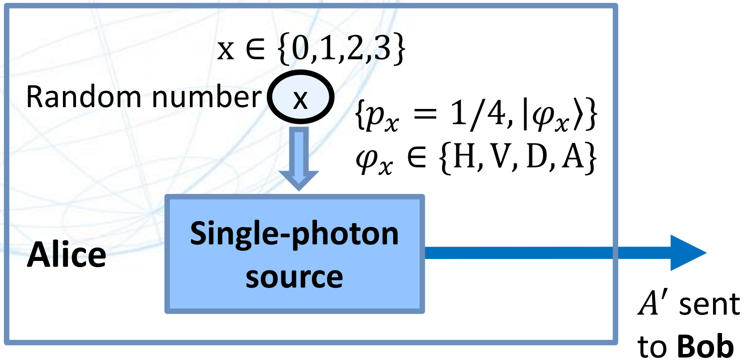
Lydersen *et al*., Nat. Photon. 4, 686 (2010)
Gerhardt *et al*., Nat. Commun. 2, 349 (2011)

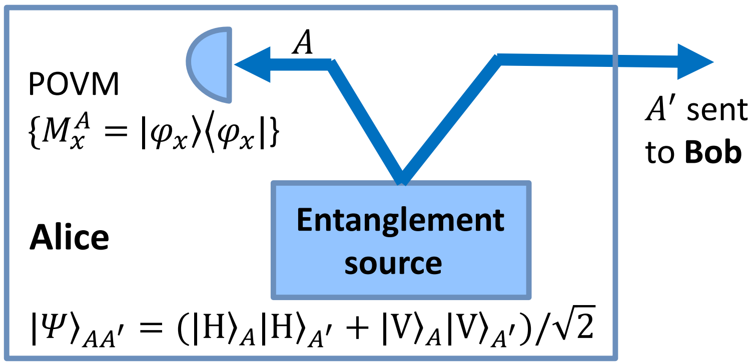
- Efficiency mismatch can cause fake violations of an entanglement witness.

  In the presence of efficiency mismatch, the detection events are not fair samples. If only detection events are used, a Bell inequality can be violated even using classical light [Gerhardt *et al*., Phys. Rev. Lett. 107, 170404 (2011)].

Protocol analyzed in this work

Prepare & Measure BB84
[Bennett and Brassard (1984)]





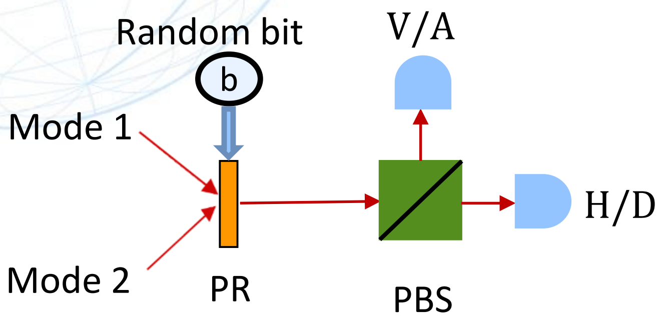
Source-replacement description
[Bennett, Brassard, Mermin, PRL 68, 557 (1992);
Curty, Lewenstein, Lütkenhaus, PRL 92, 217903 (2004);
Ferenczi, Lütkenhaus, PRA 85, 052310 (2012)]

- **Assumption**: Alice's and Bob's labs are secure and trusted.
- ➔ Use of the entanglement-based scheme for security analysis.
  1) $\rho_{AA'}$ ➔ ρ_{AB}.
  2) Alice's measurements are ideal.
- **Warning**: System A' is two-dimensional, *but* the system B arriving at Bob can be infinite-dimensional.
- Detection-efficiency mismatch exists in Bob's measurement setup.

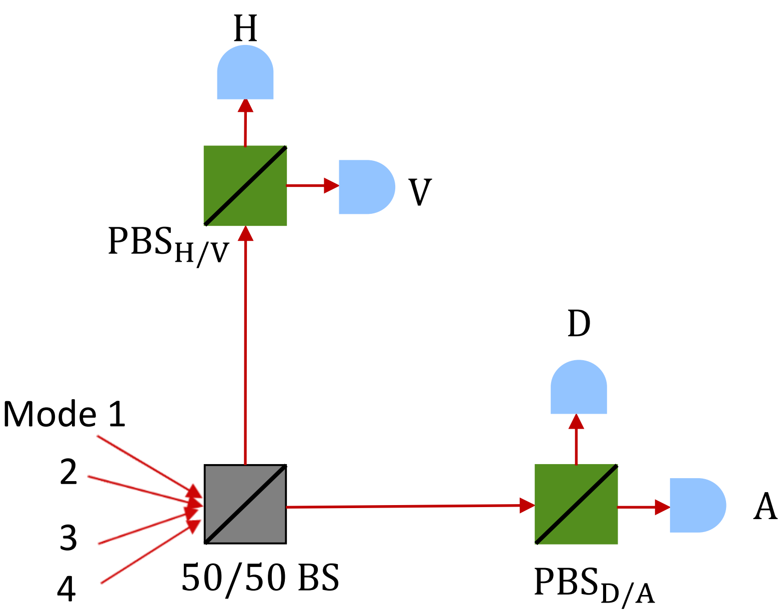
Bob's measurements & efficiency mismatch

NTT

PR – Polarization Rotator
PBS – Polarizing Beam Splitter
50/50 BS – 50/50 Beam Splitter



Active Detection



Passive Detection

Efficiency mismatch model considered

Mode	H/D	V/A
1	η_1	η_2
2	η_2	η_1

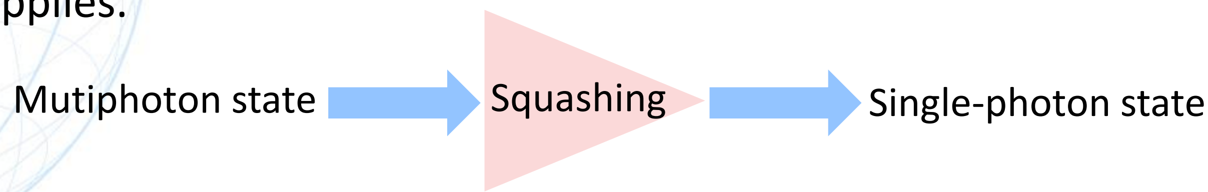
Efficiency mismatch model considered

Mode	H	V	D	A
1	η_1	η_2	η_2	η_2
2	η_2	η_1	η_2	η_2
3	η_2	η_2	η_1	η_2
4	η_2	η_2	η_2	η_1

*Our method works for arbitrary, characterized efficiency mismatch.

Obstacle to proving security with efficiency mismatch

- Without efficiency mismatch, the squashing model exists. ➔ A qubit-based security proof still applies.



[Beaudry, Moroder, Lütkenhaus, Phys. Rev. Lett. 101, 093601 (2008);
Tsurumaru and Tamaki, Phys. Rev. A 78, 032302 (2008)]

- With efficiency mismatch, the above squashing model doesn't work.

- Previous security proofs with efficiency mismatch assume that the system arriving at Bob contains at most one photon.

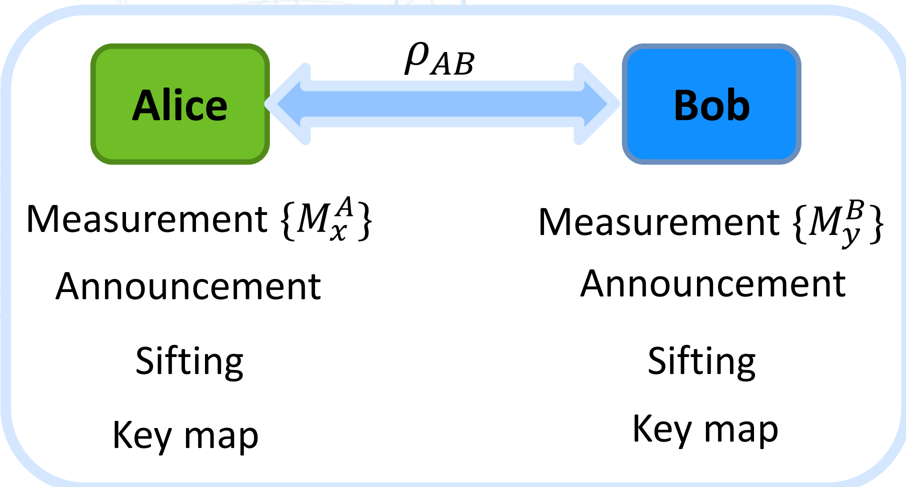
[Fung *et al*., Quantum Inf. Comput. 9, 131 (2009); Lydersen and Skaar, Quant. Inf. Comp. 10, 0060 (2010);
Bochkov and Trushechkin, Phys. Rev. A 99, 032308 (2019); Ma *et al*., Phys. Rev. A 99, 062325 (2019)]

Our contribution: We develop a method to handle the infinite-dimensional system received by Bob.

*In parallel with us, Trushechkin recently developed an alternative method [arXiv:2004.07809].

Brief introduction to a numerical approach for security proof

NTT



QKD protocol

Key rate: $K = \alpha - H(A|B)$, where α for privacy amplification and $H(A|B)$ for error correction. *Collective attacks are considered, and the key is defined by Alice.

$$\alpha = \min_{\rho_{AB}} D(\mathcal{G}(\rho_{AB})||\mathcal{Z}(\mathcal{G}(\rho_{AB})))$$

$$\begin{cases} \rho_{AB} \geq 0, \quad \mathrm{Tr}(\rho_{AB}) = 1 \\ \mathrm{Tr}\,(M_x^A \otimes M_y^B\ \rho_{AB}) = p_{AB}(x,y) \end{cases}$$

Key-rate calculation

1. A protocol can be described by a set of POVMs $\{M_x^A \otimes M_y^B\}$ (measurements), Kraus operator $\mathcal{G}$ (announcements and sifting), and Key map $\mathcal{Z}$ (forming key). The state ρ_{AB} is constrained by observations $p_{AB}(x,y)$ --- the expectation values of POVMs.
2. Once description is given, the key rate (privacy amplification part) takes the form of $\min f(\rho_{AB})$, where one needs to minimize f depending on ρ_{AB} (Eve's attack).
3. As f is a convex function, we can calculate both a lower bound and an upper bound on $\min f(\rho)$.

Coles, Metodiev, Lütkenhaus, Nat. Commun. **7**, 11712 (2016)

Winick, Lütkenhaus, Coles, Quantum 2, 77 (2018)

Dimension reduction by flag-state squasher

NTT

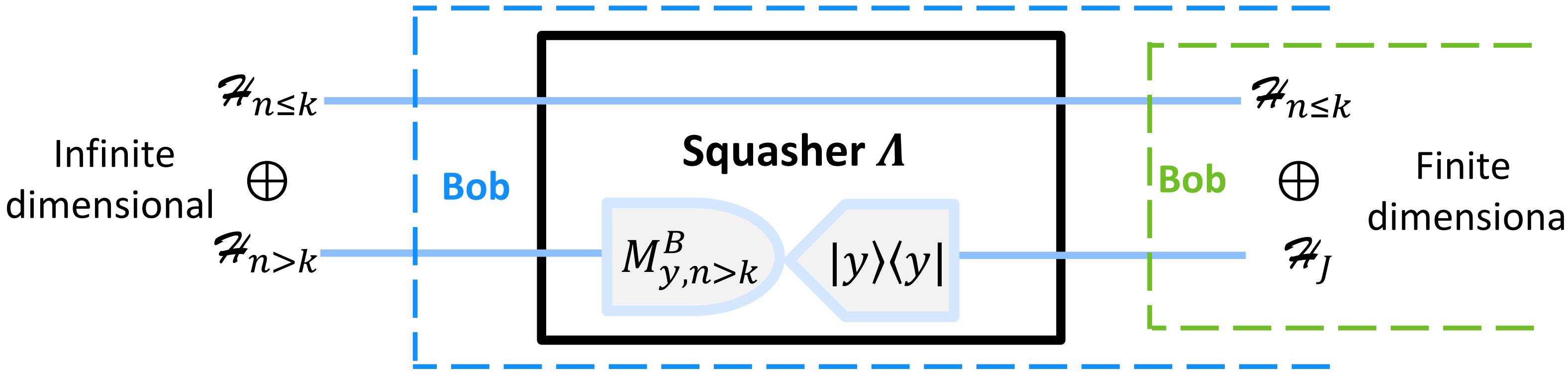
- **Key observation**: Each POVM element $M_y^B, y \in \{1,2,\dots,J\}$, is block-diagonal with respect to various photon-number subspaces.
- For a photon-number cutoff k ➔ $(n \leq k)$- and $(n > k)$-photon subspaces

Original POVM:

$$M_y^B = \begin{pmatrix} M_{y,n\leq k}^B & 0 \\ 0 & M_{y,n>k}^B \end{pmatrix}$$

Squashed POVM:

$$\widetilde{M}_y^{\widetilde{B}} = \begin{pmatrix} M_{y,n\leq k}^B & 0 \\ 0 & |y\rangle\langle y| \end{pmatrix}$$

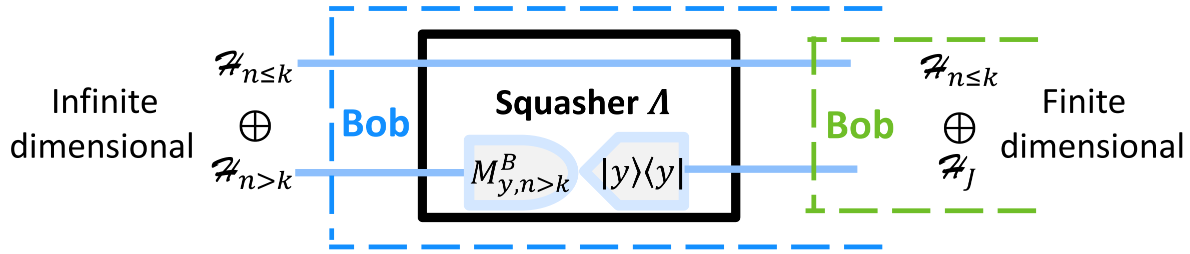


For an arbitrary input state ρ_B, Tr $(M_y^B \rho_B) = $ Tr $(\widetilde{M}_y^{\widetilde{B}} \Lambda(\rho_B))$, $\forall\, y$.

- ➢ Two equivalent descriptions of the measurement process.
- ➢ The description using the squasher Λ is pessimistic, as it allows Eve to completely learn Bob's outcome when $n > k$.
- ❑ A lower bound on $p_{n\leq k}$ is required when using the squasher Λ.

Overview of our method

Step 1: Reducing the dimension



Step 2: Bounding the photon-number distribution

Accordingly, we need only to solve a finite-dimensional convex optimization problem, and so we can obtain non-trivial lower bounds of the secret key rate.

$$\min_{\rho_{A\tilde{B}}} D(\mathcal{G}(\rho_{A\tilde{B}})||\mathcal{Z}(\mathcal{G}(\rho_{A\tilde{B}})))$$

$$\begin{cases} \rho_{A\tilde{B}} \geq 0, \quad \mathrm{Tr}(\rho_{A\tilde{B}}) = 1 \\ \mathrm{Tr}\,(M_x^A \otimes \widetilde{M}_y^{\tilde{B}}\ \rho_{A\tilde{B}}) = p_{AB}(x,y) \\ \mathrm{Tr}(\Pi_{\le k}\rho_{A\tilde{B}}) \geq b_k \end{cases}$$

Our key-rate calculation

* $\rho_{A\tilde{B}}$ is finite-dimensional;
* The operators $\widetilde{M}_y^{\tilde{B}}$ depend on efficiency mismatch.
* $\Pi_{\le k}$ is the projector onto the ($\le$-k)-photon subspace.

Photon-number distribution bounds

NTT

- Let T be an observable that depends on both the photon number n and the efficiency mismatch (e.g., double click or cross click).
- T is block-diagonal. ➔ WLOG ρ_{AB} is block-diagonal, i.e., $\rho_{AB} = \sum_{n=0}^{\infty} p_n \, \rho_{AB}^{(n)}$.

  p_n --- the probability that the system arriving at Bob has n photons.

If we can find n-dependent bounds

$$t_{\mathrm{obs},n} = \mathrm{Tr}\,(\rho_{AB}^{(n)} T) \geq \begin{cases} t_{\mathrm{obs},\,n\leq k}^{\min}, \forall n \leq k, \\ t_{\mathrm{obs},\,n>k}^{\min}, \ \forall n > k, \end{cases}$$

then we have

$$t_{\mathrm{obs}} = \sum_{n=0}^{\infty} p_n \,\mathrm{Tr}\left(\rho_{AB}^{(n)} T\right) \geq p_{n\leq k} t_{\mathrm{obs},\,n\leq k}^{\min} + (1 - p_{n\leq k}) t_{\mathrm{obs},\,n>k}^{\min}.$$

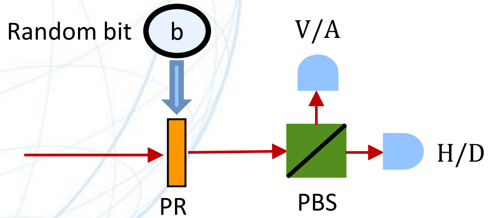
$t_{\mathrm{obs},\,n\leq k}^{\min}$ is *less than* $t_{\mathrm{obs},\,n>k}^{\min}$ ➔

$$\boxed{p_{n\leq k} \geq \frac{t_{\mathrm{obs},\,n>k}^{\min} - t_{\mathrm{obs}}}{t_{\mathrm{obs},\,n>k}^{\min} - t_{\mathrm{obs},\,n\leq k}^{\min}}.}$$

*Similar bounds have been used for security proofs of QKD *without* efficiency mismatch, see [Lütkenhaus, PRA 59, 3301 (1999) and Koashi *et al*., arXiv:0804.0891].

*We use the bounds established in [Y Z and N. Lütkenhaus, PRA 95, 042319 (2017)] for entanglement verification *with* efficiency mismatch. An alternative bound for *active detection with* efficiency mismatch was recently derived by Trushechkin, arXiv:2004.07809.

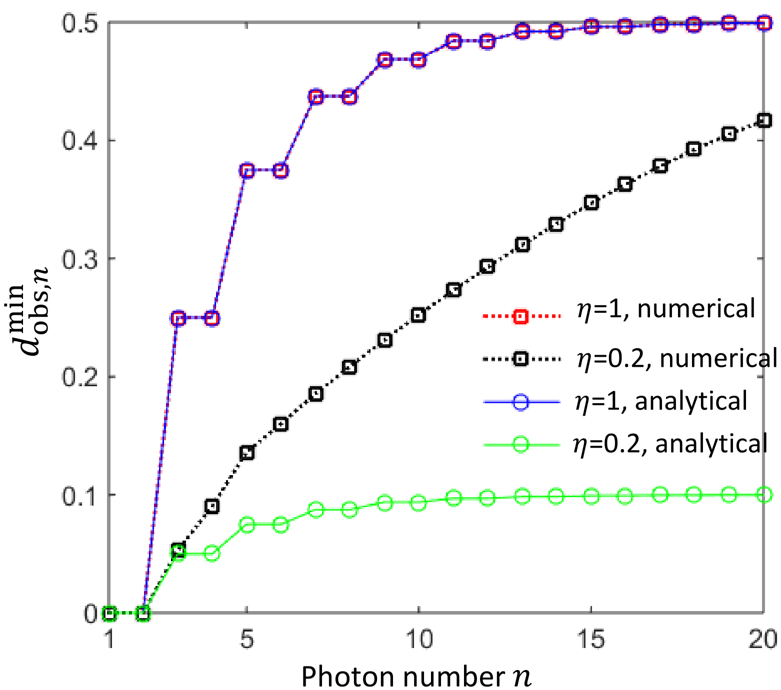
$p_{n\leq k}$ for active detection



Mode	H/D	V/A
1	η_1=1	η_2=η
2	η_2=η	η_1=1

Efficiency mismatch model considered

❖ The observable T can be the double-click operator D or the effective-error operator.



$$d_{\mathrm{obs},n} = \mathrm{Tr}\,(\rho_{AB}^{(n)} D) \geq \begin{cases} \frac{\eta}{2}\left(1-\sqrt{2^{2-n}}\right), & n \text{ is even;} \\ \frac{\eta}{2}\left(1-\sqrt{2^{1-n}}\right), & n \text{ is odd.} \end{cases}$$

*The numerical results are obtained by solving SDPs [Y Z and N. Lütkenhaus, PRA 95, 042319 (2017)].

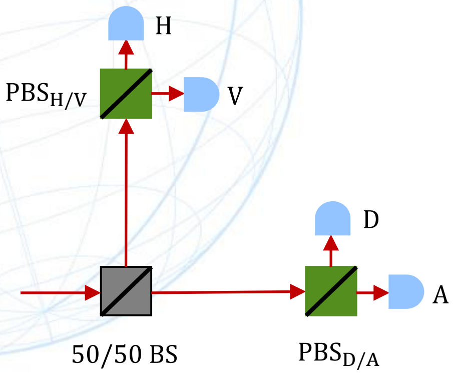
*The analytical bounds are motivated and improve the results in [Trushechkin, arXiv:2004.07809].

Due to the monotonic behavior of $d^{\min}_{\mathrm{obs},\,n}$,

$$p_{n\leq k} \geq \frac{d^{\min}_{\mathrm{obs},\,(k+1)} - d_{\mathrm{obs}}}{d^{\min}_{\mathrm{obs},\,(k+1)}}, \forall k.$$

*Our method works for arbitrary, characterized efficiency mismatch.

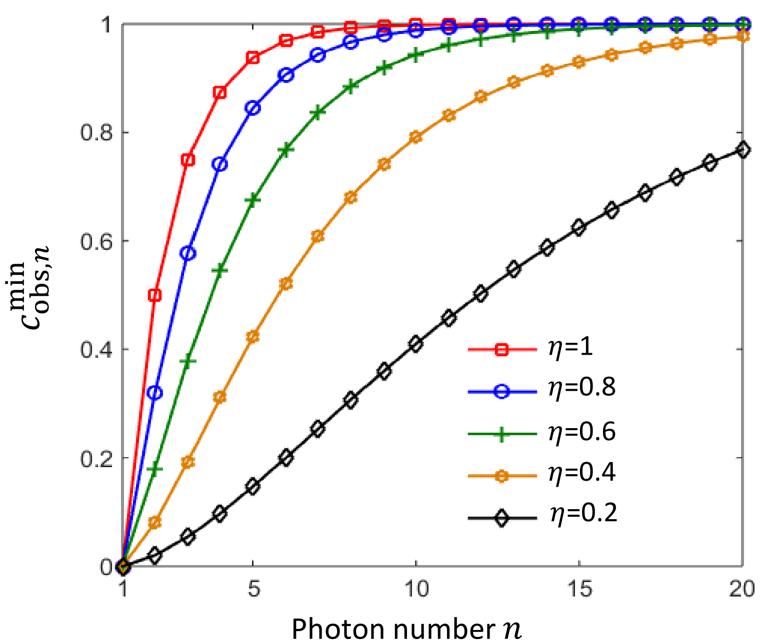
$p_{n\le k}$ for passive detection



Mode	H	V	D	A
1	η_1=1	η_2=η	η_2=η	η_2=η
2	η_2=η	η_1=1	η_2=η	η_2=η
3	η_2=η	η_2=η	η_1=1	η_2=η
4	η_2=η	η_2=η	η_2=η	η_1=1

Efficiency mismatch model considered

❖ The observable T can be the cross-click operator C.



$$c_{\text{obs},n} = \mathrm{Tr}\,(\rho_{AB}^{(n)}C) \geq 1 + (1-\eta)^n - 2\left(1-\frac{\eta}{2}\right)^n.$$

*The numerical results are obtained by solving SDPs [Y Z and N. Lütkenhaus, PRA 95, 042319 (2017)].

*The numerical bounds coincide with the analytical ones.

Due to the monotonic behavior of $c_{\text{obs},\,n}^{\min}$,

$$p_{n\le k} \geq \frac{c_{\text{obs},\,(k+1)}^{\min} - c_{\text{obs}}}{c_{\text{obs},\,(k+1)}^{\min}}, \forall k.$$

*Our method works for arbitrary, characterized efficiency mismatch.

Data simulation

We simulate experimental observations $p_{AB}(x, y)$ according to a toy model

- at each round Alice prepares a signal state (according to the protocol),
- the channel between Alice and Bob is specified by

  t --- the single-photon transmission probability,

  ω --- the depolarization noise,

  r --- the multiphoton probability, i.e., the probability that a single photon ➔ randomly depolarized m photons (in our simulation $m = 2$),

- Bob performs a measurement (according to the protocol).

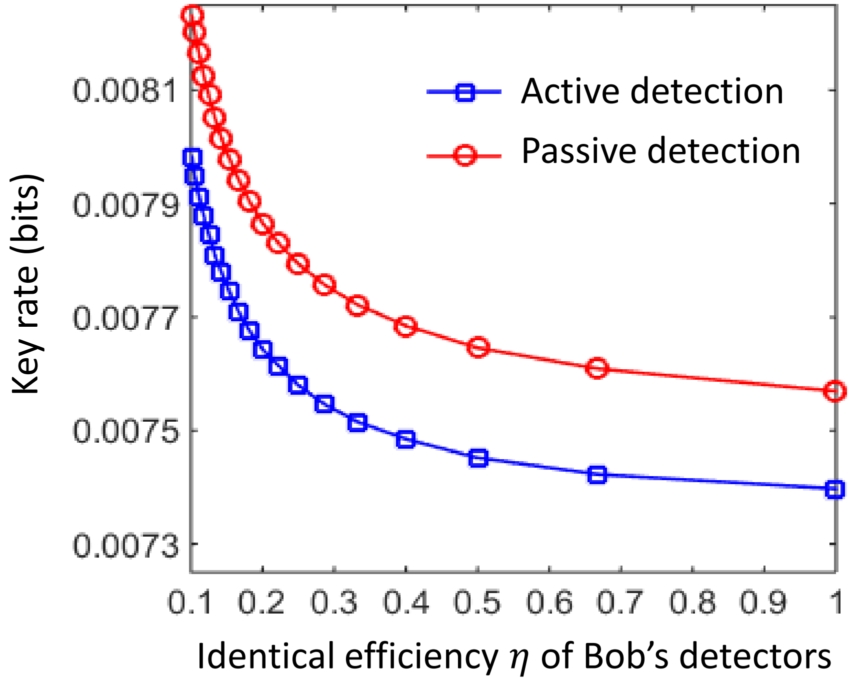
  *If Bob's detectors are coupled to several spatial-temporal modes, the optical signal is distributed uniformly at random over these modes.

Task: Lower-bound the key rate given $p_{AB}(x, y)$ and characterized efficiency mismatch.

*For this particular case, $p_{AB}(x, y)$ are determined by the channel parameters $(t,\ \omega,\ r)$ as well as the detector model.

***Our security analysis doesn't require characterizing the channel between Alice and Bob** (i.e., Eve's attack). Particularly, we don't assume that the system received by Bob is finite-dimensional.

Key rates with trusted loss
(in the absence of mismatch)



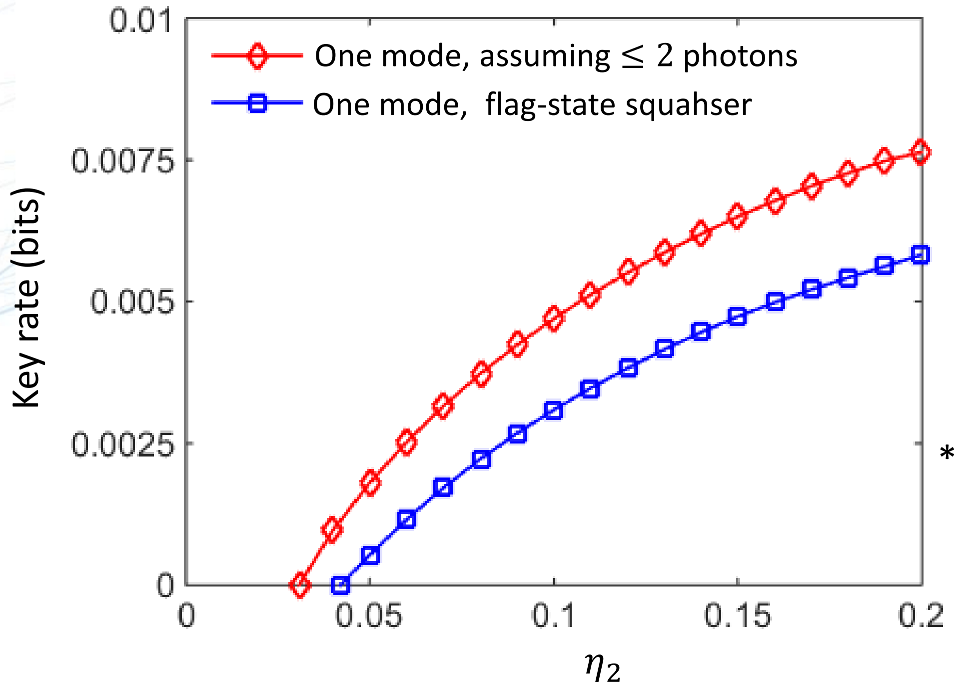
*For data simulation, $t\eta = 0.1$, $\omega = 0.05$, $r = 0.05$.

*$p_{AB}(x, y)$ doesn't change with η.

For these particular results, our security analysis

- assumes that at most two photons are received by Bob (and so a flag-state squasher is not used).
- when $\eta = 1$, returns the same key rates as using the usual squashing model [Beaudry, Moroder, Lütkenhaus, Phys. Rev. Lett. 101, 093601 (2008); Tsurumaru and Tamaki, Phys. Rev. A 78, 032302 (2008)].
- suggests that more secret keys can be distilled when the trusted loss inside of Bob's lab, $(1 - \eta)$, increases and the untrusted loss over transmission, $(1 - t)$, decreases.

Key rates for active detection with efficiency mismatch



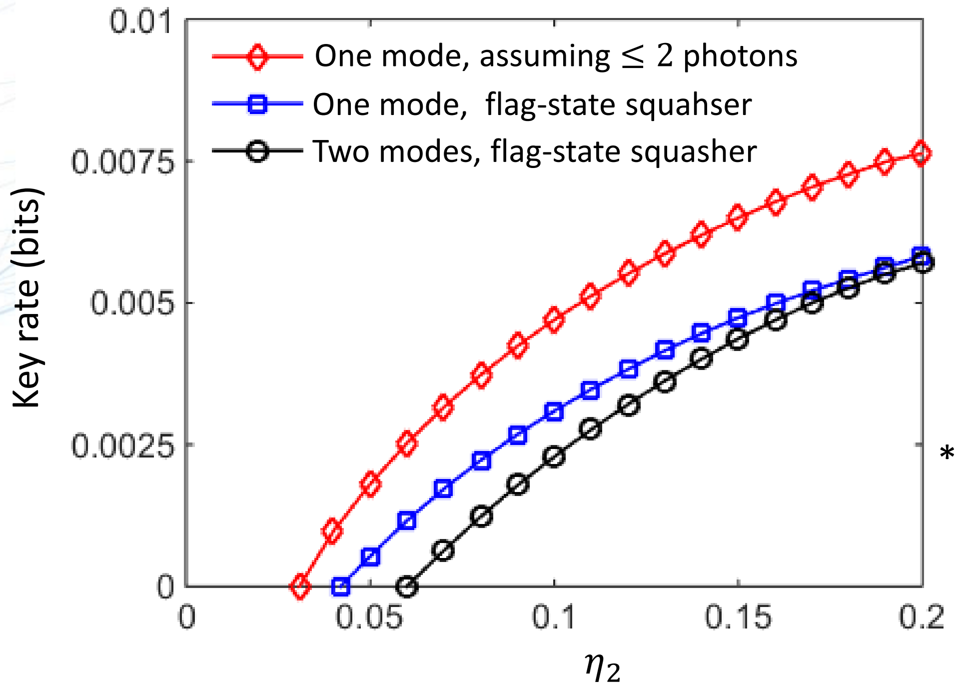
Mode	H/D	V/A
1	η_1=0.2	η_2

Efficiency mismatch studied

*For data simulation, $t = 0.5$, $\omega = 0.05$, $r = 0.05$.

- When applying a flag-state squasher, we choose the photon-number cutoff $k = 2$.
- The larger the efficiency mismatch, the lower the key rate is.
- Making assumptions on Eve's attack would overestimate the key rate.

Key rates for active detection with efficiency mismatch



Mode	H/D	V/A
1	η_1=0.2	η_2
2	η_2	η_1=0.2

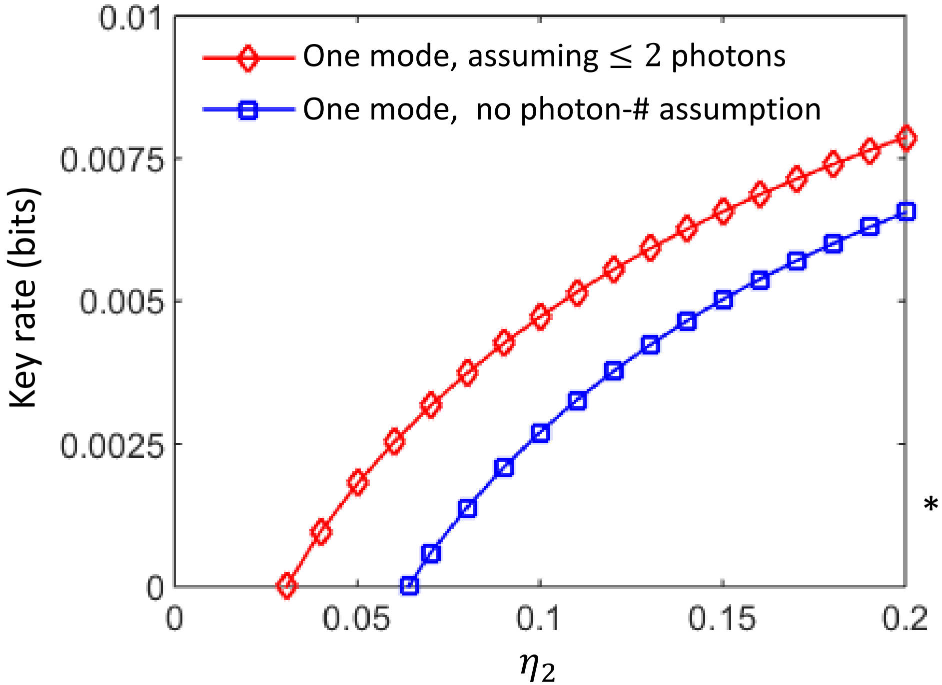
Efficiency mismatch studied

*For data simulation, $t = 0.5$, $\omega = 0.05$, $r = 0.05$.

- When applying a flag-state squasher, we choose the photon-number cutoff $k = 2$.
- The larger the efficiency mismatch, the lower the key rate is.
- Making assumptions on Eve's attack would overestimate the key rate.
- Mode-dependent mismatch helps Eve to attack the QKD system.

Key rates for passive detection with efficiency mismatch

NTT



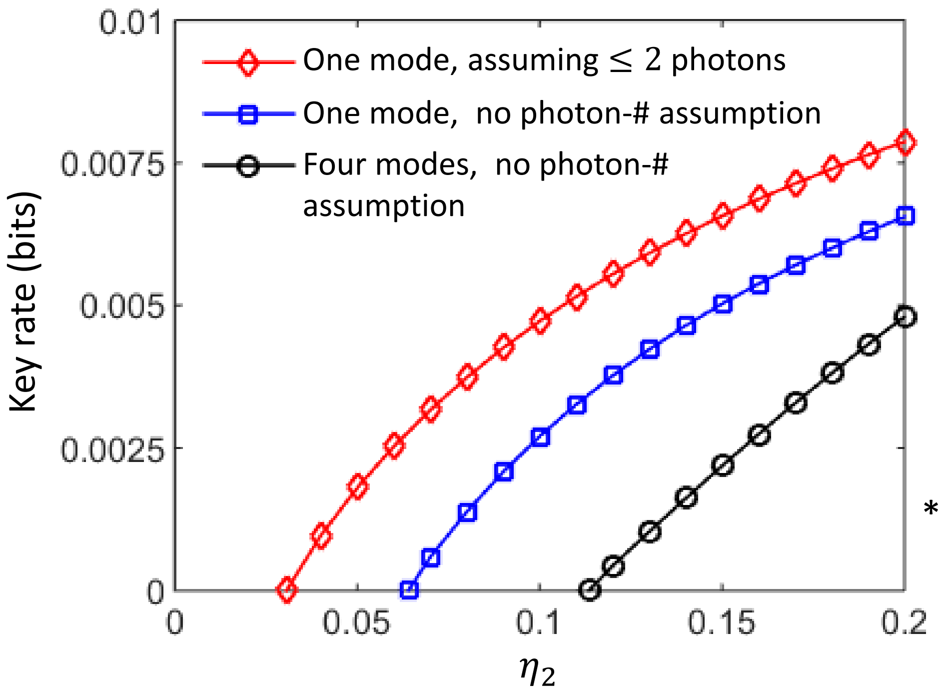
Mode	H	V	D	A
1	η_1=0.2	η_2=η	η_2=η	η_2=η

Efficiency mismatch studied

*For data simulation, $t = 0.5$, $\omega = 0.05$, $r = 0.05$.

- When applying a flag-state squasher, we choose a photon-number cutoff $k = 2$ (for one mode) or $k = 1$ (for four modes).
- The larger the efficiency mismatch, the lower the key rate is.
- Making assumptions on Eve's attack would overestimate the key rate.

Key rates for passive detection with efficiency mismatch



Mode	H	V	D	A
1	η_1=0.2	η_2=η	η_2=η	η_2=η
2	η_2=η	η_1=0.2	η_2=η	η_2=η
3	η_2=η	η_2=η	η_1=0.2	η_2=η
4	η_2=η	η_2=η	η_2=η	η_1=0.2

Efficiency mismatch studied

*For data simulation, $t = 0.5$, $\omega = 0.05$, $r = 0.05$.

- When applying a flag-state squasher, we choose a photon-number cutoff $k = 2$ (for one mode) or $k = 1$ (for four modes).
- The larger the efficiency mismatch, the lower the key rate is.
- Making assumptions on Eve's attack would overestimate the key rate.
- Mode-dependent mismatch helps Eve to attack the QKD system.

NTT

Summary

- Constructed a flag-state squasher to reduce the system dimension.
  *The flag-state squasher can be applied to other protocols, see Li and Lütkenhaus, arXiv:2007.08662.

- Established bounds on photon-number distribution directly from experimental observations.

- Proved the security of a prepare & measure BB84 protocol in the presence of efficiency mismatch *without* a photon-number limit.

- Illustrated the individual effects of trusted loss and untrusted loss on the key rate.

Finite key analysis can also be handled by numerical approach (see the talk "**Numerical Calculations of Finite Key Rate for General Quantum Key Distribution Protocols"** by Ian George).

Summary

- Constructed a flag-state squasher to reduce the system dimension.
  *The flag-state squasher can be applied to other protocols, see Li and Lütkenhaus, arXiv:2007.08662.

- Established bounds on photon-number distribution directly from experimental observations.

- Proved the security of a prepare & measure BB84 protocol in the presence of efficiency mismatch *without* a photon-number limit.

- Illustrated the individual effects of trusted loss and untrusted loss on the key rate.

Finite key analysis can also be handled by numerical approach (see the talk “**Numerical Calculations of Finite Key Rate for General Quantum Key Distribution Protocols**” by Ian George).

Thank you! yanbaoz@gmail.com