Realizing downstream access network using continuous-variable quantum key distribution

Yundi Huang[1], Tao Shen[1], Xiangyu Wang[1*], Ziyang Chen[2*], Bingjie Xu[3], Song Yu[1] and Hong Guo[2]

1 State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
2 State Key Laboratory of Advanced Optical Communication, Systems and Networks, Department of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China
3 Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China
Email: xywang@bupt.edu.cn, chenziyang@pku.edu.cn

arXiv:2107.01800

1. Introduction

- Quantum key distribution (QKD) is designed to establish symmetric keys among two legitimate parties. Continuous variable (CV) QKD that uses the coherent states and homodyne detection can only apply the cost-effective telecommunication components [1].
- Access network allows multitude end-users to connect to the nodal network [2].
- For downstream access network, signals are generated from the OLT, and broadcasted to every ONU in the network through passive beamsplitter.

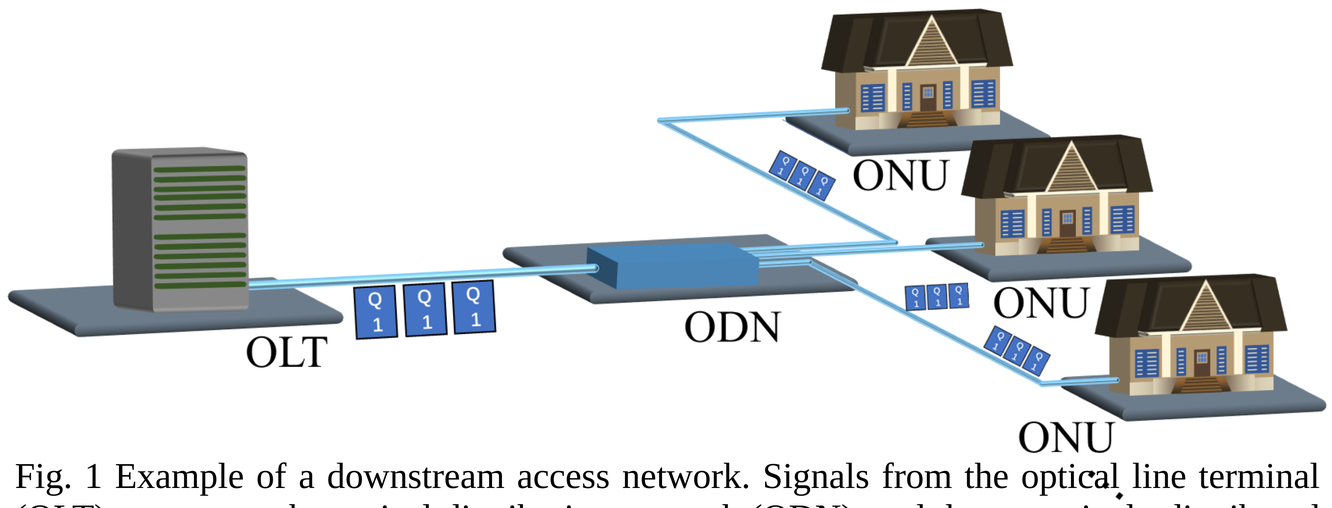

Fig. 1 Example of a downstream access network. Signals from the optical line terminal (OLT) are sent to the optical distribution network (ODN), and them passively distributed to multiple optical network units (ONUs) through the beamsplitter (BS).

2. CV-QKD downstream access network

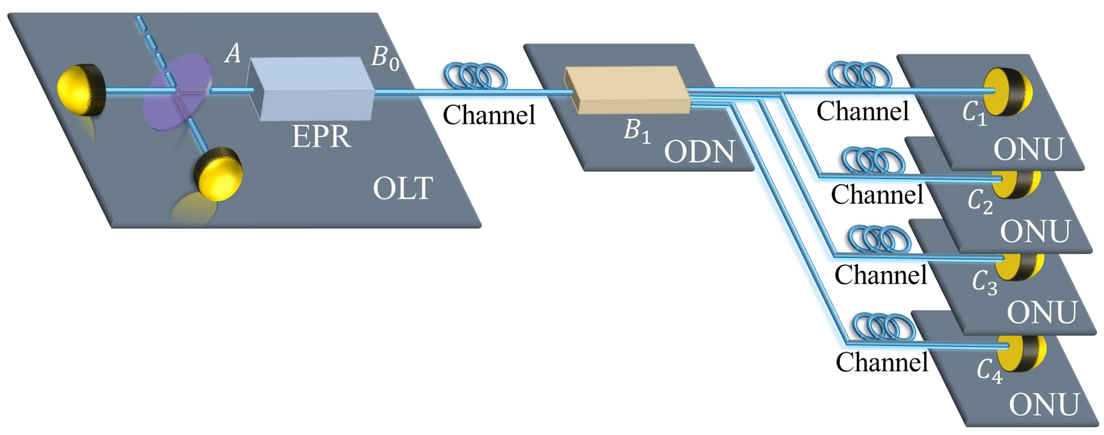

Fig. 2 Entanglement-based (EB) model of a CV-QKD downstream access network.

- The downstream access network is composed of standard CV-QKD transmitter and receivers, BS is located at the ODN to passively distribute quantum states to each ONU.
- The ODN which is located in the middle of the OLT and ONUs separates the channel into segments.
- Since every ONU gets a copy of the quantum signal, malicious ONU may try to intercept the key between the OLT and the specified ONU.

3. Security analysis

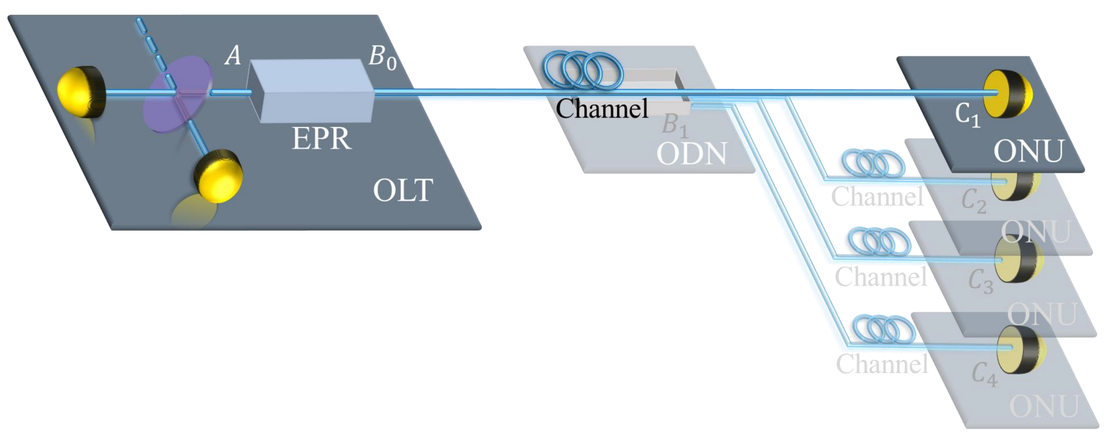

Fig. 3 Modified EB model which is applicable for the security analysis for the downstream access network. Only the OLT and the specified ONU are highlighted.

- Standard CV-QKD is designed for point-to-point distribution scenario [3]. Further modification of the security analysis is needed for downstream access network.
- Classical post-processing is conducted with one activated ONU at a time.
- Different channel segments are treated as one channel to reduce the calibration complexity of channel parameters.
- The eavesdropper Eve is considered as being able to control other parties so that the security against other parties in the downstream access network can be obtained.

4. Performance analysis

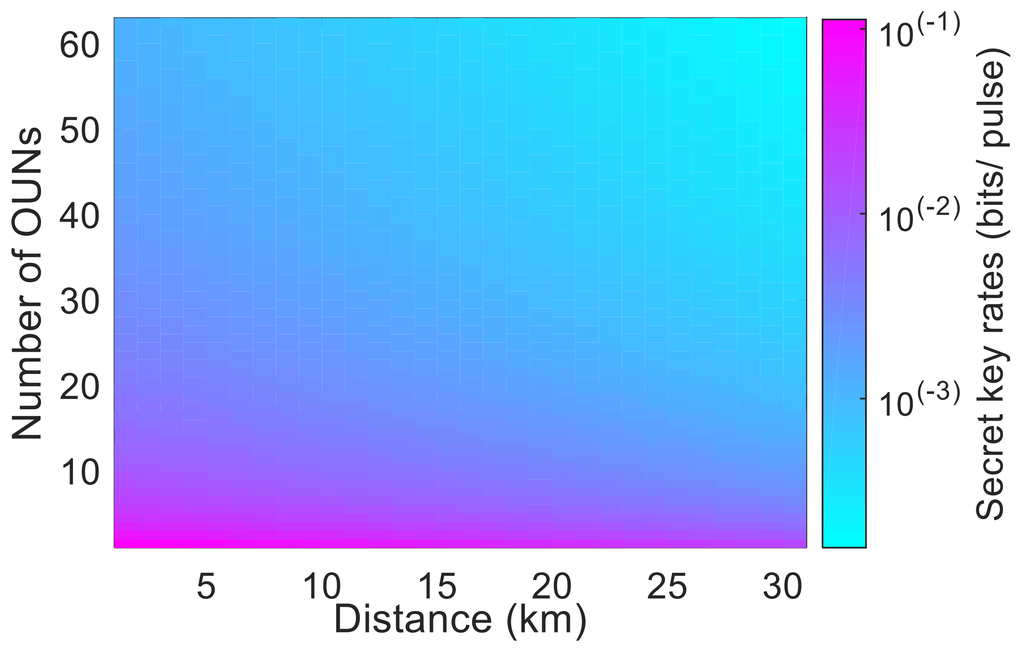

Fig. 4 Achievable secret key rates against the number of ONUs access in the network and transmission distance. The secret key rates are represented by the pseudo-colors. Simulation parameters: variance of the EPR state V=5, channel excess noise ε=0.05 (SNU), detection efficiency η_d=0.6, electronic noise η_e=0.99, and reconciliation efficiency =0.956.

- When more ONUs are connecting to the network, the secret key rate drastically decreases.
- Positive secret key rates can be obtained even with 64 ONUs access to the network, within the maximum physical reach.

5. Conclusion

- We show that quantum key distribution can be implemented in the downstream access network by using continuous-variable quantum key distribution.
- The realization of the downstream access network with our proposed security analysis can maximally maintain the implementation from the standard CV-QKD set-up.
- The security analysis is highly effective and can be conducted without the collaboration of other ONUs.
- Performance analysis shows the feasibility of the downstream access network.

References

[1] S. Pirandola, et al., "Advances in quantum cryptography," Adv. Opt. Photonics 12, 1012–1236 (2020).
[2] ITU-T, "G.984.2: : Gigabit-capable passive optical networks (gpon): Physical media dependent (pmd) layer specification," (2019).
[3] V. Scarani, et al., "The security of practical quantum key distribution," Rev. Mod. Phys. 81, 1301–1350 (2009).