Science Bulletin 62 (2017) 1025–1029

Contents lists available at ScienceDirect

Science Bulletin

journal homepage: www.elsevier.com/locate/scib

Science Bulletin
www.scibull.com

Article

Distributed secure quantum machine learning

Yu-Bo Sheng [a,*], Lan Zhou [b]

[a] Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing 210003, China
[b] College of Mathematics & Physics, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

ARTICLE INFO

Article history:
Received 15 May 2017
Received in revised form 19 June 2017
Accepted 20 June 2017
Available online 27 June 2017

Keywords:
Quantum machine learning
Quantum communication
Quantum computation
Big data

ABSTRACT

Distributed secure quantum machine learning (DSQML) enables a classical client with little quantum technology to delegate a remote quantum machine learning to the quantum server with the privacy data preserved. Moreover, DSQML can be extended to a more general case that the client does not have enough data, and resorts both the remote quantum server and remote databases to perform the secure machine learning. Here we propose a DSQML protocol that the client can classify two-dimensional vectors to different clusters, resorting to a remote small-scale photon quantum computation processor. The protocol is secure without leaking any relevant information to the Eve. Any eavesdropper who attempts to intercept and disturb the learning process can be noticed. In principle, this protocol can be used to classify high dimensional vectors and may provide a new viewpoint and application for future "big data".

1. Introduction

Quantum communication, such as quantum teleportation [1–3], quantum key distribution (QKD) [4–6], quantum secure direct communication (QSDC) [7–11], and other important protocols [12,13] have been paid widely attention, for they can perform absolutely secure communication in principle. Quantum computing has also attracted much interest because of the discovery of applications that outperform the best-known classical counterparts. For example, Shor's algorithm for integer factorization [14], Grover's algorithm [15], and the optimal Long's algorithm for unsorted database search [16], all have displayed the great computing power of quantum computers. Vast technological developments have been made for small-scale quantum computers in ions [17], photons [18], superconduction [19], and some other important quantum systems [20].

Machine learning (ML) is a branch of artificial intelligence [21]. It can learn from previous experience to optimize performance, which is widely used in computer sciences, robotics, bioinformatics, and financial analysis. Recently, ML can be also used to realize the precise quantum measurement and discriminate quantum measurement trajectories [22,23]. ML depends on the database to perform the training. The more data the computer can process, the more accurate of the ML model is. In ML, an important algorithm in mathematical picture can be described as follows: it is used to evaluate the distance and inner product between two vectors. For high-dimensional vectors, such task requires large time proportional to the size of the vectors. Therefore, the vector size will become a challenge for modern rapid growing big data and the limitation of Moore's law in a classical computer.

In 2013, Lloyd et al. [24] showed that the quantum computer can be used to perform the ML. Subsequently, several quantum machine learning (QML) protocols and experimental realization were reported [25–34]. In 2014, Rebentrost et al. [25] discussed the quantum support vector machine for big data classification. They showed that the support vector machine can be implemented on a quantum computer. Bang et al. [26] proposed an interesting method for quantum algorithm design assisted by ML. Yoo et al. [27] compared quantum and classical machines designed for learning an *N*-bit Boolean function. They concluded that quantum superposition enabled quantum learning is faster than classical learning. Cross et al. [29] discussed the quantum learning which is robust against practical noise. They showed that the class of parity functions can be learned in logarithmic time from corrupted quantum queries. Cai et al. [31] realized the first entanglement-based ML on a quantum computer. Li et al. [32] demonstrated the quantum learning algorithm for artificial intelligence on a four-qubit quantum processor.

In this paper, we will discuss another practical application for QML. Alice (client) has some important and confidential data and wants to implement QML with the learning algorithm of distance evaluation. However, she does not have enough quantum ability. Fortunately, Alice has a rich and trusted friend named Bob (server),

* Corresponding author.
E-mail address: shengyb@njupt.edu.cn (Y.-B. Sheng).

http://dx.doi.org/10.1016/j.scib.2017.06.007
2095-9273/

who has a quantum server and can perform the QML. Can Alice ask Bob for help to perform the secure QML? Let us consider a more general case. The important and confidential data are owned by Charlie. Can Alice realize the QML with the help of Bob and Charlie? Such situation may exist in the future "big data" world. For example, a medical scientist wants to perform the QML. However, all the data come from the different hospitals. As the data are the privacy of patients, they should be well protected during the data transmission. The results of the QML should also be secure. Our protocol shows that it is possible for Alice to realize the secure QML. We call it distributed secure quantum machine learning (DSQML). The concept of DSQML can be detailed as follows. A client can perform single-qubit preparation, operation and measurement but does not have sufficient quantum technology to delegate QML. He/She asks a remote trusted server who has a fully fledged quantum power to perform the QML. During the process, any Eve who attempts to intercept and disturb the learning can be noticed. Our DSQML is based on the learning algorithm of distance evaluation and it contains two models. The first model is the client-server DSQML. The second model is the client-server-database DSQML. In the first model, client owns the data and resorts to the quantum server to realize QML. In the second model, client resorts both the remote quantum server and databases to realize QML.

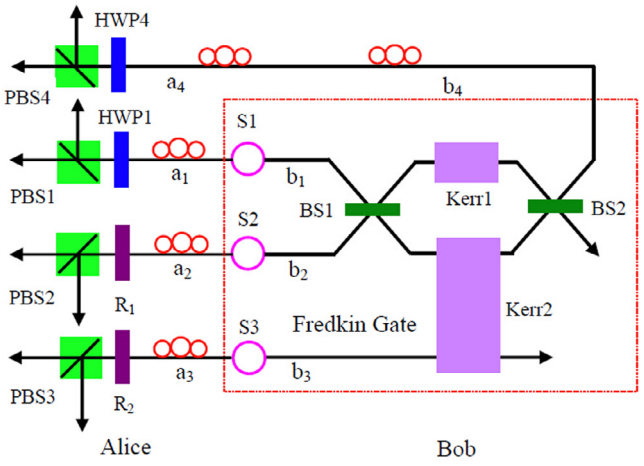

Fig. 1. (Color online) Schematic of the principle of client-server DSQML in an optical system. The Fredkin gate is constructed by the optical kerr nonlinearity [35]. HWP is the half-wave plate which can make $|H\rangle \to \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, and $|V\rangle \to \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$. PBS is the polarization beam splitter. It can transmit the $|H\rangle$ polarized photon and reflect the $|V\rangle$ polarized photon. R is an arbitrary rotation for polarization photons. S1, S2 and S3 are the entanglement sources, respectively.

2. Client-server DSQML protocol

A key mathematical task of QML algorithm is to assign a new vector $\vec{u}$ to two different clusters A and B with one reference vector $\vec{v}_A$ and $\vec{v}_B$ in each cluster [24,31]. By comparing the distance $D_A = |\vec{u} - \vec{v}_A|$ and $D_B = |\vec{u} - \vec{v}_B|$, we can assign $\vec{u}$ to the cluster with smaller distance. A quantum state has its natural advantage to be used to represent a vector. Here we describe the calculation of the distance between two two-dimensional vectors for example. This approach is also suitable for assigning high-dimensional vectors. We let $\vec{u} = |u||u\rangle$, and $\vec{v} = |v||v\rangle$, respectively. Here $|u|$ and $|v|$ are the lengths of the vectors, respectively. $|u\rangle$ and $|v\rangle$ can be described as

$$\begin{aligned} |u\rangle &= \alpha|H\rangle + \beta|V\rangle, \\ |v\rangle &= \gamma|H\rangle + \delta|V\rangle. \end{aligned} \tag{1}$$

Here α, β, γ and δ are real with $\alpha^2 + \beta^2 = 1$ and $\gamma^2 + \delta^2 = 1$. $|H\rangle$ is the horizonal polarization and $|V\rangle$ is the vertical polarization of the photon, respectively. The distance between $\vec{u}$ and $\vec{v}$ can be described as

$$\begin{aligned} D &= |\vec{u} - \vec{v}| = \sqrt{|\vec{u} - \vec{v}|^2} \\ &= \sqrt{(|u|\langle u| - |v|\langle v|)(|u||u\rangle - |v||v\rangle)} \\ &= \sqrt{|u|^2 + |v|^2 - 2|u||v|\langle u|v\rangle}. \end{aligned} \tag{2}$$

From Eq. (2), the calculation of the distance can be converted to the calculation of the overlap of the quantum states $|u\rangle$ and $|v\rangle$.

Our client-server DSQML protocol based on the optical system can be described as follows.

Step 1: As shown in Fig. 1, Bob first prepares three ordered $2N$ pairs of states $|\phi^+\rangle$ using the entanglement sources S1, S2, and S3, respectively. Here $|\phi^+\rangle$ is the form of

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle|H\rangle + |V\rangle|V\rangle). \tag{3}$$

The $2N$ pairs of photons are divided into two groups. Each group contains N pairs. The first group is named checking group and the second group is named message group. Bob sends one of the photons in each pair to Alice in each checking group in the spatial modes a_1b_1, a_2b_2 and a_3b_3 as shown in Fig. 1. Subsequently, Alice and Bob check eavesdropping by the following procedure. (1) Bob randomly measures his N photons in the checking group in the basis $\{|H\rangle, |V\rangle\}$ and $\{|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)\}$, respectively. (2) Bob tells Alice which basis he has used for each photon and all the measurement results. (3) Alice uses the same measurement basis to measure all the N photons and checks her results with Bob's. For $|\phi^+\rangle$, Alice and Bob always have the same measurement results in both basis $\{|H\rangle, |V\rangle\}$ and $\{|\pm\rangle\}$. If some of the results are different, it means that eavesdroppers exists. In this way, they have to stop and check the quantum channel to eliminate eavesdropping.

Step 2: Bob sends another three sequences of N pairs to Alice, respectively. After Alice receiving the photons, Alice and Bob can also randomly choose some photon pairs to perform security checking.

Step 3: Alice randomly measure the photons in spatial mode a_1 in the basis $\{|H\rangle, |V\rangle\}$ and $|\pm\rangle$, respectively. In Fig. 1, HWP1 and PBS1 can be used to complete the task. Here HWP is the half-wave plate which can make $|H\rangle \to \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, and $|V\rangle \to \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$. PBS is the polarization beam splitter. It can transmit the $|H\rangle$ polarized photon and reflect the $|V\rangle$ polarized photon, respectively. After measurements, Bob will obtain a random photon sequence in spatial mode b_1 such as $|H\rangle_1|-\rangle_2|V\rangle_3 \cdots |+\rangle_N$. The polarization information of each photon is only known by Alice.

Step 4: Alice rotates her photons in channel a_2. The operation R_1 can perform an arbitrary rotation as $|H\rangle \to \alpha|H\rangle + \beta|V\rangle$ and $|V\rangle \to \beta|H\rangle - \alpha|V\rangle$. Subsequently, Alice lets her photon pass through the PBS2 and measures it. If her measurement is $|H\rangle$, Bob's photon in spatial mode b_2 will become $|u\rangle = \alpha|H\rangle + \beta|V\rangle$. On the other hand, if Alice's measurement result is $|V\rangle$, Bob's photon in b_2 will become $|u\rangle\prime = \beta|H\rangle - \alpha|V\rangle$. In this way, Alice asks Bob to perform a bit-flip operation $\sigma_x = |H\rangle\langle V| + |V\rangle\langle H|$ and a phase-flip operation $\sigma_z = |H\rangle\langle H| - |V\rangle\langle V|$ to change $|u\rangle\prime$ to $|u\rangle$. Alice also rotates her photon with R_2 in spatial mode a_3 and measures it to make the related photon in Bob collapse to $|v\rangle$. Then she asks Bob to perform the Fredkin operation.

Step 5: Bob performs the Fredkin operation. The photons in spatial mode b_1 is the control qubits and the photons in b_2 and b_3 are the target qubits, respectively. In an optical system, optical Kerr effect provides us a powerful tool to realize the Fredkin gate [35]. If the control qubit is $|H\rangle$ or $|V\rangle$, the whole system can evolve as

$$|H\rangle|u\rangle|v\rangle \rightarrow |H\rangle|u\rangle|v\rangle,$$
$$|V\rangle|u\rangle|v\rangle \rightarrow |V\rangle|v\rangle|u\rangle. \quad (4)$$

On the other hand, if the control qubit is $|+\rangle$ or $|-\rangle$, the whole system can be written as

$$\begin{aligned}|\pm\rangle|u\rangle|v\rangle =& \frac{1}{\sqrt{2}}(|H\rangle|u\rangle|v\rangle \pm |V\rangle|v\rangle|u\rangle).\\ \rightarrow& \frac{1}{2}[|+\rangle(|u\rangle|v\rangle + |v\rangle|u\rangle)\\ &\pm |-\rangle(|u\rangle|v\rangle - |v\rangle|u\rangle)]. \quad (5)\end{aligned}$$

After performing the Fredkin operation, the N control qubits are sent back to Alice in spatial modes $a_4 b_4$.

Step 6: Fredkin operation does not change the polarization of control qubit. Alice knows the exact polarization information of these N photons. For the kth qubit, if it is $|H\rangle$ or $|V\rangle$, Alice measures it in the basis $\{|H\rangle, |V\rangle\}$. On the other hand, if it is $|+\rangle$ or $|-\rangle$, she measures it in the basis $\{|\pm\rangle\}$. The probability of obtaining $|+\rangle$ can be written as

$$P_+ = \frac{1 + |\langle u|v\rangle|^2}{2}. \quad (6)$$

The probability of obtaining $|-\rangle$ can be written as

$$P_- = \frac{1 - |\langle u|v\rangle|^2}{2}. \quad (7)$$

They can obtain that

$$\langle u|v\rangle = \sqrt{1-2P_-} = \sqrt{2P_+ - 1}. \quad (8)$$

Compared with Eq. (2), they can obtain

$$\begin{aligned}D =& \sqrt{|u|^2 + |v|^2 - 2|u||v|\sqrt{1-2P_-}}\\ =& \sqrt{|u|^2 + |v|^2 - 2|u||v|\sqrt{2P_+ - 1}}. \quad (9)\end{aligned}$$

From Eq. (9), similar to the approach of entanglement detection [36,37], the calculation of D is transformed to pick up the success probability of P_- or P_+. In a practical experiment, they should repeat this protocol many times to obtain a statistical accuracy simply by calculating the ratio between the detected photon number and the initial total photon number [31]. Alice first obtains the distance D_A and then repeats the similar process to obtain the distance D_B. Finally, she can compare D_A and D_B with a classical computer. In this way, the whole protocol is completed.

3. Client-server-database DSQML protocol

In Fig. 2, DB denotes the database. In "big data" world, Alice usually does not have enough data to perform the QML. She should both resorts the remote quantum server and database. Certainly, both the data and the learning results cannot be eavesdropped. In client-server-database DSQML protocol, Charlie is required to have the ability to prepare, operate and measure the single photon, analogy with Alice. By modifying the client-server DSQML, this client-server-database DSQML can be described as follows.

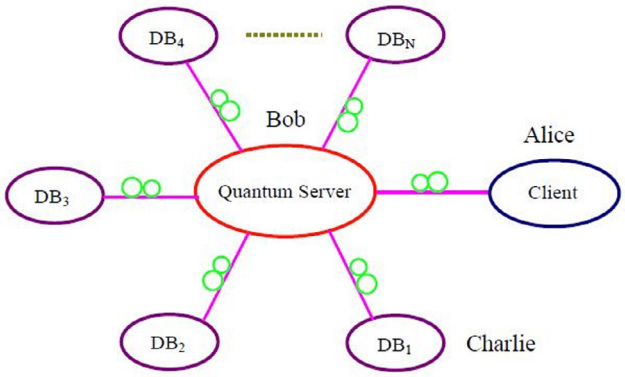

Fig. 2. (Color online) Schematic of the principle of client-server-database DSQML. $DB_1, DB_2, \ldots, DB_N$ denote the different remote databases. Quantum server owned by Bob can perform the QML. The client Alice resorts Bob and the different databases to realize the QML.

Step 1: Bob prepares and distributes one sequence of entanglement to Alice and two sequences of entanglement to Charlie (DB_1) to perform security checking, respectively.

Step 2: Bob prepares and distributes another sequence of entanglement to Alice and two sequences of entanglement to Charlie to set up the quantum channels.

Step 3: Alice randomly measures the photons in the basis $\{|H\rangle, |V\rangle\}$ and $\{|\pm\rangle\}$ and lets Bob obtain a random photon sequence such as $|H\rangle_1|-\rangle_2|V\rangle_3\cdots|+\rangle_N$.

Step 4: Charlie rotates and measures her photons to let Bob obtain the information of $|u\rangle$ and $|v\rangle$.

Step 5: Bob performs the Fredkin operation and distributes the control qubits to Alice.

Step 6: Alice performs the security checking by measuring the received $|H\rangle$ or $|V\rangle$ photons in the basis $\{|H\rangle, |V\rangle\}$, respectively, and measures the received $|\pm\rangle$ photons in $\{|\pm\rangle\}$ basis to obtain statistical results of $P_\pm$.

Finally, Alice calculates D, according to $P_\pm$. Here we should point out that in order to obtain D, Alice should know the values of $|u|$ and $|v|$. As both Alice and Charlie have the quantum ability of preparing, operating and measuring single photon, they can exploit the QKD protocol [4], or QSDC protocol with single photons [9] to transmit $|u|$ and $|v|$ and protect $|u|$ and $|v|$ from eavesdropping completely. Alice can also perform the QML with the other databases, such as DB_2, $DB_3, \ldots, DB_N$, as shown in Fig. 2.

4. Security of the DSQML protocol

The proof for the security of second protocol is analogy with the first protocol. Therefore, we take the first protocol for example. The proof for the security of our DSQML protocol is based on the security for the first transmission of the photons prepared by S1, S2 and S3 from Bob to Alice, and the second transmission of the control qubit from Bob to Alice. In the first transmission, the security checking in our protocol is similar to the QSDC protocol [7]. During the transmission, all the states are the same Bell states $|\phi^+\rangle$. Bob does not encode any information to Alice. If Eve can capture one photon in each Bell state, he gets no information. Once Alice and Bob share the same states $|\phi^+\rangle$, by measuring the photons in the same basis $\{|H\rangle, |V\rangle\}$ or $\{|\pm\rangle\}$ randomly, they always obtain the same measurement results. However, if Eve steals one photon and fakes another photon to Alice, the faked photon does not entangle with the Bob's photon. By measuring the two "entangled" photons, Alice and Bob will find that some of the photons will

induce the different measurement results, which shows that the Eve exists. Eve cannot elicit any information from the Bell states because there is no information encoded there. The information "comes into being" only after Alice performing the measurements on her photons. However, after measurement, the photons in Bob's location collapse to the corresponded states, which shows that Eve cannot elicit any information during measurement.

The security of the second transmission of the control qubits from Bob to Alice is similar to the QKD protocol [4]. Note that Bob does not change the polarization of the control qubits and he even does not know the polarization of these control qubits. Only Alice knows the exact information of these control qubits. Therefore, after Alice receiving these photons, if initial control qubit is $|H\rangle$ or $|V\rangle$, she still obtain $|H\rangle$ or $|V\rangle$ by measuring it in the basis $\{|H\rangle, |V\rangle\}$, respectively. Thus, if an unexpected measurement result occurs, for example, the initial state is $|H\rangle$ but the measurement result is $|V\rangle$ and vice versa, it means that the Eve has altered the photon. In DSQML, the important and confidential data essential are $\vec{u}$ and $\vec{v}$. After performing the DSQML, all target qubits are stayed at Bob's location. Therefore, the security of this DSQML depends on the fact that Bob is a trusted server. After Alice measuring the reference state, Bob essentially can obtain the information of $|u\rangle$ and $|v\rangle$ by measuring a range of samples. However, for Bob does not know $|u|$ and $|v|$, he still cannot know the exact information of $\vec{u}$ and $\vec{v}$ and he also cannot obtain the learning results.

5. Discussion and conclusion

So far, we have described our DSQML protocol for classifying a two-dimensional vector. This protocol is suitable for arbitrary high-dimensional vector, based on the condition that Bob has a powerful quantum computer processor to perform the Fredkin operation for high-dimensional quantum state and Alice and Charlie can measure and operate arbitrary high-dimensional single quantum state [38]. In an optical system, the photons encoded in multiple degrees of freedom [36,39,40] or the orbital angular momentum degree of freedom [41] may be the good candidates to implement the high-dimensional vector. The high dimensional vector can also be encoded with the polarization state of biphoton or multiphoton qubits [24,42], which has been demonstrated in previous QML [31]. For two-dimension system, the Fredkin operation can be realized with the help of cross-Kerr nonlinearity [35]. Recent experiment of the observation for the nonlinear phase shift due to the single post-selected photon showed that it is possible to realize such Fredkin gate [43]. For high-dimension system, it is possible to realize the Fredkin gate in four-qubit system encoded in both polarization and spatial modes degrees of freedom assisted with nitrogen-vacancy centers [38]. As shown in Eq. (9), in order to calculate D, they are required to obtain P_+ or P_-, which is decided by the initial photon number of the control qubit and the detected photon number owned by Alice. As shown in Step 3, we suppose that $N \doteq N_1 + N_2$. Here N_1 and N_2 are the number of photons which prepared in the basis $\{|H\rangle, |V\rangle\}$ and $\{|\pm\rangle\}$, respectively. We can obtain as $P_\pm = \frac{M_\pm}{N_2}$. Here $M_\pm$ are the photon numbers which are registered in the basis $\{|\pm\rangle\}$, respectively. If considering the photon loss, Alice will receive M photons and we can calculate as $\eta = 1 - \frac{M}{N}$. Here η is the probability of photon loss. Here $M \doteq M_1 + M_2$, which M_1 and M_2 are the number of photons after photon loss in the bases $\{|H\rangle, |V\rangle\}$ and $\{|\pm\rangle\}$, respectively. We can also obtain $M_2 = (1-\eta)N_2$. In this way, $P_\pm$ should be redescribed as $P_\pm = \frac{M_\pm(1-\eta)}{M_2} = \frac{(1-\eta)M_\pm}{(1-\eta)N_2} = \frac{M_\pm}{N_2}$. We show that the photon loss does not effect the results of $P_\pm$. However, the photon loss will also make the protocol insecure for they cannot discriminate that the photon is loss or intercept by Eve. Analogy with quantum communications, the quantum state amplification protocols and quantum repeaters have been proposed to protect the photon from loss [44–47]. On the other hand, environmental noise will degrade the maximally entangled state $|\phi^+\rangle$ to a mixed state. Fortunately, entanglement purification and concentration provided us the powerful tool to recover the low quality entangled states to the high quality entangled state [48–53].

In conclusion, we have proposed the concept of DSQML and described the DSQML model. The first DSQML protocol is client-server protocol and the second is client-server-database protocol, which is more general and practical. We mainly take an example of estimating the distance of two-dimension vector, exploiting the optical system and also show that this protocol is also suitable for classifying high-dimension vector. As the information secure and data privacy play important roles in future, this protocol may provide an alternative approach for the client with little quantum technology to delegate a remote and secure machine learning to the quantum server in future "big data" world.

Conflict of interest

The authors declare that they have no conflict of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (11474168 and 61401222), the Natural Science Foundation of Jiangsu Province (BK20151502), the Qing Lan Project in Jiangsu Province, and a Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions.

References

[1] Bennett CH, Brassard G, Crepeau C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys Rev Lett 1993;70:1895–9.
[2] Li TC, Yin ZQ. Quantum superposition, entanglement, and state teleportation of a microorganism on an electromechanical oscillator. Sci Bull 2016;61:163–71.
[3] Ai Q. Toward quantum teleporting living objects. Sci Bull 2016;61:110–1.
[4] Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE international conference on computers, systems and signal processing, Bangalore, India. New York: IEEE; 1984. p. 175–9.
[5] Ekert AK. Quantum cryptography based on Bell's theorem. Phys Rev Lett 1991;67:661–3.
[6] Zhang CM, Li M, Yin ZQ, et al. Multiuser-to-multiuser entanglement distribution based on 1550 nm polarization-entangled photons. Sci China Phys Mech Astron 2015;58:590301.
[7] Long GL, Liu XS. Theoretically efficient high-capacity quantumkeydistribution scheme. Phys Rev A 2002;65:032302.
[8] Deng FG, Long GL, Liu XS. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A 2003;68:042317.
[9] Wang C, Deng FG, Li YS, et al. Quantum secure direct communication with high-dimension quantum superdense coding. Phys Rev A 2005;71:044305.
[10] Hu JY, Yu B, Jing MY, et al. Experimental quantum secure direct communication with single photons. Light Sci Appl 2016;5:e16144.
[11] Zhang W, Ding DS, Sheng YB, et al. Quantum secure direct communication with quantum memory. Phys Rev Lett 2017;118:220501.
[12] Yang YG, Xu P, Yang R, et al. Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption. Sci Rep 2016;6:19788.
[13] Yang YG, Liu ZC, Li J, et al. Quantum private query with perfect user privacy against a joint-measurement attack. Phys Lett A 2016;380:4033–8.
[14] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th annual symposium on foundations of computer science. IEEE; 1994. p. 124–34.
[15] Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on theory of computing. ACM; 1996. p. 212–9.
[16] Long GL. Grover algorithm with zero theoretical failure rate. Phys Rev A 2001;64:022307.
[17] Cirac JI, Zoller P. Quantum computations with cold trapped ions. Phys Rev Lett 1995;74:4091–4.
[18] Lu CY, Zhou XQ, Guehne O, et al. Experimental entanglement of six photons in graph states. Nat Phys 2007;3:91–5.

[19] Makhlin Y, Schön G, Shnirman A. Quantum-state engineering with Josephson-junction devices. Rev Mod Phys 2001;73:357–400.
[20] Berezovsky J, Mikkelsen MH, Stoltz NG, et al. Picosecond coherent optical manipulation of a single electron spin in a quantum dot. Science 2008;320:349–52.
[21] Mohri M, Rostamizadeh A, Talwalkar A. Foundations of machine learning. Cambridge, MA: MIT Press; 2012.
[22] Hentschel A, Sanders BC. Machine learning for precise quantum measurement. Phys Rev Lett 2010;104:063603.
[23] Magesan E, Gambetta JM, Córcoles AD, et al. Machine learning for discriminating quantum measurement trajectories and improving readout. Phys Rev Lett 2014;114:200501.
[24] Lloyd S, Mohseni M, Rebentrost P. Quantum algorithms for supervised and unsupervised machine learning; 2013. arXiv: 1307.0411.
[25] Rebentrost P, Mohseni M, Lloyd S. Quantum support vector machine for big data classification. Phys Rev Lett 2014;113:130503.
[26] Bang J, Ryu J, Yoo S, et al. A strategy for quantum algorithm design assisted by machine learning. New J Phys 2014;16:073017.
[27] Yoo S, Bang J, Lee C, et al. A quantum speedup in machine learning: finding an N-bit Boolean function for a classification. New J Phys 2014;16:103014.
[28] Bang J, Lee SW, Jeong H. Protocol for secure quantum machine learning at a distant place. Quant Inf Process 2015;14:3933–47.
[29] Cross AW, Smith G, Smolin JA. Quantum learning robust against noise. Phys Rev A 2015;92:012327.
[30] Schuld M, Sinayskiy I, Petruccione F. An introduction to quantum machine learning. Contemp Phys 2015;56:172.
[31] Cai XD, Wu D, Su ZE, et al. Entanglement-based machine learning on a quantum computer. Phys Rev Lett 2015;114:110504.
[32] Li ZK, Liu XM, Xu NY, et al. Experimental realization of a quantum support vector machine. Phys Rev Lett 2015;114:140504.
[33] Zhang Y, Kim EA. Quantum loop topography for machine learning. Phys Rev Lett 2017;118:216401.
[34] Monras A, Sentis G, Wittek P. Inductive supervised quantum learning. Phys Rev Lett 2017;118:190503.
[35] Milburn GJ. Quantum optical Fredkin gate. Phys Rev Lett 1989;62:2124–7.
[36] Walborn SP, Souto Ribeiro PH, Davidovich L, et al. Experimental determination of entanglement with a single measurement. Nature 2006;440:1022–4.
[37] Zhou L, Sheng YB. Detection of nonlocal atomic entanglement assisted by single photons. Phys Rev A 2014;90:024301.
[38] Wei HR, Zhu PJ. Implementations of two-photon four-qubit Toffoli and Fredkin gates assisted by nitrogen-vacancy centers. Sci Rep 2016;6:35529.
[39] Wang XL, Cai XD, Su ZE, et al. Quantum teleportation of multiple degrees of freedom of a single photon. Nature 2015;518:516–9.
[40] Deng FG, Ren BC, Li XH. Quantum hyperentanglement and its applications in quantum information processing. Sci Bull 2017;62:46–68.
[41] Ding DS, Zhang W, Zhou ZY, et al. Quantum storage of orbital angular momentum entanglement in an atomic ensemble. Phys Rev Lett 2015;114:050502.
[42] Mikami H, Kobayashi T. Remote preparation of qutrit states with biphotons. Phys Rev A 2007;75:022325.
[43] Feizpour A, Hallaji M, Dmochowski G, et al. Observation of the nonlinear phase shift due to single post-selected photons. Nat Phys 2015;11:905–9.
[44] Osorio CI, Bruno N, Sangouard N, et al. Heralded photon amplification for quantum communication. Phys Rev A 2012;86:023815.
[45] Zhou L, Sheng YB. Recyclable amplification protocol for the single-photon entangled state. Laser Phys Lett 2015;12:045203.
[46] Briegel HJ, Dür W, Cirac JI, et al. Quantum repeaters: the role of imperfect local operations in quantum communication. Phys Rev Lett 1998;81:5932–5.
[47] Wang C, Wang TJ, Zhang Y, et al. Construction of a quantum repeater based on a quantum dot in an optical microcavity system. Laser Phys Lett 2014;11:065202.
[48] Sheng YB, Zhou L. Deterministic polarization entanglement purification using time-bin entanglement. Laser Phys Lett 2014;11:085203.
[49] Sheng YB, Zhou L. Deterministic entanglement distillation for secure double-server blind quantum computation. Sci Rep 2015;5:7815.
[50] Wang TJ, Liu LL, Zhang R, et al. One-step hyperentanglement purification and hyperdistillation with linear optics. Opt Express 2015;23:9284–94.
[51] Cao C, Chen X, Duan YW, et al. Concentrating partially entangled W-class states on nonlocal atoms using low-Q optical cavity and linear optical elements. Sci China Phys Mech Astron 2016;59:100315.
[52] Sheng YB, Pan J, Guo R, et al. Efficient N-particle W state concentration with different parity check gates. Sci China Phys Mech Astron 2015;58:060301.
[53] Du FF, Deng FG. Heralded entanglement concentration for photon systems with linear-optical elements. Sci China Phys Mech Astron 2015;58:040303.