Copyright © 2019 Tech Science Press CMC, vol.59, no.3, pp.1005-1014, 2019

A Quantum Authorization Management Protocol Based on EPR-Pairs

Yan Chang[1, *], Shibin Zhang[1], Lili Yan[1], Guihua Han[1], Haiquan Song[1], Yan Zhang[1], Xueyang Li[1] and Qirun Wang[2]

Abstract: Quantum authorization management (QAM) is the quantum scheme for privilege management infrastructure (PMI) problem. Privilege management (authorization management) includes authentication and authorization. Authentication is to verify a user's identity. Authorization is the process of verifying that a authenticated user has the authority to perform a operation, which is more fine-grained. In most classical schemes, the authority management center (AMC) manages the resources permissions for all network nodes within the jurisdiction. However, the existence of AMC may be the weakest link of the whole scheme. In this paper, a protocol for QAM without AMC is proposed based on entanglement swapping. In this protocol, Bob (the owner of resources) authenticates the legality of Alice (the user) and then shares the right key for the resources with Alice. Compared with the other existed QAM protocols, this protocol not only implements authentication, but also authorizes the user permissions to access certain resources or carry out certain actions. The authority division is extended to fin-grained rights division. The security is analyzed from the four aspects: the outsider's attack, the user's attack, authentication and comparison with the other two QAM protocols.

Keywords: Quantum authorization management, entanglement swapping, fin-grained rights division.

1 Introduction

Now, data and communications are omnipresent. The problems of security have come to assume an unprecedented importance. Cryptography is the approach to protect data secrecy in public environment. Both classical cryptosystems and quantum cryptography can solve the problems of security. However, the latter has shown the advantage of higher security because of the strong security basis assured by physical principles. Therefore, quantum cryptography has attracted a great deal of attention now.

Quantum cryptography, such as quantum key distribution (QKD) [Bennett and Brassard (1984)], quantum secure direct communication (QSDC) [Long and Liu (2002)], quantum identity authentication (QIA) [Dusek, Haderka, Hendrych et al. (1999)], quantum secret

[1] College of Information Security Engineering, Chengdu University of Information Technology, Chengdu, 610225, China.

[2] School of engineering and technology, University of Hertfordshire, Hertford, UK.

[*] Corresponding Author: Yan Chang. Email: cyttkl@cuit.edu.cn.

CMC. doi:10.32604/cmc.2019.06297 www.techscience.com/cmc

sharing (QSS) [Hillery, Buzek and Berthiaume (1999)], quantum signature (QS) [Yang, Lei and Liu (2016)], quantum private query (QPQ) [Gao, Qin, Huang et al. (2019); Wei, Cai, Liu et al. (2018); Gao, Liu, Huang et al. (2015)] provide unconditional security in theory, since the security is assured by the quantum mechanics principles rather than difficulty of computation. Entanglement swapping is a special property of entanglement states, which entangles two quantum systems that originate from independent source and do not share any common past. Entanglement swapping as an important characteristic of entangled particles has been widely used in constructing quantum repeaters and many other -quantum cryptographic protocols. By using EPR pairs and entanglement swapping, [Zhang and Man (2004)] presented DQSDC schema. Later, Wang et al. [Wang, Zhang and Tang (2007)] put forward QSDC schema and multiparty QSS protocol also by using EPR pairs and entanglement swapping. Alexander et al. [Alexander, Claudia and Zhang (2008)] proposed multistage entanglement swapping, which was used as quantum repeater, improved the distance of quantum transmission.

Privilege management infrastructure (PMI) is an application to provide authorization service management. In classical network, authorization is the act of verifying that a user is allowed to access a resource, which confirms that a user has a permission to carry out an action, such as to gain access to a specific online resource. In fact, privilege management (authorization management) includes authentication and authorization. Authentication is to verify a user's identity. Authorization is the process of verifying that an authenticated user has the authority to perform an operation, it is more fine-grained [Mark (2005)]. In most classical schemes, the authority management center (AMC) manages the resources permissions for all network nodes within the jurisdiction. If the user Alice wants to access the resources of the owner node Bob, Alice must issue a request to the AMC. The AMC will confirm the identity of Alice, then with the help of AMC, Bob and Alice share a key for accessing resources. However, the existence of AMC may likely be the weakest link of the whole scheme.

Quantum authorization management (QAM) is the quantum scheme for PMI problem. At present, the relevant reports are very few. Zhang et al. [Zhang, Xu, Tang et al. (2007)] proposed a simple quantum authorization scheme, which is a quantum scheme of password passing in basic digest authorization scheme. In Zhang's scheme, the user either can access all the resources of the owner, or they can access none. This is a coarser-grained rights division. They do not divide the rights further. Akshata et al. [Akshata, Srikanth and Srinivas (2014)] put forward a multipartite protocol in a counterfactual paradigm, which is essentially a quantum scheme of certificate authorization (CA) in e-commerce. In Akshata's protocol a semi-honest third party is introduced. Alice issues certificates in the form of digital signatures and public-private keys.

In our protocol, we propose a quantum authorization management (QAM) scheme based on entanglement swapping. Bob (the owner of resources) authenticates the legality of Alice (the user) and then shares the right key for the resources with Alice. Compared with the other two QAM protocols [Zhang, Xu, Tang et al. (2007); Akshata, Srikanth and Srinivas (2014)], our protocol not only implements authentication, but also authorizes the user permissions to access certain resources or carry out certain actions. Our authority division is more detailed (fine-grained rights division). We analyze our security from the four aspects: the outsider's attack, the user's attack, authentication and comparison with the other two QAM protocols.

2 The description of the protocol

On assumption that, M resources are included in Bob's site, each resource can be denoted as binary string $X_i^L=\{x_1, x_2, ..., x_L\}$ with length L, where $x_L \in \{0, 1\}$, $i=\{1, 2, ..., M\}$; Bob maintains a list of resource access rights for each user, while Bob has the identity information of each user. Alice is one of the user with identity information $\mathrm{ID_A}$ (a binary string), she can access the resources X_i^L and X_j^L. Our idea is to help Bob confirm the identity of Alice and distribute a pair of secret key between Alice and Bob which is known completely to Bob and partly to Alice. Here we define Bob's key as $K^M=\{K_1^L, K_2^L, ..., K_M^L\}$, where $K_i^L=\{k_1, k_2, ..., k_L\}$, $k_L \in \{0, 1\}$. Then Alice's key should be K_i^L and K_j^L. The scheme is to help them to complete the task safely.

To start with, we describe entanglement swapping of EPR pairs simply. Suppose that $|0\rangle$ and $|1\rangle$ are the horizontal and vertical polarization states of a photon, respectively. Four Bell states are represented as

$$\left|\phi^{\pm}\right\rangle=\frac{1}{\sqrt{2}}(\left|00\right\rangle\pm\left|11\right\rangle)$$

$$\left|\psi^{\pm}\right\rangle=\frac{1}{\sqrt{2}}(\left|01\right\rangle\pm\left|10\right\rangle) \tag{1}$$

Suppose that photon pairs 1 and 2, 3 and 4 are in $\left|\psi^{+}\right\rangle$ states. The following equation holds:

$$\left|\psi^{+}\right\rangle_{12}\otimes\left|\psi^{+}\right\rangle_{34}=\frac{1}{2}(\left|\phi^{+}\right\rangle_{32}\left|\phi^{+}\right\rangle_{14}-\left|\phi^{-}\right\rangle_{32}\left|\phi^{-}\right\rangle_{14}+\left|\psi^{+}\right\rangle_{32}\left|\psi^{+}\right\rangle_{14}+\left|\psi^{-}\right\rangle_{32}\left|\psi^{-}\right\rangle_{14}) \tag{2}$$

If we perform Bell basis measurements on the photon pair 2 and 3, photon pair 1 and 4 entangles. For example, if the measurement result is $\left|\phi^{+}\right\rangle_{32}$ ($\left|\phi^{-}\right\rangle_{32}$, $\left|\psi^{+}\right\rangle_{32}$ or $\left|\psi^{-}\right\rangle_{32}$), the state of photon pair 1 and 4 is $\left|\phi^{+}\right\rangle_{14}$ ($\left|\phi^{-}\right\rangle_{14}$, $\left|\psi^{+}\right\rangle_{14}$ or $\left|\psi^{-}\right\rangle_{14}$). The entanglement swapping characteristic is also workable for multi-EPR-pairs.

Step 1. Bob prepares a series of Bell states $\left|\psi^{+}\right\rangle_{12}$ and $\left|\psi^{+}\right\rangle_{34}$. All particle 1 (particle 2) in $\left|\psi^{+}\right\rangle_{12}$ states compose particle 1 (particle 2) sequence. All particle 3 (particle 4) in $\left|\psi^{+}\right\rangle_{34}$ states compose particle 3 (particle 4) sequence. Then Bob sends particle 1 sequence to Alice, and retains particles 2, 3 and 4 sequence in his own hand.

Step 2. Bob measures all particle pairs 2 and 3 with Bell basis, and records the measurement results. By doing so, all particle pairs 1 and 4 entangle.

Step3. Bob chooses a random subset U_{BT4} of particle 4 sequence and tells Alice the positions. Particles 1 at the corresponding positions form subset U_{AT1} . Particles in U_{BT4} and U_{AT1} compose a random subset U_T of EPR pairs. These EPR pairs are used to detect the entanglement of EPR pairs that Alice and Bob share. Bob measures particles in U_{BT4} with $B_0 = \sigma_Z$ or $B_1 = \sigma_X$ basis randomly. Alice measures particles in U_{AT1} with $A_0 = (\sigma_Z + \sigma_X)/\sqrt{2}$ or $A_1 = (\sigma_Z - \sigma_X)/\sqrt{2}$ basis randomly. Alice and Bob announce their basis/measurement-result pairs in U_T . We define $x = \{0,1\}$ as binary input of Alice's device, where $x = 0$ and $x = 1$ denote the measurement basis A_0 and A_1 respectively; $y = \{0,1\}$ is defined as binary input of Bob's device, where $y = 0$ and $y = 1$ denote the measurement basis B_0 and B_1 respectively. We define $a = \{0,1\}$ and $b = \{0,1\}$ as the binary outputs of Alice and Bob respectively. Bob calculates the CHSH polynomial $S = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle$, Where the $\langle a_x b_y \rangle$ is defined as $P(a = b \mid xy) - P(a \neq b \mid xy)$ ($P(a \neq b \mid xy) - P(a = b \mid xy)$) if the joint state of particles 2 and 3 is $\left|\phi^{\pm}\right\rangle_{32}$ ($\left|\psi^{\pm}\right\rangle_{32}$). As analyzed in [Pironio, Acin, Brunner et al. (2009)], the qubit measurements σ_Z , $(\sigma_Z - \sigma_X)/\sqrt{2}$, $(\sigma_Z + \sigma_X)/\sqrt{2}$ and σ_X maximize the CHSH polynomial for Bell states. Therefore, if the results violate the CHSH inequality ($S \leq 2$), Bob thinks that they share the correct entangled states, Bob continues to implement the protocol. These particles for eavesdropping detection in U_T and the corresponding particles 2 and 3 are discarded. Otherwise, it is indicated that the particle pairs are not correct entangled pairs, so Bob terminates the protocol.

By detecting in this step, even if the source and measuring equipment are completely controlled by Eve or provided by Eve, we can find whether the particles 1 and 4 that Alice and Bob share are in the correct entangled states. Then, in the following steps, because of_monogamy of non-local correlations, Bob can confirm the identity of Alice correctly and a pair of keys used for accessing resources with correct right can be distributed between Alice and Bob securely.

Step 4. Bob verify the identity of Alice by means of quantum teleportation. The detailed procedure is as follows:

(1) Alice prepares a single photon sequence S_{IDA} according to ID_A (identity information of Alice), the rule is: if the *i*th bit of ID_A is 0, Alice prepares $|0\rangle$ state, otherwise Alice prepares $|1\rangle$ state.

(2) Alice chooses some particles from particle 1 sequence randomly, and performs Bell basis measurement on particles in S_{IDA} and particles she chooses from particle 1 sequence.

(3) Alice publishes the positions she chooses and the corresponding measurement results. Then Bob can recover S_{IDA} on particle 4 sequence by performing unitary operations on particles 4 according to Alice's measurement results. For example, if the *i*th measurement

result of Alice is $\left|\phi^{+}\right\rangle_{4S_{IDA}^{i}}$ ($\left|\phi^{-}\right\rangle_{4S_{IDA}^{i}}$, $\left|\psi^{+}\right\rangle_{4S_{IDA}^{i}}$,$\left|\psi^{-}\right\rangle_{4S_{IDA}^{i}}$), Bob performs unitary operation $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ ($\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$, $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$) on the *i*th particle 4, by doing so Bob teleports the state of the *i*th particle in S_{IDA} on the *i*th particle 4.

(4) Bob measures S_{IDA} (he recovered in (3)) in Z basis and converts it to binary sequence ID'_A, the rule is: If the Bell basis measurement result of particle 2 and 3 in step 2 is $\left|\phi^{+}\right\rangle_{32}$ or $\left|\phi^{-}\right\rangle_{32}$, Bob uses $|0\rangle$ to denote 0，and $|1\rangle$ to denote 1; otherwise, he uses $|0\rangle$ to denote 1，and $|1\rangle$ to denote 0 .

(5) By comparing ID'_A and ID_A, Bob can know Alice is legitimate or not.

If Alice is legitimate, Alice and Bob discard the EPR pairs they used to verify the identity of Alice, and the protocol continues.

Step 5. Alice and Bob randomly select Z-basis or X-basis to measure particles 4 and 1 respectively. Alice and Bob publish their measurement basis one particle by one particle, until they have 2*L* pairs of particles with the same basis, then Alice and Bob stop publishing the measurement basis. Alice and Bob record the measurement basis and measurement results of the 2*L* pairs respectively.

Step 6. Alice and Bob drop the EPR pairs that have been measured. Then Alice and Bob convert the 2*L* measurement result pairs to binary string keys K_i^L and K_j^L , where K_i^L ={k_1, k_2, ..., k_L}, k_L∈ {0, 1}. The detailed process is as follows:

According to the Bell basis measurement results of particles 2 and 3 at the 2*L* positions which are obtained in Step 2, Bob can infer each other's measurement results. For example, if the state of 2-3 pair is $\left|\phi^{+}\right\rangle_{32}$ ($\left|\phi^{-}\right\rangle_{32}$), Bob infers that the state of 1-4 pair is $\left|\phi^{+}\right\rangle_{14}$ ($\left|\phi^{-}\right\rangle_{14}$), then Bob knows that his measurement result is the same with Alice's result, thus he records his result as k_i,*i*∈ {1,...2*L*}, k_i∈ {0, 1} (the rule: $|0\rangle$ or $|+\rangle$ denote 0， $|1\rangle$ or $|-\rangle$ denote 1); otherwise Bob knows that his measurement result is contrary to Alice's result, thus he records his result as $\overline{k_i}$.

According to the rule: $|0\rangle$ or $|+\rangle$ denote 0， $|1\rangle$ or $|-\rangle$ denote 1, Alice also records her results as k_i,*i*∈ {1,...2*L*}, k_i∈ {0, 1}. By doing so, Alice and Bob share a raw key {k_1, k_2, ..., k_{2L}} with length 2*L*. Bob and Alice divide the raw key {k_1, k_2, ..., k_{2L}} into two parts, each with length *L*. Then, Alice and Bob know K_i^L ={k_1, k_2, ..., k_L} and K_j^L ={k_{1+L}, k_{2+L}, ..., k_{2L}}, k_i∈ {0, 1}.

Step 7. Bob divides his remaining measurement results into *M*-2 parts, each part has *L* results. According to the rule: $|0\rangle$ or $|+\rangle$ denote 0， $|1\rangle$ or $|-\rangle$ denote 1, Bob converts the *M*-2 parts into *M*-2 binary string keys K^{M-2} ={ K_1^L , K_2^L , ... , K_{M-2}^L }, each key with length *L*. Then Bob inserts K_i^L and K_j^L in front of the *i*th and *j*th key in K^{M-2}

respectively. So far, Alice and Bob have shared a set of keys K^M ={ K_1^L, K_2^L, ... , K_M^L }, which is known completely to Bob and only the *i*th and *j*th keys to Alice. Then Bob encrypts his resources with the secret keys K_1^L, K_2^L, ..., K_M^L in order, Alice can only access the *i*th and *j*th resources.

3 Security analysis

3.1 The outsider's attack

First of all, the outsider eavesdropper Eve cannot attack successfully by providing not perfect quantum carriers (EPR pair) [Wang, Yang and Mousoli (2018)] when she provides or controlling the equipment. The reason lies in: If Eve provides not perfect EPR pairs, Alice and Bob will find her behavior by checking the violation of CHSH inequality in Step 3.

Secondly, in our protocol, the illegal user Eve cannot pass the identity authentication in Step 4, therefore the protocol will not distribute right key for him.

Thirdly, the identity of Alice is passed to Bob by means of quantum teleportation, which ensures the validity of authentication and absolute security of the identity, therefore the identity can be reused securely.

3.2 Alice's attack

In a secure quantum authorization management protocol, Alice is not wanted to access additional resources outside of her rights. Then the purpose of Alice's attack is to try to access additional resources.

If Alice is untrustworthy, she can collaborate with Eve, or they are the same person. In this case, Alice will provide untrustworthy devices and try to trick Bob by sending him pure states. However, if Alice sends Bob pure states, the CHSH inequality violation check of Bob in Step 3 will fail, then Alice's behavior is found by Bob, which leads to a termination of the protocol. Furthermore, Alice cannot publish unreal inputs and outputs in Step 3 to escape the CHSH check of Bob, because the Bell basis measurement in Step 2 will lead to four states $\left|\phi^+\right\rangle_{32}, \left|\phi^-\right\rangle_{32}, \left|\psi^+\right\rangle_{32}$ or $\left|\psi^-\right\rangle_{32}$ with equal probability 1/4, Alice does not know the state of each new EPR pair after entanglement swapping. That is to say, Alice does not know the relationship between particle 1 and 4. Therefore, wrong publishing of inputs and outputs of Alice will lead to failure of CHSH inequality violation check of Bob, which also results in a termination of the protocol.

To know more keys in K^{M-2}, Alice may perform individual attack. For example, in Step 5 Alice measures particles dishonestly in $\{|0'\rangle, |1'\rangle\}$ basis. Here,

$$|0'\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$$

$$|1'\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle \quad (3)$$

By doing so, Alice can bias the measurement result of Bob. After Alice's dishonest measurement, Bob's corresponding particles collapse into state $|0'\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$ or $|1'\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle$. For each particle, the probabilities that Bob obtains results $|+\rangle$ or $|-\rangle$ are $(1+\sin 2\theta)/2$ or $(1-\sin 2\theta)/2$ respectively; the probabilities that Bob obtains results $|0\rangle$ or $|1\rangle$ are $\cos^2\theta$ or $\sin^2\theta$ respectively. Because in Step 5, Bob does not publish the measurement basis of the remaining (*M*-2)*L* particles, Alice guesses right the basis of each particle with probability 1/2. Alice will record the state with larger probability as Bob's measurement result. For example, if Alice guesses the measurement basis of Bob is X-basis, and $(1+\sin 2\theta)/2 > (1-\sin 2\theta)/2$ is satisfied, Alice will record $|+\rangle$ as Bob's measurement result. However, because Alice does not know the relationship between particle 1 and 4, she cannot infer Bob's key. Therefore , if Alice guesses the measurement basis of Bob is X-basis, the probability that Alice knows one bit of K_i^L is $p = (1+\sin 2\theta)/4$ when $(1+\sin 2\theta)/2$ > $(1-\sin 2\theta)/2$ is satisfied; and is $p = (1-\sin 2\theta)/4$ when $(1-\sin 2\theta)/2 > (1+\sin 2\theta)/2$ is satisfied; if Alice guesses the measurement basis of Bob is Z-basis, the probability that Alice knows one bit of K_i^L is $p = \cos^2\theta/2$ when $\cos^2\theta$ > $\sin^2\theta$ is satisfied; and is $p = \sin^2\theta/2$ when $\sin^2\theta$ > $\cos^2\theta$ is satisfied. Obviously the four probability $p = (1+\sin 2\theta)/4$, $p = (1-\sin 2\theta)/4$, $p = \cos^2\theta/2$ and $p = \sin^2\theta/2$ are all less than 1/2. Therefore, the probability that Alice obtains the key K_i^L is less than $\frac{1}{2^L}$. That is to say, through this attack, Alice cannot get a better result than guess. The probability that the eavesdropper guesses right the key K_i^L is $\frac{1}{2^L}$. When *L*=4, $\frac{1}{2^L}$=0.0625, that is to say, when $L \geq 4$, the probability that the eavesdropper guesses right the key K_i^L is close to zero.

Furthermore, this attack will lead to error bits which contribute a key for Alice, and thus Alice's key is inconsistent with Bob, which will cause Alice fails to access resources X_i^L and X_j^L. Therefore, we think that the user Alice will not cheat to access extra resources at the cost of getting failed access of resources X_i^L and X_j^L.

3.3 The analysis of authentication

Bob kept the binary identity information of Alice (ID$_A$) in advance. When Bob authenticates the identity of Alice, the identity information is converted to single phone sequence and passed to Bob by means of quantum teleportation, which ensures the validity of authentication and absolute security of the identity information, so that the identity information can be reused securely.

3.4 Comparison with the other two QAM protocols

In Tab.1, we compare our protocol with the other two QAM protocols [Zhang, Xu, Tang et al. (2007); Akshata, Srikanth and Srinivas (2014)].

Table 1: The comparison of our protocol with the other two QAM protocols

	[Zhang, Xu, Tang et al. (2007)]	[Akshata, Srikanth and Srinivas (2014)]	Our protocol
Quantum carrier	Single photons	Single photons	Bell state
Whether the user is assumed to be a legitimate user has been certified	Yes	Yes	No
The resources a user can access within one authorization	All resurces in Bob's site (coarse-grained rights)	All resurces in Bob's site (coarse-grained rights)	Some resources in Bob's site, such as K_i^L and K_j^L (fine-grained rights)
Whether the semi-honest third parity is needed?	No	Yes	No
Whether the side-channel attack of Eve is resisted?	No	No	Yes

In Zhang et al. [Zhang, Xu, Tang et al. (2007)], Alice is an authenticated user of a server Bob. Alice is supposed to have shared a key with Bob previously. Bob does the authorization checking. Once Alice passes Bob's authorization checking, she can access all resouces at Bob's site. It is a coarse-grained rights division. Zhang et al. [Zhang, Xu, Tang et al. (2007)] can implement authorization checking without the help of the semi-honest third party. However, if Eve controls or provides the source and equipment, the side-channel attack of Eve cannot be resisted.

In Akshata et al. [Akshata, Srikanth and Srinivas (2014)], Alice is supposed to be an authenticated user in advance. With the help of the semi-honest third party, Alice and Bob share a key. Therefore, Akshata et al. [Akshata, Srikanth and Srinivas (2014)] is a quantum key distribution scheme in essence. If Eve controls or provides the source and equipment, the side-channel attack of Eve also cannot be resisted.

In our protocol, Alice is not supposed to be an authenticated user in advance. Bob does the authentication checking firstly. Then Alice and Bob share a pair of secret keys which is known completely to Bob but partly to Alice. Our protocol can implement authentication and fin-grained rights division without the help of the semi-honest third party. Furthermore, because of the checking of CHSH's inequality violation, even if Eve controls or provides the source and equipment, the side-channel attack of Eve can be resisted.

4 Conclusion

Here, the protocol has extended the authority division to fin-grained rights division. The protocol not only implements authentication, but also authorizes the user permission to access certain resources. Security of the protocol have been analyzed against the user's attack and outsider's attack.

Acknowledgments: This work is supported by NSFC (Grant Nos. 61572086, 61402058), the Application Foundation Project of Sichuan Province of China (Grant No. 2017JY0168), the National Key Research and Development Program (No. 2017YFB0802302), Sichuan innovation team of quantum security communication (No. 17TD0009), Sichuan academic and technical leaders training funding support projects (No. 2016120080102643), the Fund for Middle and Young Academic Leaders of CUIT (Grant No. J201511).

References

Akshata, S. H.; Srikanth, R.; Srinivas, T. (2014): Counterfactual quantum certificate authorization. *Physics Review A*, vol. 89, no. 5, pp. 1-6.

Alexander, M. G.; Claudia, W.; Zhang, Q.; Chen, Y. A.; Chen, K. et al. (2008): Multistage entanglement swapping. *Physical Review Letters*, vol. 101, no. 8, pp. 1-5.

Bennett, C. H.; Brassard, G. (1984): Quantum cryptography: public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175-179.

Dusek, M.; Haderka, O.; Hendrych, M.; Republic, C. (1999): Quantum identification system. *Physics Review A*, vol. 60, no. 1, pp. 149-156.

Gao, F.; Qin, S. J.; Huang, W.; Wen, Q. Y. (2019): Quantum private query: a new kind of practical quantum cryptographic protocols. *Science China Physics, Mechanics & Astronomy*, vol. 62, no. 7, pp. 1-12.

Gao, F.; Liu, B.; Huang, W.; Wen, Q. Y. (2015): Postprocessing of the oblivious key in quantum private query, *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 98-108.

Hillery, M.; Buzek, V.; Berthiaume, A. (1999): Quantum secret sharing. *Physics Review A*, vol. 59, no. 3, pp. 1829-1834.

Long, G. L.; Liu, X. S. (2002): Theoretically efficient high-capacity quantum-key-distribution scheme. *Physics Review A*, vol. 65, no. 3, pp. 1-4.

Mark, S. (2011): *Information Security: Principles and Practice.* Wiley, San Jose State University.

Pironio, S.; Acin, A.; Brunner, N.; Gisin, N.; Massar, S. et al. (2009): Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, vol. 11, no. 4, pp. 1-25.

Wang, J.; Zhang, Q.; Tang, C. J. (2007): Quantum secure communication protocols based on entanglement swapping. *Journal of National University of Defense Technology*, vol. 29, no. 2, pp. 56-60.

Wang, M. M.; Yang, C.; Mousoli, R. (2018): Controlled cyclic remote state preparation of arbitrary qubit states. *Computers, Materials & Continua*, vol. 55, no. 2, pp. 321-329.

Wei, C. Y.; Cai, X. Q.; Liu, B.; Wang, T. Y.; Gao, F. (2018) A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure, *IEEE Transactions on Computers*, vol. 67, no. 1, pp. 2-8.

Yang, Y. G.; Lei, H.; Liu, Z. C. (2016): Arbitrated quantum signature scheme based on cluster states. *Quantum Information Processing*, vol. 15, no. 6, pp. 2487-2497.

Zhang, Z. J.; Man, Z. X. (2004): Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations. arXiv:0403218v1.

Zhang, X. W.; Xu, X. W.; Tang, K.; Kwan, A. C. (2007): A simple secure quantum authorization scheme. *Proceedings of SPIE-the International Society for Optical Engineering.*