Journal of Information Hiding and Multimedia Signal Processing ©2019 ISSN 2073-4212
Ubiquitous International Volume **10**, Number **1**, January **2019**

An Enhanced RFID Mutual Authentication Protocol based on Quantum Dynamic Basis

Rui Wang

Software College
Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
670322496@qq.com

Hong-Feng Zhu

Software College
Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
zhuhongfeng1978@163.com

Received December 2017; revised August 2018

Abstract. *RFID technology is a type of automatic identification technology, which has broad application prospects in the fields of production, transportation, logistics and national defense. However, there are some problems about security and privacy because of the design of RFID open system, an attacker can learn the content of communication between the reader and the tag by eavesdrop and relay and can also tag tracking. Limited tag resources are the main reason why RFID security and privacy problems are difficult to solve. In this paper, a novel quantum dynamic basis theory is applied to RFID system to detect relay attacks, which the core idea is to make advantage of the quantum characteristics and once each authentication is completed, the database and tag automatically update the key. We argue that our protocol improve the security and reduce the computational cost for identifying a tag.*

Keywords: Relay attack, Low-cost RFID systems, Quantum information processing, Quantum dynamic basis

1. **Introduction.** Radio frequency identification (RFID) technology provides a non-contact method for automatic identification of tagged people or things [1, 2]. Moreover, it has the characteristics of cheap, flexible deployment, easy management and so on, which produce tremendous impact on traditional identification technology such as bar-code [3]. With the wide application of RFID technology in various fields, the security problem of RFID has become increasingly prominent [4, 5, 6]. If the tag information contained in the radio frequency signal transmission is eavesdropped or even maliciously modified, it will bring immeasurable loss to the legal owner of the tag.

Typically, the RFID system consists of three parts: reader, tag, and back-end database. When the reader sends out the query request and receives the information returned by the tag, the information is transmitted to the back-end database. In our protocol, tag and database should also equipped with devices which can send/receive, polarize, measure photons. Whats more, the database has data analysis and storage capabilities, including all tag data information. Since the default between the reader and the backstage database is a secure channel, we consider the two parts as a whole, therefore, mainly concerned about the reader and the tag two parts when we design the security protocol [7, 8]. We suppose that tag and reader equipped with devices which can send/receive, polarize, measure photons.

Relay attack brings huge security threat to RFID technology in which the attacker forwards the communication message between the valid sender and the legitimate recipient intact [9, 10, 11]. However, neither the sender nor the recipient can detect an adversary. There are two types of relay attacks including mafia fraud attacks and terrorist fraud attacks. In most of the literature, mafia fraud attacks are regarded as relay attacks since this attack can be not aware of both reader and tag. The traditional method to resist relay attacks is to use the distance bounding protocol [12, 13, 14, 15, 16, 17] and time measurement based on the communication time between the reader and the tag. The principle of the DB protocol is to measure the upper limit of the physical distance between the RFID tag and the RFID reader, and to measure the sent challenge bits and the return time (RTT) of the received response bits to ensure that the tag is located near the reader and does not occur a relay attack. However, a precise measurement of the RTT (which requires more precise clocks, sensitive tags, immediately reactions, where the speed of propagation is close to the vacuum speed in the communication medium and the fast bit exchange step) is inaccurate due to small errors. There are some challenges in the implementation of DB protocol [17].

Quantum dynamic basis theory is proposed by basing on the theory of unconditionally secure one time password [18] and quantum properties [19], its core idea is to automatically iterative update the basis of polarize and measure photons, which ensure that each session key unconditional security. Since the information stored in the classical form can be eavesdropped or copied and cannot be detected by both sides of the communication, while in the unknown quantum state cannot be measured and cloned.

In our work, we focus on proposing a novel theory that brings in one time password and quantum technologies to protect the RFID systems from relay attack with simple operation and lower resources. In our scheme, tag and database need to have the ability to polarize, measure, and send/receive photons. And a reader communicates with tag and database via classical channel and quantum channel. The security of our protocol is guaranteed by no-cloning and detection of adversary measurements from quantum mechanics.

The rest of the paper is organized as follows: We outline quantum dynamic basis in Section 2. Next, a concrete protocol base on quantum dynamic basis in Section 3, followed by the security analysis and the performance analysis are in Section 4. This paper is finally concluded in Section 5.

2. Quantum Dynamic Basis Theory.

2.1. Preliminary Theory.

Qubit is the simplest quantum system, with a two-dimensional complex vector space to describe its state, the space of the two orthogonal base vector are recorded as $|0\rangle$ and $|1\rangle$. Qubits are very different from the classical bits, and in general the quantum bits are linear superposition of $|0\rangle$ and $|1\rangle$, as $|\Phi\rangle = a\,|0\rangle + b\,|1\rangle$. The measurement of $|\Phi\rangle$, the result may be $|0\rangle$ or $|1\rangle$, corresponding with the probability of $|0\rangle$ is $|a|^2$,$|1\rangle$ is $|b|^2$. The result of the measurement operation is classical information. Note that measurement is a destructive operation and it changes the state of a qubit permanently. The state of a qubit can be written in different bases, which corresponds to the rotation of the spin of photons, if qubits are realized in that way. In this work, we utilize two bases

$\{B_Z, B_X\}$ to describe qubits, where $B_Z = \{|0\rangle, |1\rangle\}$ and $B_X = \left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$. Polarization of quantum states in different bases can be represented geometrically by rotation of basis vectors and is shown in Table 1.

Table 1. Notations utilized for states of bases

Basis	Classical bit 0	Classical bit 1
B_Z	→	↑
B_X	↗	↖

The one time basis protocol security is based on the properties of quantum and hash functions [20, 21, 22] as follow:

(1) Given a word x, it is easier to compute $H(x)$;

(2) Given a word h, it is not feasible to compute a word x such that $h = H(x)$;

(3) Given a word x, it is not feasible to find out $H(x) = H(y)$ where $y \neq x$, which is called weak collision resistant;

(4) It is not feasible to find out any (x, y) satisfies $H(x) = H(y)$, which is called collision resistant.

2.2. **One Time Basis (OTB).** In this section, we give an one time password based automatically iterated basis scheme, in which a public secure one-way hash function H is required to map the session key sk and the shared key K_1 into an m-bit binary string. Alice and Bob agree that Alice polarizes the photons, according to K the such that if the ith bit of the K is 0, the ith photon due to be sent by Alice, is polarized in B_Z. Similarly, if ith bit of the K is 1, then Alice uses basis B_X. Bob also measures the photons received from Alice according to the same rules. We assume that the quantum channel established between Alice and Bob is ideal. Alice and Bob have a pre-shared secret key, $K_1 \in \{0,1\}^{3m}$, which is used to start the protocol and polarizes the photons where $3m$ is a security parameter according to the security requirement.

2.2.1. *Pre-shared Secret Key.* Before Alice and Bob communication, there is a previously identified key K_1 and the identity of the other party saved by themselves. This paper does not focus on pre-shared key, so only a simple description is available in Fig.1. Suppose that Alice and Bob exchange public keys through a security scheme.

Step 1: Alice encrypts the message containing Alice's ID_A and N_1 with Bob's public key PU_b and sends it to Bob.

Step 2: Bob encrypts the message, including the N_1 generated by Alice and the newly generated N_2 by Bob, Bobs ID information ID_B, with the Alice public key PU_a sent to Alice. Alice at this point can confirm that the message is from Bob. Alice saves ID_B.

Step 3: Alice encrypts N_2 with PU_b, sent to Bob to confirm its source. If there is no doubt about the source, Bob store ID_A.

Step 4: Alice selects K_1 to share with Bob by sending massage $M = E_{PU_b}(E_{PR_a}(K_1))$. Bob restores K_1 by calculating $D_{PU_a}(D_{PR_b}(M))$.

The process of the OTB protocol is described in detail as follows (shown in Fig.2):

- Alice selects a random number a, sends $a \| ID_A$ to Bob via a classical channel, Bob does the similar operation sends $b \| ID_B$ to Alice. Alice and Bob identify each other by ID.

- Alice makes a series of calculations and gets $k = H_1(a \| b)$,$sk = H_1(a \| b \| K_1)$,$h_{sk} = H_1(sk \| K_1)$ and $q_A = h_{sk} \| sk \| k$. Therewith, she polarizes the photons according to the K_1, generating $|q_A\rangle$, and sends $|q_A\rangle$ to Bob via a quantum channel.

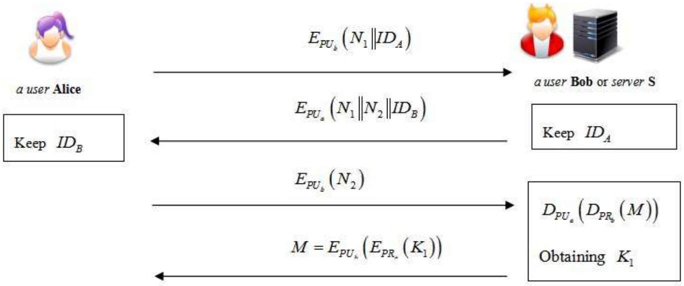

Figure 1. The process of share K_1

- Then Bob checks if $H_1\left(sk'\,\|K_1\right) = h_{sk'}$ and $k' = H_1\left(a\,\|b\right)$ to authenticate Alice by measuring qubits receiving from Alice according to the K_1.

- Bob identifies Alice as a valid user and puts k' into another secure one-way function H_2 getting K_2 automatically instead of K_1, then prepare $|q_B\rangle$ based on K_1 and send back to Alice by a quantum channel.

- Alice checks if the outcome with $h_{sk'} = h_{sk}$ to authenticate Bob. Alice prepare for next session by calculating $K_2 = H_2(k)$ as the next time pre-shared key.

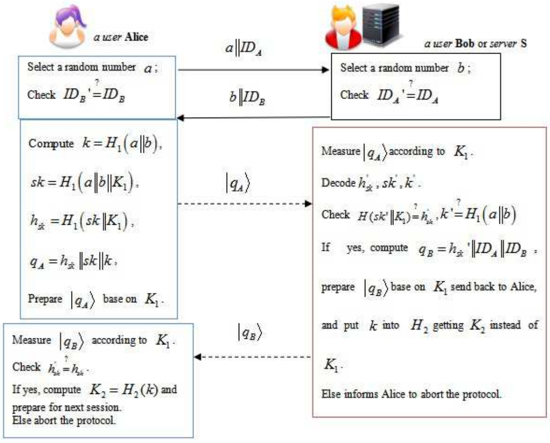
a user Alice
a user Bob or server S
$a\|ID_A$
Select a random number a;
Check $ID_B' \overset{?}{=} ID_B$
$b\|ID_B$
Select a random number b;
Check $ID_A' \overset{?}{=} ID_A$
Compute $k = H_1(a\|b)$,
$sk = H_1(a\|b\|K_1)$,
$h_{sk} = H_1(sk\|K_1)$,
$q_A = h_{sk}\|sk\|k$,
Prepare $|q_A\rangle$ base on K_1.
$|q_A\rangle$
Measure $|q_A\rangle$ according to K_1.
Decode h_{sk}', sk', k'.
Check $H(sk'\|K_1) \overset{?}{=} h_{sk}'$, $k' \overset{?}{=} H_1(a\|b)$
If yes, compute $q_B = h_{sk}'\|ID_A\|ID_B$,
prepare $|q_B\rangle$ base on K_1 send back to Alice,
and put k into H_2 getting K_2 instead of K_1.
Else informs Alice to abort the protocol.
$|q_B\rangle$
Measure $|q_B\rangle$ according to K_1.
Check $h_{sk}' \overset{?}{=} h_{sk}$.
If yes, compute $K_2 = H_2(k)$ and prepare for next session.
Else abort the protocol.

Figure 2. The OTB protocol

3. **The proposed protocol.** In this section, we propose a new protocol to put the quantum dynamic basis into the low cost RFID system against relay attack. Since the default between the reader and the backstage database is a secure channel, we consider the two parts as a whole, therefore, mainly concerned about the reader and the tag two parts when we design the security protocol [23, 24]. We suppose that tag and reader equipped with devices which can send/receive, polarize, measure photons. In this work, we utilize two bases $\{B_Z, B_X\}$ to describe qubits, where $B_Z = \{|0\rangle, |1\rangle\}$ and $B_X = \left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$. We assume that reader and tag share a secret key K_1 as the measurement basis. The notation used hereafter is shown in Table 2. The process of polarizes the photons, according to K_i the such that if the Ith bit of the K_i is 0, the ith photon is polarized in B_Z. Similarly, if ith bit of the K_i is 1, then the submitter uses B_X basis.

Table 2. Notations

Symbol	Definition
K_i	Automatically iterated basis
sk	Session key
k	A key to calculate $K_i + 1$
a, b	The random number
H	A secure one-way hash function
m	The length of k, sk, K
$\|\|$	Concatenation operation
$\|sk\rangle$	Qubit sequences according to sk
$\|B\rangle$	Qubit sequences according to B

Our protocol requires quantum and classical channels, the reader sends authentication request through the classical channel, while the authentication process of the protocol is completed through the quantum channel. The specific process of protocol is depicted in Fig. 3 and described as follows:

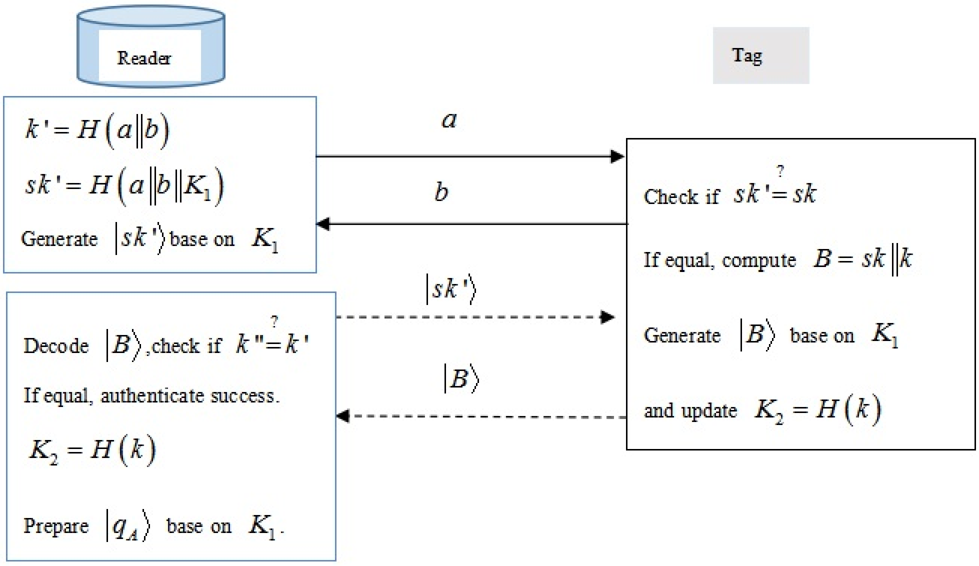
Reader
Tag
$k' = H(a\|b)$
$sk' = H(a\|b\|K_1)$
Generate $|sk'\rangle$ base on K_1
a
b
$|sk'\rangle$
$|B\rangle$
Check if $sk' \overset{?}{=} sk$
If equal, compute $B = sk\|k$
Generate $|B\rangle$ base on K_1
and update $K_2 = H(k)$
Decode $|B\rangle$,check if $k'' \overset{?}{=} k'$
If equal, authenticate success.
$K_2 = H(k)$
Prepare $|q_A\rangle$ base on K_1.

Figure 3. Authentication protocol based on quantum dynamic basis

The reader generates a random number a and sends to the tag as the authentication request. The tag also generates a random number b and sends back to the reader. The tag calculates $a\|b$ and puts it into the hash function H with secure parameter m:$\{0,1\}^* \rightarrow \{0,1\}^m$ and then gets an M-bit hash value,k. Then, the tag gets sk by putting $a\|b\|K_1$ into H. Once the reader receives the message sent by the tag, it calculates $k' = H(a\|b)$,$sk' = H(a\|b\|K_1)$. Therewith, the reader polarizes the photons according to the K_1, generating $|sk'\rangle$ base on K_1, and send $|sk'\rangle$ to tag via a quantum channel.

Upon the reception of qubits from the reader, the tag measures it according to the K_1 and authenticates the reader by checking if $sk' = sk$. In the case of inequality, the tag aborts the protocol; otherwise, the tag generates $|B\rangle$ based on K_1 by computing

$B = sk\|k$ and puts k' into H getting K_2 automatically instead of K_1, then sends $|B\rangle$ back to the reader.

The reader decodes $|B\rangle$ getting sk'',k'' and checks if $k'' = k'$ to identify the tag. If equal, authentication is successful, automatic iterative updating of keys for the reader. Otherwise, terminate authentication process.

4. Analysis.

4.1. Security Analysis.

The channel between the tag and the reader is divided into forward and backward channels. The forward channel is that information interaction between the reader and the tag, while the backward channel is the channel that the tag sends information back to the reader after receiving request from the reader. The communication between tags and readers is carried out in the form of electromagnetic waves, and there is no physical or visible contact in the process. This non-contact and wireless communication can easily be tapped, which has a great impact on the design and analysis of the system security mechanism. Thus, the tags and the readers should trust each other and should be resistant to relay attacks and impersonate attacks.

In a relay attack, an attack is performed between the tag and reader by a malicious attacker Eve, leading indirect communication between the tag and the reader. In the authentication stage, attackers will relay challenge response information transparently forwarding to both reader and tag. After receiving the correct authentication information, the reader mistakenly believes that the tag is in the around, thus making the corresponding operation.

During each authentication instance, an adversary can only observe the values including $a, b, |sk'\rangle, |B\rangle$, where a, b are the random numbers, $|sk'\rangle, |B\rangle$ are the polarized photons strings. Because of the non-cloning principle of qubits, it is impossible for any adversary to replicate qubits for their use without measurement. Once an adversary has measured, the tag and reader will recognize the presence of attack, which brings the abort of the protocol. The detailed description of the relay attack is shown in Fig 4.

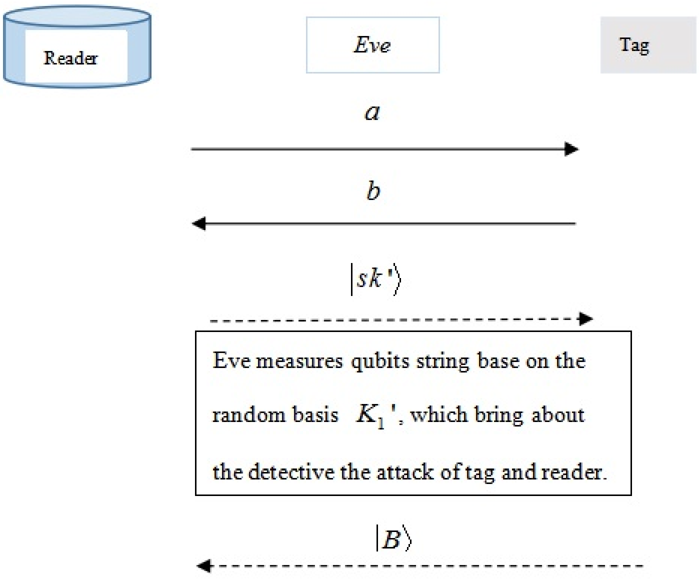
Reader
Eve
Tag
a
b
$|sk'\rangle$
Eve measures qubits string base on the random basis K_1', which bring about the detective the attack of tag and reader.
$|B\rangle$

FIGURE 4. Relay attack on the protocol

Eve does not have the security parameter m, even if he gets the random numbers a, b cannot compute k, it is also impossible to obtain the measurement basis K_2 of next round by iteration. So if Eve wants to get authentication of tag or reader can only be done in the current authentication, that is, by guessing the base of the measurement. Assume that the probability of successful relaying is $\frac{1}{2}$ when Eve guesses the base of measurement correctly. While it is $\frac{1}{4}$ when Eve guesses the basis incorrectly, however it may also has chances that tag/reader receive the correct photon, due to Eve obtains a wrong single bit and polarizes the bit by the wrong basis. The probability that Eve succeeds in relaying a photon is $\frac{3}{4}$. However, Eve relays a m-bit quantum string every time the success probability of A is just $\left(\frac{3}{4}\right)^m$. Consequently, if m is large enough, the relay attack cannot happen.

The security performance of protocol proposed in this article compared with the proposed by Jannati [8], Chien [27] is described in Table 3. Because of the unidirectional nature of hash function and the use of random numbers, attackers cannot distinguish the output of a tag even though they get the output of multiple tags. Thus, our scheme has no traceability and forward security.

Table 3. Comparison between schemes

	Jannati [8]	Chien [27]	Our scheme
No traceability	Δ	Δ	O
Forward secrecy	O	O	O
Relay attack	O	×	O
O : satisfied, Δ: partially satisfied, × : no satisfied			

4.2. **Performance Analysis.** In 2014, Zhang et al. [28] proposed the idea of applying quantum key distribution (QKD) technology to the client-server architecture, which lays the foundation for our protocol's hardware implementation. The Reader and Tag in our protocol need the capacity of polarizing, measuring, sending/receiving qubits. Zhang et al. integrate most of the resources needed on the server side, while the client only needed a non-chip polarization rotator. The server sends the light pulses generated by the continuous wave laser source to the client through the polarization maintaining fiber (PMF). The client uses the integrated polarization controller (PC) to prepare the qubit and return it to the server. The server measures the received quantum bits using a similar PC, fiber polarizing beam splitter (FPBS) and superconducting single photon detectors (SSPDs). Therefore, The reader and tag use the integrated polarization controller to generate the qubit and send it to each other through the polarization maintaining fiber (PMF). Then they measure the received qubits by using a similar PC, FPBS, SSPDs.

Whats more, our protocol makes Reader and Tag has the ability to compute a pseudo-random function. In previous work, Mandal et al. [29] proposed the simplest number of two input NAND gate equivalents for implementation, which makes it possible to implement pseudo-random functions based on simple pseudo-random number generators on low-cost devices, since such devices have 2000GEs that can be used for security features [30].

Thus, our scheme only needs simple on-chip polarization rotator and pseudo random number generator that may be integrated into a handheld device. However, due to the weak or erroneous effects of wireless transmission susceptibility to noise, applying the error correction mechanism to the system is necessary. Automatic Repeat Request (ARQ) and Forward Error Correction (FEC) are two of the most common error control schemes [29]. Error correction mechanisms will not make an impact on our protocol, while in the DB protocol which is cannot be used owing to delay during the rapid bit exchange phase. Therefore, the DB protocol is very sensitive to noise.

Moreover, only simple operations can be performed in the process making storage space are low. In our scheme, the tag and the reader both share a m-bit basis K_1. For identifying each other, the tag and the reader store the sk of m-bit. And for autoing update the measurement basis, they also save m-bit k. Therefore, to implement of our scheme, the tag and the reader respectively need 3m-bit memory. The messages of tag-to-reader communication are $b, |B\rangle$, similarly reader-to-tag are $a, |sk'\rangle$.

5. **Conclusion.** This paper has proposed quantum dynamic base theory apply to RFID system to resist attacks, mainly against relay attack with simpler operation and lower resources. Because each session generates new random numbers and measurement base, the attacker cannot get session information by cumulative access, and cannot obtain information by measuring due to the quantum principle of wave packet collapse.

In the future, we may have a higher probability of detecting relay attacks so that the current RFID systems more secure and efficient if we integrate more quantum capabilities into tags and readers. Moreover, quantum dynamic basis theory can also be applied to other aspects by its quantum security, which may make encrypted algorithm safer.

Acknowledgment. This work is supported by the Liaoning Provincial Natural Science Foundation of China (Grant No. 201602680)

REFERENCES

[1] R. Want, An introduction to RFID technology, *IEEE Pervasive Computing*, vol.5, no.1, pp.25–33, 2006.

[2] B. Nath, F. Reynolds, and R. Want, RFID Technology and Applications, *IEEE Pervasive Computing*, vol.5, no.1, pp.22–24, 2006.

[3] T. Pavlidis, J. Swartz, and Y. P. Wang, Fundamentals of bar code information theory, *Computer*, vol.23, no.4, pp.74–86, 1990.

[4] S. E. Sarma, S. A. Weis, and D. W. Engels, RFID Systems and Security and Privacy Implications, *Revised Papers From the, International Workshop on Cryptographic Hardware and Embedded Systems*, Springer-Verlag, pp.454–469, 2002.

[5] S. L. Garfinkel, A.Juels, and R.Pappu, Rfid privacy: an overview of problems and proposed solutions, *IEEE Security Privacy*, vol.3, no.3, pp.34–43, 2005.

[6] M. R. Rieback, B. Crispo, and A. S.Tanenbaum, The evolution of rfid security,*IEEE Pervasive Computing*, vol.5, no.1, pp.62–69, 2006.

[7] D. Henrici, P. Muller, Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers, *Pervasive Computing and Communications Workshops, Proceedings of the Second IEEE Conference on IEEE*, pp.149–153, 2004.

[8] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, Security and privacy aspects of low-cost radio frequency identification systems,*International Conference on Security in Pervasive Computing*, Boppard, Germany, pp.201–212, 2004.

[9] H. K.Chong, G. Avoine, RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks, *International Conference on Cryptology and Network Security*, Springer-Verlag, pp.119–133, 2009.

[10] G. Avoine, A. Tchamkerten, An asymptotically optimal rfid authentication protocol against relay attacks, *Mathematics*, vol.24, no.9, pp.72–81, 2008.

[11] G. Hancke, A practical relay attack on iso 14443 proximity cards, *Technical Report*, 2005.

[12] S. Brands, D. Chaum, Distance-bounding protocols, *The Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, Springer-Verlag New York, pp.344–359, 1994.

[13] G. P. Hancke, M. G.Kuhn, An RFID Distance Bounding Protocol, *International Conference on Security and Privacy for Emerging Areas in Communications Networks*, IEEE, pp.67–73, 2005.

[14] S. Lee, S. K.Jin, S. J.Hong, J. Kim, Distance bounding with delayed responses, *Communications Letters IEEE*, vol.16, no.9, pp.1478–1481, 2012.

[15] R. Trujillo-Rasua, B. Martin, G. Avoine, Distance bounding facing both mafia and distance frauds, *Wireless Communications IEEE Transactions on*, vol.13, no.10, pp.5690–5698, 2014.

[16] H. Jannati, Analysis of relay, terrorist fraud and distance fraud attacks on rfid systems, *International Journal of Critical Infrastructure Protection*, vol.11, no.C, pp.51–61, 2015.

[17] J. Clulow, G. P. Hancke, M. G. Kuhn, T. Moore, So near and yet so far: distance-bounding attacks in wireless networks, *European Workshop on Security in Ad-hoc and Sensor Networks*, Springer Berlin Heidelberg, pp.83–97, 2006.

[18] N. Popp, D. M'Raihi, L. Hart, One time password. EP, US 8434138 B2, 2013.

[19] M. A. Nielson, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[20] H. F. Zhu, Y. Zhang, X. Wang, A novel one-time identity-password authenticated scheme based on biometrics for e-coupon system, *International Journal of Network Security*, vol.18, no.3, pp.401–409, 2016.

[21] B. Preneel, The state of cryptographic hash functions, *Lecture Notes in Computer Science*, vol.1561, no.1, pp.158–182, 1999.

[22] W. E.Burr, A new hash competition, *IEEE Security Privacy*, vol.6, no.3, pp.60–62, 2008.

[23] D. Henrici, Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers, *Pervasive Computing and Communications Workshops, Proceedings of the Second IEEE Conference on?IEEE*, pp.149–153, 2004.

[24] S. A.Weis, S. E. Sarma, R. L.Rivest, D. W.Engels, Security and privacy aspects of low-cost radio frequency identification systems, *Lecture Notes in Computer Science*, vol.2802, pp.201–212, 2004.

[25] M. F.Tsai, C. K.Shieh, C. H. Ke, D. J. Deng, Sub-packet forward error correction mechanism for video streaming over wireless networks, *Multimedia Tools Applications*, vol.47, no.1, pp.49–69, 2010.

[26] M. F.Tsai, N. Chilamkurti, C. K. Shieh, An adaptive packet and block length forward error correction for video streaming over wireless networks, *Wireless Personal Communications*, vol.56, no.3, pp.435–446, 2011.

[27] H. Y. Chien, C. W. Huang, A lightweight authentication protocol for low-cost rfid, *Journal of Signal Processing Systems*, vol.59, no.1, pp.95–102, 2010.

[28] P. Zhang, K. Aungskunsiri, E. Martinlopez, J. Wabnig, M. Lobino, and R. W.Nock, et al, Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client, *Physical Review Letters*, vol.112, no.13, pp.1153–1165, 2014.

[29] K. Mandal, X. Fan, G. Gong, Warbler: a lightweight pseudorandom number generator for epc c1 gen2 tags, *Cryptology Information Security*, vol.2, pp.73–84, 2012.

[30] H. Jannati, E. Ardeshir-Larijani, Detecting relay attacks on rfid communication systems using quantum bits, *Quantum Information Processing*, vol.15,no.11, pp.1–13, 2016.