Experimental demonstration of 4-user quantum access network based on passive optical network

Yan Pan[(1)]*, Yiming Bian[(2)]*, Heng Wang[(1)], Jiayi Dou[(2)], Yun Shao[(1)], Yaodi Pi[(1)], Ting Ye[(1)], Jie Yang[(1) (2)], Yang Li[(1)], Wei Huang[(1)], Song Yu[(2)], Yichen Zhang[(2)]†, and Bingjie Xu[(1)]‡

[(1)] Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China, xbjpku@163.com
[(2)] State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China, zhangyc@bupt.edu.cn
* These authors contributed equally

Abstract *A 4-user high-compatibility quantum access network using coherent states is experimentally demonstrated based on passive optical network. The achieved average secret key rate is around 4.1 Mbps between the transmitter and each one user, which is two orders-of-magnitude higher than previous demonstrations.*

Introduction

Quantum key distribution (QKD) is an effective way to establish a key distribution system with information theory security between two distant parties. Nowadays, QKD technology has made significant progress in both discrete-variable (DV) and continuous-variable (CV) schemes for point-to-point links [1-7]. From the perspective of the QKD networks, point-to-point QKD links are suitable to form a backbone quantum core network for long-distance quantum secure communications [8]. However, In the "last mile" of a metropolitan or access network, point-to-point QKD is not very suitable due to the high system cost. Therefore, building a point-to-multipoint (PTMP) QKD network for multitude of users to access to the QKD infrastructure has important application value.

As early as 1997, P. D. Townsend has introduced and verified a multi-user QKD scheme on a downstream passive optical fibre network [8]. This implementation requires a single photon detector for every user, which is difficult to promote to the general public. In Ref. [9], B. Fröhlich *et al.* proposed an upstream quantum access network, in which multi-users transmit quantum signals to a common receiver. In this case, the cost is controllable, but the key rate is limited by the receiver. Furthermore, based on the downstream or upstream architecture, various schemes of QKD network have been proposed and deployed [10]. However, the maximum secret key rate (SKR) of all existing works is less than Mbps whether using DV or CV QKD scheme. This is mainly due to that no efficient protocol can natively support the secure connections of multiple users. Based on the two-user QKD protocols, even the most advanced existing metropolitan [10] and access networks [9] need relays, multiplexing technologies or simply building multiple QKD links to access multiple users. This leads to a complex network with limited load capacity quantum access networks.

Here, based on our previously proposed PTMP CV-QKD protocol, we experimentally demonstrated a high-performance downstream fibre access network including 1 transmitter and 4 receivers based on a passive optical network [11]. The investigated scheme inherits the advantages of CV-QKD (i.e., low-cost, excellent compatibility, and high key rate), which provides a better connectivity and scalability in quantum access network. The SKR of the 4 CV-QKD links between Alice and each Bob can reach to 6.68, 3.04, 5.40 and 1.30 Mbps, respectively, which resulting in 2 orders of magnitude of enhancement compared with states of art works [9, 10]. This result shows the studied scheme is a promising way of building high-rate, large-scale and cost-effective QKD network.

PTMP CV-QKD protocol and security analysis

The PTMP QKD protocol natively supports the parallel secret key generation between a network node and all users. Each quantum signal prepared by the node, which is a weak coherent state, can be received and processed by all users to establish correlations between multiple parties. Further, through a proper error correction and privacy amplification, the independence of different users is ensured, and each user can generate independent secret key with the network node. This parallelism significantly improves the efficiency of the overall network, resulting in a high key rate.

The security of the protocol is ensured by

$$K_i = \beta I_{AB_i} - \max\{\chi, I_{B_iB_1}, I_{B_iB_2}, \dots, I_{B_iB_N}\},$$

Here K_i is the SKR, which represents the secret

key bits that can be distilled from each one signal pulse between the network node and user i. β is the reconciliation efficiency caused by the imperfect error correction. I_{AB_i} is the Shannon entropy between the network node and user i, and $I_{B_iB_N}$ is the Shannon entropy between user i and the other users. χ is the Holevo bound, which is the upper limit of the information that a potential eavesdropper can get. We remark that χ is estimated by the network node and all users jointly, therefore they can get a tight estimation of the potential eavesdropping behavior, which can offset the negative impact caused by the loss of the optical power splitter. Therefore, although the splitter may introduce a huge loss with the increase of the users, the performance of the overall network is slightly affected, and the SKR of each user is ensured in protocol layer.

Experimental setup

The experimental setup of a 4-user CV-QKD network is shown in Fig. 1. At Alice's site, a continuous-wave laser (i.e., Laser 1) with a linewidth of <100 Hz is used as the carrier. Then, the light is split into two branches by a beam splitter (BS). One branch of the optical carrier is modulated by an In-phase/quadrature modulator (IQ modulator). The *x* and *p* quadrature signals with an 850 MHz frequency shift are generated by a two channel arbitrary waveform generator (AWG), and the two electrical Gaussian signals with repetition frequency of 500 MHz are modulated by the IQ modulator. Then, a variable optical attenuator (i.e., VOA1) is used to control the modulation variance V_A. The state of polarization (SOP) of the optical quantum signal is controlled by a polarization controller (i.e., PC1) and aligns to the principal axis of the polarization beam combiner (PBC). The reference path mainly consists of an optical delay line, VOA2, and PC2. Therefore, the optical quantum and high-power reference signal are multiplexed by the dimension of polarization and frequency. Then, the multiplexed signal is controlled by an acousto-optic modulator (AOM) to calibrate shot noise in real time. Here, an arbitrary function generator (AFG) is used to trigger AWG and AOM. The transmission link consists of 10 km standard single mode fibre (SSMF), 1:4 optical power splitter, and 5 (i.e., L1, L3, L4) or 8 km (i.e., L2) SSMF. At Bob's site, four independent receivers are used for simulating different users (i.e. Bob1, Bob2, Bob3 and Bob4). As an example, the internal structure of Bob1 is given. In Bob1, an independent running CW laser (i.e., Laser 2) with a linewidth of <100 Hz is used as the local oscillator, and the centre wavelength is about 1.75 GHz shift from laser 1. Then, the optical signal and local oscillator are coherently detected by a polarization diversity receiver. The polarization diversity receiver consists of a polarization beam splitter (PBS), a BS, two polarization-maintaining optical couplers, and two balanced photo-detectors. Finally, the received electrical signals are digitalized by digital storage oscilloscopes (DSO) at 5 Gsa/s, and offline DSP is performed for signal demodulation and parameters estimation. Details of the DSP can be found in Ref. [12].

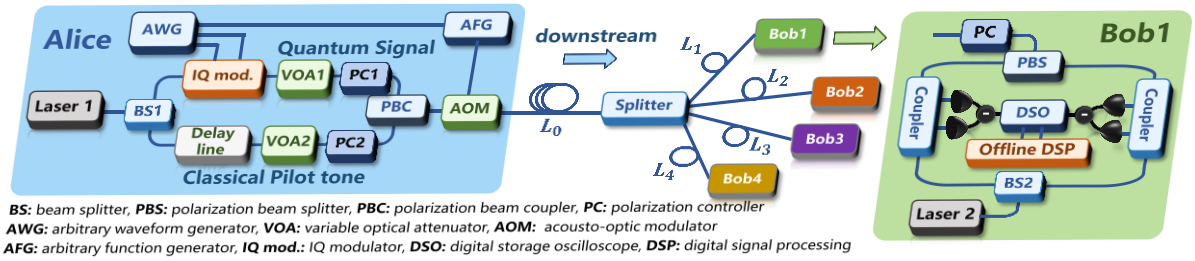

Fig. 1. The experimental schematic of the 4-user quantum access network. The main features of key devices are: <100 Hz linewidth lasers, 23 GHz arbitrary waveform generator with 30 GSa/s sampling rate and 8 bits resolution, 23 GHz IQ modulator, 8 GHz oscilloscope with 5 GSa/s sampling rate and 8 bits resolution.

Results

As a stability investigation, we measure the PTMP system SKR performance for each user with 11 times, and the results are shown in Fig. 2. Here, the interval between each test is about 15 minutes (i.e., acquiring, processing, and saving the desired data), and the block size of parameter estimation for each test is 1×10^7. The modulation variance is set to 4.3 in shot noise unit (SNU), the detection efficiency of the receivers is around 0.7, the electronic noise of the receivers is around 0.1 SNU. The fibre links L0 = 10 km, L1 = L3 = L4 = 5 km, L2 = 8 km, and the total loss for each link is about 12 dB (i.e., including the loss of fibre links, 1:4 optical power splitter, PC, PBS, and connectors). The reconciliation efficiency is 95.6% [13], and the ratio of training sequence is set to 20%. As shown in Fig. 2, the SKR is not stable, this is mainly because of the fluctuating excess noise that introduced by quantum signal recovery and detection noise. Especially, the detection

noise will be amplified when calculate the equivalent excess noise at Alice's site. Meanwhile, the SKR is not same for different users due to the different performance of receiver. However, most of the test results are >Mbps, and the average SKR is considerable.

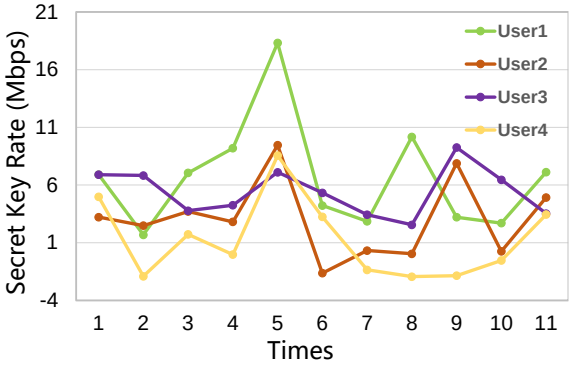

Fig. 2. SKR of 4 users as a function of test times. For each user, the block size of parameter estimation $N = 1\times10^7$, modulation variance $V_A = 4.3$, reconciliation efficiency $\beta = 95.6\%$, electronic noise is ~0.1, link loss is ~12 dB, detection efficiency is ~0.7.

The averaged SKR performance are shown in Fig. 3 and Tab. 1. As can be seen from Fig. 3, the average asymptotic SKR of the 4 QKD links are 6.68 Mbps, 3.04 Mbps, 5.40 Mbps and 1.30 Mbps, and the average SKR of the 4 users is 4.11 Mbps. Compared with the existing networks using two-user protocols (47.5 kbps@16.2 km [10] and 49.5 kbps@18 km [9]), our results get an enhancement of 2 orders of magnitude. Even if comparing with those results based on wavelength-dense-division multiplexing scheme (303 kbps @16.2 km [9]), which means less loss but much more complex system, our results still have an enhancement higher than an order of magnitude. In this case, the investigated scheme has a practical potential for high-speed quantum access network.

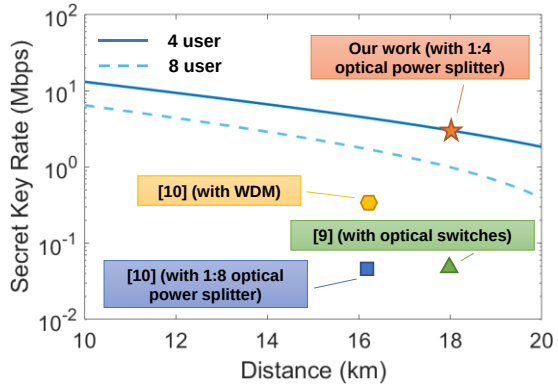

Fig. 3. Experimental results of SKR performance. The SKR of the QKD link with 18 km length in the experiment is compared with the states of art works.

Tab. 1: SKR for the 4-user CV-QKD system with repetition rate of 500 MHz.

Link Distance	Link 1 15 km	Link 2 18 km	Link 3 15 km	Link 4 15 km	Average
SKR (bits/pulse)	1.34 $\times10^{-2}$	0.61 $\times10^{-2}$	1.08 $\times10^{-2}$	0.26 $\times10^{-2}$	0.82 $\times10^{-2}$
SKR (Mbps)	6.68	3.04	5.40	1.30	4.11

Conclusions

A high-performance 4-user QKD access network is experimentally reported which firstly enable to support multiple users natively and demonstrated a solution in QKD protocol layer for interconnecting multiple users securely. The proposed scheme makes full use of the information from the source and all the receivers, which contributes to a tight estimation of the channel parameters and >Mbps SKR for both single user and overall network is achieved. Moreover, the scheme can be realized with low-cost devices compatible with classical passive optical network. It is notable that, here our experiment is demonstrated with offline DSP and post-processing. In the future, a real-time data processing can further enhance the practicality of the network. In summary, our work can be easily integrated into the existing optical communication networks, providing higher rate, larger scale, and better compatibility for building QKD network.

Acknowledgements

This research was supported by the National Key Research and Development Program of China (2020YFA0309704), the National Natural Science Foundation of China (62001044, U19A2076, U22A201034, 62101516, 62171418, 62201530 and 61901425), the Basic Research Program of China (JCKY2021210B059), the Sichuan Science and Technology Program (2022ZYD0118, 2023JDRC0017, 2023YFG0143, 2022YFG0330, 2022ZDZX0009 and 2021YJ0313), the Natural Science Foundation of Sichuan Province (2023NSFSC1387 and 2023NSFSC0449), the Chengdu Major Science and Technology Innovation Program (2021-YF08-00040-GX), the Equipment Advance Research Field Foundation(315067206), the Chengdu Key Research and Development Support Program (2021-YF05-02430-GX and 2021-YF09-00116-GX), the Foundation of Science and Technology on Communication Security Laboratory (61421030402012111).

References

[1] F. Xu, X. Ma, Q. Zhang, H. K. Lo, J. Pan, "Secure quantum key distribution with realistic devices," Reviews

of Modern Physics, **92**(2), 025002 (2020). DOI: 10.1103/RevModPhys.92.025002

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photonics, **12**(4), 1012-1236 (2020). DOI: 10.1364/AOP.361502

[3] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Physical Review Letters, **88**, 057902 (2002). DOI: 10.1103/PhysRevLett.88.057902

[4] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations," Entropy, **17**(9), 6072-6092 (2015). DOI: 10.3390/e17096072

[5] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," Physical Review Letters, **125**, 010502 (2020). DOI: 10.1103/PhysRevLett.125.010502

[6] N. Jain, H. Chin, H. Mani, C. Lupo, D. Nikolic, A. Kordts, S. Pirandola, T. Pedersen, M. Kolb, B. Ömer, C. Pacher, T. Gehring, and U. Andersen, "Practical continuous-variable quantum key distribution with composable security," Nature Communications, **13**(4740), 1-8 (2022). DOI: 10.1038/s41467-022-32161-y

[7] H. Chin, N. Jain, D. Zibar, U. Andersen, and T. Gehring, "Machine learning aided carrier recovery in continuous-variable quantum key distribution," npj Quantum Information, **7**(1), 1-6 (2021). DOI: 10.1038/s41534-021-00361-x

[8] P. D. Townsend, "Quantum cryptography on multiuser optical fibre networks," Nature **385**, 47-49 (1997). DOI: 10.1038/385047a0

[9] B. Fröhlich, J. F. Dyne, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," Nature **501**, 69-72 (2013). DOI: 10.1038/nature12493

[10] T. Chen, X. Jiang, S. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L. Chen, W. Liu, H. Zhang, K. Cui, H. Liang, X. Li, Y. Mao, L. Wang, S. Feng, Q. Chen, Q. Zhang, L. Li, N. Liu, C. Peng, X. Ma, Y. Zhao, and J. Pan, "Implementation of a 46-node quantum metropolitan area network," npj Quantum Information, **7**(134), 1-6 (2021). DOI: 10.1038/s41534-021-00474-3

[11] Y. Bian, Y. Zhang, C. Zhou, S. Yu, Z. Li, and H. Guo, "High-rate point-to-multipoint quantum key distribution using coherent states," arXiv:2302.02391 (2023). DOI: 10.48550/arXiv.2302.02391

[12] Y. Pi, H. Wang, Y. Pan, Y. Shao, Y. Li, J. Yang, Y. Zhang, W. Huang, and B. Xu, "Sub-Mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber," Optics Letters, **48**(7), 1766-1769 (2023). DOI: 10.1364/OL.485913

[13] L. Ma, J. Yang, T. Zhang, Y. Shao, J. Liu, Y. Luo, H. Wang, W. Huang, F. Fan, C. Zhou, L. Zhang, S. Zhang, Y. Zhang, Y. Li, B. Xu, "Practical Continuous-variable Quantum Key Distribution with Feasible Optimization Parameters," arXiv:2111.12942 (2021). DOI: 10.1007/s11432-022-3712-3