SCIENCE CHINA
Information Sciences

• LETTER •

August 2023, Vol. 66 189402:1–189402:2
https://doi.org/10.1007/s11432-022-3619-0

Highly efficient twin-field quantum key distribution with neural networks

Jingyang LIU[1,2,3], Qingqing JIANG[1,2,3], Huajian DING[1,2,3], Xiao MA[1,2,3], Mingshuo SUN[1,2,3], Jiaxin XU[1,2,3], Chun-Hui ZHANG[1,2,3], Shipeng XIE[3], Jian LI[1,2,3], Guigen ZENG[2,3*], Xingyu ZHOU[1,2,3*] & Qin WANG[1,2,3*]

[1]*Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing* 210003*, China;*
[2]*Key Lab of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing* 210003*, China;*
[3]*Telecommunication and Networks National Engineering Research Center, Nanjing University of Posts and Telecommunications, Nanjing* 210003*, China*

Received 30 May 2022/Revised 5 August 2022/Accepted 11 November 2022/Published online 13 July 2023

Citation Liu J Y, Jiang Q Q, Ding H J, et al. Highly efficient twin-field quantum key distribution with neural networks. Sci China Inf Sci, 2023, 66(8): 189402, https://doi.org/10.1007/s11432-022-3619-0

Quantum key distribution (QKD) allows two legitimate parties, Alice and Bob, to share a series of random bits that are secured by the laws of quantum mechanics. As a remarkable theoretical progress towards longer distances, the proposal of twin-field QKD (TF-QKD) [1] shows the capability to break a repeaterless bound and provides a key rate in the square-root scale of channel transmittance (i.e., $R \sim \sqrt{\eta}$), promising preponderant transmission distance. However, TF-QKD implementation requires the precise acquisition of a global phase drift, which rapidly fluctuates due to long fibers. Typically, the phase scan method via time-divisional modulation [2] is adopted for phase compensation, where a brighter reference light should be implemented for scanning the phase drift. Therefore, a very limited transmission efficiency which refers to the ratio of the time of the quantum part to the whole cycle, is obtained.

To address this problem, we develop a phase-drift forecasting technique that can overcome the efficiency limit of the current phase calibration. This technique can achieve accurate predictions and active feedback control on the phase drift of TF-QKD with a fiber distance of over 500 km, drastically accelerating the transmission efficiency.

Data processing. A phase drift caused by ambient disturbances on optical fiber is particularly significant in TF-QKD systems. As a phase drift shows correlations with time and environment dependence, we consider it as a time series. Time series forecasting involves analyzing the dynamics and correlations between historical data for predicting future behavior. Deep neural networks excel in handling these tasks [3] due to their excellent performance in modeling non-linear temporal patterns, identifying complex structures across time series, and constructing a mapping relationship by learning from known data. Here, we design appropriate features and labels for supervised learning. The feature comprises the count matrix, temperature, and humidity. Meanwhile, the label includes the phase modulator's zero-phase voltage that reflects the global phase drift, and is obtained via a two-phase scan (2PS). The detailed data structure is presented in Figure 1(a). Due to the extremely limited counting time and light intensity, the count matrix containing shot noise and systematic errors results in inaccurate voltage labels. Thus, we further introduce a real-time denoising procedure via the filter matrix, which can be physically represented by a wiener filtering algorithm or a feed-forward neural network. Using this procedure, the confidence coefficient of supervised learning is restored, and the clean count matrix during training and predictions can be derived.

Network structure. As shown in Figure 1(b), we implemented the sequence-to-sequence (S2S) model [4], which comprises an encoder and decoder, for mapping history sequences to future ones. The encoder is one long short-term memory (LSTM) network [5] that reads the input feature vector from the observation horizon, and each timestep obtains fixed six-dimensional vector representations. Before the input, an attention layer was placed to assign weights to ten timesteps. The attention weights indicate the importance of each observation for the current input sequence, by which the outlier detection is also provided. Conversely, the decoder is another LSTM network for directly extracting output predictions of a zero-phase voltage.

In our design, each cycle contains one-timestep observation and four-timestep forecasting, corresponding to transmitting strong reference light and weak quantum light, respectively. The interval of one timestep T is determined based on the number of phase slices and our measured max-

* Corresponding author (email: zgg@njupt.edu.cn, xyz@njupt.edu.cn, qinw@njupt.edu.cn)

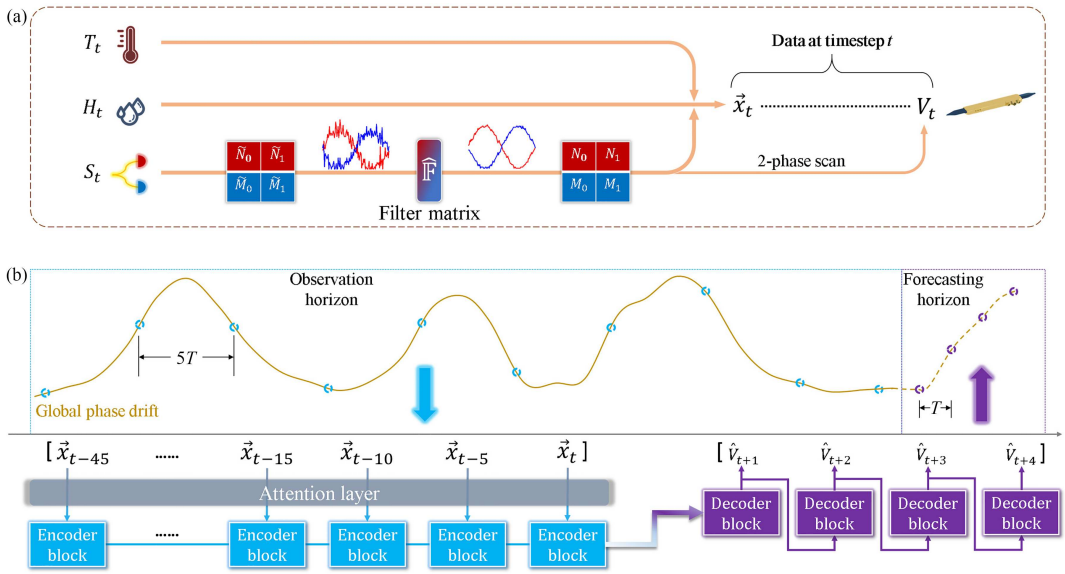

Figure 1 (Color online) Data and network structure for forecasting. (a) T_t: temperature; H_t: humidity; S_t: count matrix; $\vec{x}_t$ and V_t: feature vector and zero-phase voltage at timestep t, respectively; $\tilde{N}$ ($\tilde{M}$): noisy counts of detector D0 (D1); N (M): the clean counts. Subscript 0 (1) denotes the phase difference of 0 ($\pi/2$). The filter matrix filters out the noise and error of the count matrix so that the zero-phase voltage estimated by 2PS has higher confidence. (b) Each sample comprises ten feature vectors in the observation horizon and one voltage vector of the subsequent four timesteps in the forecasting horizon.

imum phase drift velocity at a fiber distance of 500 km (21.12 rad ms^{-1}). The forecasting strategy is illustrated in Figure 1(b). Apparently, there exists a $5T$ time interval between two adjacent observation timesteps and a $1T$ time interval between two contiguous forecasting timesteps. Unlike other time series forecasting tasks [3], any ground-truth features or labels of these timesteps in the forecasting horizon cannot be replenished. This is because the forecasting horizon belongs to the quantum part, which only allows the transmission of weak quantum light and the detection of unexposed quantum bits. To address the mismatch of the time interval between the model's input and output, we propose a simplified time-aware long short-term memory (T-LSTM) unit on the encoder and decoder. This architecture can not only avoid accumulative errors during rolling predictions but also settle the mismatch between the input and output series, achieving a drastic low root-mean-square-error (RMSE) of less than 0.2. The detailed descriptions and evaluations of the model are presented in Appendices A and B, respectively. The model is evaluated on our personal computer, and then deployed to a proper field programmable gate array (FPGA) for high-speed parallel computing during system running. The FPGA working at a clock rate of 200 MHz (Xilinx Zynq UltraScale+ MPSoCs EV series) is sufficient to actively predict fast global phase drifts.

Experiments and results. Appendix C presents the experimental setup. In our experiment, the interference visibility of the S2S model is concentrated around 95.13% with a standard deviation of 0.55% at a fiber distance of 500 km. Accordingly, a transmission efficiency of up to 84.86% can be obtained by using the proposed method. We compared the transmission efficiencies between our present work and previous TF-QKD experiments. Appendix D presents the detailed results.

Conclusion. We proposed a neural network augmented TF-QKD scheme and performed the corresponding experimental demonstration. By incorporating the proposed S2S network with a commercial FPGA, we realize the proof-of-principle demonstration of TF-QKD with excellent performance. Improving the efficiency of TF-QKD can not only boost the key rate but also help reduce Rayleigh scattering noise. These results represent a further step towards the realization of highly efficient TF-QKD and may play a role in practical applications.

Acknowledgements This work was supported by National Key R&D Program of China (Grant Nos. 2018YFA0306400, 2017YFA0304100), National Natural Science Foundation of China (Grant Nos. 12074194, U19A2075, 12104240, 62101285), Industrial Prospect and Key Core Technology Projects of Jiangsu Provincial Key R&D Program (Grant No. BE2022071), Natural Science Foundation of Jiangsu Province (Grant Nos. BK20192001, BK20210582), and Postgraduate Research & Practice Innovation Program of Jiangsu Province (Grant No. KYCX19_0951).

Supporting information Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Lucamarini M, Yuan Z L, Dynes J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature, 2018, 557: 400–403
2 Wang S, Yin Z Q, He D Y, et al. Twin-field quantum key distribution over 830-km fibre. Nat Photon, 2022, 16: 154–161
3 Bandara K, Bergmeir C, Smyl S. Forecasting across time series databases using recurrent neural networks on groups of similar series: a clustering approach. Expert Syst Appl, 2020, 140: 112896
4 Sutskever I, Vinyals O, Le Q V. Sequence to sequence learning with neural networks. In: Proceedings of the 27th International Conference on Neural Information Processing Systems, 2014. 2: 3104–3112
5 Hochreiter S, Schmidhuber J. Long short-term memory. Neural Comput, 1997, 9: 1735–1780