 CMC, vol.59, no.2, pp.635-648, 2019

Message Authentication with a New Quantum Hash Function

Yalan Wang[1, 2], Yuling Chen[1, *], Haseeb Ahmad[3] and Zhanhong Wei[4]

Abstract: To ensure the security during the communication, we often adopt different ways to encrypt the messages to resist various attacks. However, with the computing power improving, the existing encryption and authentication schemes are being faced with big challenges. We take the message authentication as an example into a careful consideration. Then, we proposed a new message authentication scheme with the Advanced Encryption Standard as the encryption function and the new quantum Hash function as the authentication function. Firstly, the Advanced Encryption Standard algorithm is used to encrypt the result of the initial message cascading the corresponding Hash values, which ensures that the initial message can resist eavesdropping attack. Secondly, utilizing the new quantum Hash function with quantum walks can be much more secure than traditional classical Hash functions with keeping the common properties, such as one-wayness, resisting different collisions and easy implementation. Based on these two points, the message authentication scheme can be much more secure than previous ones. Finally, it is a new way to design the message authentication scheme, which provides a new thought for other researchers in the future. Our works will contribute to the study on the new encryption and authentication functions and the combination of quantum computing with traditional cryptology in the future.

Keywords: Message authentication, symmetric encryption, quantum Hash function, quantum walk.

1 Introduction

Nowadays, we are absorbed in a world where most information can be obtained on the internet. The point-to-point quantum communication is being changed to the multi-party quantum network communication. A wide range of research meanings are focused on this problem in some network structures [Guo, Zhang and Liu (2017); Pang, Liu, Zhou et al. (2017); Li, Wang, Li et al. (2018); Shen, Song, Li et al. (2018).]. Regarding the quantum networks, the feasibility and construction have been fully researched theoretically [Dong, Zhang and Zhang et al. (2014); Jiang, Jiang and Ling (2014)]. Therefore, the security of

[1] GuiZhou University, State Key Laboratory of Public Big Data, GuiZhou Guiyang, 550025, China.

[2] Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China.

[3] Department of Computer Science National Textile University, Faisalabad, 37610, Pakistan.

[4] College of Information Engineering, Beijing Institute of Petrochemical Technology, Beijing, 102617, China.

[*] Corresponding Author: Yuling Chen. Email: ylchen3@gzu.edu.cn.

information is paid so much attention during communication. There are many different ways to improve the security of the transmitted messages during communication. In information security, authentication [Needham and Schroeder (1978); Krawczyk, Bellare and Canetti (1997)] is one way of resisting active attacks, which plays an important role in various communication systems.

In general, there are two types of authentication, which are entity authentication [Bellare and Rogaway (1993)] and message authentication [Krawczyk, Bellare and Canetti (1997); Tsudik (1992)]. The purpose of entity authentication is to verify the identity of the sender during communication. However, we can also use the message authentication to confirm the information source and integrity of the messages. In this manuscript, we will not give more details about the entity authentication. On the contrary, we will attach our importance to the message authentication.

In the message authentication, we adopt a technology to realize the message authentication, which is called Message Authentication Code (MAC) [Bernstein (2005)]. Using this technology, the message can be transformed to a data block with the shared keys between the sender and receiver through the authentication function, the length of which is determinate. Thereafter, we cascade the data block to the message. Based on the feature of the Message Authentication Code, Hash functions are often the first choice to act as the authentication function. In classical cryptography [Vignesh, Sudharssun and Kumar (2009)], hash function [Coron, Dodis, Malinaud et al. (2005)] is an important branch. Arbitrary input can be transformed into the output whose length is fixed through the Hash function. Therefore, Hash function can compress the message which is a one-way function. Nowadays, there are many different concrete algorithms called Hash function, such as MD5 [Rivest (1992)], SHA1 [Eastlake 3rd and Jones (2001)], SHA256 [Wolrich, Yap, Guilford et al. (2014)] and SHA512 [Gueron, Johnson and Walker (2011)]. These Hash algorithms have some in common that the input is always divided into some blocks at the beginning of the scheme. As the computing power improves, existing Hash algorithms have difficulties in resisting various attacks.

Considering the above problems, we try to introduce quantum Hash functions to work as authentication function to improve security during communication. Due to the Shor's algorithm and Grover's search algorithm, quantum information processing develops so fast. In addition, there is a memory-efficient simulation method of this algorithm [Tang, Xu and Duan (2018)]. Nowadays, quantum information processing are developing so fast, including quantum network coding [Li, Chen, Xu et al. (2015); Xu, Chen, Li et al. (2015)], quantum key management [Xu, Chen, Duo et al. (2015); Liu, Xu, Yang. et al (2018)], quantum secret sharing [Chen, Tang, Xu et al. (2018)], quantum remote state preparation [Xu, Chen, Dou et al. (2016); Chen, Sun, Xu et al. (2014); Qu, Wu, Wang et al. (2017)], quantum information hiding [Wei, Chen, Niu et al. (2015); Qu, Cheng, Liu et al. (2018); Qu, Chen, Ji et al. (2018)], quantum multi-party computation[Liu, Wang, Yuan et al. (2016)] and quantum relief algorithm[Liu, Gao, Yu et al. (2018)]. Quantum Hash function is supposed to have better performance than classical Hash function in execution and security. Recently, many researchers proposed their quantum Hash function schemes. In 2013, Li et al. [Li, Zhang, Guo et al. (2013)] put forward a kind of quantum Hash scheme based on the two-particle interacting quantum walk. This kind of

quantum Hash scheme can be executed in classical computer and practical but still need to be improved in some aspects. In 2018, Li et al. [Li, Yang, Bi et al. (2018)] presented a kind of quantum Hash function based on two-particle controlled interacting quantum walks. This quantum Hash function guarantees the security of hash function by infinite possibilities of the initial state and the irreversibility of measurement rather than hard mathematic problems. Therefore, this Hash function has better performance than the Hash scheme in Li et al. [Li, Zhang, Guo et al. (2013)]. Lately, Yang et al. [Yang, Bi, Chen et al. (2018)] proposed the latest Hash scheme by introducing alternate single-qubit coin operators into discrete-time quantum walk. In addition, they showed that the implementation of this Hash function is simpler than previous quantum Hash functions. Moreover, this Hash function has a variable output length to meet the needs of various security levels desired among different applications.

As we described, the quantum Hash function has much better performance than previous classical Hash function used in the message authentication. However, if the initial message is cascaded to the hash values without any additional operations, this message authentication will be faced with eavesdropping attacks. In order to settle this problem, the Advanced Encryption Standard (AES) [Zeghid, Machhout, Khriji et al. (2007)] algorithm is naturally introduced into this message authentication scheme. That is to say, we can use the AES algorithm to encrypt the results of the initial messages cascading the hash values. When the receiver receives the ciphertexts, receiver can execute the AES algorithm to get the initial message and corresponding hash values. With the AES algorithm added, the security of the initial message can be guaranteed.

All in all, in our paper, we use the AES algorithm to serve as the encryption function and the latest Hash scheme [Yang, Bi, Chen et al. (2018)] as the authentication function in our message authentication scheme. Firstly, the AES algorithm is used to encrypt the initial message and the hash values of the initial message, which ensures that the initial message can resist eavesdropping attacks. Secondly, utilizing the new quantum Hash function with quantum walks can be much more secure than traditional classical Hash functions with keeping the common properties like one-wayness, resisting different collisions and easy implementation. Based on these two points, the message authentication scheme can be much more secure than previous ones. Finally, the security level of the message authentication will be improved greatly. Our works can offer a new aspect for utilizing quantum hash function to the traditional classical cryptology to improve the security of communication.

The remaining layout of our manuscript is organized as below. Some basic knowledge involved in our scheme will be given in Section 2. We will describe the process of the message authentication in detail in Section 3. Then, some analyses about our scheme will be provided in Section 4. Finally, conclusions will be made in Section 5.

2 Preliminaries

In the message authentication, the encryption function is supposed to be reversible. Only in this way, can the receiver decrypts the ciphertext to get the plaintext after receiving the ciphertext. However, the authentication function must be one-way so that the message can be more secure.

2.1 Symmetric encryption algorithm

In the message authentication, the encryption function should be reversible. Therefore, we take the symmetric encryption scheme into account. We can use the same keys to encrypt and decrypt messages during the communication. Generally speaking, symmetric encryption consists of two types of encryption schemes, e.g., the block cipher and the sequential cipher (stream cipher). In our scheme, the block cipher will be focused. In block cipher scheme, firstly, the plaintext will be converted into a sequence of binary digits. Then, the sequence of binary digits will be partitioned to some equal-sized data blocks. Finally, every data block is supposed to be encrypted through some calculations with keys. This is the whole process of the block cipher scheme. All in all, when researchers design the block cipher schemes, two principles must be met, that is confusion and diffusion. Based on these two principles, the block cipher can efficiently resist the statistic analysis attacks. In our applications, there are two kinds of block cipher schemes, e.g., Data Encryption Standard (DES) [Mahajan and Sachdeva (2013)] and AES [Mahajan and Sachdeva (2013)].

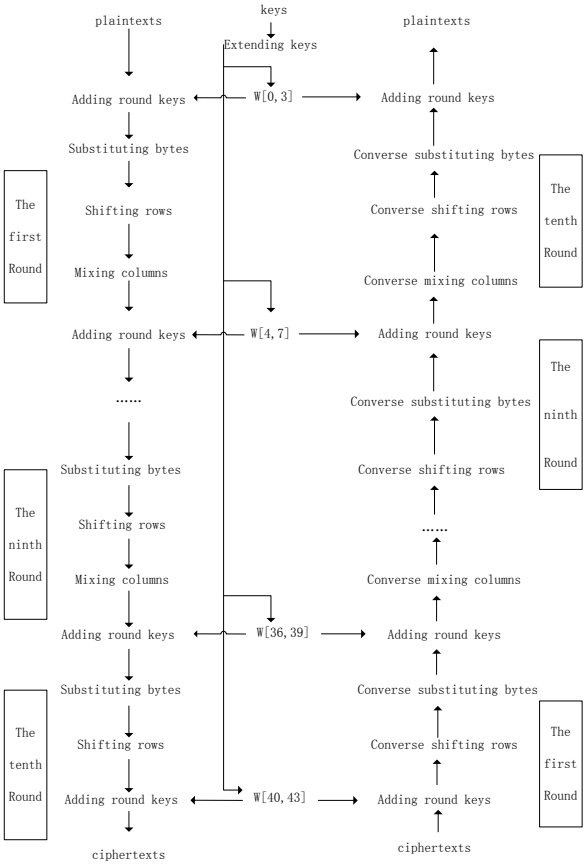

Figure 1: The process of one round of AES. We take the 10 rounds AES algorithm as an example

Considering the security requirement, we adopt the AES to work as the encryption function in our scheme. There are three types of AES structures according the length of data block and keys, e.g., the length of the data block is 128 bits and keys can be 128 bits, 192 bits or 256 bits, and 10 rounds, 12 rounds or 14 rounds for encryption, respectively. We choose the first one. There are four operations in every round, which are substituting bytes, shifting rows, mixing columns and adding round keys. The whole process of the AES is shown in Fig. 1.

We can learn about the process of the whole AES in Fig. 1. Here, we adopt the scheme of 10 rounds. However, there are some things worth noticing. In the last round, there is no mixing column operation. Additionally, before the first round, the plaintext and initial keys will be encrypted by through adding round keys.

2.2 Discrete-time quantum walk

In our paper, there is a notion involved in the quantum Hash function that is quantum walk. Quantum walk, as the counterpart of the classical random walk, has attracted as much as possible attention since proposed [Aharonov, Davidovich and Zagury (1993)]. In general, quantum walk is mainly divided as continuous-time quantum walk [Norio (2005)] and discrete-time quantum walk [Lovett, Cooper, Trevers et al. (2010); Rohde, Schreiber, Štefaňák et al. (2011)]. We attach the importance to the discrete-time quantum walk. Walkers are controlled by coin operators in the discrete-time quantum walk. Naturally, at the present, the number of walkers and coins is variable. There are two spaces, which are coin space denoted by $\mathcal{H}_c$ and walker space denoted by $\mathcal{H}_w$, respectively. Then, the whole space is the Hilbert space $\mathcal{H} = \mathcal{H}_c \otimes \mathcal{H}_w$. The movement of the walker is controlled by the conditional shift operator as follows:

$$S = \sum \left(|x+1\rangle\langle x| \otimes |0\rangle\langle 0| + |x-1\rangle\langle x| \otimes |1\rangle\langle 1| \right) \tag{1}$$

which displays the summation over all possible positions. The whole process is under the control of the coin flipping operator and the conditional shift operator S. The coin flipping operator is denoted by $I \otimes C$, in which I is the identity operator controlling the walker and C is the coin flipping operator applied to the coin state. On the circle, when we employ identity operator I, the walker will walk clockwise. Correspondingly, if the Pauli operator σ_x is employed on the circle, then, the walker will walk anticlockwise. The circumstances we describe are demonstrated in Fig. 2. In our literature, the one-coin one-walker quantum walk takes place on the circle, the node number of which is N.

(a) I σ_x

Figure 2: The possible directions of the walker walks on the circle. (a) The direction is clockwise under the control of the coin operator I. (b) The direction is anticlockwise under the control of the coin operator σ_x

2.3 Quantum Hash function

After giving simple descriptions about the block cipher schemes, in the following part, one-way Hash function will be described in detail. In choosing the authentication function, we pay our attention to the one-way quantum Hash function. After studying the Yang et al. [Yang, Bi, Chen et al. (2018)], the main properties of a Hash function are one-wayness, strong collision resistance and weak collision resistance. The properties of the quantum Hash function in Xu et al. [Xu, Chen, Duo et al. (2015)] are given as follows.

• One-wayness: given a message M , it is possible to compute the Hash value $h(M)$ while it is infeasible to deduce the initial message M with a given Hash value $h(M)$ computationally.

• Weak collision resistance: given a message M , it is infeasible to find another message M_1 computationally so that $h(M)=h(M_1)$.

• Strong collision resistance: it is infeasible to find arbitrary two different messages M and M_1 computationally so that $h(M)=h(M_1)$.

These three properties are main principles worth considering when adopting a Hash function. Compared with classical Hash function, quantum Hash function has more advantages, such as easy execution, higher level security. Introducing the quantum Hash function proposed in Yang et al. [Yang, Bi, Chen et al. (2018)], our message authentication scheme will be more secure. The detailed process of the quantum Hash function in Yang et al. [Yang, Bi, Chen et al. (2018)] is depicted as follows.

• Select the parameters $(n,\theta_1,\theta_2,\alpha)$ under the constraints: n is an odd number and $0<\theta_1,\theta_2,\alpha<\pi/2$. Here α is the parameter determining the initial coin state $|\upsilon\rangle=\cos\alpha|0\rangle+\sin\alpha|1\rangle$. n is the number of nodes on a cycle. Moreover, θ_1 and θ_2 are parameters of two coin operators controlling the quantum walk. The two coin operators are C_1 and C_2,

$$C_1=\begin{bmatrix}\cos\theta_1 & \sin\theta_1\\ \sin\theta_1 & -\cos\theta_1\end{bmatrix},\ C_2=\begin{bmatrix}\cos\theta_2 & \sin\theta_2\\ \sin\theta_2 & -\cos\theta_2\end{bmatrix} \tag{2}$$

The initial message bit “1” decides C_1 and “0” decides C_2.

• Run the one-coin one-walker discrete-time quantum walk on a cycle under the control of the message M and generate the probability distribution.

• Amplify all values in the resulting probability distribution by 10^j times and keep only their integer part modulo 2^k to form a binary string as the Hash value, with $j\geq k$. The bit length of the hash value is nk .

This is the process of the latest quantum Hash function scheme, whose security is higher than previous ones. Deservedly, we decide to adopt this quantum Hash function to be the authentication function.

3 The process of message authentication

In previous section, we have discussed the MAC. The DES with Cipher Block Chaining (CBC) model was often adopted into the message authentication in the past, which is defined CBC-MAC. However, recently, the hash function is taken to construct the corresponding MAC, which is called HAMC. One of the reasons is that the hash function can be executed easily and quickly. In this manuscript, we take a new kind of quantum hash function to work as the authentication function. We will give detailed descriptions about the general message authentication scheme and the explicit message authentication scheme we are going to take.

Firstly, we briefly introduce the process of the general message authentication scheme. In a general message authentication scheme, the initial message M will be encrypted with keys K using an encryption algorithm to get the ciphertexts $C(K,M)$. Thereafter, the sender Alice cascades the initial message M and the ciphertexts $C(K,M)$ to get the result $C(K,M)\|M$. Then, Alice sends the result $C(K,M)\|M$ to the receiver Bob. After receiving the result $C(K,M)\|M$, the receiver Bob uses the same keys K to encrypt the initial message M to get $C'(K,M)$. Finally, Bob compares the result $C(K,M)$ with the result $C'(K,M)$. If $C(K,M)=C'(K,M)$, the message M is not tampered and truly sent from the sender Alice, or the message authentication is invalid, that is to say, the initial message M may be tampered or not truly sent from the sender Alice. Finally, the whole process is shown in Fig. 3.

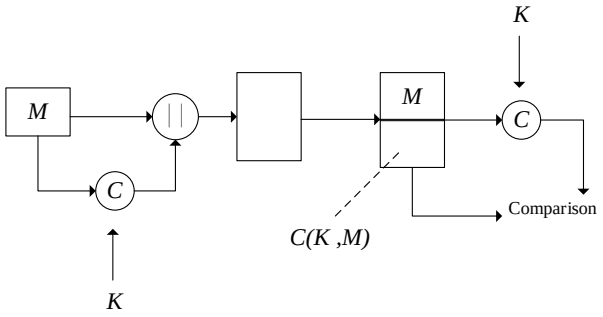

Figure 3: The general process of message authentication. M is the initial message which is going to be transferred from the sender to the receiver. C is the authentication function used to encrypt the initial message M. "||" is an operation used to cascade the initial message and the ciphertexts. The rectangular frame is used to stand for the channel during communication. K is the keys used to encrypt the initial message

In Fig. 3, we can learn about the general process of message authentication. After learning about the process of the general message authentication scheme, based on these knowledge, we do some adjustments to the general message authentication scheme. In the following parts, we will describe the process of the explicit message authentication scheme in detail. The process of our message authentication scheme is shown in Fig. 4.

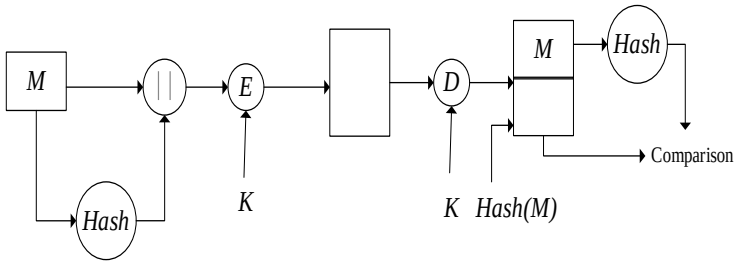

Figure 4: The process of explicit message authentication. M is the initial message which is going to be transferred from the sender to the receiver. *Hash* is the authentication function used to encrypt the initial message M. "||" is an operation used to cascade the initial message and the ciphertexts. The rectangular frame is used to stand for the channel during communication. K is the keys used to encrypt the initial message and decrypt the ciphertexts. E is the encryption operation. D is the decryption operation

As shown in Fig. 4, we can learn about the process of the explicit message authentication scheme in detail. In this process, the parameters of the one-way quantum Hash function are n, θ_1, θ_2 and α. n is the node number of a cycle which is an odd number. These descriptions about parameters are mentioned in Subsection 2.3. Here, we will not give too much descriptions about that. There are some differences between the general message authentication scheme and the explicit message authentication scheme. We choose a new kind of quantum Hash function into the explicit message authentication scheme to work as the authentication function. In addition, before transmitting the result of the initial message cascading the Hash values, we will use the AES algorithm to encrypt the result of the initial message cascading the Hash values, which can ensure the security of the initial message during the transmission. In the following, our message authentication scheme can be given by following steps.

• To begin with, we choose the appropriate values for parameters $(n,\theta_1,\theta_2,\alpha)$ and keys K pre-shared between the sender Alice and receiver Bob. The initial message M decides the coin operators to control the quantum walk. Then, we can get the possibility distribution to be transformed to quantum hash value $Hash(M)$.

• The sender Alice cascades the initial message M with the quantum Hash value $Hash(M)$ to get the result $M \| Hash(M)$. Considering the security of the initial message M, the block cipher algorithm AES is utilized to encrypt the result $M \| Hash(M)$ using keys K (generated by the pseudo-random number generator) to get the ciphertexts $E(K,[M \| Hash(M)])$. The sender Alice sends the ciphertexts $E(K,[M \| Hash(M)])$ through the channel (Assume that the channel is absolutely secure).

• After receiving the ciphertexts $E\left(K,[M \| Hash(M)]\right)$, the receiver Bob firstly uses the same keys K to decrypt the ciphertexts $E\left(K,[M \| Hash(M)]\right)$ with AES algorithm. Then, Bob adopts pre-shared parameters $(n,\theta_1,\theta_2,\alpha)$ to perform quantum Hash operation on the initial message M to get $Hash'(M)$. Finally, Bob compares the values of $Hash(M)$ with that of $Hash'(M)$. If $Hash(M)=Hash'(M)$, it is reasonable to believe that the initial message M is not forged or tampered and really sent from the sender Alice. However, if $Hash(M)\neq Hash'(M)$, it is reasonable to believe that the message M is forged or tampered or the message M is not sent by the sender.

This is the whole process of the explicit message authentication scheme. Note that in this message authentication scheme, on the one hand, AES algorithm works as the encryption function to ensure the security of the initial message M. In this way, can the scheme resist the passive attacks, such as eavesdropping attacks. On the other hand, we adopt the one-way quantum Hash function to serve as the authentication function to resist active attacks, such as forging or tampering the initial messages. Therefore, this message authentication scheme will be much more secure than the previous ones. After giving our detailed message authentication scheme, in the following parts, analyses for this message authentication scheme will be given.

4 Analyses

In this proposed message authentication scheme, the encryption function and authentication function are two main parts. So we decide to analyze our message authentication scheme from these two aspects in the following parts.

4.1 The encryption function

In this paper, we use the AES algorithm to be the encryption function. In the process of the message authentication scheme, after receiving the ciphertexts, the receiver Bob is going to decrypt the ciphertexts using the same encryption algorithm. Therefore, the encryption function should be reversible. And until now, it is no doubt that the AES algorithm is a better choice no matter from the security or the implementation. Even the length of the block data and keys are 64 bits and 56 bits, respectively, the DES algorithm still cannot meet the security requirements under the present circumstances. Therefore, we choose the AES algorithm to act as the encryption function in our message authentication scheme.

In AES algorithm, there are four important operations which are substituting bytes, shifting rows, mixing columns and adding round keys. Moreover, before the four operations, with the operation extending keys added, the security of AES is greatly improved. We mainly analyze the AES algorithm from four aspects, e.g., security, performance, space and implementation.

• As for the security of the AES algorithm, S box in the operation substituting bytes is non-linear and the operation mixing columns contributes to the diffusion of the AES

algorithm. Additionally, the complexity of all the four operations and the operation extending keys ensure the security of the AES algorithm.

• The performance of the AES algorithm is evaluated by how many attacks the algorithm can resists, encryption, decryption and keys used in the message authentication scheme. Firstly, the AES can resist the energy attack and timing attack. At the same time, the execution is not influenced. Then, the process of the encryption is not same with that of decryption. And the time to execute the encryption and decryption is very close. Finally, the length of the data block and keys can be selective for 128 bits, 192 bits and 256 bits. This displays that we can decide the data block and keys flexibly, which improve the security of the message authentication scheme. After these analyses, on the whole, the performance of the AES algorithm is much better than the previous symmetric algorithms.

• The steps for encryption are not same with that for decryption, therefore, the AES algorithm is suitable for the limited space and circumstances to execute encryption or decryption operations.

• On one hand, it is very convenient for the AES to be executed on different systems including the 8-bit, 64-bit and DSP. The built-in distribution mechanism can make better use of CPU resources. This is the advantages of the AES algorithm in software. On the other hand, in hardware, when adopted 128 bits for the length of data block and keys, time to execute the AES algorithm is extremely less than other symmetric algorithms. However, more rounds are needed if the length of the keys becomes larger. Then, we need more time to execute the AES algorithm, which means that we need more time to execute the message authentication scheme naturally. Honestly, this is a weakness of the AES algorithm.

Through these analyses, it is obvious that the AES algorithm is a relatively better choice to act as the encryption function in the message authentication scheme.

4.2 The authentication function

We have mentioned some advantages in previous sections so that the one-way quantum Hash function has better performance than one-way classical Hash function. In designing classical Hash message authentication code (HMAC), there are some principles to be considered, which are listed in RFC 2104. Though we adopt the quantum Hash function, the analyses are still similar to that of the classical Hash function.

• The quantum Hash function in the message authentication scheme should be easily implemented in corresponding software. In this message authentication scheme, the quantum Hash values are generated by the one-coin one-walker quantum walk. With classical computer, the process of quantum walk can be easily realized to get the corresponding Hash values. Therefore, our quantum Hash function has no difficulties in software implementation.

• It should be convenient and easy to apply the keys and operations involved in the Hash function. The main operation of the quantum Hash function is quantum walk, which can be easily executed in classical computer. As for the keys, parameters of the keys are $(n,\theta_1,\theta_2,\alpha)$ and K which are determined in the beginning without complex computation. So the keys and operations involved in this quantum Hash function can be realized easily.

• When designing the Hash function in the message authentication scheme, the properties of the Hash function should be kept. The quantum Hash function, proposed in Yang et al. [Yang, Bi, Chen et al. (2018)], still has basic properties. The quantum Hash function has properties of one-wayness, resistance to birthday attack, good avalanche effect and good sensitivity to the initial message M . In addition, the diffusion and confusion properties are still be kept shown in Yang et al. [Yang, Bi, Chen. et al (2018)]. In general, the essential properties of the classical Hash function are still kept in this quantum Hash function.

• If the security of the Hash function can be ensured, the security of the message authentication scheme will be guaranteed too. In a message authentication scheme, the security of the authentication function is greatly fundamental to the whole scheme. First, the initial state is infinite and the modular arithmetic is irreversible involved in the quantum Hash function. Second, on a classical computer, assuming N possible items of the set for the variables (N is infinite theoretically), it obviously takes $O(N)$ operations to determine the items. So it is computationally hard to find collision for this quantum Hash function. Finally, when generating the Hash values, we amplify the resulting probability distribution by 10^j times and keep only the integer part modulo 2^k . This makes the process irreversible because it is a many-to-one relationship. Based on these properties, it is reasonable to believe that the quantum Hash function is very secure.

Based on the above analyses, no matter from the performance or security, the one-way quantum Hash function is very suitable to be adopted in the message authentication scheme.

5 Conclusions

After the above discussions, we will give some conclusions about our message authentication scheme. In traditional message authentication scheme, there are two main functions called encryption function and authentication function, respectively. Generally speaking, the encryption function is reversible, however, the authentication function is irreversible. Based on these principles, considering the security and implementation of the whole message authentication scheme, we take the AES algorithm as the encryption function and a new kind of one-way quantum Hash function as the authentication function.

In existing circumstances, the AES algorithm is relatively secure than other symmetric encryption algorithms. More importantly for this paper, we adopt the quantum Hash function to serve as the authentication function for the first time. Due to the improvements to the computing power, existing encryption and authentication algorithms are being faced with big challenges. So it is a trend to try new and more secure encryption and authentication functions. The quantum Hash function based on the quantum walks is a good choice. The quantum Hash function has the common properties with classical Hash functions, such as irreversibility, sensitive to the initial message M and resisting different collisions. In addition, the quantum Hash function is implemented very easily on classical computer. Last but not least, the quantum Hash function is more secure than classical Hash functions. Because in the process of the one-way quantum Hash function, the initial states are infinite and some operations in the generation of the Hash values are non-linear. In conclusion, the quantum Hash function used in the

message authentication scheme makes this message authentication scheme absolutely more secure.

Every coin has two sides. The quantum Hash function maybe has some weakness left to be improved in the future, such as all-round security tests and mature applications. But it is worth believing that the quantum Hash function will be a good choice in wide application sooner or later.

Acknowledgement: Project supported by NSFC (Grant Nos. U1836205, 61702040), the Major Scientific and Technological Special Project of Guizhou Province (Grant No. 20183001), the Foundation of Guizhou Provincial Key Laboratory of Public Big Data (Grant No. 2018BDKFJJ016), the Foundation of State Key Laboratory of Public Big Data (Grant No. 2018BDKFJJ018) and Beijing Natural Science Foundation (Grant No. 4174089).

References

Aharonov, Y.; Davidovich, L.; Zagury, N. (1993): Quantum random walks. *Physical Review A*, vol. 48, pp. 1687.

Bernstein, D. J. (2005): The Poly1305-AES message-authentication code. *International Workshop on Fast Software Encryption*, pp. 32-49.

Bellare, M.; Rogaway, P. (1993): Entity authentication and key distribution. *Annual International Cryptology Conference*, pp. 232-249.

Coron, J. S.; Dodis, Y.; Malinaud, C.; Puniya, P. (2005): Merkle-Damgård revisited: how to construct a Hash function. *Annual International Cryptology Conference*, pp. 430-448.

Chen, X. B.; Tang, X.; Xu, G.; Dou, Z.; Chen, Y. L. et al. (2018): Cryptanalysis of secret sharing with a single d-level quantum system. *Quantum Information Processing*, vol. 17, pp. 225.

Chen, X. B.; Sun, Y. R.; Xu, G.; Jia, H. Y.; Qu, Z. et al. (2014): Controlled bidirectional remote preparation of three-qubit state. *Quantum Information Processing*, vol. 16, pp. 244.

Dong, H. H.; Zhang, Y. F.; Zhang, Y. F.; Yin, B. S. (2014): Generalized bilinear differential operators, binary bell polynomials, and exact periodic wave solution of boiti-leon-manna-pempinelli equation. *Abstract and Applied Analysis*, vol. 2014, pp. 1-6.

Eastlake 3rd, D.; Jones, P. (2001): *US Secure Hash Algorithm 1 (SHA1).* https://www.rfc-editor.org/rfc/rfc3174.txt.

Guo, R. N.; Zhang, Z. Y.; Liu, X. P. (2017): Existence, uniqueness, and exponential stability analysis for complex-valued memristor-based BAM neural networks with time delays. *Appllied Mathmatics and Computation*, vol. 311, pp. 100-117.

Gueron, S.; Johnson, S.; Walker, J. (2011): SHA-512/256. *Eighth International Conference on Information Technology: New Generations*, pp. 354-358.

Jiang, T.; Jiang, Z.; Ling, S. (2014): An algebraic method for quaternion and complex least squares coneigen-problem in quantum mechanics. *Appllied Mathmatics and Computation*, vol. 249, pp. 222-228.

Krawczyk, H.; Bellare, M.; Canetti, R. (1997): HMAC: Keyed-Hashing for message

authentication. https://www.rfc-editor.org/rfc/rfc2104.txt.

Li, D.; Yang, Y. G.; Bi, J. L.; Xu, J. (2018): Controlled alternate quantum walks based quantum Hash function. *Scientific Reports*, vol. 8, no. 1, pp. 225.

Li, D.; Zhang, J.; Guo, F. Z; Huang, W.; Wen, Q. Y. et al. (2013): Discrete-time interacting quantum walks and quantum Hash schemes. *Quantum Information Processing*, vol. 12, no. 3, pp. 1501-1513.

Li, J.; Chen, X. B.; Xu, G.; Yang, Y. Y.; Li, Z. P. (2015): Perfect quantum network coding independent of classical network solutions. *IEEE Communications Letters*, vol. 19, no. 2, pp. 115-118.

Li, L.; Wang, Z.; Li, Y. X.; Shen, H.; Lu, J. W. (2018): Hopf bifurcation analysis of a complex-valued neural network model with discrete and distributed delays. *Appllied Mathmatics and Computation*, vol. 330, pp. 152-169.

Liu, W. J.; Gao, P. P.; Yu, W. B.; Qu, Z. G.; Yang, C. N. (2018): Quantum relief algorithm. *Quantum Information Processing*, vol. 17, no. 10.

Liu, W. J.; Wang, H. B.; Yuan, G. L.; Xu, Y.; Chen, Z. Y. et al. (2016): Multiparty quantum sealed-bid auction using single photons as message carrier. *Quantum Information Processing*, vol. 15, no. 2, pp. 869-879.

Liu, W. J.; Xu, Y.; Yang, C. N.; Gao, P. P.; Yu, W. B. (2018): An efficient and secure arbitrary n-party quantum key agreement protocol using bell states. *International Journal of Theoretical Physics*, vol. 57, no. 1, pp. 195-207.

Lovett, N. B.; Cooper, S.; Trevers, M.; Kendon, V. (2010): Universal quantum computation using the discrete-time quantum walk. *Physical Review A*, vol. 81, no. 4, 042330.

Mahajan, P.; Sachdeva, A. (2013): A study of encryption algorithms AES, DES and RSA for security. *Global Journal of Computer Science and Technology*, vol. 13, no. 15.

Norio, K. (2005): Limit theorem for continuous-time quantum walk on the line. *Physical Review E*, vol. 72, no. 2, 026113.

Needham, R. M.; Schroeder, M. D. (1978): Using encryption for authentication in large networks of computers. *Communications of the ACM*, vol. 21, no. 12, pp. 993-999.

Pang, Z.; Liu, G.; Zhou, D. et al. (2017): Data-based predictive control for networked nonlinear systems with packet dropout and measurement noise. *Journal of Systems Science and Complexity*, vol. 30, pp. 1072-1083.

Qu, Z. G.; Chen, S. Y.; Ji, S.; Ma, S. Y.; Wang, X. J. (2018): Anti-noise bidirectional quantum steganography protocol with large payload. *International Journal of Theoretical Physics*, vol. 57, no. 6, pp. 1-25.

Qu, Z. G.; Cheng, Z. W.; Liu, W. J.; Wang, X. J. (2018): A novel quantum image steganography algorithm based on exploiting modification direction. *Multimedia Tools and Applications*, pp. 1-21.

Qu, Z. G.; Wu, S. Y.; Wang, M. M.; Sun, L.; Wang, X. J. (2017): Effect of quantum noise on deterministic remote state preparation of an arbitrary two-particle state via various quantum entangled channels. *Quantum Information Processing*, vol. 16, no. 306, pp. 1-25.

Rohde, P. P.; Schreiber, A.; Štefaňák, M.; Jex, I.; Silberhorn, C. (2011): Multi-walker discrete time quantum walks on arbitrary graphs, their properties and their photonic implementation. *New Journal of Physics*, vol. 13, no. 1, 013001.

Rivest, R. (1992): The MD5 message-digest algorithm. https://www.rfc-editor.org/rfc/rfc1321.txt.

Shen, H.; Song, X.; Li, F.; Wang, Z.; Chen, B. (2018): Finite-time L2-L1 filter design for networked Markov switched singular systems: a unified method. *Appllied Mathmatics and Computation*, vol. 321, pp. 450-462.

Tsudik, G. (1992): Message authentication with one-way Hash functions. *ACM SIGCOMM Computer Communication Review*, vol. 22, no. 5, pp. 29-38.

Tang, X. W.; Xu, J.; Duan, B. J. (2018): A memory-efficient simulation method of grover's search algorithm. *Computer, Materials & Continua*, vol. 57, no. 2, pp. 307-319.

Vignesh, R. S.; Sudharssun, S.; Kumar, K. J. J. (2009): Limitations of quantum & the versatility of classical cryptography: a comparative study. *Second International Conference on Environmental and Computer Science*, pp. 333-337.

Wolrich, G. M.; Yap, K. S.; Guilford, J. D. (2014): Instruction set for message scheduling of SHA256 algorithm. *U.S. Patent 8*, vol. 838, no. 997, pp. 9-16.

Wei, Z. H.; Chen, X. B.; Niu, X. X.; Yang, Y. Y. (2015): The quantum steganography protocol via quantum noisy channels. *International Journal of Theoretical Physics*, vol. 54, no. 8, pp. 2505-2515.

Xu, G.; Chen, X. B.; Duo, Z. (2015): A novel protocol for multiparty quantum key management. *Quantum Information Processing*, vol. 14, no. 8, pp. 2959-2980.

Xu, G.; Chen, X. B.; Dou, Z. (2016): Novel criteria for deterministic remote state preparation via the entangled six-qubit state. *Entropy*, vol. 18, no. 7, pp. 267.

Xu, G.; Chen, X. B.; Li, J.; Li, J.; Wang, C. et al. (2015): Network coding for quantum cooperative multicast. *Quantum Information Processing*, vol. 14, no. 11, pp. 4297-4322.

Yang, Y. G.; Bi, J. L.; Chen, X. B.; Yuan, Z.; Zhou, Y. H. et al. (2018): Simple Hash function using discrete-time quantum walks. *Quantum Information Processing*, vol. 17, no. 8, pp. 189.

Zeghid, M.; Machhout, M.; Khriji, L. (2007): A modified AES based algorithm for image encryption. *International Journal of Computer Science and Engineering*, vol. 1, no. 1, pp. 70-75.