SCIENCE CHINA
Information Sciences

• **Supplementary File** •

High efficient twin-field quantum key distribution with neural network

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]*Broadband Wireless Communication and Sensor Network Technology Key Lab of Ministry of Education, Ministry of Education, Nanjing* 210003*, China;*
[3]*Telecommunication and Networks National Engineering Research Center, NUPT, Nanjing* 210003*, China*

Appendix A Neural network model

Utilizing long short-term memory (LSTM) or gated recurrent unit (GRU) as the recurrent neural network (RNN) block outperforms multi-layer perceptron (MLP) and other models in most of all datasets [1]. There are two popular architectures in constituting an RNN. One is the stacked architecture, in which the same RNN unit repeats for every timestep, sharing the same weights and biases. Multiple LSTM layers are stacking on top of one another. The other is sequence-to-sequence (S2S) architecture, inside of which two different RNNs act on input and output time series in the form of an encoder and decoder [2]. In this task, we face the dual challenges of multi-variable input and multi-step output. The recursive strategy and multi-input multi-output (MIMO) strategy [3] of stacked architecture in multi-step forecasting are unable to avoid accumulative errors in rolling predictions. Therefore, we select S2S architecture as our prediction model after evaluation. Given the output horizon size 4 and considering sequential execution time of field programmable gate array (FPGA), we make the input horizon size slightly bigger than the output one which is 10. The resulting S2S network f_{S2S} can be expressed as:

$$[\hat{V}_{t+1}, \hat{V}_{t+2}, \hat{V}_{t+3}, \hat{V}_{t+4}] = f_{S2S}(x_{t-45}, ..., x_{t-10}, x_{t-5}, x_t), \tag{A1}$$

where $x_t = [S_t, T_t, H_t]^T \in \mathbb{R}^m$, S_t is the count matrix after denoising, T_t is the temperature and H_t is the humidity at timestep t.

To address time interval mismatch of input observations ($5T$) and output predictions (T), we propose a simplified time-aware LSTM (T-LSTM) unit as basis encoder block and decoder block. Connecting with peepholes, the states are updated as follows:

$$i_t = \sigma(W_i \cdot h_{t-1} + U_i \cdot x_t + P_i \cdot C_{t-1} + b_i), \tag{A2}$$
$$o_t = \sigma(W_o \cdot h_{t-1} + U_o \cdot x_t + P_o \cdot C_t + b_o), \tag{A3}$$
$$f_t = \sigma(W_f \cdot h_{t-1} + U_f \cdot x_t + P_f \cdot C_{t-1} + b_f), \tag{A4}$$
$$\tilde{C}_t = tanh(W_c \cdot h_{t-1} + U_c \cdot x_t + b_c), \tag{A5}$$
$$C_t = i_t \odot \tilde{C}_t + f_t \odot [C_{t-1} \cdot g(\Delta t)], \tag{A6}$$
$$h_t = o_t \odot tanh(C_t), \tag{A7}$$

where $W \in \mathbb{R}^{d\times d}$, $U \in \mathbb{R}^{d\times m}$, $P \in \mathbb{R}^{d\times d}$ denotes the weight matrices, $b \in \mathbb{R}^d$ denotes the corresponding bias vector. The subscript i, o, f,c denotes input gate i_t, output gate o_t, forget gate f_t, and cell state $C_t \in \mathbb{R}^d$ of current state respectively. $\tilde{C}_t \in \mathbb{R}^d$ is the candidate cell state at time step t. $h_{t-1}, h_t \in \mathbb{R}^d$ are hidden state of last time step and current step. σ of the gates denotes sigmoid activation function which outputs values in the range $[0, 1]$, and $tanh$ denotes tangent function that outputs in the range $[-1, 1]$. $\odot$ denotes the element-wise multiplication. The time interval is imported into encoder and decoder through $g(\Delta t) = 1/\Delta t \times 10^{-6}$ [4].

Appendix B Evaluations

For evaluation purposes, the datasets are divided into 80% training and 20% test sets. By scrolling through time, the test set consists of the last part of each individual time series within the dataset, and the former part of time series is the training set. This division has been applied equally to all datasets, obtaining 50 time series at every fiber length, and each time series contains $3,100$ time steps. We then transform the time series into training instances to be fed to the model. Table. B1 lists the parameter settings that are used throughout the training. Adam optimiser is used during training on our computer (CPU, Intel Core i7 9700@ 3.6 GHz; GPU, NVIDIA GeForce RTX 2080; RAM, DDR4 8 GBytes). In particular, since time interval is implanted into the T-LSTM cell, data of different fiber lengths can be trained together in principle. Here, we give priority to ensure the accuracy and train the model separately for each lengths.

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

Table B1 Parameter settings during the training.

Hyperparameter	*value (range)*
$cell-dimension$	128
$maximal-epochs$	300
$minibatch-size$	50
$Learning-rates$	$(10^{-4}, 10^{-2})$
$Gaussian-noise$	0.001

We adopt the distortion Loss including shape and Time (DILATE) loss function [5] which is designed for sudden changes and multi-step forecasting. The loss is defined as:

$$\mathcal{L}_{DI}(\hat{\mathrm{V}}, V^*) = \frac{1}{2}\mathcal{L}_s(\hat{V}, V^*) + \frac{1}{2}\mathcal{L}_t(\hat{V}, V^*), \tag{B1}$$

where V^* denotes the ground truth target and $\hat{V}$ denotes the predicted counterpart. $\mathcal{L}_s(\hat{V}, V^*)$ is shape loss function which describes the dissimilarity of vector shape and $\mathcal{L}_t(\hat{V}, V^*)$ is the temporal term which penalizes temporal distortions between $\hat{V}$ and V^*. The shape loss is based on dynamic time warping (DTW) [6] and can be calculated by:

$$\mathcal{L}_s(\hat{V}, V^*) = -\gamma log(\sum_{A\in\mathcal{A}_{4,4}} exp(-\frac{\langle A, \Delta(\hat{V}, V^*)\rangle}{\gamma})), \tag{B2}$$

where $\gamma > 0$, $A \subset \{0,1\}^4, 4$ is the warping path and $\mathcal{A}_{4,4}$ is the set of all valid warping paths, $\Delta(\hat{V}, V^*) := [\delta(\hat{V}, V^*)]_{i,j}$ denotes the distance matrix defined as euclidean distance. And the temporal loss is the smooth approximation of time distortion index (TDI) [7],

$$\mathcal{L}_t(\hat{V}, V^*) = \frac{1}{\sum_{A\in\mathcal{A}_{4,4}} exp(-\frac{\langle A, \delta(\hat{V}, V^*)\rangle}{\gamma})} \sum_{A\in\mathcal{A}_{4,4}} \langle A, \Omega\rangle exp(-\frac{\langle A, \delta(\hat{V}, V^*)\rangle}{\gamma}), \tag{B3}$$

where $\Omega = (i,j)^2/k^2$ is the squared penalization for any $i \neq j$. After batch training, the corresponding DILATE loss is 2.65 ± 1.03.

Appendix C Setup

The setup is a large symmetric Mach-Zehnder interferometer (MZI) with one 50 MHz discrete laser pulses at the center wavelength of 1550.51 nm. To be noted, the laser sources of Alice and Bob should be independent from each other in a practical TF-QKD setup. However, considering the obstacle arising from the frequency difference of the laser sources has been successfully removed by either the optical phase-locked loop method [8–10], or the frequency locking approach with ultra-stable cavity [11, 12], here we focus our attention on dealing with the phase drift arising from transmission channels. Therefore, what we carried out is a proof-of-principle demonstration of TF-QKD. At the detection side, the light pulses from Alice's and Bob's sides are meet at a 50/50 BS and are further detected by two superconducting nanowire single-photon detectors (SNSPDs), each corresponding to the constructive or destructive result of single-photon interference. Before the BS, a PM is immediately positioned for real-time phase drift compensations, which is controlled by the FPGA.

Appendix D Experimental results

In the TF-QKD, it is necessary to keep the phase drift lying within the same phase slice in a coding cycle [13]. By referring [8,12,14], we reasonably set it less than 0.3 rad (17 °) per maintenance period T. Based on the measured maximum phase drift velocity, we can determine the unit maintenance period T. Each cycle of traditional two-phase scan (2PS) method [15] contains a classical part and a quantum part, and the former is mainly composed of transmitting reference light and the recovery time of SNSPD, consuming times are 10 μs and 600 ns respectively in our experiment, which can not be used for quantum key transmission. Differently, each cycle of S2S contains 1-timestep observation and 4-timestep forecasting, corresponding to transmitting strong reference light and the weak quantum light respectively. In Table. D1, we show the maintenance period T and transmission efficiency η at different fiber distance based on our measurements. The efficiency of 2PS is measured as $\eta_{2PS} = (T - 10 - 0.6)/T$, while the efficiency of S2S is measured as $\eta_{S2S} = (5T - 10 - 0.6)/(5T)$.

We do comparisons on the transmission efficiencies between our present work and previous TF-QKD experiments, see Fig. D1. Moreover, considering direct comparisons are not a complete account of superiority, we also plot the efficiency of 2PS (crosses) without any redundancy. In every sense, the prediction method based on our S2S model (stars) greatly boosts the transmission efficiency at various distances.

To illustrate the practical performance of our prediction method, we further characterize the interference visibility at 500 km fiber distance in Fig. D2. The visibility distribution of 2PS with filter matrix is concentrated around 95.27% with a standard deviation of 0.56%, and the visibility distribution of S2S model is concentrated around 95.13% with a standard deviation of 0.55%. Similar visibility results show that the S2S model can suppress prediction errors well and facilitate stable interference control. We highlight that the visibility statistics of S2S model are not all lower than those of 2PS. It can provide a 0.1% higher mean value of visibility at 0 km fiber length. Additionally, the long term stability of S2S method over 3 hours is demonstrated. We test the interference visibility of 2PS without filter matrix, and it can only provide less than 95% visibility at all fiber lengths.

Table D1 Transmission efficiency of traditional 2-phase scan with filter matrix η_{2PS} and the S2S prediction model η_{S2S} under different fiber length. Along with its maintenance periods of voltage (T).

Distance	T	η_{2ps}	η_{S2S}
$0km$	$200\mu s$	94.7%	98.9%
$100km$	$80\mu s$	86.75%	97.35%
$200km$	$50\mu s$	78.8%	95.8%
$300km$	$40\mu s$	73.5%	94.7%
$400km$	$20\mu s$	47.0%	89.4%
$500km$	$14\mu s$	24.29%	84.86%

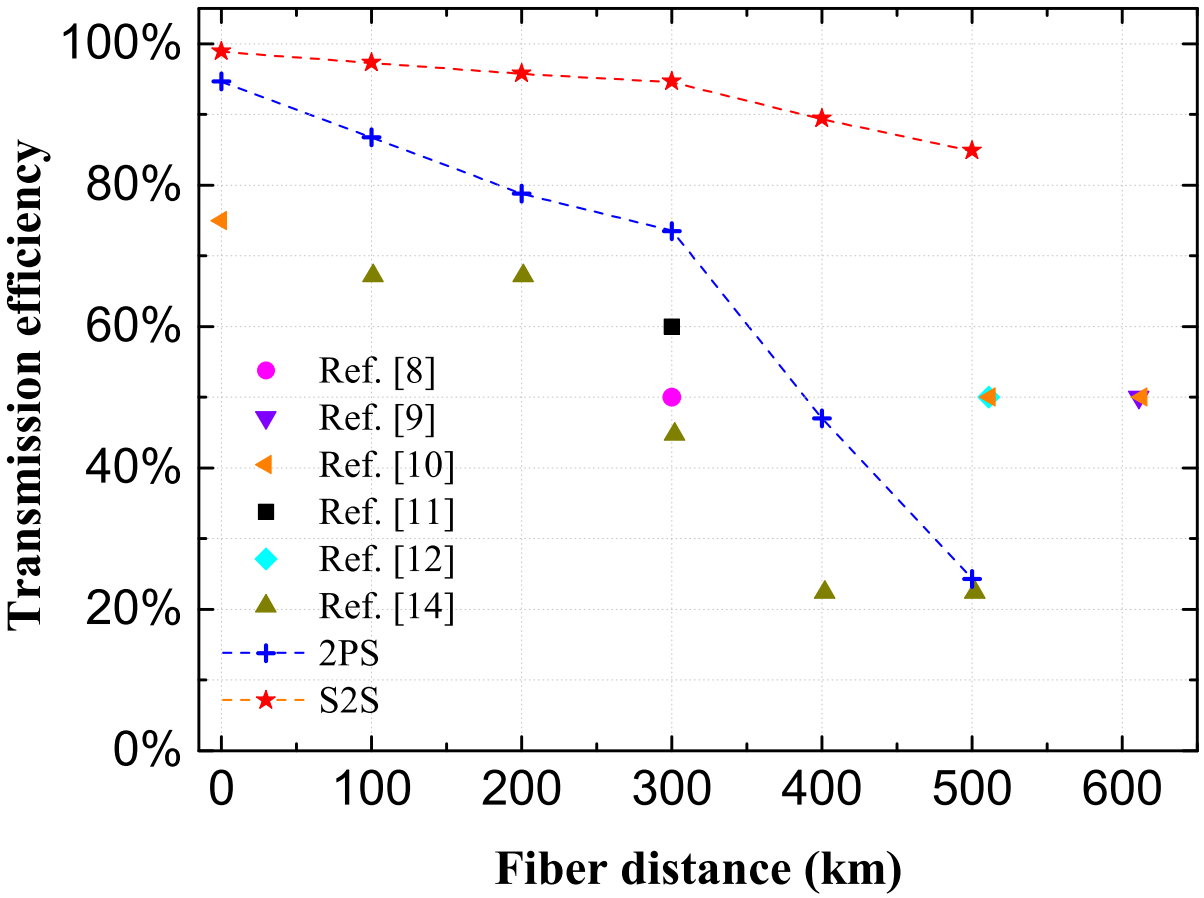

Figure D1 Characteristics of phase drift at 500 km fiber distance. (a) Free phase drift without feedback loop. (b) Compensating by 2PS with filter matrix. (c) Predicting by the S2S model.

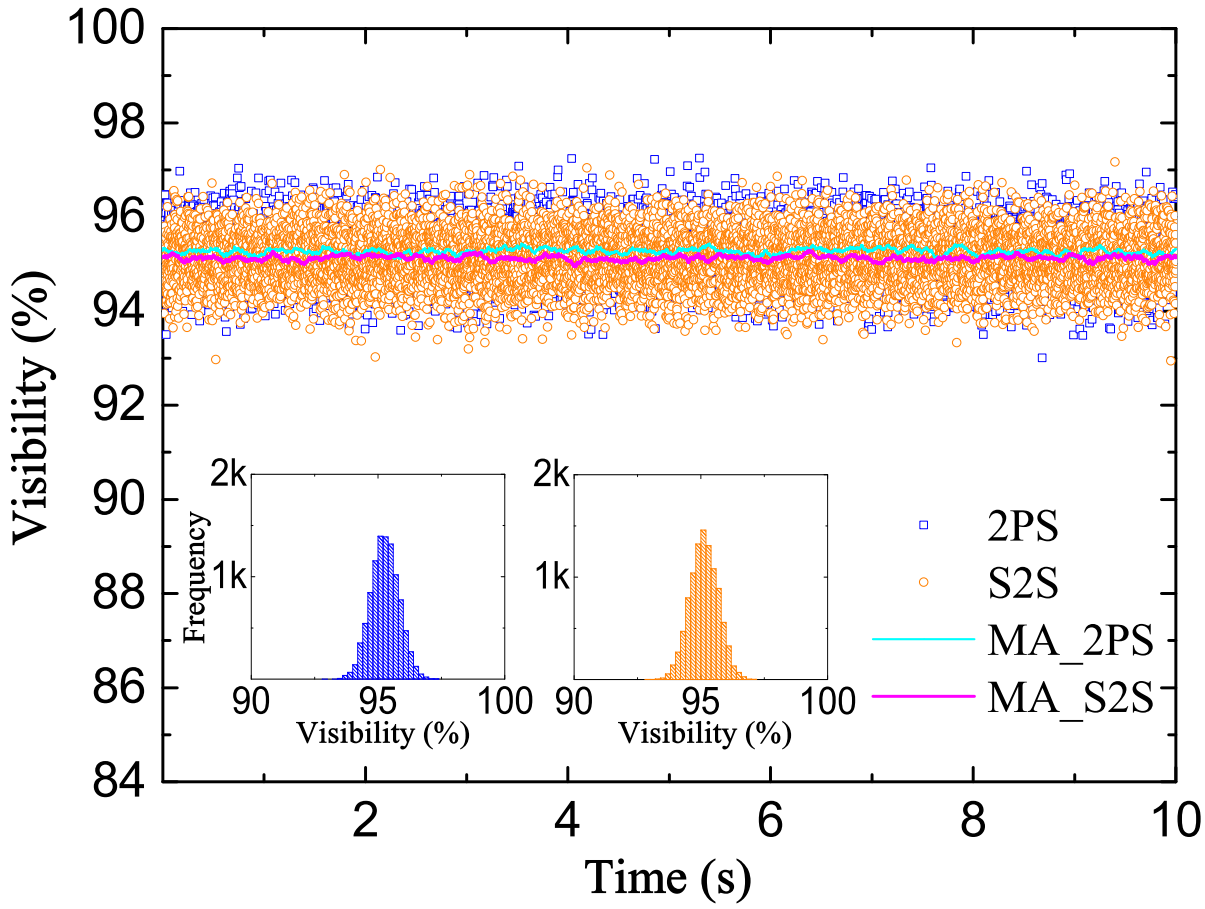

Figure D2 Interference visibility at a 500 km fiber length. MA_2PS: moving averages of 2PS; MA_S2S: moving averages of S2S. Each point is calculated with 1 ms cumulative counts.

References

1 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
2 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, Canada, 2014, 2: 3104-3112
3 Ben S T, Bontempi G, Atiya A, et al. A review and comparison of strategies for multi-step ahead time series forecasting based on the NN5 forecasting competition. Expert Syst Appl, 2012, 39: 7067-7083
4 Baytas I M, Xiao C, Zhang X, et al. Paient subtyping via time-aware lstm networks. In: Proceedings of the 23rd ACM/SIGKDD International Conference on Knowledge Discovery and Data Mining, Canada, 2017, 65-74
5 Guen V L, Thome N. Shape and time distortion loss for training deep time series forecasting models. In: 33rd conference on advances in neural information processing systemss (NeurIPS 2019), Canada, 2019, 4191-4203
6 Sakoe H, Chiba S. Dynamic programming algorithm optimization for spoken word recognition. IEEE Trans. Acoust., Speech, Signal Processing, 1978, 26: 43-49
7 Frias-Paredes L, Gaston-Romeo M, Leon T. Assessing energy forecasting inaccuracy by simultaneously considering temporal and absolute errors. Energ Convers Manage, 2017, 142: 533-546
8 Wang S, He D Y, Yin Z Q, et al. Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. Phys Rev X, 2019, 9: 021046
9 Pittaluga M, Minder M, Lucamarini M, et al. 600-km repeater-like quantum communications with dual-band stabilization. Nat Photon, 2021, 15: 530-535
10 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
11 Liu Y, Yu Z W, Zhang W J, et al. Experimental twin-field quantum key distribution through sending or not sending. Phys Rev Lett, 2019, 123: 100505
12 Chen J P, Zhang C, Liu Y, et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. Nat Photon, 2021, 15: 570-575
13 Lucamarini M, Yuan Z L, Dynes J F, et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature (London), 2018, 557: 400
14 Fang X T, Zeng P, Liu H, et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. Nat Photon, 2020, 14: 422-425
15 Liu H, Jiang C, Zhu H T, et al. Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km. Phys Rev Lett, 2021, 126: 250502