

Parameter estimation of continuous variable quantum key distribution system via artificial neural networks

Hao Luo(罗浩), Yi-Jun Wang(王一军), Wei Ye(叶炜), Hai Zhong(钟海), Yi-Yu Mao(毛宜钰), and Ying Guo(郭迎)
Citation: Chin. Phys. B, 2022, 31 (**2**): 020306. DOI: 10.1088/1674-1056/ac2807
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Three-party reference frame independent quantum key distribution protocol

Comfort Sekga and Mhlambululi Mafu
Chin. Phys. B, 2021, 30 (**12**): 120301. DOI: 10.1088/1674-1056/abff1f

Reference-frame-independent quantum key distribution of wavelength division multiplexing with multiple quantum channels

Zhongqi Sun(孙钟齐), Yanxin Han(韩雁鑫), Tianqi Dou(窦天琦), Jipeng Wang(王吉鹏), Zhenhua Li(李振华), Fen Zhou(周芬), Yuqing Huang(黄雨晴), and Haiqiang Ma(马海强)
Chin. Phys. B, 2021, 30 (**11**): 110303. DOI: 10.1088/1674-1056/abf350

Realization of simultaneous balanced multi-outputs for multi-protocols QKD decoding based onsilica-based planar lightwave circuit

Jin You(游金), Yue Wang(王玥), and Jun-Ming An(安俊明)
Chin. Phys. B, 2021, 30 (**8**): 080302. DOI: 10.1088/1674-1056/abe2ff

Practical decoy-state BB84 quantum key distribution with quantum memory

Xian-Ke Li(李咸柯), Xiao-Qian Song(宋小谦), Qi-Wei Guo(郭其伟), Xing-Yu Zhou(周星宇), and Qin Wang(王琴)
Chin. Phys. B, 2021, 30 (**6**): 060305. DOI: 10.1088/1674-1056/abda31

Continuous-variable quantum key distribution based on photon addition operation

Xiao-Ting Chen(陈小婷), Lu-Ping Zhang(张露萍), Shou-Kang Chang(常守康), Huan Zhang(张欢), and Li-Yun Hu(胡利云)
Chin. Phys. B, 2021, 30 (**6**): 060304. DOI: 10.1088/1674-1056/abd931

Parameter estimation of continuous variable quantum key distribution system via artificial neural networks

Hao Luo(罗浩)[1,3], Yi-Jun Wang(王一军)[1], Wei Ye(叶炜)[2], Hai Zhong(钟海)[2,†], Yi-Yu Mao(毛宜钰)[1], and Ying Guo(郭迎)[1,‡]

[1] *School of Automation, Central South University, Changsha* 410083, *China*
[2] *School of Computer Science and Engineering, Central South University, Changsha* 410083, *China*
[3] *College of Applied Science, Jiangxi University of Science and Technology, Ganzhou* 341000, *China*

(Received 26 July 2021; revised manuscript received 11 September 2021; accepted manuscript online 18 September 2021)

Continuous-variable quantum key distribution (CVQKD) allows legitimate parties to extract and exchange secret keys. However, the tradeoff between the secret key rate and the accuracy of parameter estimation still around the present CVQKD system. In this paper, we suggest an approach for parameter estimation of the CVQKD system via artificial neural networks (ANN), which can be merged in post-processing with less additional devices. The ANN-based training scheme, enables key prediction without exposing any raw key. Experimental results show that the error between the predicted values and the true ones is in a reasonable range. The CVQKD system can be improved in terms of the secret key rate and the parameter estimation, which involves less additional devices than the traditional CVQKD system.

Keywords: quantum key distribution, artificial neural networks, secret key rate, parameter estimation

PACS: 03.67.–a, 87.85.dq **DOI:** 10.1088/1674-1056/ac2807

1. Introduction

Quantum key distribution (QKD)[1] enables two legitimate parts, Alice and Bob, to exchange secret keys through an insecure channel controlled by a potential eavesdropper, Eve. This technology can be combined with the classical one-time-pad cryptographic system, thereby providing information transmission with unconditional security.[2] There are two branches for QKD, *i.e.*, continuous-variable (CV) QKD and discrete-variable (DV) QKD. Unlike the latter using the single-photon resources(or detectors),[1] the former has the potential of high-key rate and low-cost implementations as it can be compatible with current standard telecom components such as homodyne and heterodyne detectors.[3] Over the past few years, achievements have been made for CVQKD in both theories and experiments.[4–13] The most mature CVQKD protocol is the prestigious Gaussian-modulated coherent state (GMCS) protocol,[4] which has been proved secure against collective attacks and coherent attacks.[14–17] In the GMCS protocol, Alice first encodes the secret key information by modulating the quadratures x and p of coherent states with independent Gaussian distributions[18] and then sends them to Bob through an insecure quantum channel. After that, Bob proceeds homodyne detection (measures one of the two quadratures randomly) or heterodyne detection (measures both the two quadratures).[6,19–21] After the post-processing process that involves sifting, parameter estimation, reconciliation and privacy amplification, Alice and Bob share the correlated raw keys.

In order to estimate a bound on the maximum information that may have been eavesdropped by Eve, the channel transmittance T and excess noise ξ need to be estimated. Traditional channel parameter estimation needs disclose parts of the raw keys. The more raw keys disclosed, the more accuracy the channel estimation would be. However, more disclosed raw keys leads to less capacity for carrying information, resulting in a lower secret key rate. Recent years, several works have been done on channel parameter estimation. For example, a parameter estimation was suggested for performance improvement of the CVQKD system,[22] which can be applied to low-Earth orbits and underwater communication scenarios by using the Monte Carlo approach. Chai *et al.* proposed a parameter estimation method for implementation of the atmospheric GMCS CVQKD.[23] Guo[24] suggested a method for phase estimation and compensation of the CVQKD system, which can reconstruct the phase drifts even at low signal-to-noise ratio conditions. Wang *et al.* improved the accuracy of parameter estimation, realized by exchanging the order of parameter estimation and information reconciliation.[25] Yang suggested an improved four-state protocol in which the covariance matrix can be estimated from experimental data without using the linear channel assumption, guaranteeing its unconditional security in the asymptotical limits.[26] Li *et al.* considered an impact of denial-of-service attack on channel parameter estimation and suggested a method to prevent this attack.[27] How-

†Corresponding author. E-mail: zhonghai@csu.edu.cn
‡Corresponding author. E-mail: yingguo@csu.edu.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

ever, the tradeoff between the secret key rate and the accuracy of parameter estimation is still unsolved.

In this paper, we propose an ANN-based parameter estimation scheme for performance improvement of the CVQKD system. In post-processing, Alice and Bob have to do some pretreatment to the raw keys (data dividing and normalizing), which are sequentially sent to the ANN for the training, aiming to learn the relationship between the initially prepared and received data. The ANN has the capacity of predicting all the data that Alice holds with few errors. Using this method, Alice and Bob can proceed estimation without disclosing any raw key to Eve. It can be used for the parameter estimation and attack prediction without heavily loading any additional devices, which is feasible to implement for the traditional CVQKD system.

This paper is organized as follows. In Section 2, we illustrate the framework of ANN-based parameter estimation scheme, and establish the ANN model for the CVQKD system. In Section 3, we show the performance of the ANN-involved CVQKD system in terms of the secret key rate. In Section 4, the experimental results demonstrate the effect of the ANN-based parameter estimation scheme on the CVQKD system, including the secret key rate, the error range between the predicted values and the true values, as well as the relationship between the prediction accuracy and the block length. Finally, we make conclusions in Section 5.

2. ANN-based parameter estimation of CVQKD

For a traditional GMCS CVQKD protocol, it can be described as follows. Alice prepares the signal carriers with Gaussian modulation, which are sent to Bob through an unreliable quantum channel monitored by Eve. For the received signals, Bob proceeds the measurements by using homodyne or heterodyne detectors. Subsequently, Alice and Bob perform the data post-processing through an authenticated classical channel. As for the post-processing, Alice and Bob compare their encoding and measurement quadratures with each other and keep the data that they have performed with the same quadratures. By disclosing a subset of the raw keys, the parameter estimation is then proceeded to obtain an upper bound of the information that Eve can steal from. In the end, Alice and Bob could decorrelate their joint data from Eve via reconciliation and privacy amplification, while their data remain correlated.[28] The secret key rate K can be given by

$$K = I_{\mathrm{C}} - I_{\mathrm{E}} - M, \tag{1}$$

where I_{C} is the mutual information between Alice and Bob, I_{E} the upper bound of information that Eve can obtain, and M the amount of the information revealed during the post-processing.

It is known that the post-processing has became a main restraint on the performance of CVQKD systems. Recently, the hardest issues have been devoted to parameter estimation,[23,25,29] reconciliation,[30–32] and privacy amplification,[33,34] but the tradeoff between the secret key rate and the accuracy of parameter estimation is still faced with challenges.

Fortunately, the ANN, known as the MP model,[35] is now a popular machine learning technique[36,37] based on the principle of neural networks in biology and network topology, aiming to process complex information by simulating nervous system of human brain.[38] It is an operational model composing a large number of nodes (neurons). In Fig. 1(a), it shows the structure of a multiple-input neuron. The j-th output o_j reads

$$o_j = \varphi(net_j) = \varphi\left(\sum_{i=1}^{n} x_i w_{ij} + b\right), \tag{2}$$

where x_i is the i-th input, w_{ij} is the weight of x_i on the j-th path, b is bias that measures the difficulty of activation, and $\varphi(\cdot)$ represents the activation function. Figure 1(b) shows the structure of back propagation (BP) neural networks, which is employed in this paper. BP neural network is a multi-layer feed-forward neural networks, composed of input layer, hidden layer and output layer, the amount of the hidden layer can be one or more.

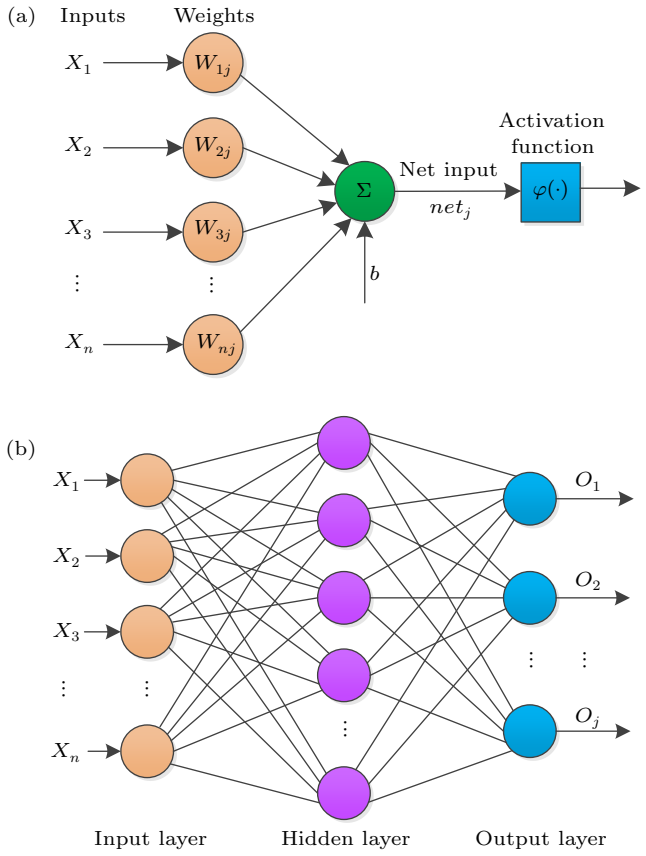


Fig. 1. (a) Structure of a multiple-input neuron. (b) Structure of the BP neural networks.

The ANN-based CVQKD is shown in Fig. 2. A set of coherent states, with desired modulation variance V_A, are prepared and multiplexed with the strong local oscillator (LO) by a polarization beam splitter. In the LO path, the delay line is employed to separate the LO from the signal in the time domain so that the time multiplexing can be realized. At the receiver, demultiplexing is executed by using polarization controller and polarization beam splitter. Through another delay line placed in the signal path, the delay of the LO due to the time multiplexing design is compensated so that both the signal and the LO can be precisely aligned. After Bob's homodyne detection, Alice and Bob have two correlated sequences x_i and y_i, respectively. Taking into account the additive white Gaussian noise (AWGN) channel,[39] x_i and y_i can be related by

$$y_i = t x_i + z_i, \quad \forall i \in \{1,2,\ldots,N\}, \tag{3}$$

where N is the total number of the raw keys, z_i represents Gaussian noise, $x_i \sim \mathcal{N}(0, V_A)$, $t = \sqrt{\eta T}$ is the quantum channel loss with transmittance $T \in [0,1]$, $z_i \sim \mathcal{N}(0, \sigma^2)$, and $y_i \sim \mathcal{N}(0, t^2 V_A + \sigma^2)$. Here η represents the efficiency of the detector, $\sigma^2 = N_0 + \eta T \xi + V_{el}$, N_0 is the variance of the shot noise, and V_{el} denotes the detector's electronic noise.

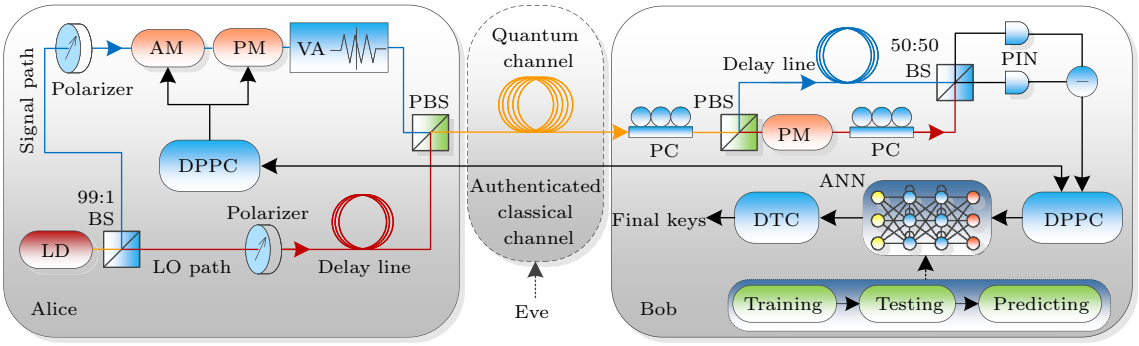


Fig. 2. Schematic diagram of the ANN-based CVQKD system. LD: Laser diode. BS: Beam splitter; LO: Local oscillator; AM: Amplitude modulator; PM: Phase modulator; VA: Variable attenuator; PBS: Polarization beam splitter; PC: Polarization controller; PIN: PIN photodiode; DPPC: Data pre-processing center; Alice and Bob do pretreatment (including data dividing and data normalizing) to their own original data through their respective DPPC, then the data are transmitted through an authenticated channel. ANN: Artificial neural networks; DTC: Data terminal center, including reconciliation and privacy amplification.

For the parameter estimations, we take into account the transmittance T, the excess noise ξ, and the maximum information I_E. Traditionally, we needs to disclose part of the raw keys, typically 50%, whereas in the proposed method none of the raw keys will be wasted. The ANN-based post-processing can be described as follows, it is worth noting that the data exchanged between Alice and Bob is achieved through the authentication channel, that is, the data may be eavesdropped, but cannot be tampered with.

(i) Alice and Bob divide their correlated raw keys (X,Y) into d-dimensional strings x_j^d and y_j^d, $\forall j \in \{1,2,\ldots,m\}$ with $m = N/d$.

(ii) Alice and Bob normalize their d-dimensional vectors respectively, obtaining $x_j'^d = x_j^d / \|x_j\|$ and $y_j'^d = y_j^d / \|y_j\|$, where $\|x_j\| = \sqrt{(x_j, x_j)}$, $\|y_j\| = \sqrt{(y_j, y_j)}$.

(iii) Alice sends the first $m/2$ vectors $x_1'^d, x_2'^d, \ldots, x_{(m/2)}'^d$ to Bob.

(iv) Bob uses the ANN to learn the relationship between $x_1'^d$ and $y_1'^d$, $x_2'^d$ and $y_2'^d, \ldots, x_{(m/2)}'^d$ and $y_{(m/2)}'^d$, as $M(y_j'^d) = x_j'^d$.

(v) Bob uses the ANN to predict remaining vectors $x_{(m/2)+1}'^d = M(y_{(m/2)+1}'^d), x_{(m/2)+2}'^d = M(y_{(m/2)+2}'^d), \ldots, x_m'^d = M(y_m'^d)$. After that, Bob has all the $x_j'^d$, $j = 1,2,\ldots,m$.

(vi) Alice sends the values of $\|x_{(m/2)+1}\|, \|x_{(m/2)+2}\|, \ldots, \|x_m\|$ to Bob.

(vii) Bob uses the ANN again to learn the relationship between $\|x_{(m/2)+1}\|$ and $\|y_{(m/2)+1}\|, \|x_{(m/2)+2}\|$ and $\|y_{(m/2)+2}\|, \ldots, \|x_m\|$ and $\|y_m\|$, as $Q(\|y_j\|) = \|x_j\|$.

(viii) Bob uses the ANN to predict $\|x_1\|, \|x_2\|, \ldots, \|x_{(m/2)}\|$ and gets all the $\|x_j\|$, $j = 1,2,\ldots,m$.

(ix) Bob calculates the vectors $x_j^d = x_j'^d \cdot \|x_j\|$, $j = 1,2,\ldots,m$. Then he combines x_j^d into $X = (x_1, x_2, \ldots, x_N)$.

Theoretically, through the above-mentioned steps, Bob could have exactly all the same X as Alice has. Then, along with his own raw keys Y, he can proceed the parameter estimation without sacrificing any raw keys to the potential adversary, Eve. Consequently, Alice and Bob can achieve not only the high accuracy of parameter estimation but also the high secret key rate. But note that since the ANN algorithm is nothing more than an approximation of arbitrary function by learning the observed data and making prediction, it is impossible to obtain the completely correct results. Simply put, there are errors in the predicted data, which will lead to the deviation of parameter estimation, and eventually lead to the lower key rate than the ideal case. However, it is possible to achieve as high accuracy as possible by optimizing the structure of the ANN-involved CVQKD system and adjusting the suitable parameters.

3. Security analysis

After elaborating the schematic diagram of the ANN-based CVQKD system, we shall pay attention to the derivation of secret key rate. In the asymptotical case,[8] the key rate can be given by

$$K_\infty(T,V_\xi) = \beta I(x:y) - S_{\varepsilon_{\rm PE}}(y:E), \tag{4}$$

where V_ξ represents the variance of excess noise, $\beta \in [0,1]$ refers to the efficiency of the reconciliation, $I(x:y)$ is the mutual information of Alice and Bob, $S_{\varepsilon_{\rm PE}}(y:E)$ is the upper bound of information that Eve can obtain from Bob's information, $\varepsilon_{\rm PE}$ is the probability that the true values of the parameters are not inside the confidence region. In order to ensure the security of the CVQKD system as much as possible without underestimating the eavesdropping, the worst case, that is, the case with the minimum key rate, needs to be considered. For this case, the minimum value $T_{\rm min}$ for T and the maximum value $V_{\xi_{\rm max}}$ should be used. Then we can get the key rate in the finite-size case[39]

$$K = \frac{n}{N}[K_\infty(T_{\rm min}, V_{\xi_{\rm max}}) - \Delta(n)], \tag{5}$$

where n is the amount of the raw keys used for key extraction, while $m = N - n$ raw keys can be used for estimation, and $\Delta(n)$ is related to the security of the privacy amplification (PA). The parameter $\Delta(n)$ has the form

$$\Delta(n) \equiv (2\dim\mathcal{H}_x + 3)\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}} + \frac{2}{n}\log_2(1/\varepsilon_{\rm PA}), \tag{6}$$

where $\mathcal{H}_x$ is the Hilbert space of variable x, $\bar{\varepsilon}$, and $\varepsilon_{\rm PA}$ are components of the failure probability of the whole CVQKD protocol. We assume $\dim\mathcal{H}_x = 2$, and a conservative value 10^{-10} for $\bar{\varepsilon}$. Thus, $\Delta(n)$ can be approximated as

$$\Delta(n) \approx 7\sqrt{\frac{\log_2(2/10^{-10})}{n}}. \tag{7}$$

Note although theoretically there is no raw key disclosed for parameter estimation in this scheme, it does not mean that $n = N$ (details will be shown in Section 4). In homodyne detection, $I(x:y)$ can be derived from[40]

$$I_{\rm hom}(x:y) = \frac{1}{2}\log_2\frac{V_{\rm B}}{V_{\rm B|A}} = \frac{1}{2}\log_2\frac{V_{\rm A}+1+\chi_{\rm tot}}{1+\chi_{\rm tot}}, \tag{8}$$

where $V_{\rm B}$ is Bob's measured variance, $V_{\rm B|A}$ is the conditional variance, $\chi_{\rm tot} = \chi_{\rm line} + \chi_{\rm hom}/T_{\rm min}$ is the total noise, $\chi_{\rm line} = 1/T_{\rm min} - 1 + \xi$ is the channel-added noise, and $\chi_{\rm hom} = [(1-\eta) + V_{\rm el}]/\eta$ is detection-added noise. We note that $T_{\rm min} = t_{\rm min}^2/\eta$ and $V_{\xi_{\rm max}} = (\sigma^2_{\rm max} - 1 - V_{\rm el})/t^2_{\rm min}$.

To acquire $t_{\rm min}$ and $\sigma^2_{\rm max}$, the maximum-likelihood estimators $\hat{t}$ and $\hat{\sigma}^2$ can be used for the transmission model of Eq. (3)

$$\hat{t} = \frac{\sum_{i=1}^N x_i y_i}{\sum_{i=1}^N x_i^2}, \quad \hat{\sigma}^2 = \frac{1}{N}\sum_{i=1}^N (y_i - \hat{t}x_i)^2, \tag{9}$$

where $\hat{t}$ and $\hat{\sigma}^2$ are given by

$$\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma^2}{\sum_{i=1}^N x_i^2}\right), \quad \frac{N\hat{\sigma}^2}{\sigma^2} \sim \chi^2(N-1), \tag{10}$$

t and σ^2 are true values of parameters, respectively. We can figure out $t_{\rm min}$ and $\sigma^2_{\rm max}$ approximately by[41]

$$\begin{aligned} t_{\rm min} &\approx \hat{t} - z_{\varepsilon_{\rm PE}/2}\sqrt{\frac{\hat{\sigma}^2}{NV_{\rm A}}}, \\ \sigma^2_{\rm max} &\approx \hat{\sigma}^2 + z_{\varepsilon_{\rm PE}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{N}}, \end{aligned} \tag{11}$$

with $1 - {\rm erf}(z_{\varepsilon_{\rm PE}/2}/\sqrt{2})/2 = \varepsilon_{\rm PE}/2$. Here ${\rm erf}(x)$ is the error function. In addition, we take the expected values for $\hat{t}$ and $\hat{\sigma}^2$,[39]

$$E[\hat{t}] = \sqrt{\eta T}, \quad E[\hat{\sigma}^2] = N_0 + \eta T\xi + V_{\rm el}. \tag{12}$$

For the Holevo bound,[8] it can be simplified as

$$S_{\varepsilon_{\rm PE}}(y:E) = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{13}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, λ_i is symplectic eigenvalue of the corresponding covariance matrix given by (in homodyne detection case)

$$\begin{aligned} \lambda^2_{1,2} &= \frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right), \\ \lambda^2_{3,4} &= \frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right), \\ \lambda_5 &= 1, \end{aligned} \tag{14}$$

where we have

$$\begin{aligned} A &= V^2(1 - 2T_{\rm min}) + 2T_{\rm min} + T^2_{\rm min}(V + \chi_{\rm line})^2, \\ B &= T^2_{\rm min}(V\chi_{\rm line} + 1)^2, \\ C &= \frac{A\chi_{\rm hom} + V\sqrt{B} + T_{\rm min}(V + \chi_{\rm line})}{T_{\rm min}(V + \chi_{\rm tot})}, \\ D &= \sqrt{B}\frac{V + \sqrt{B}\chi_{\rm hom}}{T_{\rm min}(V + \chi_{\rm tot})}, \\ V &= V_A + 1. \end{aligned} \tag{15}$$

Using Eq. (9), the estimators $\hat{t}$ and $\hat{\sigma}^2$ can be derived. After substituting them into Eq. (11), we obtain $t_{\rm min}$ and $\sigma^2_{\rm max}$. Combining Eq. (8) with Eq. (13), we get $I_{\rm hom}(x:y)$ and $S_{\varepsilon_{\rm PE}}(y:E)$, and hence derive the secret key rate K from Eq. (5).

4. Numerical simulation

In the ANN-based scenario, the value of n/N should be one in theory as no raw key is sacrificed. But it is impossible for the actual neural networks to make the predicted value exactly the same as the real one, meaning that n is always less than N. Therefore, it is still valid in Eq. (4) for this scheme except that n represents the amount of Alice's raw keys that

predicted correctly by Bob. We take into account

$$S = \frac{n}{N}, \tag{16}$$

which is the prediction accuracy. Then we have

$$K = S[\beta I(x:y) - S_{\varepsilon_{\rm PE}}(y:E) - \Delta(n)]. \tag{17}$$

The value of n/N is usually assumed to be 0.5 in our experiment, as in the traditional scheme. However, the value of S depends on the performance of the ANN.

We set the parameters of the ANN in Table 1, that is a BP neural networks which has a hidden layer with 12 neurons. In hidden layer, we take the activation function

$$\text{tansig}(x) = \frac{2}{1+\text{e}^{-2x}} - 1, \quad \forall x \in R, \tag{18}$$

and the output layer activation function

$$\text{purelin}(x) = x, \quad \forall x \in R. \tag{19}$$

As for the training function, we take the Levenberg–Marquardt algorithm, which is used for solving the non-linear least squares problems. These can minimize the problems arise in training process of the ANN.

Table 1. Parameter settings.

Parameter	Value	Parameter	Value
Maximum number of epochs to train	500	Maximum time to train in seconds	inf
Learning rate	0.01	Minimum performance gradient	10^{-12}
Epochs between showing progress	50	Maximum validation failures	10
Performance goal	10^{-5}	Momentum constant	0.9

At the beginning, all the variables and vectors are calculated and fed into the ANN, which randomly divides the data into three parts, *i.e.*, training data, verification data, and test data, accounting for 70%, 15%, and 15%, respectively. After that, the networks begins to learn. The learning process will be repeated until the lowest level of error is achieved.

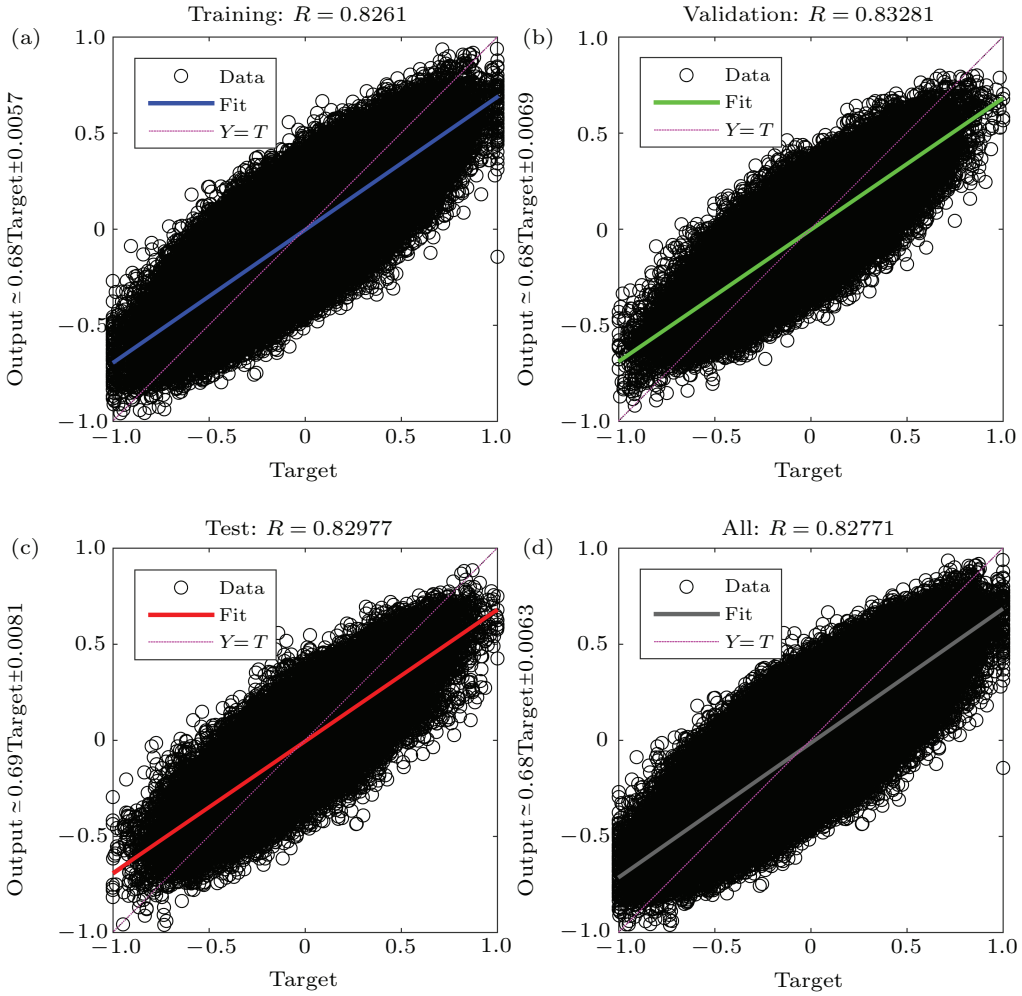


Fig. 3. Regression diagram of the first learning for $M(y_j'^d) = x_j'^d$ ($L = 20$ km, $d = 80$, $N = 1.2 \times 10^6$).

Figure 3 shows the regression graph of the first learning (for the relationship $M(y_j'^d) = x_j'^d$), while figure 4 represents the second learning (for the relationship $Q(\|y_j\|) = \|x_j\|$). In these two graphs, the horizontal axis and the vertical axis represent the target value and the output value, respectively. Ideally, the output value should be equal to the target value, which is represented by a dotted line in the diagram. The black circles represent the data points, and the solid lines represent the

fitting curves based on them. Theoretically, the closer the fitting curve is to the dotted line, the better the training effect of the ANN will be. After adequate training, the fitting curve of a perfect ANN should coincide with the "$Y = T$" curve, reflecting the most accurate description of the data relationship. But in reality, on the one hand, under the existing technology, such ideal ANN can not be constructed. On the other hand, if the fitting degree is too high ($R = 1$), the overfitting occurs, that is, the training effect is perfect but the prediction effect is greatly deviated. During the two stages of training in our experiment, the fitting curve is close to the dotted line. The value of R is greater than 0.8, meaning that the output and the target fit well. Besides, the values of minimum mean squared error (MSE) in two sequential training processes are relatively small, 0.026163 and 0.023441, respectively. Both the regression diagram and the MSE reveal that the ANN is well trained.

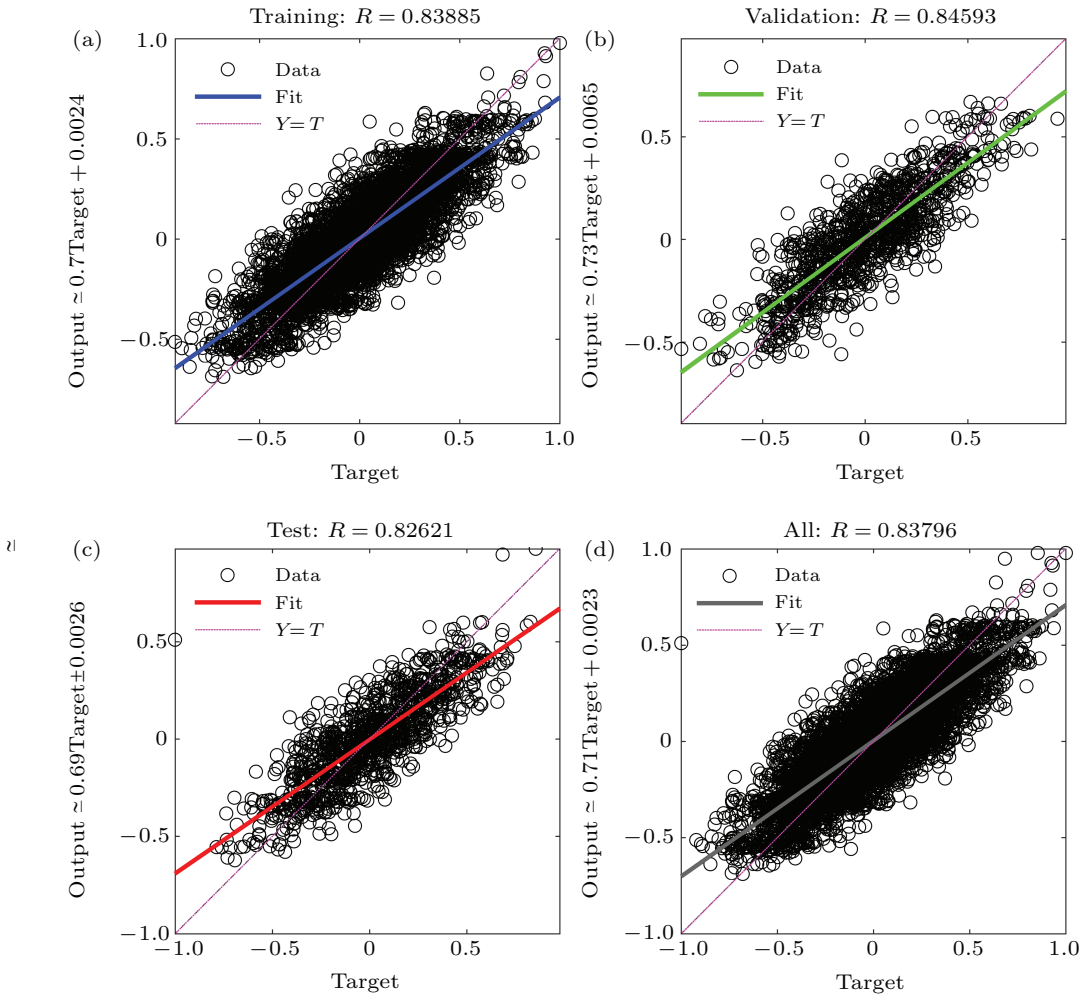


Fig. 4. Regression diagram of the second learning for $Q(\|y_j\|) = \|x_j\|$ ($L = 20$ km, $d = 80$, $N = 1.2 \times 10^6$).

After sufficient training, we began with the prediction process. To demonstrate the effect of the prediction, we randomly select some of Alice's raw keys, and compare them with the predicted values. As shown in Fig. 5, it shows that the two values are relatively close. In fact, the final mean relative error (MRE) we obtain from the experiment is 0.0246, which indicates that the prediction works well.

After Bob acquires all the predicted data (denoted as X_{out}), the parameter estimation can be proceeded. In Fig. 6, we performance of the ANN-based CVQKD system in terms of the secret key rate. For $S = 1$, it is the case of the ideal ANN scheme that the neural networks can predict all the data with complete accuracy. In addition, we also test the performance of secret key rate at different block lengths. We find that the ANN-based scheme has more advantages than the traditional one in terms of both transmission distance and secret key rate. The closer the value of prediction accuracy S approaches to 100%, the higher the secret key rate is, as shown in Eq. (17). The performance of the ANN-based scheme is closer to that of the ideal one, which results from the tunable parameter n/N.

The improvement of S depends much on block length. Within certain range, prediction accuracy, as well as transmission distance, can be improved by the increased block length since more data provide the sufficient training. In Fig. 7, we show effect of block length (blue-solid line) on the prediction accuracy S. For the block length that is no less than 10^6,

the value of S is between $[80\%, 83\%]$, whereas for the data length less than 10^6, a significant decrease of prediction accuracy can be observed, which indicates that adequate data are required for the performance improvement. In addition, due to the finite-size effect, small amounts of data may lead to the decrease of the secret key rate. However, when the block length is up to 10^7, S can be improved slightly. The reason is that once there is enough data for the training, without optimizing the ANN, increasing data length makes no sense to improve the training and predicting ability of the ANN. As the growth of the block length, it takes more time in the training and predicting, which will be a great challenge for the real-time performance of the system. The time spent in the post-processing of CVQKD system via ANN depends on the structure of ANN itself, the algorithm of training and prediction, and the performance of the computer running ANN. The most important factor is the block length of the data. When the blocks length are 10^5, 10^6, and 10^7, the times required to complete the post-processing are about two minutes, ten minutes and two hours, respectively. The performance of the computer used in our experiments is middling, with following configuration: core i5-10400F, 16G RAM, and 500G SSD. Obviously, The training time can be significantly reduced with a more powerful computer. In addition, during one working process of CVQKD system in optical fiber, the fitting relationship obtained by training the first data block can also be used in the subsequent data blocks. Therefore, we do not need to train every data block. Meanwhile, in Fig. 7, we can also find that with the increase of transmission distance, the prediction accuracy gradually decreases. This is because the longer the distance, the more distorted the signal.

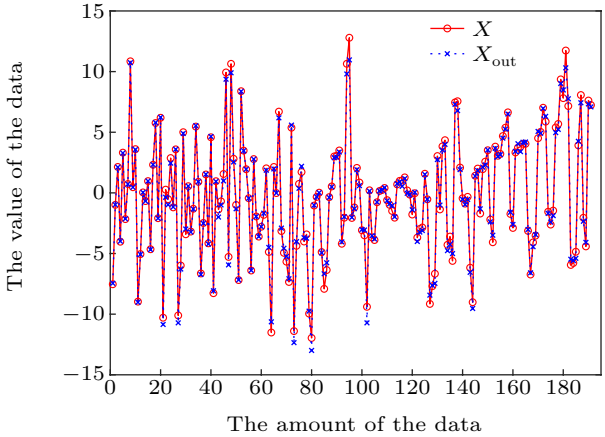


Fig. 5. Comparison between X and X_{out}. X represents the true values of Alice's raw keys, and X_{out} denotes the predicted values that Bob gets through the ANN.

In order to illustrate the characteristics of our scheme better, the method-of-moments (MM) scheme[42] and the transformed scheme by changing the implementation order of estimation and reconciliation (we call it exchanging order scheme for short)[25] are selected, to compare with our scheme. All of them can be used for the parameter estimations. The principles of these three schemes are completely different, our scheme uses a trained ANN to predict raw keys, while the MM scheme and the exchanging order scheme uses MM method to find a new estimator for σ^2 and changes the implementation order of parameter estimation and reconciliation, respectively. Compared with the other two competitors, our scheme is algorithmically simpler. In terms of disadvantages, more time is needed to train the networks in the ANN-based scheme, the performance of the estimator in the MM scheme is poor in minimizing variance and bias, and the exchanging order scheme requires an additional parameter estimation for channel characteristics, which increases the system complexity. And in terms of applicable scenario, our scheme is suitable for medium block length and unstable channel scenarios, while MM scheme is appropriate for long block length and high-loss channel, and the remaining scheme is applied to the stable system with slowly changing characteristics. Finally, we compared the secret key rates of the three schemes when the block length $N = 10^8$ and the transmission distance $L = 30$ km, there are 0.0507, 0.085, and 0.036, respectively. It is important to note that this is not the best performance of our scheme, we can increase the key rate by improving the structure of the neural networks, adjusting the parameters'value, and optimizing the training and predicting algorithm. For example, instead of BP neural networks, we can use the radial basis function (RBF) neural networks, which contains input layer, hidden layer (only one) and output layer. Various forms of RBF function can be used as the activation function in hidden layer, take Gaussian function for example, its expression can be written as follows:

$$\varphi_i(x_p - c_i) = \exp\left(-\frac{\|x_p - c_i\|^2}{2\sigma_i^2}\right), \tag{20}$$

where $\varphi_i(\cdot)$ represents the i-th RBF function, x_p is the p-th input, c_i represents the center of i-th node in the hidden layer, and σ_i^2 is the variance of the Gaussian function. Then the j-th output of the RBF neural networks reads

$$y_j = \sum_{i=1}^{h} w_{ij} \exp\left(-\frac{\|x_p - c_i\|^2}{2\sigma_i^2}\right), \quad j = 1, 2, \ldots, n, \tag{21}$$

where w_{ij} is the connection weight of the hidden layer to the output layer. Compared with BP networks, RBF networks can approximate arbitrary function with higher precision. Our experiments show that the key rate can be increased by 3% or even more by using the RBF networks and selecting appropriate parameters, such as the dimension of the input data, the spread of radial basis function, and so on. It should be noted that although RBF networks can avoid the local minimum problem and thus achieve higher prediction accuracy,

its structure can be more complex. Since there is no specific law to follow in neural networks design at present, quite a lot of continuous attempts are essential to improve the key rate. We believe that different approaches, or combinations of them, may lead to better performance. In general, although the key rate of the ANN-based scheme is not the highest, the complexity of the algorithm is low, and additional hardware is barely required. The property that ANN can approach any rational number in theory makes it have the most prominent advantage, that is, suitable for the complex, variable and unstable channels.

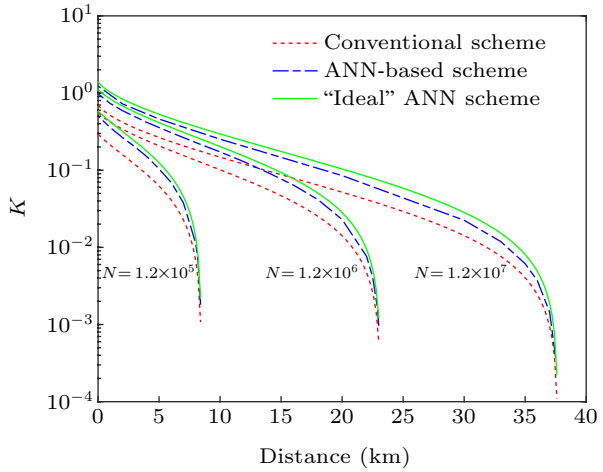


Fig. 6. Secret key rate as a function of transmission distance. From left to right, red-dotted lines, blue-dashed lines, and green-solid lines, correspond to the traditional scheme, the ANN-based scheme, and the ideal ANN scheme, respectively.

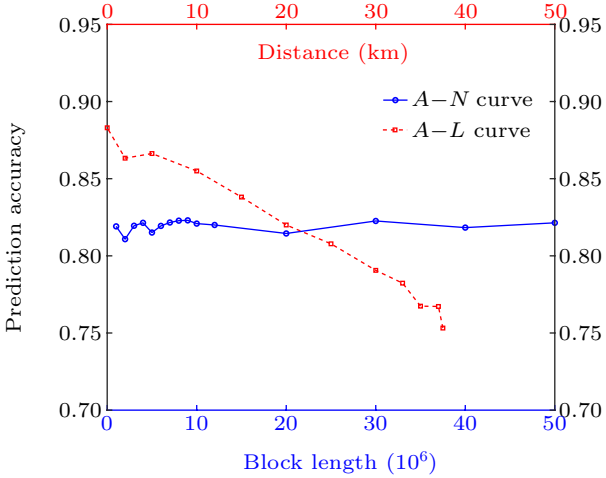


Fig. 7. The A–N curve shows how the prediction accuracy varies with the length of the data (blue-solid line, $L = 20$ km). The A–L curve represents the variation of the prediction accuracy with transmission distance (red-dotted line, $N = 1.2 \times 10^7$).

5. Conclusion

We have presented an ANN-involved parameter estimation scheme for performance improvement of the CVQKD system, where BP neural networks are placed in the data post-processing stage without disclosing the raw keys. After being preprocessed, Alice's and Bob's original data are fed into the ANN to start the training experiments, in which the structure and the parameters of the ANN are constantly adjusted until the regression curve and error curve show that the ANN has achieved its best performance. Relationship between the data is obtained at the end of the training experiments before the ANN's prediction. It is secure from Eve's eavesdropping since none of the original data is disclosed. Simulation results suggest that the ANN-based scheme has shown better performance in the parameter estimation, secret key rate, capacity for carrying information and the accuracy of prediction, compared with the traditional scheme and other schemes. Besides, the ANN-based scheme, which requires very few additional devices, can be expediently implemented in the practical CVQKD systems.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers Systems, and Signal Processing*, December 10–12, 1984, Bangalore, India, pp. 175–179
[2] Ruppert L, Usenko V C and Filip R 2014 *Phys. Rev. A* **90** 062310
[3] Diamanti E and Leverrier A 2015 *Entropy* **17** 6072
[4] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[5] Lance A M, Symul T, Sharma V, Weedbrook C, Ralph T C and Lam P K 2005 *Phys. Rev. Lett.* **95** 180503
[6] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
[7] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 *Nat. Photon.* **7** 378
[8] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, TualleBrouri R, McLaughlin S W and Grangier P 2007 *Phys. Rev. A* **76** 042305
[9] Mao Y Y, Huang W T, Zhong H, Wang Y J, Qin H, Guo Y and Huang D 2020 *New J. Phys.* **22** 083073
[10] Wu X D, Wang Y J, Guo Y, Zhong H and Huang D 2021 *Phys. Rev. A* **103** 032604
[11] Liao Q, Xiao G, Zhong H and Guo Y 2020 *New J. Phys.* **22** 083086
[12] Su X L, Wang W Z, Wang Y, Jia X J, Xie C D and Peng K C 2009 *Europhys. Lett.* **87** 20005
[13] Su X L 2014 *Chin. Sci. Bull.* **59** 1083
[14] M Navascués, Grosshans F and Acin A 2006 *Phys. Rev. Lett.* **97** 190502
[15] Furrer F, Franz T, Berta M, Leverrier A, Scholz V B, Tomamichel M and Werner R F 2012 *Phys. Rev. Lett.* **109** 100502
[16] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[17] Leverrier A 2015 *Phys. Rev. Lett.* **114** 070501
[18] Wang Y J, Mao Y Y, Huang W T, Huang D and Guo Y 2019 *Opt. Express* **27** 25314
[19] Zeng G H 2010 *Quantum private communication* (Beijing: Higher Education Press and Springer Publishing Company) pp. 293–297
[20] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 *Phys. Rev. Lett.* **93** 170504
[21] Brunner H H, Comandar L C, Karinou F, Bettelli S, Hillerkuss D, Fung F, Wang D W, Mikroulis S, Yi Q, Kuschnerov M, Poppe A, Xie C S and Peev M 2017 *19th International Conference on Transparent Optical Networks (ICTON)*, July 2–6, 2017, Girona, Spain, pp. 1–4
[22] Guo Y, Xie C L, Huang P, Li J W, Zhang L, Huang D and Zeng G H 2018 *Phys. Rev. A* **97** 052326
[23] Chai G, Cao Z W, Liu W Q, Wang S Y, Huang P and Zeng G H 2019 *Phys. Rev. A* **99** 032326
[24] Guo Y, Zhou Z H, Wang X D, Wu X D, Zhang L and Huang D 2019 *Int. J. Theor. Phys.* **58** 1613
[25] Wang X Y, Zhang Y C, Yu S and Guo H 2019 *Quantum Inf. Process.* **18** 1
[26] Yang J, Xu B J, Peng X and Guo H 2012 *Phys. Rev. A* **85** 052302
[27] Li Y, Huang P, Wang S Y, Wang T, Li D W and Zeng G H 2018 *Phys. Lett. A* **382** 3253

[28] Garcia-Patron Sanchez Raul 2007 *Quantum information with optical continuous variables: from bell tests to key distribution*, Ph.D. Dissertation (Brussels: Université libre de Bruxelles)
[29] Chai G, Li D W, Cao Z W, Zhang M H, Huang P and Zeng G H 2020 *Quantum Engineering* **2** e37
[30] Gyongyosi L and Imre S 2018 *Appl. Sci.* **8** 87
[31] Jiang X Q, Yang S Y, Huang P and Zeng G H 2018 *IEEE Photon. J.* **10** 1
[32] Gyongyosi L and Imre S 2014 *Advances in Photonics of Quantum Computing, Memory, and Communication VII*, February 19, 2014, San Francisco, USA, pp. 28–40
[33] Liu B, Zhao B K, Zou D J, Wu C Q, Yu W R and You I 2013 *Information and Communication Technology-EurAsia Conference*, March, 2013, Yogyakarta, Indonesia, pp. 453–458
[34] Li D W, Huang P, Zhou Y M, Li Y and Zeng G H 2018 *IEEE Photon. J.* **10** 1
[35] McCulloch W S and Pitts W 1943 *The bulletin of mathematical biophysics volume* **5** p. 115
[36] Wang W Y and Hoi-Kwong Lo 2019 *Phys. Rev. A* **100** 062334
[37] Zhou M G, Liu Z P, Liu W B, Li C L, Bai J L, Xue Y R, Fu Y, Yin H L and Chen Z B 2021 arXiv: 2108.02578v1 [quant-ph]
[38] Beale H D, Demuth H B and Hagan M 1997 *Neural network design* (Boston: PWS Publishing Co.) Chapter 1 pp. 4–7
[39] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev. A* **81** 062343
[40] Fossier S, Diamanti E, Debuisschert T, Tuallebrouri R and Grangier P 2009 *J. Phys. B: At. Mol. Opt. Phys.* **42** 114014
[41] Leverrier A and Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
[42] Thearle O, Assad S M and Symul T 2016 *Phys. Rev. A* **93** 042343