Simple Method for Asymmetric Twin-Field Quantum Key Distribution

Wenyuan Wang[1,2] and Hoi-Kwong Lo[1]

[1] *Centre for Quantum Information and Quantum Control (CQIQC), Department of Electrical and Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*

[2] *(current address:) Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*

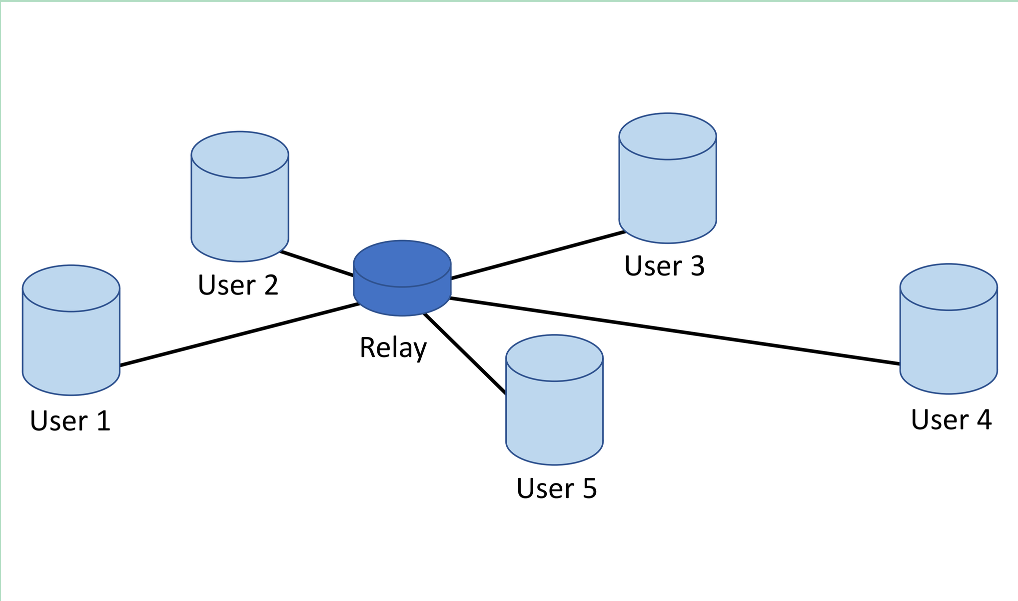
UNIVERSITY OF TORONTO

Twin-Field quantum key distribution (TF-QKD) can beat the linear bound of repeaterless QKD systems. After the proposal of the original protocol, multiple papers have extended the protocol to prove its security. However, these works are **limited to the case where the two channels have equal amount of loss (i.e. are symmetric)**. In a practical network setting, it is very likely that the channels are **asymmetric** due to e.g. geographical locations. In this work we extend the "simple TF-QKD" protocol to the scenario with asymmetric channels. We show that **by simply adjusting the two signal states** of the two users (and not necessarily the decoy states) they can effectively compensate for channel asymmetry and consistently obtain higher key rate than either using no compensation or using the strategy of deliberately adding fibre to the shorter channel. We perform simulation with realistic parameters and finite data size, and show that our method works well and has **a clear advantage over prior art methods in the presence of channel asymmetry.**

Background 1

Twin-Field (TF) QKD [1] **can beat the linear repeaterless bound [2,3]** for QKD and provide better rate-distance tradeoff. In addition, it provides **measurement-device-independence** just like MDI-QKD [4].

In the setup of TF-QKD, two parties Alice and Bob each send signals through a channel to a third party Charles. The original proposal of TF-QKD, along with many early security proofs, only considers the **symmetric case** where Alice's and Bob's channels have the same amount of loss.



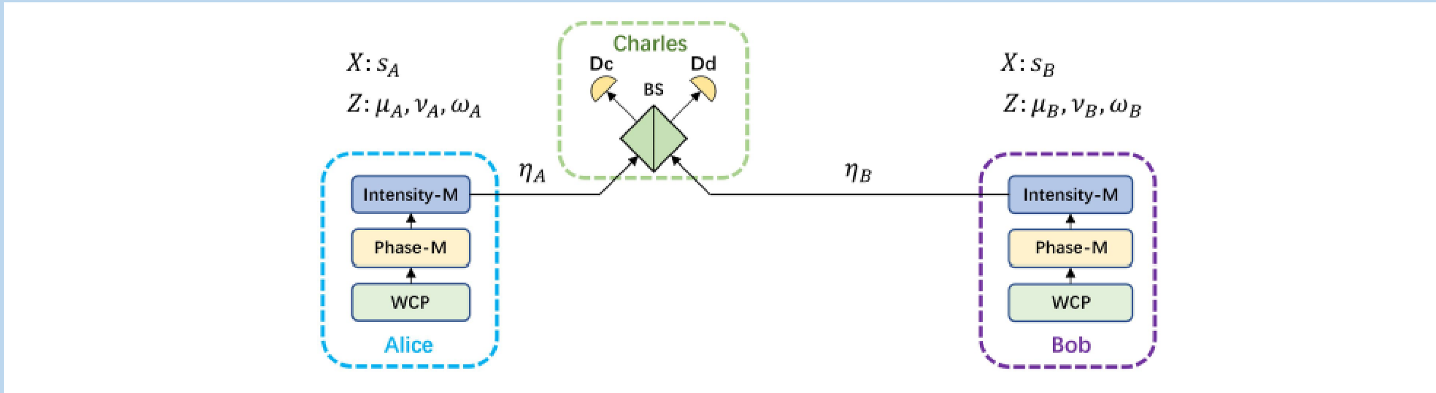
In a realistic setting, it is very likely that the channels are **asymmetric**.

This is especially important in a **network setting** (e.g. a star-shaped network) where numerous users at arbitrary locations are connected to a central node – where the network has to be able to **cater for pairs of asymmetric channels**.

Contact Email: wenyuan.wang@uwaterloo.ca;

Reference for this work: New J. Phys. 22.1 (2020): 013020.

Protocol 2



Here we extend the version of TF-QKD protocol proposed in Ref. [5] (which we call **"CAL" protocol**) to the asymmetric scenario. In this protocol, Alice and Bob send:

(1) **non-phase-randomized** coherent states as signals in X basis (for **coding**), with intensities s_A, s_B;
(2) **phase-randomized** decoy states in the Z basis (for **testing**), with multiple levels of decoy intensities.

We show that by simply allowing Alice and Bob to have **asymmetric signal intensities** they can effectively **compensate for asymmetric channel losses** and maintain **good key rate**.

Our asymmetric protocol has been recently **experimentally demonstrated in Ref. [6].** Also, a similar idea for MDI-QKD has been previously demonstrated by us and collaborators in Refs. [7,8].

Theory 3

We discuss two main points for our asymmetric CAL protocol, on its **security and performance**:

(1) Security: Neither asymmetric channels nor asymmetric intensities between Alice and Bob affects security.

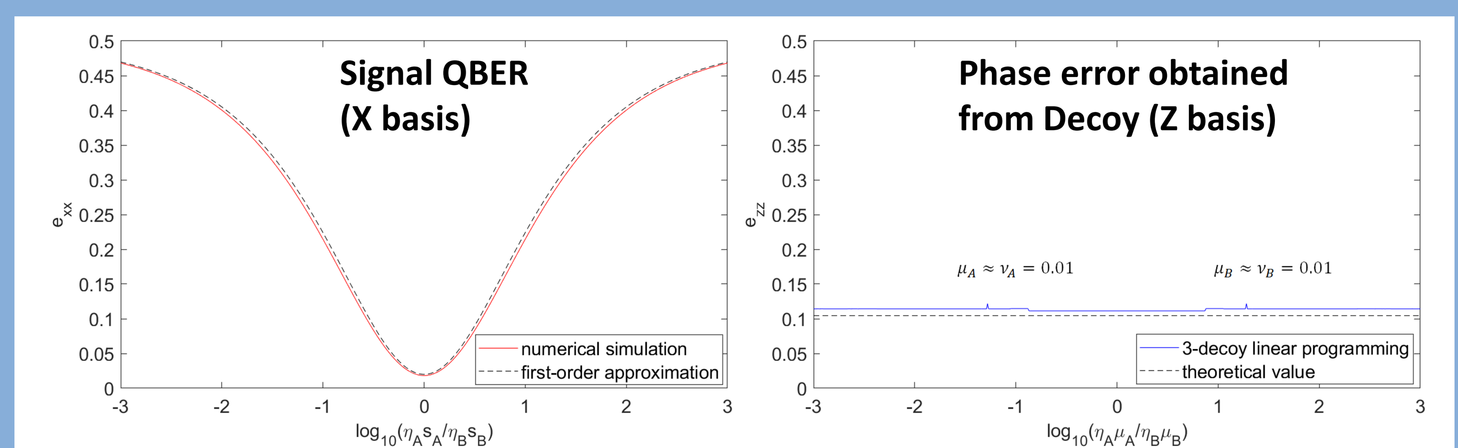
In the security proof of CAL protocol, The channel is modeled as a set of **Kraus operators** (which are treated as blackboxes whose actual expressions are not used in the proof). Having **asymmetric channels** does not affect the form of the Kraus operators.

The phase error rate is obtained by considering the virtual protocol where Alice and Bob sent **cat states** $(|\sqrt{s}\rangle \pm |-\sqrt{s}\rangle)/\sqrt{2}$, the statistics of which can be bounded by decoy-state analysis on the Z basis data. As the cat states are allowed to be different for Alice and Bob, using **asymmetric signals** would not affect security either. More details can be found in our paper [9].

(2) Performance: Channel asymmetry, if not compensated, will greatly reduce key rate of TF-QKD. By adjusting X basis signal intensity for Alice/Bob, we can compensate for channel asymmetry and get good key rate.

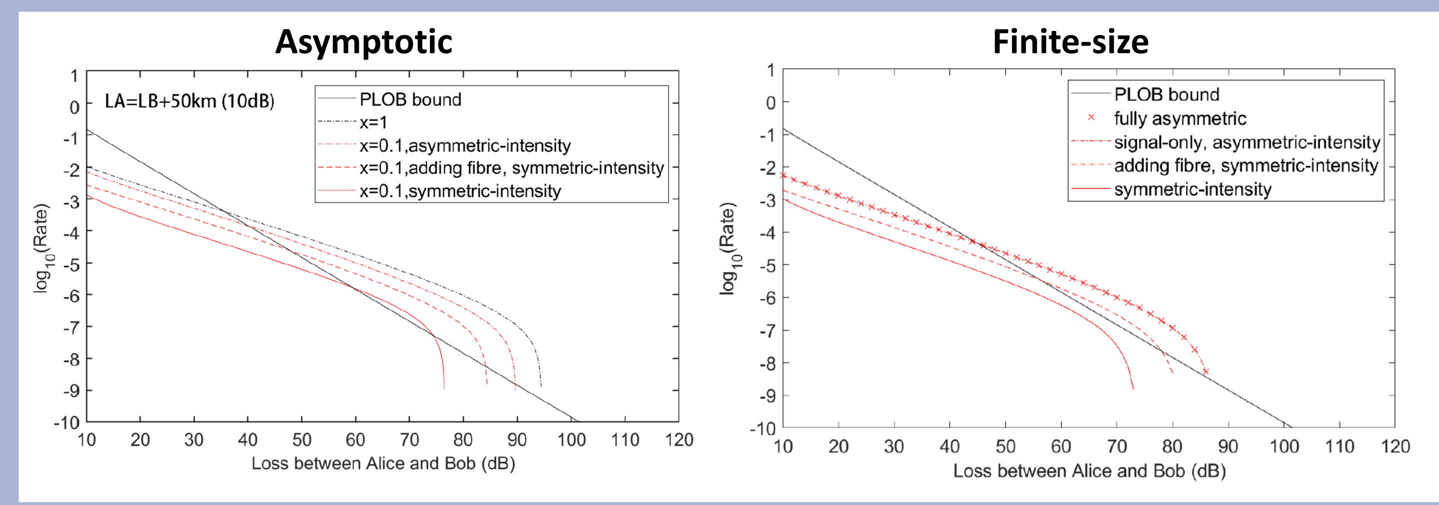
Points (2) can be observed by studying the X basis QBER versus arriving intensity ratio at Charles. **Asymmetric arriving intensities decrease interference visibility**, hence resulting in higher QBER.

Using asymmetric signal intensities to maintain a **balanced arriving intensity** improves X basis QBER. On the other hand, ratio of decoy-state intensities affects the phase error rate very little (since only the Gain data and not QBER is obtained in Z basis). Therefore decoy-states need not be balanced.



Numerical Results 4

We perform **numerical simulation** of the asymmetric-intensity protocol versus **prior art implementations** of (1) not doing any compensation or (2) adding additional loss to the shorter channel to achieve symmetry.



Above figures show both asymptotic (infinite-data, infinite-decoys) and realistic (3-decoys, finite-data analysis) cases.

Here 10^{-8} **dark count rate**, 2% **misalignment** for Alice and Bob each, and N=10^{12} (for the **finite-size** case) are used. The example plots consider a **10dB difference** between Alice and Bob's channels. For simplicity, **standard error analysis** is used for finite-size case.

As can be seen, using asymmetric signal intensities **consistently provides higher key rate** than either prior art strategies, when channels are asymmetric.

Also, the case with fully-optimized signal intensities *and decoy intensities* is also included (right figure crosses), which shows that allowing **asymmetric decoy intensities do not improve key rate.**

References 5

[1] M Lucamarini, ZL Yuan, JF Dynes, AJ Shields, Nature 557.7705:400 (2018).

[2] M Takeoka, S Guha, M Wilde, Nat. Comm. 5:5235 (2014).

[3] S Pirandola, R Laurenza, C Ottaviani, L Banchi, Nat. Comm. 8:15043 (2017).

[4] HK Lo, M Curty, and B Qi, Phys. Rev. Lett., 108.13:130503 (2012).

[5] M Curty, K Azuma, HK Lo, npj Quantum Inf. 5.1 (2019): 1-6.

[6] X Zhong, W Wang, L Qian, HK Lo, arXiv:2001.10599 (2020).

[7] W Wang, F Xu, HK Lo, Phys. Rev. X 9, 041012 (2019).

[8] H Liu, et al., Phys. Rev. Lett. 122.16, 160501 (2019).

[9] W Wang, HK Lo, New J. Phys. 22.1 (2020): 013020.