Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 8844178, 14 pages
https://doi.org/10.1155/2021/8844178

Research Article

A Novel Security Authentication Protocol Based on Physical Unclonable Function for RFID Healthcare Systems

He Xu,[1,2] **Xin Chen**,[1,2] **Feng Zhu**,[1,2] **and Peng Li**[1,2]

[1] *School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China*
[2] *Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Jiangsu Province, Nanjing 210023, China*

Correspondence should be addressed to Peng Li; lipeng@njupt.edu.cn

Received 26 August 2020; Revised 20 May 2021; Accepted 5 July 2021; Published 23 July 2021

Academic Editor: Arun K. Sangaiah

The Radio Frequency Identification (RFID) technology has been integrated into healthcare systems for the purpose of improving healthcare management. However, people have concerns about the security and privacy of this kind of RFID systems. In order to solve the security problems faced by RFID-based healthcare systems, a novel security authentication protocol based on Physical Unclonable Function (PUF) and Advanced Encryption Standard (AES) encryption algorithm is designed. The protocol uses PUF technology to output unique and random responses to different excitation inputs, encrypts the authentication information sent by the tag, and uses the AES encryption algorithm to encrypt the authentication information between the cloud database and the reader. At the same time, in the authentication process, once the communicating entity completes the identity authentication of the other two entities, it immediately starts to update the key. The security analysis and formal analysis of BAN (proposed by Burrows et al.) logic prove the security and correctness of the protocol. Analysis results show that the computation cost and security performance of the proposed protocol are better than the compared protocols. Our findings will contribute to further enhancing the security for RFID healthcare systems.

1. Introduction

Radio Frequency Identification (RFID) technology is one of the important technologies in the realization of Internet of Things (IoT). In RFID systems, radio frequency signal is used to achieve contactless authentication and identification. Because of its advantages of rapid identification and reuse rate, it has been widely used in many areas. As one of the key technologies of IoT, RFID technology has been applied to offer services like patient monitoring, drug administration, and medical asset tracking. However, people have concerns about the security and privacy of RFID-based healthcare systems. And RFID is widely used in healthcare monitoring system for patient safety and traceability [1–5]. With the feature of noncontact automatic identification, in recent years, RFID technology has been applied in healthcare systems for providing intelligent services such as patient monitoring, drug administration, and medical asset tracking. The improvement of drug management can help to reduce the number of medication errors. By integrating with RFID technology, hospitals can track medical assets in order to mitigate theft loss, improve resource utilization, and save costs. Thus, patients and medical staff can benefit a lot from these services.

However, the security risks brought by RFID healthcare systems have also attracted the attention of scholars and engineers, so many authentication schemes are proposed for RFID healthcare systems [6, 7]. Although an RFID-based healthcare system has lots of advantages over a traditional one, it suffers from new security and privacy risks. For example, if an adversary can track a tag embedded in the smart wristband of a patient, the location of the patient is known by the adversary. Furthermore, an adversary may impersonate as a legitimate reader to collect a patient's medical data from the patient's smart wristband, leading to medical privacy leakage. Hence, a suitable solution to secure RFID-based healthcare systems is urgently needed.

Over the last several years, researchers have proposed a variety of authentication schemes, aiming to secure RFID-based healthcare systems. In 2014, Zhao [8] proposed an

RFID authentication protocol based on elliptic curve cryptosystem (ECC) to secure communications in healthcare environments. Zhang and Qi [9] proposed an ECC-based RFID authentication protocol for medical systems to enhance patient safety. However, Farash et al. [10] analyzed the protocols in [8, 9] and pointed out that these two protocols cannot ensure forward secrecy. Farash et al. also suggested an improved protocol based on ECC to enhance the security of healthcare environments in [10]. Later, researchers proposed more ECC-based RFID authentication protocols [11–16] for healthcare applications. Because of the high hardware requirement of ECC, these ECC-based protocols are not well compatible with the EPC C1G2 standard.

In this paper, we use cloud database and active tag to get high security for RFID healthcare systems, which is compatible with the EPC C1G2 standard. In traditional RFID systems, the wireless channel between tag and reader is vulnerable to be attacked, and the channel between cloud database and reader is also vulnerable to network attack. In order to solve the previous problem, this paper combines Physical Unclonable Function (PUF) with one-way hash function and Advanced Encryption Standard (AES) encryption algorithm to realize a cloud-based RFID authentication protocol using active tag. The key contributions of this paper are as follows:

(1) Active tag and AES encryption are used to ensure the RFID systems' security to resist the typical wireless attacks, and we present a novel security authentication protocol based on Physical Unclonable Function is proposed for RFID healthcare systems

(2) In order to deduce the security goal and prove the security of the proposed protocol, we use BAN (proposed by Burrows et al. in reference [17]) logic, which is a security analysis model and is used for RFID application systems, to perform security analysis for our proposed protocol

(3) The proposed protocol updates the key at real time with the PUF and Cloud technology, which is more effective for privacy protection in RFID healthcare systems

The rest of this paper is organized as follows. Section II describes the security problems of RFID systems and physical unclonable technology. Section III describes related works. Section IV presents the proposed RFID security authentication protocol based on PUF and AES. The security analysis, proof of the proposed protocol, and computing overhead and space analysis are given in Section V. Section VI concludes the paper works.

2. An Overview of RFID System Security

2.1. Common Security Issues in RFID Healthcare Systems. RFID systems' devices communicate with each other in a common channel using radio frequency signals, which means that the signals between devices are basically exposed. In addition, because some RFID systems lack of security protection mechanism, attackers can attack RFID healthcare systems and illegally obtain the data using wireless signal analysis equipment which brings serious network security threats to enterprises and consumers. The following will make a specific description of common security attack means to RFID systems [18].

(1) *Counterfeiting Attack*. Some RFID security authentication protocols only require the reader to authenticate the tag, but not authenticate the reader. In this case, attackers can use forged readers or tags to impersonate trusted devices for authentication [19].

(2) *Replay Attack*. The attacker repeats the authentication message eavesdropped before to the reader or tag, trying to cheat the reader or tag to trigger it response.

(3) *Replication Attack*. The attacker completely copies the legal tag's information, and the cloned tag has the true ID and key information stored in the legal tag. When the reader sends the radio frequency signal to the covering area, the clone tag sends a response signal to the reader, which is consistent with the response signal generated by the legal tag.

(4) *Desynchronization Attack*. The attacker intercepts the information sent by the communication entity, so that the other party's communication device does not update the information [20]. In the next round of authentication, if the key information stored among the communication parties is inconsistent, the two parties will not be able to authenticate each other.

(5) *Tag-Tracking Attack*. The attacker intercepts the authentication information of reader and tag and infers information about the tag's or reader's identity.

(6) *Forward Privacy Attack*. After the attacker cracked an RFID tag, the information used in previous authentication can be inferred from the information in the authentication process.

2.2. Security Mechanism for RFID Systems. Aiming at various security problems encountered in RFID systems, security mechanisms can be divided into two categories: physical security mechanism and security authentication protocol.

The existing physical security mechanisms [21] mainly include Faraday cover, tag "kill" mechanism, and tag blocking. Although these physical security mechanisms protect the security of the RFID systems in a certain extent, but because these methods require additional hardware equipment, and once it is attacked while opening the defense mechanism which will affect the subsequent use of tags, so it is not practical in large RFID systems.

At present, the research on RFID security protocols based on logic method and encryption technology can be divided into the following three directions according to the complexity of encryption algorithm [22]: ultralightweight authentication protocol based on simple XOR logic operation, lightweight authentication protocol based on simple one-way function such as hash operation, and heavy-weight authentication protocol based on symmetric encryption or asymmetric encryption algorithm. Among them, the first two authentication protocols have limitations by the simplicity of the algorithm, so they are only suitable for occasions with low-security requirements. Compared with the first two authentication protocols, the encryption algorithm used in the heavy-weight authentication protocol is more complex, which is suitable for the occasions with high-security requirements.

2.3. Physical Unclonable Technology. For the problem of replication attack, some scholars put forward Physical Unclonable Function (PUF) technology. PUF technology is a group of micro delay circuits [23], which generates numerous unique and unpredictable "keys" by extracting the differences in the chip manufacturing process. The input is called challenge, and the output is called response. A group of input and output of PUF is called challenge-response pair (CRP). The relationship between CRP is only determined by some physical differences of devices. Because of the differences in the chip manufacturing process, it has the characteristics of nonduplication. Therefore, PUF technology makes the chip to have anticounterfeiting function.

The ideal PUF module has three characteristics [24]: uniqueness, unidirectionality, and invulnerability. These characteristics of ideal PUF are described as follows:

(1) *Uniqueness*. For the same excitation, the response generated by the same PUF module is the same, and the response generated by different PUF modules is different.

(2) *Unidirectionality*. The response generated by PUF module is unpredictable, and the excitation generating this response cannot be found through the response and specific PUF module.

(3) *Invulnerability*. Any physical attack on the device containing PUF module will result in the destruction of the physical characteristics of its PUF module [25]. Therefore, in any probability polynomial time, the success rate of physical attack on the device can be ignored.

3. Related Works

Chou et al. proposed a mutual authentication protocol based on the combination of elliptic curve cryptography (ECC) and hash function in reference [26]. The protocol authentication process does not involve inversion operation, which reduces the amount of calculation. In 2013, Liao and Hsiao analyzed the security problem in [27], proposed an RFID mutual authentication protocol based on ECC, and proved the security of the protocol. However, reference [8] points out that the Liao's protocol is easy to deduce the private key of the tag, and thus, a new RFID security authentication protocol based on ECC is proposed.

Liao and Hsiao proposed an RFID security authentication protocol based on ECC in reference [28] and claimed that the protocol can resist various attacks. However, He pointed out in reference [29] that the protocol could not resist tag-tracking attacks and counterfeiting attacks and did not meet the requirements of anonymity. Thus, an improved RFID security authentication protocol based on ECC was proposed. Zhang and Qi proposed a new RFID authentication protocol based on elliptic curve in reference [9] and proved that the protocol can well resist various attacks. However, in 2016, Farash et al. pointed out that the protocol in [10] does not have the ability to protect the forward privacy security of tags and proposed an improved protocol combining ECC and hash functions. Moosavi et al. also proposed an RFID mutual authentication protocol based on ECC and hash in reference [30], but Khatwani and Roy proved that the protocol could not resist DoS (denial of service) attack in reference [31].

Xie et al. proposed an RFID security authentication protocol in cloud environment in reference [32] and used virtual private network proxy to establish a secure back-end channel to provide users with anonymous access to the cloud. The structure of cloud database is an encrypted hash table. However, the session initiator of the protocol is the tag. If the attacker forges the tag and continues to send authentication request, it will cause denial of service (DoS) attack on cloud database.

In addition, with the development of RFID-based IoT technology, a blockchain-enabled distributed security framework using edge cloud and software-defined networking (SDN) is presented in the literature [33], where the SDN server is a kind of cloud server used in our proposed architecture. In literature [34], mobile edge computing is used in real-time industrial informatics which inspires us to present our protocol based on the cloud computing to enforce the RFID healthcare systems' security. In addition, the authors in literature [35] propose an energy-aware green adversary model for its use in smart industrial environment through achieving confidentiality, which gives us a motivation that our presented protocol should ensure the information confidentiality for RFID-based healthcare systems.

4. Proposed RFID Security Authentication Protocol Based on PUF and AES

Figure 1 shows the RFID and cloud-based healthcare system's architecture. Our proposed protocol runs on this architecture. This paper combines PUF technology and AES encryption algorithm to design a cloud-based RFID authentication protocol using active tag (C-RAPA) for RFID systems. In C-RAPA protocol, cloud database needs to perform AES encryption and one-way hash encryption capabilities, reader needs to perform AES decryption and one-way hash encryption capabilities, tag needs to have PUF module and perform one-way hash encryption. The symbols used in C-RAPA protocol are shown in Table 1.

4.1. Initialization Phase. The initialization phase of C-RAPA protocol needs to be carried out in a secure environment. In

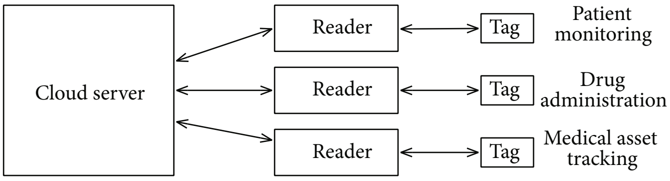

Figure 1: RFID and cloud-based healthcare system's architecture.

Table 1: Symbols used in the C-RAPA protocol.

Symbols	Representations
RID_n	The camouflage identifier of the reader in the n-th authentication process, with the length of L
TID_n	The camouflage identifier of the tag in the n-th authentication process, with the length of L
r_r	Random number generated by the reader in the authentication process, with the length of L
r_t	Random number generated by the tag in the authentication process, with the length of L
r_c	Random number generated by the cloud-based database in the authentication process, with the length of L
K_n	In the n-th session, the shared key used between the tag and the cloud-based database, with the length of L
K_r	In the n-th session, the shared key used between the reader and the cloud-based database, with the length of L
$\oplus$	XOR operation by bit
$H(X)$	One-way hash encryption operation of X
$PF_i = \text{PUF}(X_i)$	Get the response from PUF module when input X_i
$Y = E_K(X)$	AES encryption of data X with the key K
$X = D_K(Y)$	AES decryption of data Y with the key K

the secure initialization process, the initial key information among the cloud database, reader, and tag is established and shared. It can also be regarded as "identity registration" of tag, reader, and background database. At this time, the tag is new produced and has not communicated with the cloud database or reader. To facilitate the analysis, we select a reader that has never been authenticated with the cloud database to describe the following authentication process. In the initialization phase, the reader is also needed to register.

In this stage, the reader first sends initialization request information to the cloud database. After receiving the information, the cloud database generates a random number r_c with the length of L. The random number is sent to the reader. The reader received a random number r_c, and an initialization request information and a random number r_c are sent to tag. After the tag receives the initialization request information sent by the reader, as shown in equation (1), the random number r_c is regarded as the input to get the response PF_0 from the PUF module of the tag. At the same time, a random number r_t is generated. The true ID of the tag and the response PF_0 and random number r_t were recorded and sent to the reader.

$$PF_0 = \text{PUF}(r_c). \tag{1}$$

After the reader receives the true ID of the tag, response PF_0, and random number r_t, a random number r_r with length of L is generated. The random numbers r_t and r_r, response PF_0, the ID of the reader, and the ID of the tag are sent to the cloud database. After receiving the information, the cloud database uses the random numberr_c (generated by the cloud database and tag), the tag's ID, and response PF_0 to generate the camouflage mark $\text{TID}_0^{(C)}$ of tag, and the shared key $K_0^{(C)}$ of tag, the random number generated by the cloud database and the reader, and the ID of the reader are used to generate the reader's camouflage identity $\text{RID}_0^{(C)}$ and the shared key $K_0^{(CR)}$ with reader. Finally, the cloud database sends $\text{TID}_0^{(C)}$, $K_0^{(C)}$, and $\text{RID}_0^{(C)}$, $K_0^{(CR)}$ to the reader; the reader stores the camouflage identity $\text{RID}_0^{(C)}$ and the shared key $K_0^{(CR)}$, which is, respectively, regarded as R ID_0 and $K_0^{(cr)}$. Then, the reader sends $\text{TID}_0^{(C)}$ and $K_0^{(C)}$ to the tag. The tag holds the camouflage identity $\text{TID}_0^{(C)}$ and the shared key $K_0^{(C)}$ which is, respectively, regarded as TID_0 and K_0; then, the initialization process ends. The information stored in cloud database, reader, and tag is shown in Table 2.

In the authentication process, aiming at cloud database, readers, and tags, key information need to be saved, respectively: (1) the camouflage identification and shared key used in the previous round of authentication and (20) the camouflage identity and shared key used in this round of authentication. In the initialization stage, it is necessary to save the two groups of key information for subsequent authentication. Since the cloud database, tag, and reader have not been authenticated, the camouflage identification and key

Table 2: Storage information table in initialization phase.

Entity	Storage information
Tag	TID_0, K_0
Reader	RID_0, $K_0^{(cr)}$
Cloud database	$\mathrm{TID}_0^{(C)}$, $K_0^{(C)}$, $\mathrm{RID}_0^{(C)}$, $K_0^{(CR)}$, $\mathrm{TID}_{-1}^{(C)}$,$K_{-1}^{(C)}$, $\mathrm{RID}_{-1}^{(C)}$, $K_{-1}^{(CR)}$

information used in the last round of authentication are the following: $\mathrm{TID}_{-1}^{(C)}$, $K_{-1}^{(C)}$, $\mathrm{RID}_{-1}^{(C)}$, $K_{-1}^{(CR)}$, and the camouflage identity and the shared key used in this round of authentication are the following: $\mathrm{TID}_0^{(C)}$, $K_0^{(C)}$, $\mathrm{RID}_0^{(C)}$, $K_0^{(CR)}$. For tag, $\mathrm{TID}_0^{(C)} = \mathrm{TID}_{-1}^{(C)} = \mathrm{TID}_0$, and $K_0^{(C)} = K_{-1}^{(C)} = K_0$; For readers, $\mathrm{RID}_0^{(C)} = \mathrm{RID}_{-1}^{(C)} = \mathrm{RID}_0$, and $K_0^{(CR)} = K_{-1}^{(CR)} = K_0^{(cr)}$. The sequence diagram of initialization phase is shown in Figure 2.

4.2. Cloud Database Authentication Phase. At the end of the initialization phase, tags and readers begin to start the authentication phase which is shown in Figure 3, including cloud database authentication phase, reader authentication phase, and tag authentication phase.

While entering the stage of cloud database authentication, it indicates that the cloud database, reader, and tag have been successfully initialized. In the following descriptions, we assume it is the n-th authentication process among the cloud database, reader, and tag. In the n-th authentication process, the cloud database needs to store two groups of key information and the camouflage identity shared with the tag: $\mathrm{TID}_{n-1}^{(C)}$, $K_{n-1}^{(C)}$ and $\mathrm{TID}_n^{(C)}$, $K_n^{(C)}$, where $\mathrm{TID}_{n-1}^{(C)}$, $K_{n-1}^{(C)}$ represents the key information used in the $(n-1)$-th authentication process and $\mathrm{TID}_n^{(C)}$, $K_n^{(C)}$ represents the updated key information after the $(n-1)$-th authentication process, that is, the key information to be used for the n-th authentication which is stored by the tag. Similarly, the cloud database also stores two sets of the shared keys with the reader and the reader's camouflage identity: $\mathrm{RID}_{n-1}^{(C)}$, $K_{n-1}^{(CR)}$ and $\mathrm{RID}_n^{(C)}$, $K_n^{(CR)}$, where $\mathrm{RID}_{n-1}^{(C)}$, $K_{n-1}^{(CR)}$ represents the key information used in the $(n-1)$-th authentication process and $\mathrm{RID}_n^{(C)}$, $K_n^{(CR)}$ represents the updated key information after the $(n-1)$-th authentication process, that is, the key information to be used for the n-th authentication which is stored by the reader. In addition, in order to resist the desynchronization attack, the key information of reader and tag is saved, respectively, in cloud database. Which group of key information is stored by the tag and reader needs to be judged according to the information sent to the cloud database by the tag and reader in the authentication process. Next, the n-th authentication process will be described in detail.

In the stage of the cloud database authenticating the tag, firstly, the reader sends a request authentication information to the cloud database. After receiving the request authentication information, the cloud database generates a random number r_c and sends it to the reader. When the reader received the random number r_c, a random number r_r is generated, and after then, the random numbers r_r and r_c and the request authentication information are sent to the tag. After the tag receives the random numbers r_r, and r_c and request authentication information, as shown in formula (2), the random number r_c is selected as the input to the PUF module to produce the response PF_n. Then, it will generate a random r_t, as is shown in formula (3), and r_r, r_t, r_c, and K_n are used to perform one-way hash encryption to get the result A. At last, the tag sends the following value of A, TID_n, r_t, and PF_n to the reader.

$$PF_n = \mathrm{PUF}(r_c), \tag{2}$$

$$A = H(r_r \bigoplus K_n \bigoplus r_t \bigoplus r_c). \tag{3}$$

After the reader receives the result of tag's A, camouflage identity TID_n, random number r_t, and response result PF_n, the result A is saved. Next, as shown in equation (4), the reader performs one-way hash encryption using its RID_n, random numbers r_r and r_c, and the shared key $K_n^{(cr)}$ with the cloud database to get result B. At last, the reader sends the following value of PF_n, TID_n, RID_n, r_r, r_t, A, and B to the cloud database.

$$B = H\left(r_r \bigoplus K_n^{(cr)} \bigoplus r_c \bigoplus \mathrm{RID}_n\right). \tag{4}$$

After the cloud database receives response result PF_n, camouflage identity TID_n, RID_n, random numbers r_r and r_t, and the results A and B sent by reader, it first verifies the result B produced by the reader. The cloud database first searches the reader's RID_n in the database; there exist three kinds of situations:

(1) RID_n does not exist in the cloud database

If RID_n does not exist in the cloud database, it indicates that the reader is not an illegal one. At this time, the cloud database will refuse communication.

(2) $\mathrm{RID}_n = \mathrm{RID}_{n-1}^{(C)}$

If $\mathrm{RID}_n = \mathrm{RID}_{n-1}^{(C)}$, it shows that in the $n-1$ round of authentication process, after the cloud database completes authentication phase, the authentication information sent to the reader may be intercepted, or due to network problems, the reader does not receive the authentication information sent by the cloud database, so there is no update information for the key and camouflage identity. At this condition, the cloud database will use $\mathrm{RID}_{n-1}^{(C)}$ and $K_{n-1}^{(CR)}$ to make authentication with the reader.

(3) $\mathrm{RID}_n = \mathrm{RID}_n^{(C)}$

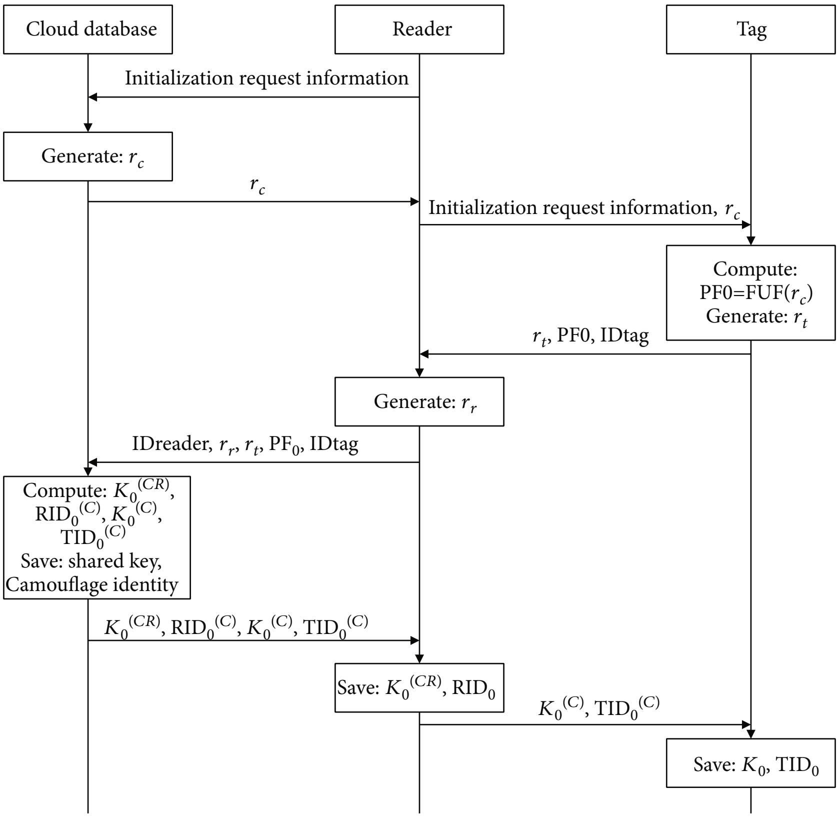
Cloud database
Reader
Tag
Initialization request information
Generate: r_c
r_c
Initialization request information, r_c
Compute:
PF0=FUF(r_c)
Generate: r_t
r_t, PF0, IDtag
Generate: r_r
IDreader, r_r, r_t, PF_0, IDtag
Compute: $K_0{}^{(CR)}$, $\mathrm{RID}_0{}^{(C)}$, $K_0{}^{(C)}$, $\mathrm{TID}_0{}^{(C)}$
Save: shared key, Camouflage identity
$K_0{}^{(CR)}$, $\mathrm{RID}_0{}^{(C)}$, $K_0{}^{(C)}$, $\mathrm{TID}_0{}^{(C)}$
Save: $K_0{}^{(CR)}$, RID_0
$K_0{}^{(C)}$, $\mathrm{TID}_0{}^{(C)}$
Save: K_0, TID_0

FIGURE 2: Sequence diagram of initialization phase.

If $\mathrm{RID}_n = \mathrm{RID}_n^{(C)}$, it shows that in the $n-1$ round of authentication process, after the cloud database sends the authentication information, the reader verifies the authentication information, passes the authentication process for cloud database, and updates the camouflage identity and shared key. At this condition, the cloud database will use $\mathrm{RID}_n^{(C)}$ and $K_n^{(CR)}$ to make authentication with the reader.

Take the third case as an example to explain the protocol process in detail. As shown in equation (5), after searching the RID_n, the cloud database will perform hash encryption using the reader's $\mathrm{RID}_n^{(C)}$, random numbers r_r and r_c, and the key $K_n^{(CR)}$ to get the result B'.

$$B' = H\left(r_r \bigoplus K_n^{(CR)} \bigoplus r_c \bigoplus \mathrm{RID}_n^{(C)}\right). \qquad (5)$$

Next, the cloud database needs to judge whether B is equal to B'. If $B \neq B'$, then the cloud database will refuse to communicate; otherwise, the cloud database will pass the reader authentication and continue to authenticate tag.

After completing the reader authentication, the cloud database starts to authenticate the tags. Cloud database first searches the tag's camouflage identity TID_n. The following are the three kinds of situations:

(1) TID_n does not exist in the cloud database

If TID_n cannot match any camouflage identity, it indicates that the tag is not a trusted one. At this time, the cloud database will refuse communication and terminate the entire protocol authentication process.

(2) $\mathrm{TID}_n = \mathrm{TID}_{n-1}^{(C)}$

If $\mathrm{TID}_n = \mathrm{TID}_{n-1}^{(C)}$, the shared key used by the tag is $K_n = K_{n-1}^{(C)}$, that is, the tag did not update the shared key in this round of session due to some reasons (such as network problems or network attacks). So, the cloud database will use $\mathrm{TID}_{n-1}^{(C)}$ and $K_{n-1}^{(C)}$ for this round of session, and the protocol will continue.

(3) $\mathrm{TID}_n = \mathrm{TID}_n^{(C)}$

If $\mathrm{TID}_n = \mathrm{TID}_n^{(C)}$, the shared key used by the tag is $K_n = K_n^{(C)}$, that is, the shared key used by the cloud database and the tag in this round of session is equal, which indicates that the cloud database, reader, and tag are normal and secure in the protocol authentication process. So, the cloud database will use $\mathrm{TID}_n^{(C)}$ and $K_n^{(C)}$ to communication with reader and tag at this round of session, and the protocol will continue.

Take the third case as an example to explain the protocol process in detail. In the following, we will descript the $\mathrm{TID}_n^{(C)}$

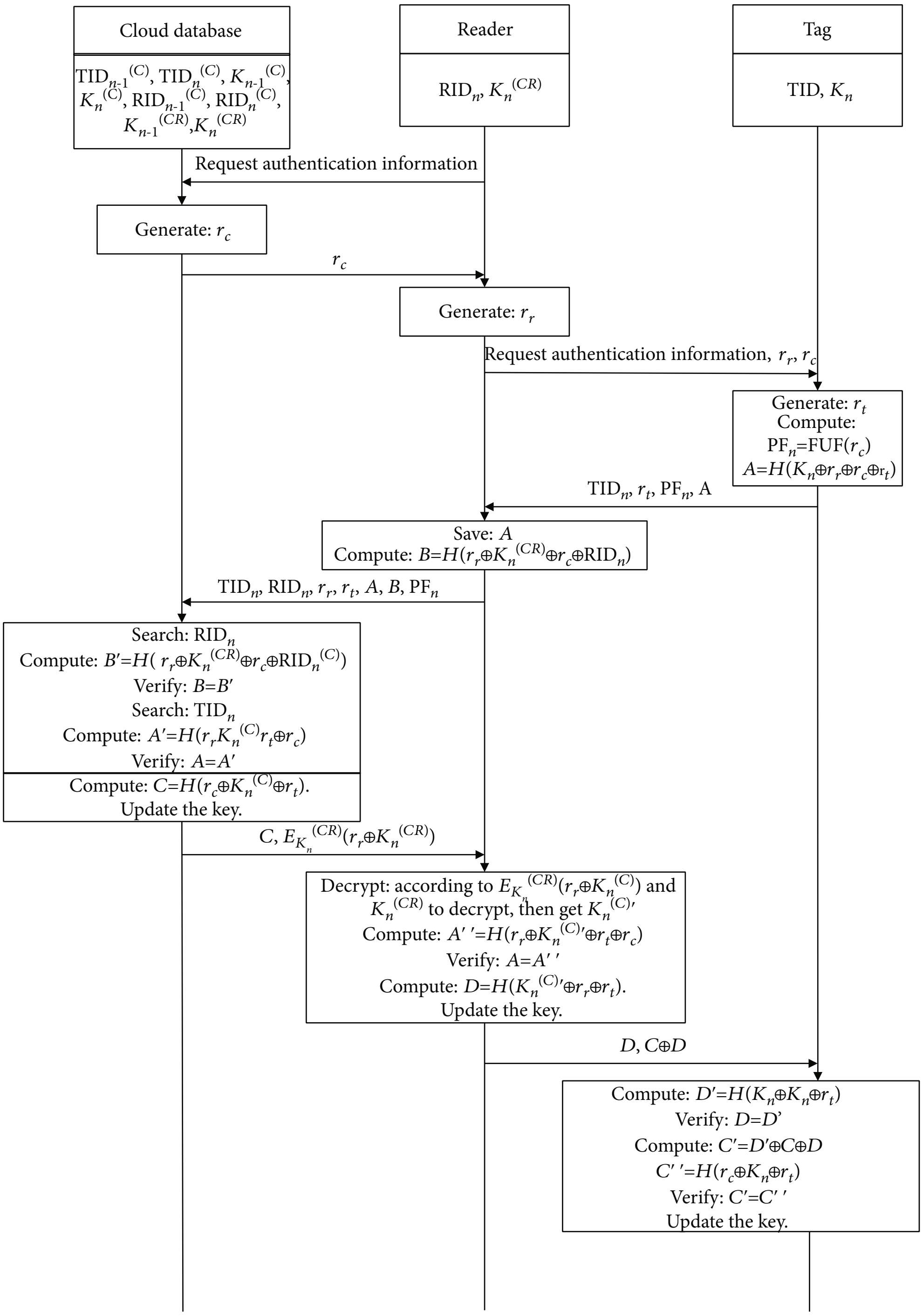
Cloud database
$\mathrm{TID}_{n\text{-}1}^{(C)}$, $\mathrm{TID}_n^{(C)}$, $K_{n\text{-}1}^{(C)}$, $K_n^{(C)}$, $\mathrm{RID}_{n\text{-}1}^{(C)}$, $\mathrm{RID}_n^{(C)}$, $K_{n\text{-}1}^{(CR)}$,$K_n^{(CR)}$
Reader
RID_n, $K_n^{(CR)}$
Tag
TID, K_n
Request authentication information
Generate: r_c
r_c
Generate: r_r
Request authentication information, r_r, r_c
Generate: r_t
Compute:
PF_n=FUF(r_c)
A=H(K_n⊕r_r⊕r_c⊕r_t)
TID_n, r_t, PF_n, A
Save: A
Compute: B=H(r_r⊕$K_n^{(CR)}$⊕r_c⊕RID_n)
TID_n, RID_n, r_r, r_t, A, B, PF_n
Search: RID_n
Compute: B'=H(r_r⊕$K_n^{(CR)}$⊕r_c⊕$\mathrm{RID}_n^{(C)}$)
Verify: B=B'
Search: TID_n
Compute: A'=H($r_r$$K_n^{(C)}$$r_t$⊕$r_c$)
Verify: A=A'
Compute: C=H(r_c⊕$K_n^{(C)}$⊕r_t).
Update the key.
C, $E_{K_n}{}^{(CR)}$(r_r⊕$K_n^{(CR)}$)
Decrypt: according to $E_{K_n}{}^{(CR)}$(r_r⊕$K_n^{(C)}$) and $K_n^{(CR)}$ to decrypt, then get $K_n^{(C)}$'
Compute: A''=H(r_r⊕$K_n^{(C)}$'⊕r_t⊕r_c)
Verify: A=A''
Compute: D=H($K_n^{(C)}$'⊕r_r⊕r_t).
Update the key.
D, C⊕D
Compute: D'=H(K_n⊕K_n⊕r_t)
Verify: D=D'
Compute: C'=D'⊕C⊕D
C''=H(r_c⊕K_n⊕r_t)
Verify: C'=C''
Update the key.

Figure 3: Sequence diagram of authentication phase.

and $K_n^{(C)}$ are used by the cloud database to make authentication with readers and tags.

As shown in equation (6), according to the random numbers r_r, r_t, and r_c and the key $K_n^{(C)}$, the cloud database will perform hash encryption to get the result A'; then, we compare whether A is equal to A'. If $A \neq A'$, then the cloud database will refuse to communication. Otherwise, the cloud database will pass the authentication for readers and tags.

$$A' = H\left(r_r \bigoplus K_n^{(C)} \bigoplus r_t \bigoplus r_c\right). \quad (6)$$

When the cloud database has completed the authentication of reader and tag, it needs to prepare for the next stage of reader authentication and tag authentication. At the same time, after the cloud database has verified $A = A'$, the key will be updated.

First of all, as shown in equation (7), the cloud database uses the random numbers r_c and r_t and key $K_n^{(C)}$ to perform one-way hash encryption to get the result C. Next, the cloud database uses the shared key $K_n^{(CR)}$ with the reader to perform AES encryption of the shared key $K_n^{(C)}$ between the cloud database and the tag to obtain the result $E_{K_n^{(CR)}}(r_r \bigoplus K_n^{(C)})$. Finally, the cloud database sends the result C and $E_{K_n^{(CR)}}(r_r \bigoplus K_n^{(C)})$ to the reader. At the same time, as shown in equations (8) and (9), the cloud database updates the key and the camouflage identity of the tag using the response PF_n and random numbers r_c and r_t. As shown in equations (10) and (11), the reader's key and camouflage identity are updated with the random numbers r_c and r_r, and then, the protocol will enter the next phase.

$$C = H\left(r_c \bigoplus K_n^{(C)} \bigoplus r_t\right), \tag{7}$$

$$K_{n+1}^{(C)} = H(r_c \bigoplus PF_n \bigoplus r_t), \tag{8}$$

$$\mathrm{TID}_{n+1}^{(C)} = H\left(K_{n+1}^{(C)} \bigoplus r_c \bigoplus PF_n \bigoplus r_t\right), \tag{9}$$

$$K_{n+1}^{(CR)} = H(r_c \bigoplus r_r), \tag{10}$$

$$\mathrm{RID}_{n+1}^{(C)} = H\left(K_{n+1}^{(CR)} \bigoplus r_c \bigoplus r_t\right). \tag{11}$$

4.3. Reader Authentication Phase. The purpose of this phase is to allow the reader to authenticate the identity of the tag and the cloud database. In previous section, we have discussed the cloud database authentication of readers and tags. If either of the reader or tag is illegal, the protocol process will be terminated. Therefore, in this section, assume that both the reader and the tag are trusted users. For convenience, the cloud database and tag use $\mathrm{TID}_n^{(C)}$, $K_n^{(C)}$, and cloud database and reader use $\mathrm{RID}_n^{(C)}$ and $K_n^{(CR)}$ to perform authentication. The following illustrates the detailed protocol process.

After the reader receives the result C and $E_{K_n^{(CR)}}(r_r \bigoplus K_n^{(C)})$ sent by the cloud database, firstly, the shared key $K_n^{(cr)}$ with cloud database is used to perform AES decrypt $E_{K_n^{(CR)}}(r_r \bigoplus K_n^{(C)})$; then, random number r_r with XOR operation is used to get the result $K_n^{(C)\prime}$. As shown in equation (12), the random numbers r_r, r_t, and r_c and the key $K_n^{(C)\prime}$ are combined to perform one-way hash encryption to get the result A''. At this time, the reader needs to compare the calculated result A'' with the saved value of A: if $A'' \neq A$, the reader will refuse communication; if $A'' = A$, in the process of calculating the result A'', the reader first needs to use the key $K_n^{(cr)}$ shared with the cloud database to decrypt and get the result $K_n^{(C)\prime}$, and after then, $K_n^{(C)\prime}$ and the random numbers generated by tag and cloud database are used by one-way hash encryption to get the result A''. Therefore, both the tag and the cloud database will be authenticated by the reader, as shown in equation (13), which uses random number r_r and decrypted key $K_n^{(C)\prime}$ to perform XOR operation, and one-way hash encryption is used to get the result D, and after then, the reader sends the result D and $C \bigoplus D$ to the tag. Finally, as shown in equations (14) and (15), the reader updates the key and camouflage identification, and the reader authentication phase ends.

$$A'' = H\left(r_r \bigoplus K_n^{(C)\prime} \bigoplus r_t \bigoplus r_c\right), \tag{12}$$

$$D = H\left(K_n^{(C)\prime} \bigoplus r_r \bigoplus r_t\right), \tag{13}$$

$$K_{n+1}^{(cr)} = H(r_c \bigoplus r_r), \tag{14}$$

$$\mathrm{RID}_{n+1} = H\left(K_{n+1}^{(cr)} \bigoplus r_c \bigoplus r_t\right). \tag{15}$$

4.4. Tag Authentication Phase. In this stage, the tag receives the result D and $C \bigoplus D$ sent by the reader. The tag uses the random numbers r_r and r_t and the result D where XOR operation is used for them to obtain result C. Then, as shown in equation (16), the tag uses the random number r_r and the shared key K_n to perform XOR operation and one-way hash encryption is used to get the result D', and finally, we compare D' and D. If $D = D'$, then the tag is authenticated to the reader. If $D \neq D'$, then the tag will terminate the protocol process.

$$D' = H(K_n \bigoplus r_r \bigoplus r_t). \tag{16}$$

Next, the tag will authenticate the cloud's reader. First, the tag uses the received $C \bigoplus D$ and D' calculated from equation (16) to obtain the XOR operation result C'. Then, as shown in equation (17), the tag uses the random numbers r_c and r_t and the shared key K_n to perform XOR operation and one-way hash encryption is used to get the result C'', and finally, the tag compares C' and C''. If $C'' = C'$, then the tag is authenticated to the cloud's reader. If $C'' \neq C'$, then the tag will terminate the protocol process.

$$C'' = H(r_c \bigoplus K_n \bigoplus r_t). \tag{17}$$

If the tag has passed the authentication of reader and cloud database, the tag will be shown in equations (18) and (19), combined with the response PF_n and random numbers r_c and r_t to update the key and the tag's camouflage identification, and then, the protocol process ends.

$$K_{n+1} = H(r_c \bigoplus PF_n \bigoplus r_t), \tag{18}$$

$$\mathrm{TID}_{n+1} = H\left(K_{n+1}^{(C)} \bigoplus r_c \bigoplus PF_n \bigoplus r_t\right). \tag{19}$$

At last, the n-th authentication process ends.

5. Security Analysis and Proof of Protocol

5.1. Security Analysis. In this section, we will mainly analyze C-RAPA protocol from two aspects: security analysis and BAN logic proof. C-RAPA protocol is a security

Table 3: Comparisons of different protocols' security.

Attack methods	C-RAPA protocol	Chou protocol [26]	Liao protocol [27]	Xie protocol [32]
Counterfeiting attack	✓	×	×	✓
Replay attack	✓	✓	✓	✓
Replication attack	✓	✓	✓	✓
Forward privacy attack	✓	×	✓	✓
Desynchronization attack	✓	✓	✓	✓
Tag-tracking attack	✓	✓	×	×

authentication protocol for RFID systems, which uses cloud database and active tags. The protocol uses AES encryption algorithm and PUF technology to ensure the reliability and security. AES encryption algorithm is used to encrypt the authentication information between cloud database and reader, and one-way hash function and PUF technology are used to encrypt the authentication information among the tag, the reader, and the cloud database. After the cloud database and tag pass the authentication between each other, the key update is started immediately and not waiting for the protocol process to complete.

The following contents show that the security of the protocol is verified by analyzing common attack methods.

(1) Counterfeiting attack

Attackers use fake readers or fake tags to attack the RFID systems.

In the cloud database authentication phase, the tag uses the random numbers r_r, r_t, and r_c and the shared key K_n to calculate the result A which will be sent to the reader, and after then, it will be forwarded to the cloud database. Cloud database searches the identification TID_n to obtain the shared key and calculate A' and determines the identity of the tag by verifying $A = A'$. In each round of authentication, the random number is randomly generated by the cloud database, reader, and tag in each round of session. After each round of authentication, the shared key will be updated by combining the random number and response by using one-way hash encryption. As a result, the attacker cannot calculate the value of the shared key and thus a counterfeit tag cannot calculate the result A. Similarly, the reader uses the random number and key to calculate and get the result A'' and determines the identification of the tag by verifying $A = A''$. The attacker cannot calculate the value of the key to get the result A'' to counterfeit the tag.

In the same way, attackers cannot use fake readers.

(2) Replay attack

The attacker eavesdropped the n-th authentication process and captured the authentication information: (1)r_t, TID_n, PF_n, A; (2) TID_n, RID_n, PF_n, r_r, r_t, A, B; (3) C, $E_{K_n^{(CR)}}(K_n^{(C)})$; and (4) D, $C \bigoplus D$. The attacker replays the information to the communicating entity, but the results A, B, C, and D depend on the random number generated in each round of authentication, and uses the updated key and the one-way hash to generate encryption value. Therefore, if the information replayed by the attacker is not equal to the result calculated by both sides of the communication, the replay attack fails.

(3) Replication attack

The proposed C-RAPA protocol is a security authentication protocol based on Physical Unclonable Function and AES encryption algorithm. Cloud database and tags update the key by using the response generated by Physical Unclonable Function for subsequent authentication. Because of the nonreplicability of PUF technology, the attacker cannot copy the same PUF module to produce the same response and pass the authentication. Therefore, the attacker's replication attack will fail.

(4) Forward privacy attack

Suppose that the attacker eavesdrops the n-th authentication process and cracks the authentication information to obtain the shared key. Since each round of key is encrypted and updated by one-way hash function, the attacker cannot calculate the key information used in the previous $n-1$ authentication from the key information of this round.

(5) Desynchronization attack

Suppose that the attacker eavesdrop some parts of the n -th authentication session and captures the authentication information: (1) r_t, TID_n, PF_n, A; (2) TID_n, RID_n, PF_n, r_r, r_t, A, B; (3) C, $E_{K_n^{(CR)}}(K_n^{(C)})$; and (4) D, $C \bigoplus D$. The attacker blocks the authentication information 3 to prevent the reader and tag from updating the key. In the $(n+1)$-th authentication, the attacker's desynchronization attack fails because the cloud database stores two groups of key information of tag and reader, respectively.

(6) Tag-tracking attack

In C-RAPA protocol, tag ID is only used in the initialization phase. At the same time, the tag needs to send authentication information r_t, TID_n, PF_n, A to the reader, and the reader will forward it to the cloud database, and after then, the cloud database and reader will authenticate the tag. The randomness of random number, the unidirectionality of response, and hash function make it impossible for attackers to infer the ID and other information of tags even if they eavesdrop on multiple sessions.

To sum up, the security comparison of the protocols mentioned above in C-RAPA protocol is shown in Table 3.

It can be seen from Table 3 that the Chou protocol [26] cannot resist counterfeiting attacks and forward privacy attacks. If the attacker breaks the n-th authentication, the $n-1$ communication between the tag and the reader will be cracked by the attacker. Liao protocol [27] cannot resist counterfeiting attacks and tag-tracking attacks. Attackers can obtain the real information of tags by tracing the authentication of specific tags. Similarly, Xie protocol [32] cannot resist tag-tracking attacks. Therefore, the C-RAPA protocol proposed in this paper has greater advantages in resisting common security attacks.

5.2. BAN Logic Proof. In this section, firstly, we will explain the BAN logic expression and derivation rules and then prove the correctness of the proposed C-RAPA protocol using BAN logic. BAN logic was proposed by Burrows et al. in 1989 [17]. In short, BAN logic is a kind of method based on reasoning structural, using logic system to infer whether the protocol meets its security specification by starting from messages sent and received by users through a series of axioms and rules. The steps of BAN logic proof include protocol description, protocol initialization, and the presentation and proof of the security objectives.

The BAN logic expression is as follows:

(1) *Expression 5-1:* $X\mid\equiv Y$. In the whole protocol process, subject X assumes that Y is trusted.

(2) *Expression 5-2:* $X\mid\sim Y$. Subject X has sent a message containing Y.

(3) *Expression 5-3:* $X\triangleleft Y$. Subject X receives a message containing Y.

(4) *Expression 5-4:* $X\mid\Rightarrow Y$. Subject X is used for the arbitration right of Y.

(5) *Expression 5-5:* $\#(X)$. Subject X appears for the first time in the protocol process.

(6) *Expression 5-6:* $X\overset{K}{\leftrightarrow}Y$. Subject X and subject Y have a shared key (K), and only X and Y know it and use the shared key (K).

(7) *Expression 5-7:* $\{X\}_K$. The ciphertext is obtained by encrypting X with the key (K).

BAN logic reasoning rules are as follows:

(1) The message meaning rule is shown in equation (20). If X believes the shared key K between X and Y, and X has received the ciphertext encrypted by the shared key K to Z, then X believes Y has sent Z. Note that this rule requires that X never sends Z

$$\frac{\left(X|\equiv Y\overset{K}{\leftrightarrow}X,X\triangleleft\{Z\}_K\right)}{X|\equiv Y|\sim Z}. \tag{20}$$

(2) The arbitration rule is shown in equation (21). If X believes that Y has sent Z, and X believes that Y believes Z, then X believes Z. This rule is used to get trust relationship between the two sides through a middleman

$$\frac{(X|\equiv Y|\Rightarrow Z,X|\equiv Y|\equiv Z)}{X|\equiv Z}. \tag{21}$$

(3) The trust rule is shown in equation (22). Only if X trusts Y and X trusts Z, then X trusts a set of messages sent by Y and Z

$$\frac{(X|\equiv Y,X|\equiv Z)}{X|\equiv\{Y,Z\}}. \tag{22}$$

(4) The message splitting rule is shown in equation (23), which can be recognized as the inverse proposition of belief rule. If X trusts a group of messages composed of Y, Z, and Q, then X trusts every clause in the group of messages

$$\frac{X|\equiv\{Y,Z,Q\}}{(X|\equiv Y,X||\equiv Z,X|\equiv Q)}. \tag{23}$$

(5) The freshness value verification rule (also called random number verification rule) is shown in equation (24), and the information with the participation of fresh random number can be trusted

$$\frac{(X|\equiv\#Y,X|\equiv Z|\sim Y)}{X|\equiv Z|\equiv Y}. \tag{24}$$

(6) Suppose Y appears for the first time in the protocol, and the sender X trusts Y; thus, the freshness value verification rule can be shown as equation (25).

$$\frac{X|\equiv\#Y}{X|\equiv\#\{Y,Z\}}. \tag{25}$$

(7) The rules for receiving messages are shown in equation (26) and equation (27), which indicates that X receives information containing Y and Z, which means that X receives information containing Y. Equation (27) shows that X trusts the shared key K between Y and X, and X receives the information sent by Y containing the ciphertext encrypted by Z using the shared key K; then, X can decrypt Z by using the shared key K, that is, X receives the information containing Z

$$\frac{X\triangleleft\{Y,Z\}}{X\triangleleft Y}, \tag{26}$$

$$\frac{\left(X|\equiv Y\overset{K}{\leftrightarrow}X,X\triangleleft\{Z\}_K\right)}{X\triangleleft Z}. \tag{27}$$

(8) The transmission rule is shown in equation (28). If X believes that Y has sent information containing Z and Q, then X also believes that Y has sent information containing Z

$$\frac{X|\equiv Y| \sim \{Z, Q\}}{X|\equiv Y| \sim Z}. \quad (28)$$

In C-RAPA protocol, there are three entities: cloud database (C), reader (R), and tag (T). The following will analyze and prove the n-th certification process.

The C-RAPA protocol is described as follows:

(1) $R \rightarrow C$: request

(2) $C \rightarrow R$: r_c

(3) $R \rightarrow T$: r_r, r_c, request

(4) $T \rightarrow R$: r_t, TID_n, PF_n, $H(r_r \bigoplus K_n \bigoplus r_t \bigoplus r_c)$

(5) $R \rightarrow C$: TID_n, RID_n, PF_n, r_r, r_t, $H(r_r \bigoplus K_n \bigoplus r_t \bigoplus r_c)$, $H(r_r \bigoplus K_n^{cr} \bigoplus r_c \bigoplus \mathrm{RID}_n)$

(6) $C \rightarrow R$: $H(r_c \bigoplus K_n^{(C)} \bigoplus r_t)$, $E_{K_n^{(CR)}}(K_n^{(C)})$

(7) $R \rightarrow T$: $H(K_n^{(C)\prime} \bigoplus r_r \bigoplus r_t)$, $H(r_c \bigoplus K_n^{(C)} \bigoplus r_t) \bigoplus H(K_n^{(C)\prime} \bigoplus r_r \bigoplus r_t)$

The initialization of C-RAPA protocol is as follows:

(1) $T|\equiv C \overset{\mathrm{TID}_n, K_n}{\leftrightarrow} T$

(2) $C|\equiv T \overset{\mathrm{TID}_n^{(C)}, K_n^{(C)}}{\leftrightarrow} C$

(3) $R|\equiv C \overset{K_n^{(cr)}}{\leftrightarrow} R$

(4) $C|\equiv R \overset{K_n^{(CR)}}{\leftrightarrow} C$

(5) $T|\equiv \#r_t$

(6) $R|\equiv \#r_r$

(7) $C|\equiv \#r_c$

(8) $C \triangleleft \mathrm{TID}_n$, RID_n, PF_n, r_r, r_t, $H(r_r \bigoplus K_n \bigoplus r_t \bigoplus r_c)$, $H(r_r \bigoplus K_n^{cr} \bigoplus r_c \bigoplus \mathrm{RID}_n)$

(9) $R \triangleleft H(r_c \bigoplus K_n^{(C)} \bigoplus r_t)$, $E_{K_n^{(CR)}}(r_r \bigoplus K_n^{(C)})$

(10) $T \triangleleft H(K_n^{(C)\prime} \bigoplus r_r \bigoplus r_t)$, $H(r_c \bigoplus K_n^{(C)} \bigoplus r_t) \bigoplus H(K_n^{(C)\prime} \bigoplus r_r \bigoplus r_t)$

Next, we propose the three security goals for C-RAPA protocol and prove their correctness using BAN logic.

Security Objective 1. The cloud database believes that the reader has sent information $H(r_r \bigoplus K_n \bigoplus r_t \bigoplus r_c)$, $H(r_r \bigoplus K_n^{cr} \bigoplus r_c \bigoplus \mathrm{RID}_n)$, that is,

$$C|\equiv R| \equiv \{H(r_r \bigoplus K_n \bigoplus r_t \bigoplus r_c), H(r_r \bigoplus K_n^{cr} \bigoplus r_c \bigoplus \mathrm{RID}_n)\}. \quad (29)$$

Prove.

(1) According to $C|\equiv R \overset{K_n^{(CR)}}{\leftrightarrow} C$ and $C \triangleleft \mathrm{TID}_n$, RID_n, PF_n, r_r, r_t, $H(r_r \bigoplus K_n \bigoplus r_t \bigoplus r_c)$, $H(r_r \bigoplus K_n^{cr} \bigoplus r_c \bigoplus \mathrm{RID}_n)$ and the rules of message meaning $(X|\equiv Y \overset{K}{\leftrightarrow} X, X \triangleleft \{Z\}_K)/X|\equiv Y| \sim Z$, the following can be deduced

$$C| \equiv R| \sim \{H(r_r \bigoplus K_n \bigoplus r_t \bigoplus r_c), H(r_r \bigoplus K_n^{cr} \bigoplus r_c \bigoplus \mathrm{RID}_n)\}. \quad (30)$$

(2) According to $C|\equiv \#r_c$ and the freshness validation rules $X|\equiv \#(Y)/\mathrm{X}|\equiv \#(Y, Z)$, the following can be deduced

$$C| \equiv \#\{H(r_r \bigoplus K_n \bigoplus r_t \bigoplus r_c), H(r_r \bigoplus K_n^{cr} \bigoplus r_c \bigoplus \mathrm{RID}_n)\}. \quad (31)$$

(3) According to the above two steps' results and freshness validation rules $X|\equiv \#(Y), X|\equiv Z| \sim Y/X|\equiv Z| \equiv Y$, the following can be deduced

$$C|\equiv R| \equiv \{H(r_r \bigoplus K_n \bigoplus r_t \bigoplus r_c), H(r_r \bigoplus K_n^{cr} \bigoplus r_c \bigoplus \mathrm{RID}_n)\}. \quad (32)$$

Thus, security objective 1 is proved.

Security Objective 2. The reader believes that the cloud database has sent the information $H(r_c \bigoplus K_n^{(C)} \bigoplus r_t)$, $E_{K_n^{(CR)}}(r_r \bigoplus K_n^{(C)})$, that is,

$$R|\equiv C| \equiv \left\{H\left(r_c \bigoplus K_n^{(C)} \bigoplus r_t\right), E_{K_n^{(CR)}}\left(r_r \bigoplus K_n^{(C)}\right)\right\}. \quad (33)$$

Prove.

(1) According to $R|\equiv C \overset{K_n^{(cr)}}{\leftrightarrow} R$, $R \triangleleft H(r_c \bigoplus K_n^{(C)} \bigoplus r_t)$, $E_{K_n^{(CR)}}(r_r \bigoplus K_n^{(C)})$ and the rules of message meaning $(X|\equiv Y \overset{K}{\leftrightarrow} X, X \triangleleft \{Z\}_K)/X|\equiv Y| \sim Z$, the following can be deduced

$$R|\equiv C| \sim \{H(PF_n \oplus r_t)\}. \quad (34)$$

(2) According to $R|\equiv \#r_r$ and the freshness validation rules $X|\equiv \#(Y)/X|\equiv \#(Y, Z)$, the following can be deduced

Table 4: Information stored in each stage of C-RAPA.

Process	Cloud database	Reader	Tag
Initialization	$\mathrm{TID}_n^{\mathrm{new}}$, K_n^{new}, $\mathrm{TID}_n^{\mathrm{old}}$, K_n^{old}, K_{rc}	K_{rc}, RID	TID_n, K_n
Cloud-based database authentication	$\mathrm{TID}_n^{\mathrm{new}}$, K_n^{new}, RID, K_{rc}, A, B, PF_n	K_{rc}, RID, A	TID_n, K_n
Reader authentication	$\mathrm{TID}_{n+1}^{\mathrm{new}}$, K_{n+1}^{new}, $\mathrm{TID}_{n+1}^{\mathrm{old}}$, K_{n+1}^{old}, K_{rc}	K_{rc}, RID, A	TID_n, K_n
Tag authentication	$\mathrm{TID}_{n+1}^{\mathrm{new}}$, K_{n+1}^{new}, $\mathrm{TID}_{n+1}^{\mathrm{old}}$, K_{n+1}^{old}, K_{rc}	K_{rc}, RID	TID_{n+1}, K_{n+1}, C, D

$$R| \equiv \#\left\{H\left(r_c \oplus K_n^{(C)} \oplus r_t\right), E_{K_n^{(CR)}}\left(r_r \oplus K_n^{(C)}\right)\right\}. \tag{35}$$

(3) According to the above two steps' results and freshness validation rules $X \mid \equiv \#(Y), X \mid \equiv Z \mid \sim Y/X| \equiv Z| \equiv Y$, the following can be deduced

$$R| \equiv C| \equiv \left\{H\left(r_c \oplus K_n^{(C)} \oplus r_t\right), E_{K_n^{(CR)}}\left(r_r \oplus K_n^{(C)}\right)\right\}. \tag{36}$$

Thus, security objective 2 is proved.

Security Objective 3. The tag believes that the cloud database has sent the information $H(K_n^{(C)\prime} \oplus r_r \oplus r_t)$, $H(r_c \oplus K_n^{(C)} \oplus r_t)$, that is,

$$T| \equiv C| \equiv \left\{H\left(K_n^{(C)\prime} \oplus r_r \oplus r_t\right), H\left(r_c \oplus K_n^{(C)} \oplus r_t\right)\right\}. \tag{37}$$

Prove.

(1) According to $T \mid \equiv C \overset{\mathrm{TID}_n, K_n}{\leftrightarrow} T$ and $T \triangleleft H(K_n^{(C)\prime} \oplus r_r \oplus r_t)$, $H(r_c \oplus K_n^{(C)} \oplus r_t) \oplus H(K_n^{(C)\prime} \oplus r_r \oplus r_t)$ and the rules of message meaning $(X| \equiv Y \overset{K}{\leftrightarrow} X, X \triangleleft \{Z\}_K)/X \mid \equiv Y \mid \sim Z$, the following can be deduced

$$T| \equiv C| \sim \left\{H\left(K_n^{(C)\prime} \oplus r_r \oplus r_t\right), H\left(r_c \oplus K_n^{(C)} \oplus r_t\right)\right\}. \tag{38}$$

(2) According to $T \mid \equiv \# r_t$ and the freshness validation rules $X \mid \equiv \#(Y)/X \mid \equiv \#(Y, Z)$, the following can be deduced

$$T| \equiv \#\left\{H\left(K_n^{(C)\prime} \oplus r_r \oplus r_t\right), H\left(r_c \oplus K_n^{(C)} \oplus r_t\right)\right\}. \tag{39}$$

(3) According to the above two steps' results and freshness validation rules $X \mid \equiv \#(Y), X \mid \equiv Z \mid \sim Y/X| \equiv Z| \equiv Y$, the following can be deduced

$$T| \equiv C| \equiv \left\{H\left(K_n^{(C)\prime} \oplus r_r \oplus r_t\right), H\left(r_c \oplus K_n^{(C)} \oplus r_t\right)\right\}. \tag{40}$$

Thus, security objective 3 is proved.

5.3. Computing Overhead Analysis. In this section, we will analysis the computing overhead of C-RAPA protocol in n times authentication process, which includes the following: cloud-based database authentication phase, reader authentication phase, and tag authentication phase. The PUF module will generate a corresponding operation for a random excitation which is referred to the PUF response time that is recorded as T_{PUF}. The time of one AES encryption and decryption is recorded as T_{AES}. The time of one-way hash encryption function is T_{Hash}. Generating a random number operation time is recorded as T_R. In the elliptic curve encryption algorithm, the time of one time point-addition is T_{EA}, and the time of multiplication of a point is T_{EM}.

In C-RAPA protocol, for cloud database, the time required is $3T_{\mathrm{Hash}} + T_{\mathrm{AES}} + T_R$ which includes the generating random number operation, three times of one-way hash encryption, and one AES encryption operation. For the reader, the time required is $3T_{\mathrm{Hash}} + T_{\mathrm{AES}} + T_R$ which includes the generating random number operation, three times of one-way hash encryption, and one AES decryption operation. For tags, it takes $3T_{\mathrm{Hash}} + T_{\mathrm{PUF}} + T_R$ to perform one random number generation operation, three times of one-way hash encryption, and one PUF response operation. Therefore, the whole RFID systems need a total time of 9 $T_{\mathrm{Hash}} + 2T_{\mathrm{AES}} + T_{\mathrm{PUF}} + 3T_R$ in the authentication process.

Chou protocol [26] needs two multiplication operations, three point-addition operations, and two times of hash operations in the authentication process, namely, $2T_{\mathrm{Hash}} + 2T_{EA} + 3T_{EM}$. In the authentication process of Liao protocol [27], there are two times of multiplication operations and five point-addition operations, namely, $2T_{EA} + 5T_{EM}$. Therefore, the computation time of C-RAPA protocol is less than that of Chou protocol [26] and Liao protocol [27]. In the process of communication, Xie protocol [32] needs to perform two times of random number generation operations, seven hash encryption operations, one AES encryption operation, and one AES decryption operation, namely, $7T_{\mathrm{Hash}} + 2T_{\mathrm{AES}} + 2$ T_R. Although the computation cost of Xie protocol [32] is less than that of C-RAPA protocol in two times of hash encryption, one time of PUF operation, and one time of generating random number operation, it can be seen from Table 3 that Xie protocol [32] does not have tag's anonymity, and PUF operation generated in C-RAPA protocol can resist replication attack. Considering the computation cost and security analysis, C-RAPA protocol is better than the compared three protocols.

5.4. Storage Space Analysis. In this section, the storage space of C-RAPA protocol is analyzed. Suppose the bit length of random number and shared key are both L, and the bit length of the results obtained by AES encryption algorithm and one-way hash encryption is also L. Therefore, in the C-RAPA protocol, the information stored in the cloud database, reader, and tag during the authentication process is shown in Table 4.

For cloud database, a total of $7L$ of space is required for specific tags, in the C-RAPA protocol process. For RFID tags, a total of $3L$ of storage space is needed in the C-RAPA protocol process. For RFID readers, a total of $4L$ of storage space is needed in the C-RAPA protocol process.

6. Summary

In this paper, aiming at the security requirements for RFID healthcare applications, combined with the characteristics of active tags and cloud database, we proposed an RFID security authentication protocol based on AES encryption algorithm and PUF technology. The presented protocol uses AES encryption algorithm to encrypt the authentication information between the cloud database and the reader, and PUF technology and one-way hash function are used to encrypt the authentication information among the tag, the reader, and the cloud database. Moreover, after the cloud database and tags pass the authentication between each other, they both immediately start to update the key, rather than wait until the end of the authentication process. Finally, the security and performance of protocol are analyzed, including the computing overhead and storage space.

This paper makes the following three main academic contributions: (1) a novel security authentication protocol based on Physical Unclonable Function is proposed for RFID healthcare systems, which use active tag and AES encryption to ensure the RFID systems' security to resist the typical wireless attacks. (2) BAN logic is used to deduce the security goal and prove the security of the proposed protocol, which gives a security analysis model for RFID application systems. (3) With the application of PUF and Cloud technology, the key in our protocol is updated at the real time while other protocols update the key at the end of the authentication process.

We expect our findings will contribute to further enhancing the security for RFID healthcare systems. And accordingly, this research results have many practical applications, such as in RFID-based intelligent transportation in Internet of Vehicle environment and RFID-based high security door system. We proposed a protocol to more effectively ensure the privacy of RFID holders that will be prepared for future smart and intelligent applications based on RFID technology.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Key R&D Program of China under Grant 2019YFB2103003, in part by the National Natural Science Foundation of China (No. 61602261, No. 61872196, No. 61872194, and No. 61902196), in part by the Scientific and Technological Support Project of Jiangsu Province (No. BE2019740, No. BK20200753, and No. 20KJB520001), in part by the Major Natural Science Research Projects in Colleges and Universities of Jiangsu Province (No. 18KJA520008), Six Talent Peaks Project in Jiangsu Province (RJFW-111), Postgraduate Research and Practice Innovation Program of Jiangsu Province (No. SJKY19_0761, No. SJKY19_0759, and No. KYCX20_0759), and in part by the 1311 Talent Plan of the Nanjing University of Posts and Telecommunications (NUPT).

References

[1] S. Khan, "Health care monitoring system in Internet of Things (IoT) by using RFID," in *IEEE's 6th International Conference on Industrial Technology and Management (ICITM 2017)*, Cambridge, UK, 2017.

[2] M. Haddara and A. Staaby, "RFID applications and adoptions in healthcare: a review on patient safety," *Procedia Computer Science*, vol. 138, pp. 80–88, 2018.

[3] B. Alsinglawi, Q. Nguyen, U. Gunawardana, A. Maeder, and S. J. Simoff, "RFID systems in healthcare settings and activity of daily living in smart homes: a review," *E-Health Telecommunication Systems and Networks*, vol. 6, pp. 1–17, 2017.

[4] H. Q. Omar, A. Khoshnaw, and W. Monnet, "Smart patient management, monitoring and tracking system using radio-frequency identification (RFID) technology," in *2016 IEEE EMBS Conference on Biomedical Engineering and Sciences (IECBES)*, Kuala Lumpur, Malaysia, 2017.

[5] M. P. María, D. Carlos, and G. Ángel, "Traceability in patient healthcare through the integration of RFID technology in an ICU in a hospital," *Sensors*, vol. 18, no. 5, p. 1627, 2018.

[6] N. Kumar, K. Kaur, S. C. Misra, and R. Iqbal, "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud," *Peer-to-Peer Networking and Applications*, vol. 9, no. 5, pp. 824–840, 2016.

[7] K. Fan, S. Zhu, K. Zhang, H. Li, and Y. Yang, "A lightweight authentication scheme for cloud-based RFID healthcare systems," *IEEE Network*, vol. 33, no. 2, pp. 44–49, 2019.

[8] Z. Zhao, "A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem," *Journal of Medical Systems*, vol. 38, no. 5, p. 46, 2014.

[9] Z. Zhang and Q. Qi, "An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography," *Journal of Medical Systems*, vol. 38, no. 5, p. 47, 2014.

[10] M. S. Farash, O. Nawaz, K. Mahmood, S. A. Chaudhry, and M. K. Khan, "A provably secure RFID authentication protocol

based on elliptic curve for healthcare environments," *Journal of Medical Systems*, vol. 40, no. 7, p. 165, 2016.

[11] C. Jin, C. Xu, X. Zhang, and J. Zhao, "A secure RFID mutual authentication protocol for healthcare environments using elliptic curve cryptography," *Journal of Medical Systems*, vol. 39, no. 3, p. 24, 2015.

[12] C. Jin, C. Xu, X. Zhang, and F. Li, "A secure ECC-based RFID mutual authentication protocol to enhance patient medication safety," *Journal of Medical Systems*, vol. 40, no. 11, p. 12, 2016.

[13] S. Qiu, G. Xu, H. Ahmad, and L. Wang, "A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems," *IEEE Access*, vol. 6, pp. 7452–7463, 2017.

[14] D. Abbasinezhad-Mood and M. Nikooghadam, "Efficient design of a novel ECC-based public key scheme for medical data protection by utilization of NanoPi fire," *IEEE Transactions on Reliability*, vol. 67, no. 3, pp. 1328–1339, 2018.

[15] V. Kumar, M. Ahmad, and A. Kumari, "A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS," *Telematics and Informatics*, vol. 38, pp. 100–117, 2019.

[16] K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," *International Journal of Information Security*, vol. 19, no. 1, pp. 129–146, 2020.

[17] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *ACM Transactions in Computer Systems*, vol. 8, no. 1, pp. 18–36, 1990.

[18] S. Zhou, W. Zhang, and J. Luo, "Survey of privacy of radio frequency identification technology," *Journal of Software*, vol. 26, no. 4, pp. 960–976, 2015.

[19] M. Wei and Z. Sun, "Open-loop RFID ownership transfer protocol based on PUF," *Journal of Cyber Security*, vol. 4, no. 4, pp. 19–32, 2019.

[20] S. D. Kaul and A. K. Awasthi, "Privacy model for threshold RFID system based on PUF," *Wireless Personal Communications*, vol. 95, pp. 2803–2828, 2017.

[21] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. E. Tapiador, and A. Ribagorda, "LMAP: a real lightweight mutual authentication protocol for low-cost RFID tags," *Workshop on RFID Security*, vol. 6, pp. 6–12, 2006.

[22] H. He, X. Chen, and L. Ukkonen, "Clothing-integrated passive RFID strain sensor platform for body movement-based controlling," in *2019 IEEE International Conference on RFID Technology and Applications (RFID-TA)*, pp. 236–239, Pisa, Italy, 2019.

[23] B. Leonid and R. Gabriel, "Physically unclonable function-based security and privacy in RFID systems," in *IEEE International Conference on Pervasive Computing and Communications*, pp. 211–220, White Plains, NY, USA, 2007.

[24] T. Idriss and M. Bayoumi, "Lightweight highly secure PUF protocol for mutual authentication and secret message exchange," in *IEEE International Conference on RFID Technology and Application*, pp. 214–219, Warsaw, Poland, 2017.

[25] H. Idriss, T. Idriss, and M. Bayoumi, "A highly reliable dual-arbiter PUF for lightweight authentication protocols," in *IEEE International Conference on RFID Technology and Application*, pp. 248–253, Warsaw, Poland, 2017.

[26] J. S. Chou, Y. Chen, and C. L. Wu, "An efficient mutual authentication RFID scheme based on elliptic curve cryptography," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 75–94, 2014.

[27] Y. P. Liao and C. M. Hsiao, "A secure ECC-based RFID authentication scheme using hybrid protocols," *Advances in Intelligent Systems and Applications*, vol. 2, pp. 1–13, 2013.

[28] Y. P. Liao and C. M. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol," *Ad Hoc Networks*, vol. 18, no. 7, pp. 133–146, 2014.

[29] J. He, *Research on RFID Mutual Authentication Protocol Based on ECC*, Xidian University, Xi'an, 2014.

[30] S. R. Moosavi, E. Nigussie, S. Virtanen, and J. Isoaho, "An elliptic curve-based mutual authentication scheme for RFID implant systems," *Procedia Computer Science*, vol. 32, pp. 198–206, 2014.

[31] C. Khatwani and S. Roy, "Security analysis of ECC based authentication protocols," in *International Conference on Computational Intelligence and Communication Networks*, pp. 1167–1172, Jabalpur, India, 2016.

[32] W. Xie, L. Xie, C. Zhang, and C. Tang, "Cloud-based RFID authentication," in *IEEE International Conference on RFID*, pp. 168–175, Orlando, FL, USA, 2013.

[33] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, "Blockchain-enabled distributed security framework for next-generation IoT: an edge cloud and software-defined network-integrated approach," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6143–6149, 2020.

[34] A. K. Sangaiah, D. V. Medhane, T. Han, M. S. Hossain, and G. Muhammad, "Enforcing position-based confidentiality with machine learning paradigm through mobile edge computing in real-time industrial informatics," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 7, pp. 4189–4196, 2019.

[35] A. K. Sangaiah, D. V. Medhane, G. B. Bian, A. Ghoneim, M. Alrashoud, and M. S. Hossain, "Energy-aware green adversary model for cyberphysical security in industrial system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3322–3329, 2020.