Refined finite-size security analysis of discrete-modulation continuous variable quantum key distribution based on reverse reconciliation

Takaya Matsuura *, Shinichiro Yamano *, Yui Kuramochi *, Toshihiko Sasaki *, and Masato Koashi *

* The University of Tokyo, Japan.

Abstract

We developed a refined finite-size security proof of the binary-modulation CV-QKD protocol. As a result, the protocol has

☺ asymptotic key rate that scales almost optimally against loss

☺ improved key rates even in finite-key cases

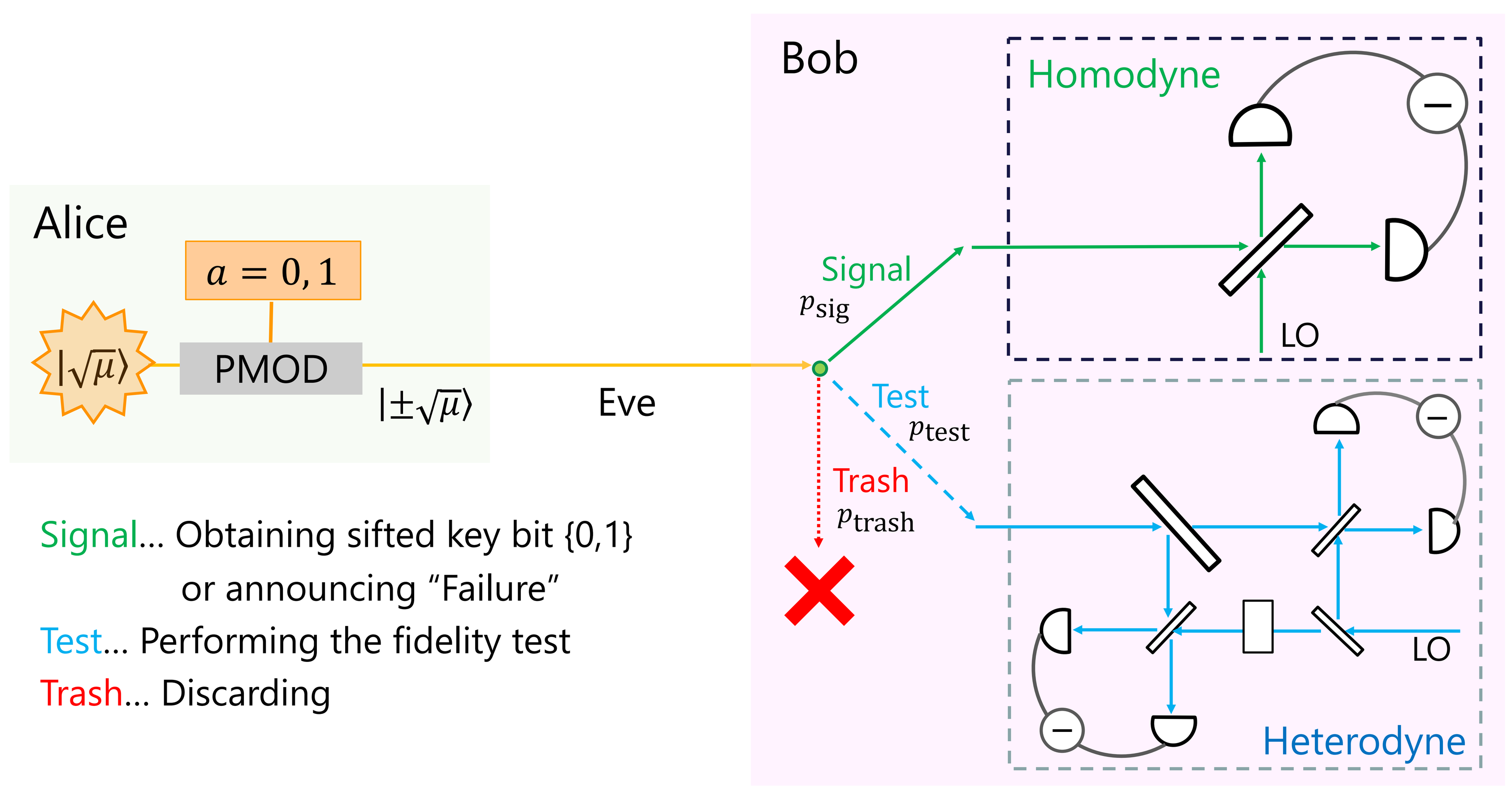
☹ the same fragility against excess noise

Preliminaries

1. Previous result

- ❑ Finite-size security of the binary-modulation CV-QKD protocol

[1] T. Matsuura *et al*., Nat. Commun. 12, 252 (2021).



Signal… Obtaining sifted key bit {0,1} or announcing "Failure"

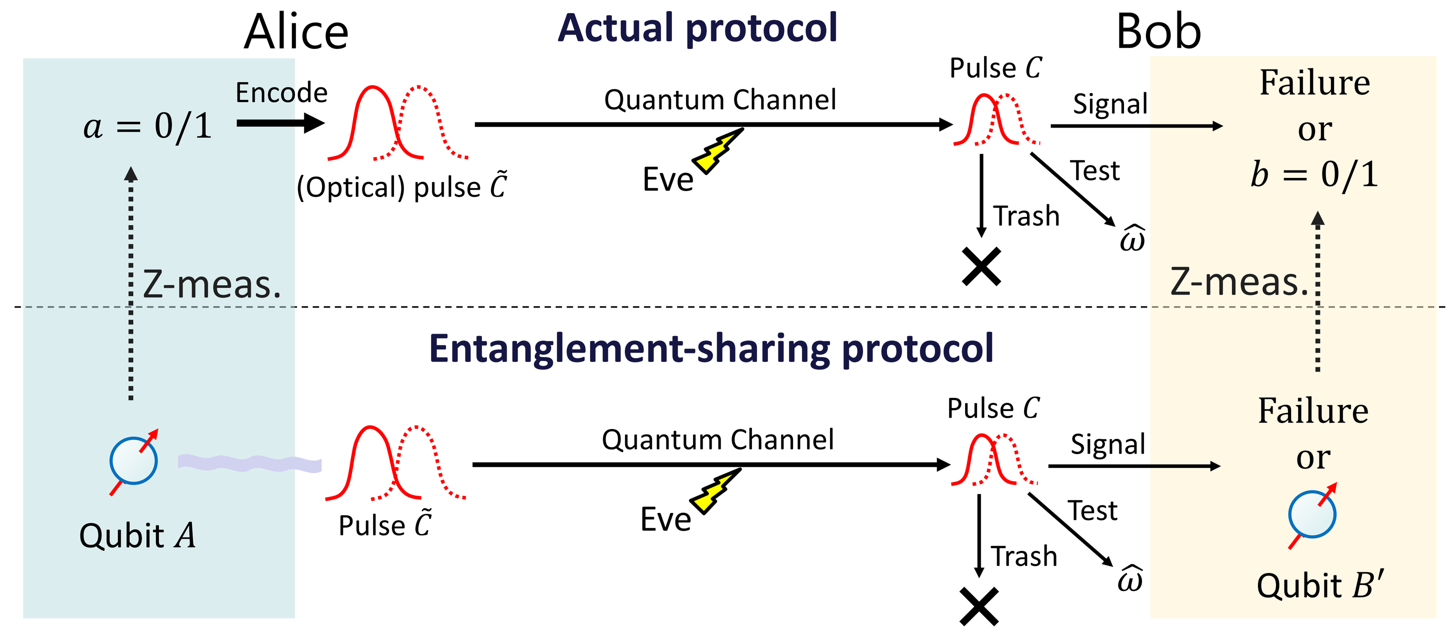
Test… Performing the fidelity test

Trash… Discarding

→ At this moment the **only** discrete-modulation CV-QKD protocol proven to be secure against general attacks in finite-size regime

2. Idea of the security proof

- ❑ Reduction to the entanglement distillation



$Z\otimes Z$… Bit error, $X\otimes X$… Phase error

- ❑ Inequality on the phase error (operator inequality)

Expectation w.r.t. arbitrary conditional state at i-th round

=1 when phase error occurs in Signal

=1 when Alice's qubit is in $|-\rangle$ in Trash

$$\mathbb{E}\left[p_{sig}^{-1}\,\hat{N}_{ph}^{suc,(i)} + p_{test}^{-1}\,\kappa\,\hat{F}^{(i)} - p_{trash}^{-1}\,\gamma\,\hat{Q}_{-}^{(i)}\right] \le B(\kappa,\gamma)$$

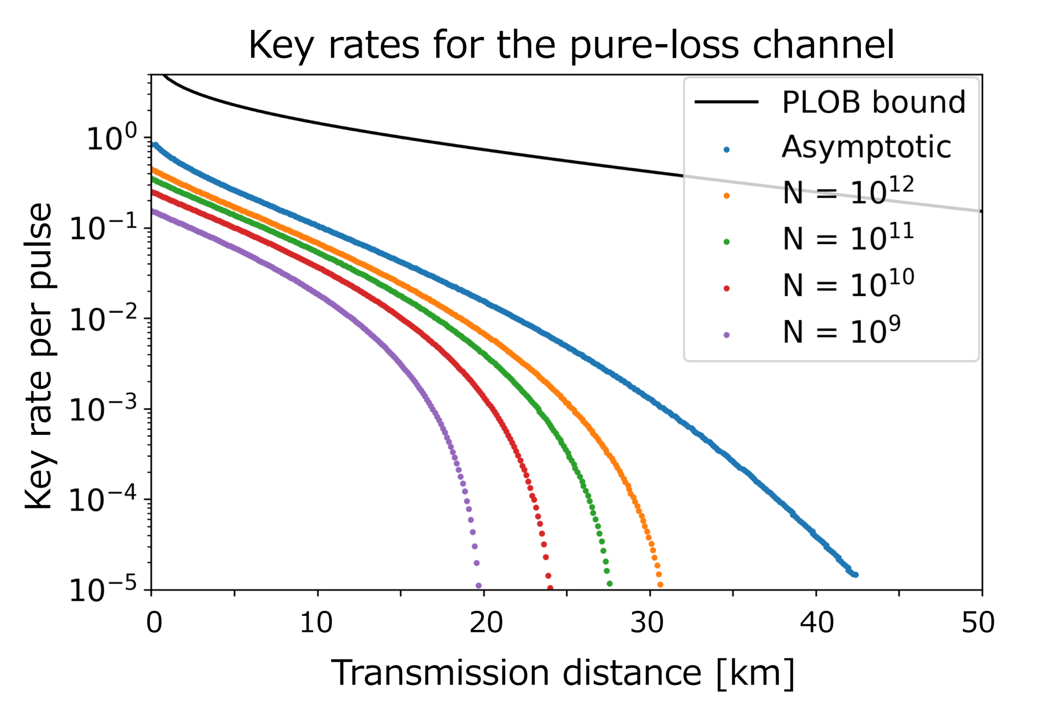
κ, γ: positive numbers (dual parameters)

$= \Lambda_{m,r}\left(|\hat{\omega}^{(i)} - (-1)^a\beta|^2\right)$ in Test, where $\mathbb{E}[\hat{F}^{(i)}] \le \langle(-1)^a\beta|\rho^{(i)}|(-1)^a\beta\rangle$ holds

3. Problems of the previous results

- ❑ Key rate rapidly decreases against transmission distance under pure loss.
- ❑ This behaviour is much worse than that anticipated from the asymptotic analyses of discrete-modulation CV QKD.
- ❑ This may be because of the unnecessarily stronger requirement on security.

Question… Can we develop a refined security analysis that leads to a tighter lower bound on the key rate?



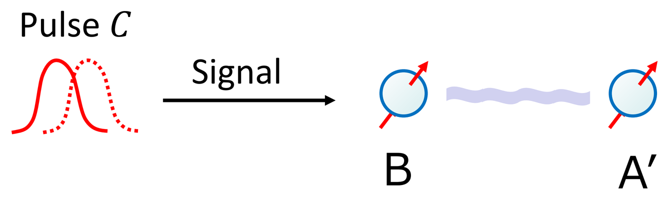
Our Results

1. Summary of our results

- ❑ We developed a refined security proof that achieves almost optimal key rate scaling in the asymptotic limit.
- ❑ The improvement in the key rate is sustained in finite-size cases, but lost under the existence of excess noises.

2. Refined security proof

- ❑ Isometric extension of Bob's signal measurement



upon "Success"

(A′ is an auxiliary qubit)

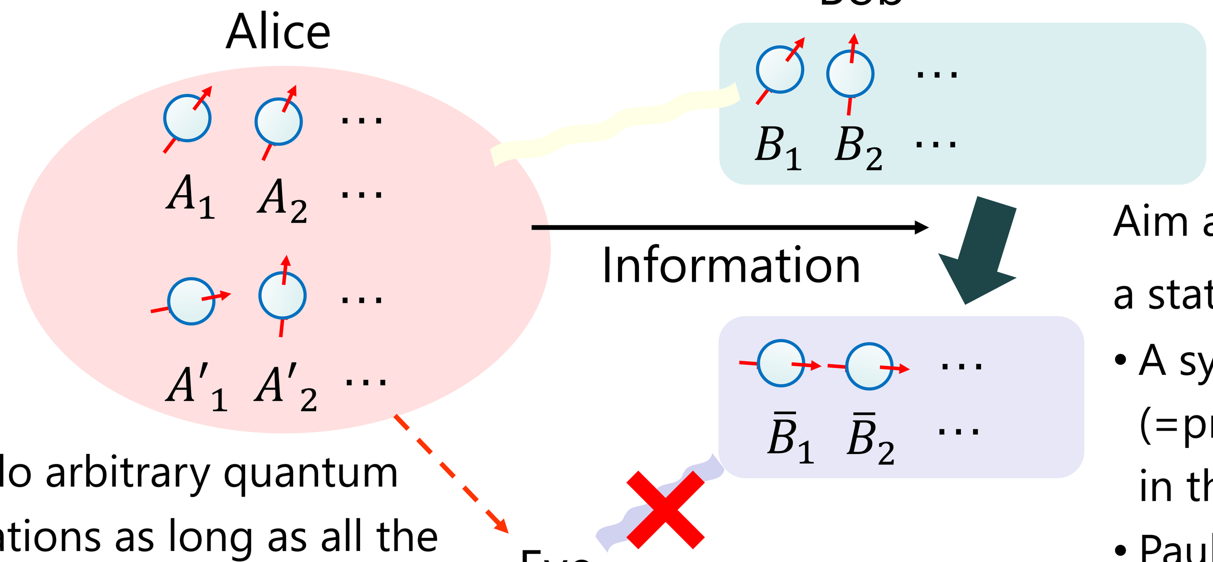
$$\mathcal{F}(\rho_C) = \int dx\, K'^{(x)} \rho_C\, K'^{(x)\dagger},$$

where $K'^{(x)} = \sqrt{f_{suc}(x)}\left(|0\rangle_B|0\rangle_{A'}\langle x|_C + |1\rangle_B|1\rangle_{A'}\langle -x|_C\right)$

* The idea comes from the equality condition of the entropic uncertainty relation. (See also arXiv:2009.08823)

- ❑ Security proof based on complementarity with reverse reconciliation

In the virtual protocol…



Can do arbitrary quantum operations as long as all the statistics and information to Eve are the same as those in the actual

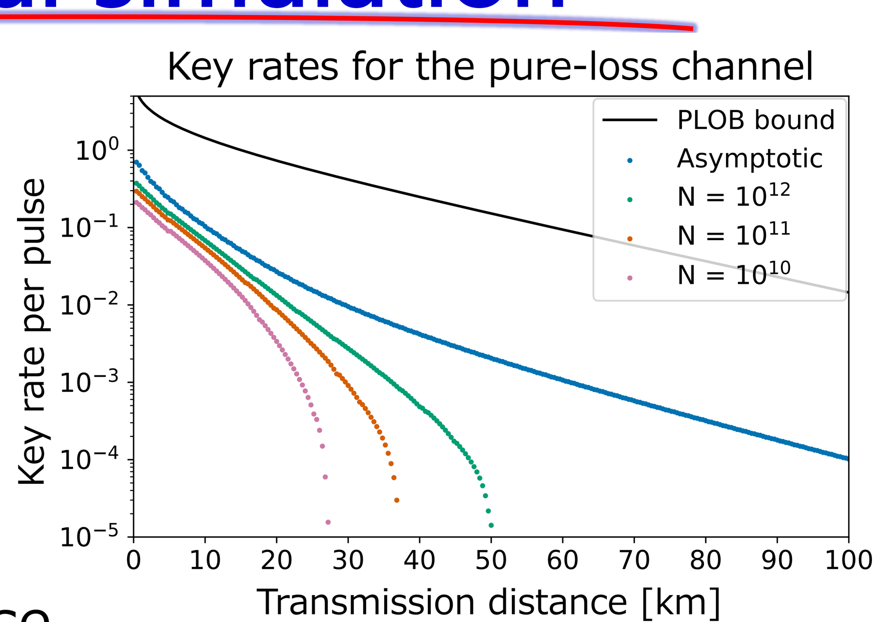
Aim at transforming into a state $|+\rangle^{\otimes N_{fin}}$ with

- A syndrome extraction (=privacy amplification in the actual)
- Pauli-Z operations (=no effect in the actual)

→ Entangled measurement $P_{AA'}^{\pm}$ to optimally distinguish Bob's $|\pm\rangle$ on B

3. Numerical simulation

- ❑ Improvement in key rate
  - The logarithm of the asymptotic key rate scales (almost) linearly against transmission distance.
  - Even finite-size key rates surpass the asymptotic key rate of the previous analysis.



- ❑ Fragility against excess noise
  - The key rates are largely degraded when the excess noise is present.
  - Excess noise as small as $\xi = 10^{-3.0}$ **at the channel output** (untrusted noise) restricts the performance.

→ Will extensions to four-state protocols save the day?