Journal of Information Hiding and Multimedia Signal Processing ©2018 ISSN 2073-4212
Ubiquitous International Volume **9**, Number **4**, July **2018**

A Lightweight RFID Authentication Protocol using Qubits against Relay Attack

Hongfeng Zhu, Rui Wang and Junlin Liu

Software College, Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
zhuhongfeng1978@163.com;670322496@qq.com;272297257@qq.com

Received December, 2017; revised December, 2017

Abstract. *Radio Frequency Identification (RFID), which through the radio frequency to read and receive information to achieve the purpose of automatic identification, is a non-contact automatic identification technology. Compared with the bar code, it is easy, flexible to use in the long-distance, harsh environment and can be moving objects for data collection and automatic identification. RFID is widely used in the sale of goods and distribution, logistics management, production line automation and so on. Furthermore, low-cost RFID with computational and memory limited resources become increasingly used in market, which is still a challenge to find a technique that satisfies high security lightweight RFID authentication protocols. In this paper, we present a novel quantum technique using qubits to detect relay attacks on low-cost RFID systems.*
Keywords: Relay attack; RFID; Quantum cryptography

---

1. **Introduction.** RFID is a technology that enables remote identification of objects, and it does not require the visual contact to access the information, making the identification process much more reliable and faster. This property gives RFID an impressive range of new applications. Thus, it can be used in different field such as supermarket checkout, identify and track people, orientation in buildings, counterfeit detection and much more. A radio frequency identification (RFID) system mainly consists of three components: radio frequency tags, readers, and a back-end server/database (or a set of distributed databases) which maintains information on the tagged objects. Generally, the tag consists of a microchip with some data storage and an antenna, in different applications, different types of information are stored in the RFID tags. A reader queries tags to obtain tag contents though wireless communications.

With the wide application of RFID technology, the tag should be low cost, which means reduce the consumption of power supply, storage, and logic gates and so on. To achieve this goal, Li et al. [1], based on only the Partial ID concept, pseudo random numbers and bit-wise XOR ($\oplus$), proposed a lightweight RFID authentication protocol for low-cost RFIDs. While different from other existing solutions [2-4], Li et als scheme do not use conventional cryptographic primitives, it still has several security weaknesses. Gao et al. [5] utilizes cyclic redundancy checking, permutation and bit-wise XOR functions that can be integrated on passive tags providing an ultra-lightweight RFID authentication protocol that provides resistance to tracking, replay and secret disclosure attacks. However, an attacker can authenticate itself to relay the protocol by relaying messages between the reader and the tag.

Relay attacks are performed on RFID systems used in many areas. In this attack, the adversary relays transmitted messages between the valid sender and the legitimate recipient, yet the sender and the recipient are not aware of the presence of an adversary. It is feasible that even when the adversary knows nothing about security parameters used in the protocol. There are two types of relay attacks, namely, mafia fraud attacks and terrorist fraud attacks. Mafia fraud attack is the most serious since this attack cannot be aware of both reader and tag [6]. In most of the literature, the mafia fraud attack performed on RFID systems is considered to be relay attack [7]. In classical channels, distance-bounding (DB) protocols have been proposed [8,9] to against relay attacks. The DB protocol measures the upper limit of the physical distance between the RFID tag and the RFID reader by measuring the time of the sent challenge bit and the received response bit called RTT to ensure that the tags are located near the readers and that no relay attack occurs [10-12]. However, the RTT time that requires accurate measurement (it takes a more accurate clock, sensitive tag which is instantly react, where the propagation speed is close to the speed of light in vacuum in the communication medium and the fast bit exchange step) is not accurate due to small errors, which makes some challenges in the implementation of the DB protocol [13,14].

Based on the theory of quantum mechanics, quantum technology is rapidly developing which is brought an unconditionally secure way being applied to a variety of systems. Quantum communication and cryptography have been developed over the recent decades and have been put into commercial applications. In particular, QKD (Quantum Key Distribution) provides unconditional security to classical keys, which makes quantum cryptography much more interesting [15]. In a recent work, Jannati et al. [16] proposed a apply QKD scheme with the client-server model so that the client only uses minimal quantum resources and send/receive qubits with prepare and measure qubits equipment.

Motivated by this, we present a novel theory that brings in quantum technologies to protect the RFID systems from relay attack with simple operation and lower resources. In our scheme, tag and reader need to have the ability to polarize, measure, and send/receive photons. And a back-end server/database communicates with reader just via classical channel. The security of our protocol is guaranteed by no-cloning and detection of adversary measurements of quantum mechanics. Moreover, our protocol uses qubits transmission to avoid RTT measurement, making the protocol more efficient in low-cost RFID systems.

The rest of the paper is organized as follows: We outline preliminaries in Section 2. Next, a concrete protocol base on quantum technology in Section 3, followed by the security analysis and the performance analysis are shown in Section 4. Then, the hardware requirements of implementing our protocol are described in Section 5. This paper is finally concluded in Section 6.

2. **Preliminary Theory.** Qubit is the abbreviation of quantum bit. It 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 $|1\rangle$. Corresponding with $|0\rangle$ is column matrix $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$,$|1\rangle$ is column matrix $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$. The state vector can be expressed as

$$|\Phi\rangle = a\,|0\rangle + b\,|1\rangle \; (2.1)$$

which column matrix is $\begin{bmatrix} a \\ b \end{bmatrix}$, where a and a are plural, satisfying $|a|^2 + |b|^2 = 1$. If $a = 0$,$|\Phi\rangle = b\,|1\rangle$,$|b|^2 = 1$ which means $|\Phi\rangle$ always in the state of $|1\rangle$.Similarly, if $b = 0$,$|\Phi\rangle = a\,|0\rangle$,which means $|\Phi\rangle$ always in the state of $|0\rangle$.These two special cases are similar to the classical bits 1 and 0. However, the qubits are very different from the classical bits, and in general the quantum bits are linear superposition of $|0\rangle$ and $|1\rangle$, as (2.1).The measurement of $|\Phi\rangle$, the result may be $|0\rangle$ or $|1\rangle$. The probability of $|0\rangle$ is $|a|^2$,$|1\rangle$ is $|b|^2$.Unitary and measurement are two kinds of operations that can be applied on qubits. Note that measurement is a destructive operation and it changes the state of a qubit permanently, because the result of the measurement operation is classical information.

Qubits can be entangled. In any four-dimensional space, any vector can be expressed as $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, where $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. If $b = c = 0, a = b = 1/\sqrt{2}$, there is $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$), which is called a Bell state, cannot be decomposed into two single qubit states. Measuring one of the qubits will fix the state of the other qubit, even if they are physically separated [17]. The principle of no-cloning is the basic principle of quantum cryptography, which can be expressed as: the quantum state of the position cannot be copied without changing its original state. If the quantum state is known, we can repeat it. The difficulty is that we cannot get the exact characteristics of the quantum system through a single measurement. Since once the measurement is made, the original quantum state is changed and the measured result is only one of the possible states that make up this quantum state. Unless the measured sub-state happens to be the eigenvalue of the measure operator, the measurement will inevitably irreversibly alter the original quantum state. It is also impossible to measure the quantum state of the system without measuring it.

The state of a qubit can be expressed in different bases, which corresponds to the rotation of the spin of photons [17]. 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. Symbol describing the state of bases

Basis	Classical bit 0	Classical bit 1
B_Z	$\rightarrow$	$\uparrow$
B_X	$\nearrow$	$\nwarrow$

3. **The Proposed Protocol.** In this section, we propose a new protocol to put the quantum technology 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 [18-19]. We suppose that tag and reader equipped with devices which can send/receive, polarize, and measure photons. Our proposed protocol is depicted in Fig 1 and described as follows.

We assume that back-end server/database and tag share a secret key K_1, reader and tag share l-bit sequences key K_2. The notation used hereafter is shown in Table 2.

There are two phases in our protocol: bit transmission phase and qubit transmission phase. Bit transmission means all bits are transmitted through a classical channel, while in quantum communication phase, quantum bit is transmitted via the quantum channel.

The Reader polarizes the photons according to the K_2, which if the ith bit of the K_2 is 0, the ith photon is polarized in B_Z. Similarly, if ith bit of the K_2 is 1, then the Reader uses B_X basis. The Tag also measures the photons received from the Reader according to bases K_2. The Tag polarizes the photons according to the B, assuming that if the ith bit of the B is 0, the ith photon is polarized in B_Z. Likewise, if ith bit of the B is 1, then the

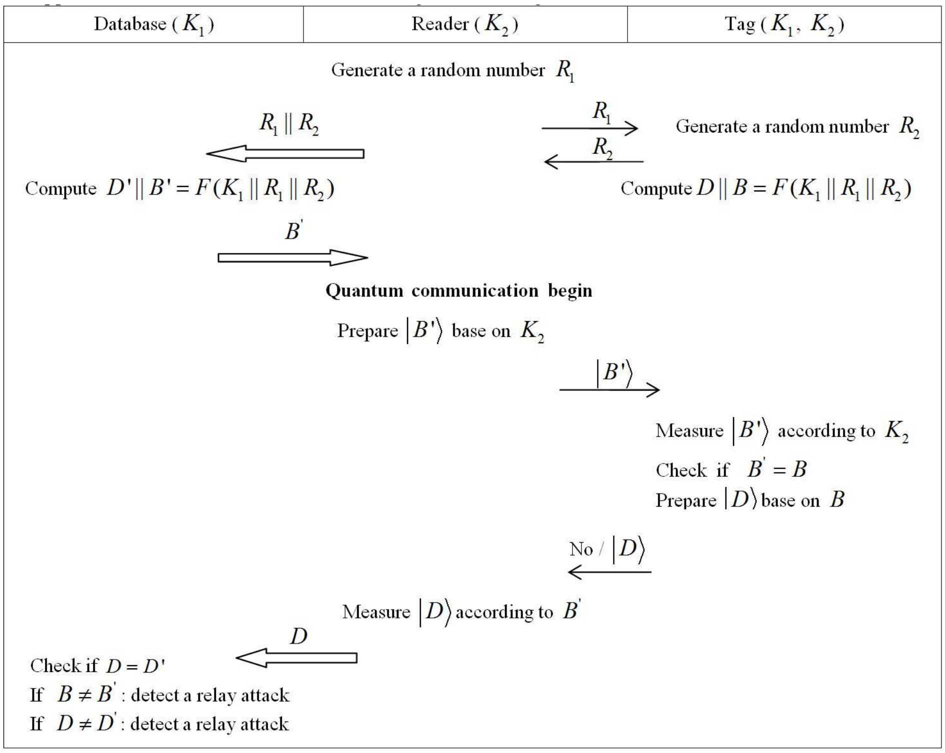

FIGURE 1. Detecting relay attacks

TABLE 2. Notations

Symbol	Definition
K_1	The secret l bits key share between tag and back-end server/database
K_2	The secret l bits key share between tag and reader
F	one-way pseudo-random function
A_i	ith bit of a string A
a_i	ith bit of a string a
$\|\|$	Means that two adjacent messages are concatenated
R	The random number
$\|D\rangle$	Qubit sequences according to B
$\|B\rangle$	Qubit sequences according to K_2
D, B	l-bit sequences
K_A	Adversary A choose basis bit randomly
B_1	Adversary A choose basis bit randomly

Tag uses B_X basis. The Reader measures the photons received from the Tag according to bases B'.

Step 1 (bit transmission): Firstly, the Reader generates a random number R_1 and deliveries it to the Tag. After the reception of R_1 , the Tag also generates a random number R_2 and sends R_2 back to the Reader. Then, the Tag computes two l-bit sequences D and B as $D||B = F(K_1||R_1||R_2)$.

Step 2 (bit transmission): Once reception of R_2, the Reader forwards R_1 and R_2 to the database. The server searches its data to find a matched K_1 there with compute

$D'||B' = F(K_1||R_1||R_2)$. The database sends back B' to Reader. The Reader polarizes the photons according to the K_2, generating $|B'\rangle$.

Step 3 (qubit transmission): Reader sends $|B'\rangle$ to Tag, measuring outcome which checks whether B' equals B to authenticate the Reader. If the Reader is authenticated successfully, the tag begin to prepare $|D\rangle$ according to B and sent it to Reader; otherwise, it responds with no information and terminate the conversation.

Step 4 (bit transmission): Receiving qubits from the Tag, Reader measures them according to the B' getting the string D therewith sends to database. Then database checks the equality of the measurements result (which is classical) with D' to authenticate the Tag. In the case of inequality, database detects a relay attack has happened; otherwise, the server identifies Tag as a valid tag.

4. Analysis.

4.1. Security Analysis.

In this section, we will analyze the security of our proposed scheme in detecting relay attacks. Because of the non-cloning principle of qubits, it is impossible for any adversary to replicate qubits for their use without measurement. Thus, they must perform measurement in order to obtain accurate information, which is destructive operation, meaning that it is not only disturbs the states permanently, but also its outcome depends on which a base is eventually chosen. These fundamental properties of quantum technique make easily for us to detect relay attack. Theorem 1 and Theorem 2 below establish its security, and then, a more detailed analysis of the relay attack is provided.

Theorem 4.1. *Assume that there is an adversary A between Reader and Tag, who relay a qubit send by Reader to Tag correctly with probability $\frac{3}{4}$ where A has not known the basis of the qubit. This attack is shown in Fig 2.*

Proof: Assume that Reader polarizes the photon according to the k, generating $|b\rangle$ and send it to Tag. However, adversary A eavesdrop and capture $|b\rangle$ who does know nothing about k which is the qubit encoded, then it chooses a basis k_A randomly. Then, adversary obtains a single bit b_A by measuring the qubit in that basis. Obviously, if the adversary chooses the correct basis, it can get the correct bit, i.e., $b_A = b$ iff $k_A = k$; Similarly, if the adversary guesses the wrong basis, it would get the incorrect bit, i.e., if $k_A \neq k$, $b_A \neq b$.

Thus, it obtains the single bit correctly by half the probability. Then, the adversary must send the $|b_A\rangle$, encoded by the basis k_A chosen by adversary, to Tag measuring it as b_A. Once the adversary correctly guesses the basis, it sends a photon encoded in a correct basis and the Tag obtains a correct single bit. But if the adversary guesses the basis incorrectly, the Tag obtains it correctly with probability of half. It means that $P[k_A = k] = P[k_A \neq k] = \frac{1}{2}$. Consequently, there are two situations where the Tag can get $b_A = b$ and described as follows:

(1) The adversary A guesses the basis correctly i.e.,$k_A = k$ and send to Tag correctly, which probability is :

$$P_1 = P[b_A = b|k_A = k]P[k_A = k] = \frac{1}{2}$$

(2) The adversary A guesses the basis incorrectly i.e.,$k_A \neq k$, however it may also has chances that Tag receive the correct $|b_A\rangle$, due to the adversary A obtains a wrong single bit and polarizes the bit by the wrong basis. This probability is:

$$P_2 = P[b_A = b|k_A \neq k]P[k_A \neq k] = \frac{1}{4}$$

When an adversary relays a single bit between the reader and the tag, the probability that the single bit measured by the Tag is equal to the single bit sent by the Reader is:

$$P = P_1 + P_2 = \frac{3}{4}$$

Theorem 4.2. *Assume that there is an adversary A still between Reader and Tag, and this time adversary relay a qubit send by Tag to Reader correctly with probability $\frac{3}{4}$ where A does not know the basis of the qubit. This attack is shown in Fig 3.*

Proof: Assume that Tag polarizes the photon according to the b, generating $|d\rangle$ and send it to Reader. Adversary catches $|d\rangle$, it chooses a random basis b_1. Then, adversary measures the qubit according to b_1, obtaining a single bit d_1. If the adversary chooses the correct basis, it can get the correct bit, i.e., $d_1 = d'$ iff $b_1 = b$; Similarly, if the adversary guesses the wrong basis, it would get the incorrect bit, i.e.,if $b_1 \neq b$, $d_1 \neq d'$. The detailed process of proof is the same as the process of Theorem 1, then will not be repeated. In this scenario,$P_1 = P[d_1 = d|b_1 = b]P[b_1 = b] = \frac{1}{2}$, $P_2 = P[d_1 = d|b_1 \neq b]P[b_1 \neq b] = \frac{1}{4}$, the probability of the events that the single bit measured by the Reader is equal to the single bit sent by the Tag is $P = P_1 + P_2 = \frac{3}{4}$.

Theorem 1 and Theorem 2 have clearly shown that a qubit can be successfully relayed with probability. However, each message contains l qubits during an actual transmission. Thus the adversary A has to relay l qubits each time, the success probability of A is just $\left(\frac{3}{4}\right)^l$. Consequently, if l is large enough, the relay attack cannot happen.

Of course, all of these are the theoretical speculation. In practical applications, there will inevitably be some interferences from the current limited technology. Thus, any practical quantum cryptosystem must consider counter measures against possible attacks that exploit such compromises [20-25].

4.2. **Performance Analysis.** Due to the weak or erroneous effects of wireless transmission susceptibility to noise, reliable transmission over wireless channels is a challenge. Once an error occurs during transmission, a fault occurs when determining a relay attack. Thus, in the proposed method, the error correction process must be performed during the bit transmission phase. It is not necessary to perform a quantum error correction method in the quantum bit transmission phase [20]. Automatic Repeat Request (ARQ) and Forward Error Correction (FEC) are two of the most common error control schemes. In ARQ, the lost data will be retransmitted after a timeout or requestor's request, but it will cause a delay. Due to the short transmission delay, additional redundancy can be added to improve the reliability of transmission, FEC mechanism for real-time interactive information transmission is more appropriate. The sender has k source packets send to the receiver, which adds $(n - k)$ redundancy according to the network environment to form a block with n packets. After the recipient receives the information and checks it, if the received value is more than or equal to k, the decoder can recover the lost or erroneous information through the redundant part [28], which is shown in Fig 4. However, the DB protocol cannot use the error correction process due to the delay during the rapid bit exchange phase. Therefore, the DB protocol is very sensitive to noise. In systems that use the DB protocol, there is always a trade-off between security and performance. Therefore, the method we propose can be achieved in the noisy environment by correctly selecting the error correction method.

As K_1, K_2 are l-bit. Reader, Tag, Database only need little storage space and do some simple operations, which is suitable for low-cost RFID systems. Our protocol is performed faster since transmits all qubits together not separately in l rounds. In Table

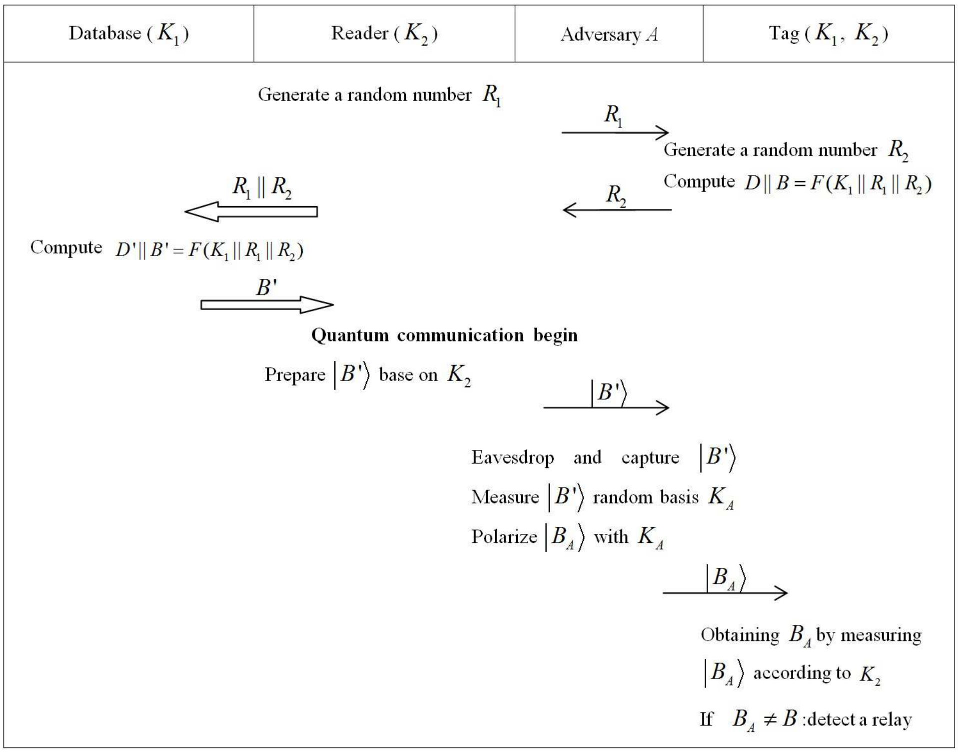

FIGURE 2. Relay qubits sent by Reader to Tag

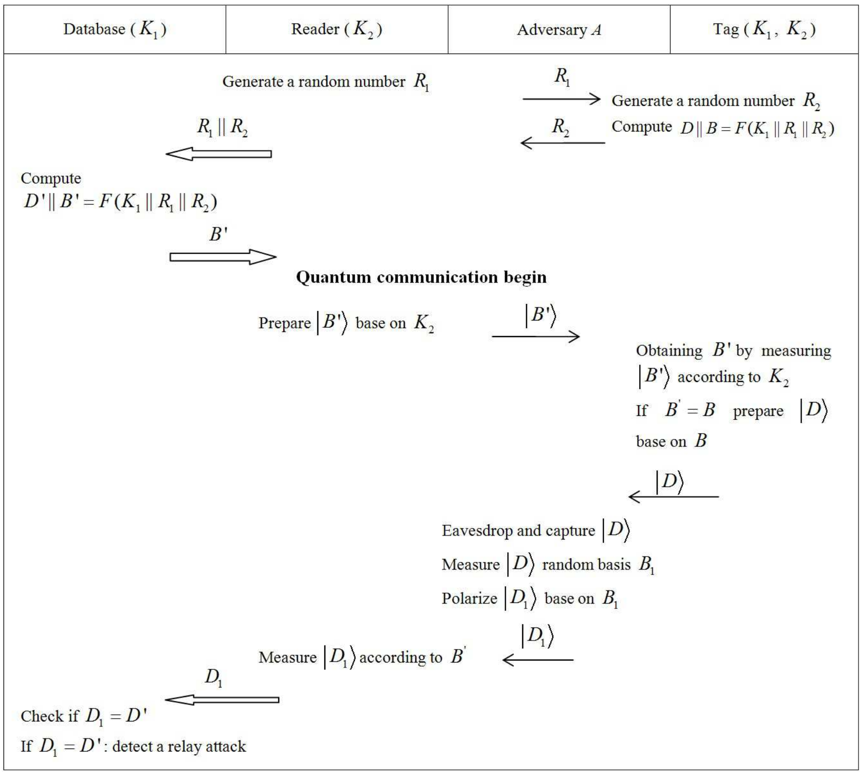

FIGURE 3. Relay qubits sent by Tag to Reader

3, we examine the performance of our scheme in terms of storage space, computational cost.

Storage space: In our scheme, the Tag has to store the secret key between Tag and Database,K_1 of length l, an l-bit secret key K_2. The Reader just stores an l-bit secret key K_2. Similarly, the Database stores an l-bit secret key K_1.

Computational cost: In our scheme, the tag only needs random number generation and pseudo-random function operation. While the Reader and the Database only need random number generation and pseudo-random function operation separately.

Table 3. Performance analysis

	Tag	Reader	Database
Storage space	$2l$	l	l
Computational cost	h	–	h
Notations: l: size of required memory, h: cost of a pseudo-random function operation			

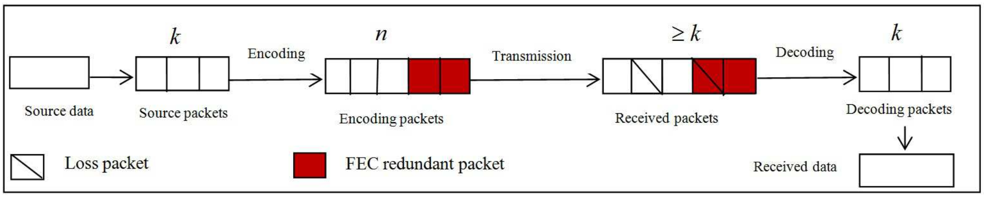

Figure 4. FEC mechanism

5. **Hardware requirements.** The Reader and Tag in the protocol have quantum devices that can polarize, measure, send/receive qubit. Our protocol makes Database and Tag has the ability to compute a pseudo-random function. In previous work, Mandal et al. [26] 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 [20].

The system should have FEC controllers, encoders and decoders. The FEC controller selects the appropriate number of packets and packets of blocks (k, n) according to the network environment. The encoder adds redundant operations to the transmitted packets k to get the block, then the controller transfers the data. The decoder decodes the received information to obtain the information sent by the sender [29]. This will be shown in Fig 5.

Zhang et al. [27] proposed the idea of applying quantum key distribution (QKD) technology to the client-server architecture. They put 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, our mechanism can integrate required devices of server and client required on the reader and the tag, in order to implement the technique proposed in this paper. 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.

However, manipulating quantum information in free space (such as in an RFID system) has some problems (such as reference frames being aligned). For example, the tag needs to receive the qubits, measure qubits, send the polarized state using the wave plate. In the case of fiber implementation, the direction is determined by fiber, which is easy to implement; however, in the case of an RFID system might present challenges [27].

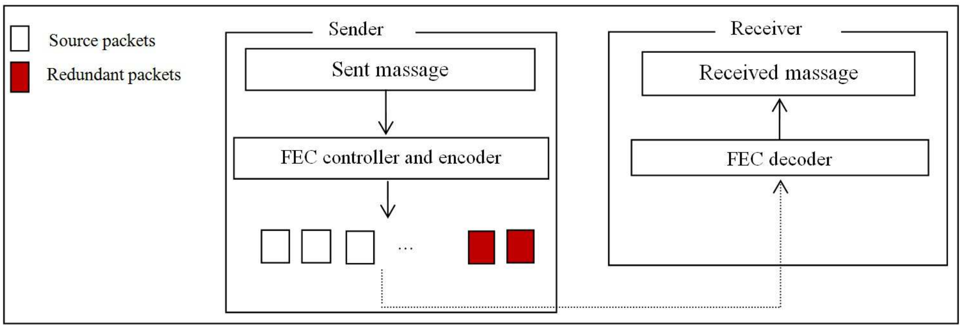

FIGURE 5. FEC in system

6. **Conclusion.** We described an efficient low-cost RFID protocol, mainly based on emerging quantum cryptography, which has no-cloning and non-deterministic properties. In our protocol, we bring in quantum technologies to protect the RFID systems from relay attack with simpler operation and lower resources. The protocol is proven secure against relay attacks. The tag and reader need abilities to measure, polarize, send/receive qubits and they perform classical bits and qubits via classical channel and quantum channel respectively. The database only needs to communicate with the reader through classical channel, which is thought a security channel. The security of our scheme is ensured by no-cloning and detection of adversary measurements of quantum mechanics. In addition, our protocol avoids precise RTT measurements though using qubits transmission, which make protocol more efficient and useful in low-cost RFID systems. In the future, if we integrate more quantum capabilities into tags and readers, we may have a higher probability of detecting relay attacks so that the current RFID systems more secure and efficient.

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

REFERENCES

[1] Y. Z. Li, Y. B. Cho, N. K. Um, and S. H. Lee, Security and Privacy on Authentication Protocol for Low-Cost RFID, *Computational Intelligence and Security, International Conference*, Guangzhou, China, pp.788–794, 2006.

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

[3] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, Security and privacy aspects of low-cost radio frequency identification systems, *Lecture Notes in Computer Science*, vol.2802, pp.201–212, 2003.

[4] K. L. Yong, and I. Verbauwhede, Secure and low-cost rfid authentication protocols, *Faseb Journal*, vol.21, pp.1–5, 2005.

[5] L. Gao, M. Ma, Y. Shu, and Y. Wei, An ultralightweight rfid authentication protocol with crc and permutation, *Journal of Network and Computer Applications*, vol.41, no. 1, pp.37–46, 2014.

[6] H. K.Chong, and G. Avoine, *RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks*, Springer Berlin Heidelberg, Germany, 2009.

[7] G. Hancke, A practical relay attack on iso 14443 proximity cards, *Technical Report*, no. 1, pp.1–13, 2005.

[8] S. Brands, and 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.

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

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

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

[12] 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.

[13] H. J. Wang, H. Zhang, J. X. LI, and X. Chen, A(3,3) visual cryptography scheme for authentication, *Journal of Shenyang Normal University (Natural Science Edition)*, vol.5, no. 2, pp.397–400, 2013.

[14] G. P. Hancke, Design of a secure distance-bounding channel for rfid, *Journal of Network and Computer Applications*, vol.34, no. 3, pp.877–887, 2013.

[15] C. H. Bennett, and G.Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proc. IEEE International Conference on Computers Systems and Signal Processing*, IEEE, pp.175–179, 1984.

[16] P. Zhang, K. Aungskunsiri, E. Martinlopez, J. Wabnig, M. Lobino, and R. W.Nock, 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.

[17] M. A. Nielsen, I. Chuang, and L. K. Grover, Quantum computation and quantum information, *Acm Sigsoft Software Engineering Notes*, vol.70, no. 5, pp.558–559, 2000.

[18] D. Henrici, and P. Muller, Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers, *IEEE Conference on Pervasive Computing and Communications Workshops*,IEEE Computer Society, pp.149, 2004.

[19] S. A.Weis, S. E. Sarma, R. L. Rivest and D. W.Engels, Security and privacy aspects of low-cost radio frequency identification systems, *Lecture Notes in Computer Science*, vol.2802, pp.201–212, 2003.

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

[21] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, *Physical Review A*, vol.73, no. 2, pp.457–460, 2005.

[22] Q. Y.Cai, Eavesdropping on the two-way quantum communication protocols with invisible photons, *Physics Letters A*, vol.351, no. 2, pp.23–25, 2006.

[23] Z. Sun, C. Zhang, B. Wang, Q. Li, and D. Long, Improvements on multiparty quantum key agreement with single particles, *Quantum Information Processing*,vol.12, no. 11, pp.3411–3420, 2013.

[24] J. Lin, and T. Hwang, New circular quantum secret sharing for remote agents, *Quantum Information Processing*,vol.12, no. 1, pp.685–697, 2013.

[25] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. Yuan, and A. J. Shields, Practical security bounds against the trojan-horse attack in quantum key distribution, *Quantum Physics*,vol.5, no. 3, pp.1–19, 2015.

[26] K. Mandal, X. Fan, and G. Gong, Warbler: a lightweight pseudorandom number generator for epc c1 gen2 tags, *?Radio Frequency Identification System Security* pp.73–84, 2012.

[27] P. Zhang, K. Aungskunsiri, E. Martinlopez, J. Wabnig, M. Lobino, and R. W.Nock, 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.

[28] M. F. Tsai, C. K. Shieh, C. H. Ke, Sub-packet forward error correction mechanism for video streaming over wireless networks, *Multimedia Tools and Applications*,vol.47, no. 1, pp.46–69, 2010.

[29] M. F. Tsai, N. Chilamkurti, and 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.