Finite-size security proof of discrete-modulation continuous-variable quantum key distribution using only heterodyne measurement

Shinichiro Yamano[1], Takaya Matsuura[1], Yui Kuramochi[2], Toshihiko Sasaki[1,2], Masato Koashi[1,2]

[1]*Department of Applied Physics, Graduate School of Engineering,The University of Tokyo, 7-3-1 Hongo Bunkyo-ku, Tokyo 113-8656, Japan*

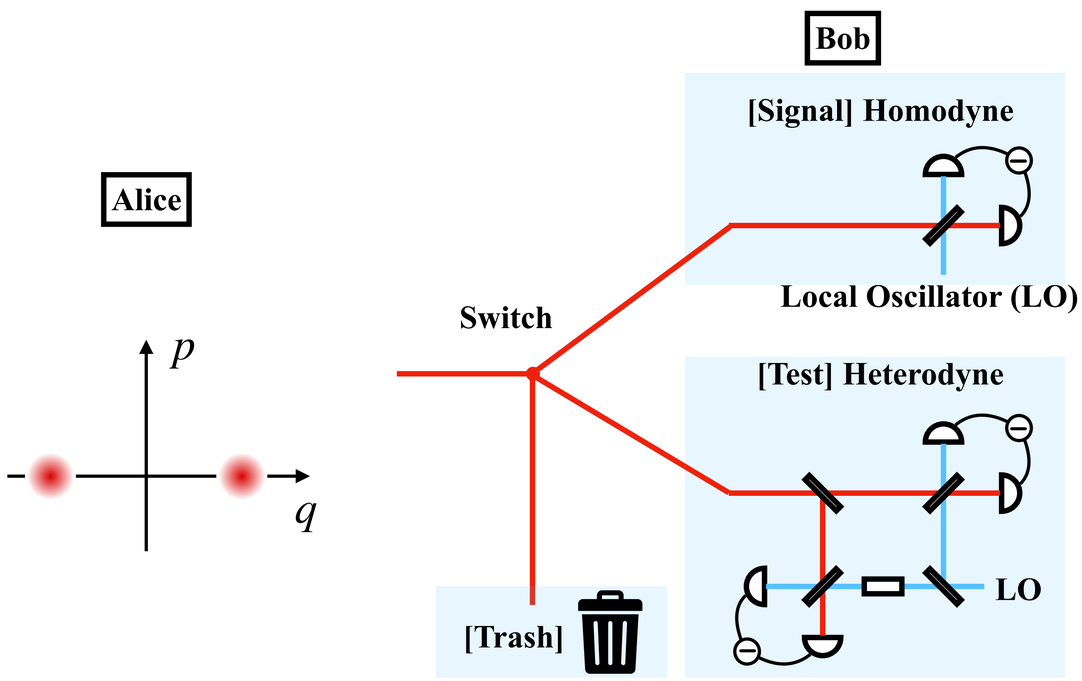
[2]*Photon Science Center, Graduate School of Engineering,The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan*

Abstract

Recently the finite-size security of a continuous-variable quantum key distribution protocol was reported[1], in which homodyne measurement is used for generating raw key and heterodyne measurement for monitoring. Here we improve the security proof to allow the use of heterodyne measurement for both purposes. The new protocol not only simplifies the receiver apparatus but also alleviates the necessity of actively locking the phases of the sender's and the receiver's local oscillators (LO). The comparison of the key rates of the two protocols shows that replacing homodyne measurement with heterodyne measurement worsens the channel loss dependence by only 1 dB,

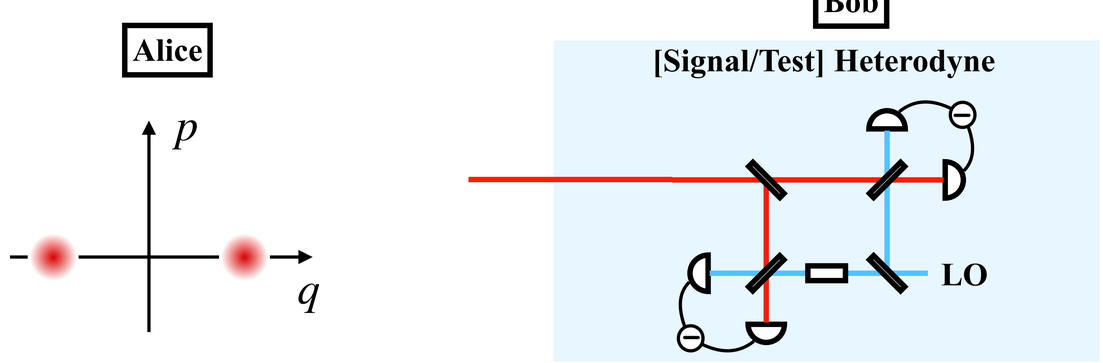
Method

Previous protocol [1]



- ✓ In “Signal”, the bit value is obtained. In “Test”, Bob estimate the fidelity and monitor Eve’s attack. In “Trash”, the pulse is discarded.
- ✓ Bob switches “Signal” “Test” or ”Trash” in each pulse. In previous protocol, Homodyne measurement is used to take bit value.

Our protocol



- ✓We improve the security proof of the previous protocol [1] to replace the use of homodyne measurement with heterodyne measurement.
- ✓ Alice and Bob do not have to lock their LO phases as long as the phase difference is tracked and estimated, which can be compensated afterwards by data processing. It enables omitting real-time phase compensate system[2,3].
- ✓ Moreover, our proof dispenses with “Trash” round.

Reference

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

[2] Bing Qi et al., Phys. Rev. X, 5:041009, Oct 2015.

[3] Daniel B et al., Phys. Rev. X, 5:041010, Oct 2015.

Results

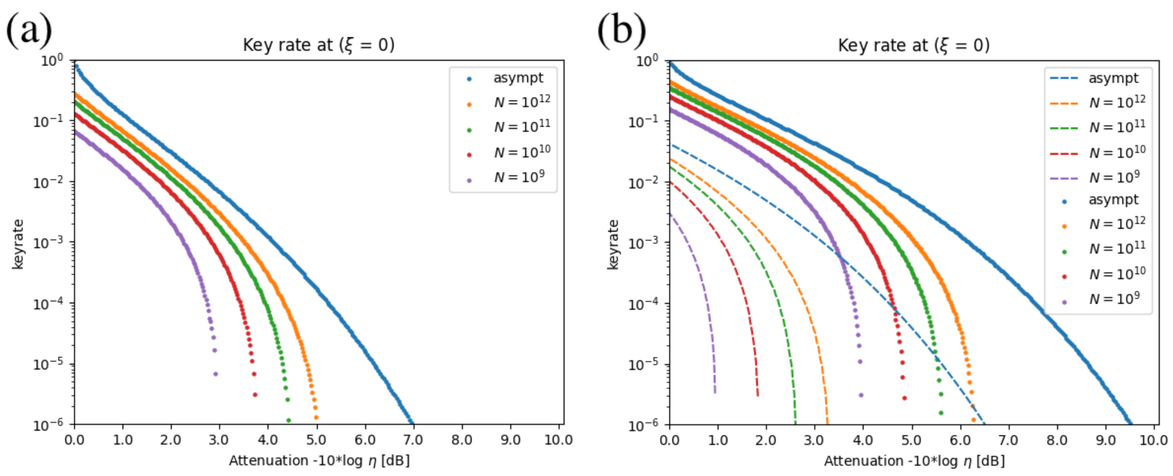
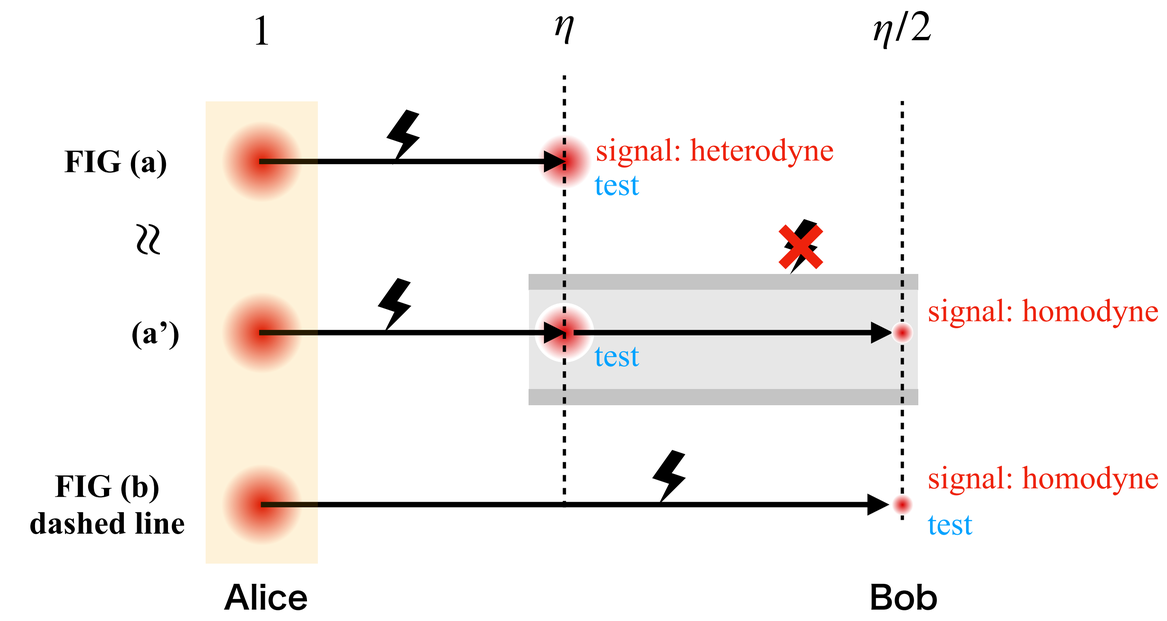


FIG : Key rates plotted against the channel transmission η with a total number N of transmitted pulses. We assume a pure loss channel with no excess noise ($\xi = 0$). (a) Our protocol. (b) Solid line: previous protocol [1]. Dashed Line: previous protocol shifted by 3 dB.

- ✓Distinguishing between two coherent states in a heterodyne measurement is equivalent to halving the intensity of an optical pulse and then performing a homodyne measurement.
- ✓It naively predicts that replacing homodyne measurement with heterodyne measurement worsens the channel loss dependence by about 3 dB (FIG. (b)). However, our protocol (FIG. (a)) suffers only a 1 dB penalty in finite-key regime.

Discussion

The discussion about the reason why only a 1 dB penalty instead of 3dB: to compare Fig (a) and Fig (b) dashed line protocol, we introduce another protocol (a’).



- ✓In (a’), Bob tests the fidelity at η and take signal with homodyne measurement at $\eta/2$. Between η and $\eta/2$, Eve can not attack. Key rate (a) is equal to (a’).
- ✓Then comparing (a’) and (b), the restriction of Eve’s attack enables more precise evaluate of phase error. It could be a factor in the key rate improvement.