



# A Cloud-Based Distance Bounding Protocol for RFID Conforming to EPC-C1 G2 Standards

Zhenjiang Dong<sup>1,3(✉)</sup>, Xinluo Wang<sup>2</sup>, Miao Lei<sup>2</sup>, Wei Wang<sup>3</sup>, and Hui Li<sup>2</sup>

<sup>1</sup> Shanghai Jiao Tong University, Shanghai, China

<sup>2</sup> Beijing University of Posts and Telecommunications,  
Beijing 100876, People's Republic of China

{2013212985,lihui11}@bupt.edu.cn, sinper1005@163.com

<sup>3</sup> ZTE Cloud Computing and IT Research Institute,  
Nanjing, People's Republic of China

{dong.zhenjiang,wang.wei8}@zte.com.cn

**Abstract.** The development and maturation of cloud computing provides a new idea for deploying RFID systems. A Cloud-based RFID system becomes a new promising architecture. It can be offered as a service of cloud computing to individuals and organizations. However, the cloud-based RFID systems are confronted with more special security and privacy threats, especially the untrustworthy cloud provider and insecure backward communications. Unfortunately, most current RFID authentication schemes fail to meet the special security and privacy requirements of cloud-based RFID, i.e. to provide anonymity and confidentiality against the cloud and build secure backend channels. In this paper, we propose a secure distance bounding protocol for a RFID system, which is cloud-based RFID mutual authentication protocol compatible with the mature EPC-C1 G2 standards. It can effectively resist various threats in cloud environment comparing with other cloud-based RFID authentication protocol and reduce the success probability of a Mafia attack and make it lower than the optimal situation  $(1/2)^n$  in academic circles.

**Keywords:** RFID · Authentication · Distance bounding  
Cloud computing

## 1 Introduction

Radio Frequency Identification (RFID) is a wireless communication technology in which readers can automatically identify tags attached to objects and transfer data through radio signals without a mechanical or optical contact. Due to its ability for automatic identification and low cost, RFID systems are pervasively deployed in both military and civilian fields.

A traditional RFID system consists of three parts: a backend server, readers and tags. In this architecture, a reader relays messages from tags to a backend server and the backend server helps the reader to verify tags according to the database the server maintains. Readers and tags use a radio channel for communication which is commonly assumed to be insecure. While the private connection (wired or wireless) between a reader and the backend server is always assumed to be secure.

However, there exist some limitations in the deployment of traditional RFID systems. Firstly, establishing the entire RFID system would take high costs and therefore does not meet the small and medium-sized enterprises economic benefits, which greatly hinders the market promotion of RFID systems. Secondly, we need to erect a dedicated server and cables for a traditional RFID system, which is not suitable for a trans-regional enterprise.

Cloud-based RFID is a new promising architecture. It is composed of tags, readers, and a serving cloud to store and process data instead of the traditional backend server. Comparing with traditional RFID architecture, the cloud-based one has advantages in many aspects. Global deployment of the Internet and mobile networks make it available to access a cloud service almost everywhere. Therefore, the pervasive RFID service would be accessible using fixed or mobile readers over the Internet whenever and wherever needed. Moreover, users commitments for investment and operations are minimized, and costs are in direct relation to usage and demand.

Meanwhile, the cloud-based RFID systems are confronted with more special security and privacy threats, especially in two aspects:

Firstly, cloud-based RFID authentication schemes are required to secure backend communications besides protections of the frontend security. In the cloud-based RFID, readers access the public cloud through open Internet connections, which cannot be asserted as secure [1].

Secondly, cloud-based RFID authentication schemes are required to prevent tags from privacy-revealing to the untrustworthy cloud. In the cloud-based RFID, the cloud provider is not trusted by the reader holders; therefore, it needs provide tags with confidentiality of data storage and anonymity of access [1].

**Contribution:** In this paper, we introduce a novel cloud-based RFID authentication protocol. It is the first EPC C1 G2 standards compliant cloud-based RFID authentication protocol, which achieves mutual authentication between tags and readers, and scalability with  $O(1)$  computational complexity of verifying a tag. It is proved to be resistant to various attacks like impersonating attack, terrorist attack, desynchronizing attack and tracking attack. Meanwhile, its able to reduce the probability of a Mafia attack less than the optimal  $(1/2)^n$ .

**Organization:** Sect. 2 gives the current state of the art and explain the necessity of our work. The proposed protocol is presented in Sect. 3, followed by security analyses and comparisons with another representative cloud-based RFID authentication scheme in Sect. 4. At last, we conclude the article in Sect. 5.

## 2 Background

### 2.1 Existing Attacks and Related Work on RFID Security Schemes

This subsection will introduce some attacks, they still exist in RFID scheme and threaten RFID's security and privacy.

As [2] said, An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system or in a communications protocol. In RFID scheme, this attack can make impersonated adversary be regarded as a real tag or a authority reader to corrupt the RFID security.

As for the Mafia Fraud, according to the paper [3], an adversary can use the pre-ask or post-ask strategy to achieve this attack, and the former is more effective. That is, before attacking the reader, the adversary sends predicted challenges  $C'_j$ s to the tag and gets the responses  $R'_j$ s from the tag. Then the adversary executes the rapid bit exchange with the reader and receives the challenges  $C_j$ s. In half of all cases, the adversary has guessed the right challenge bit, that is  $C'_j = C_j$ , so the adversary sends the correct response with probability of 1. Otherwise, if  $C'_j \neq C_j$ , the adversary can reply with a guessed bit and its probability of being correct is 1/2. If just considering the rapid bit exchange, the adversary therefore has a 3/4 probability of replying correctly for each challenge bit and hence  $(3/4)^n$  for the n-round rapid bit exchange.

The Terrorist Fraud is an attack where an adversary defeats a distance bounding protocol with a man-in-the-middle between the reader and a dishonest tag located outside of the neighborhood, such that the latter actively helps the adversary to maximize her attack success probability, without giving to him any advantage for future attacks. The definition of the Terrorist Attack means the dishonest tag cannot give the adversary the secrets or the information with which the adversary can determine the secrets.

In Tracking Attack, attackers usually disguise as one or more real readers and send authentication messages to each tags. So the attacker can get and analyze the response messages from tags and track the movements of each tag.

The Desynchronizing Attack is based on the protection of Tracking Attack. In order to prevent the tag from returning the same message and being tracked, the RFID system requires synchronizing the label and the backend database and refresh the authentication key from time to time. After refreshed, both the tag and reader will save the new key for the next authentication process, so after synchronization, the message returned by tag is different from previous one. Therefore, if attacker interrupts the update process, the label will not be able to update the key, when the next scan, the label using the key and the reader is not the same, the reader will prohibit the label authentication request, thus deleting the label.

In 1987, Desmedt et al. [4] introduced the Mafia Fraud and Terrorist Frauds that can defeat all the RFID authentication protocols. In these attacks, an adversary can successfully pass the authentication by simply relaying the signals between reader and tag without dealing with the authentication cryptography.

To resist these frauds, one idea is to measure the round trip time of exchanged messages between the reader and tag.

In 1993, Brands and Chaum [5] proposed the first distance-bounding protocol with this idea to prevent Mafia Fraud while leaving the Terrorist Attack as an open issue.

In 2005, Hancke and Kuhn [6] published a new distance bounding protocol which become a key reference later.

In 2013, Xie et al. [1] provide a new RFID authentication architecture focused on solving the security and privacy challenges about the cloud-based RFID. It is the first research considered this new architecture and we will discuss it in next subsection.

In 2014, protocols [7–9] which use the round trip time method have been proposed to resist against Mafia and Terrorist attacks. And they agree that the maximum resistance to mafia frauds is  $(1/2)^n$ , which is the probability of a naive adversary who answers randomly to the -verifiers challenges during the rapid bit exchange phase.

## 2.2 When RFID Meets Cloud Computing

As the development of cloud computing. The cloud-based RFID architecture has attracted more attentions. However, new architecture brings new problems about security and privacy. In the cloud-based RFID, reader holders do not totally trust the cloud provider. They need to keep data plain-text from exposing to the cloud while using the computing and storage resources of the cloud, and even to maintain anonymity of tags from cloud in the process of authentication. Existing traditional RFID authentication protocols are obviously inapplicable to cloud-based applications.

Besides, to the best of my knowledge, up to now not many researches have fully considered the security challenges in cloud environment. The research in [1] is the one considered that, while the other cloud-based RFID schemes [10–13] did not. However, the protocol in [1] still cannot resist Tracking Attack, Mafia Attack [4] and Terrorist Attack [4]. Take the Tracking Attack as an example: after truncating the last message in the protocol, an adversary can track the tag by eavesdropping the first message  $H(R||T||S)$  next time the protocol executed. Furthermore, the reader in this scheme needs to search the cloud constantly which may increase network delay and result in low efficiency. Besides, the scheme is designed based on hash functions, difficult to be compatible with the prevailing EPC Class 1 Generation 2 standards.

## 2.3 EPC RFID Standard

In order to foster and publicize RFID technology, standardization is certainly important to allow interoperability at large scale. As one of the most viable standard providers, EPCglobal Inc is focusing on the area of logistical supply chain and try to enhance the transparency and traceability of supply chain.

And Being compatible with ISO – another biggest RFID standard provider can ensure the EPC standard’s compatibility. The latest RFID standard ratified by EPCglobal is named UHF Class 1 Gen 2 Standard version 2.0.0 (EPC-C1 G2 RFID for short) [14]. Three properties of a G2 RFID tag are briefly listed as follows:

- G2 RFID tag is passive, meaning that its power is triggered by the readers.
- G2 RFID tag communicates with readers in UHF band (800–960 MHz) and its communication range is from 2 m to 10 m.
- G2 RFID tag only supports on-chip Pseudo-Random Number Generator (PRNG) and Cyclic-redundancy check (CRC).

In recent years, several protocols [15–18] are compatible with the EPC-C1 G2 standards have been proposed. However, most of them are vulnerable to Tracking Attack and Desynchronizing Attack [19–22]. And this paper [20] points out that the two kinds of attacks are both based on the linear attributes of CRC functions.

### 3 Proposal

Since the EPC-C1 G2 standards stipulates that G2 RFID tag only supports PRNG and CRC function as well as other lightweight operations such as XOR and concatenation, A cloud-based RFID authentication protocol is designed to conform to the EPC-C1 G2 standards.

#### 3.1 Notations and Attack Model

Notations in the protocol are listed in Table 1.

**Table 1.** Notations

| Symbol      | Meaning  |
|-------------|--|
| $K_1$       | Authentication keys shared between a reader and a tag    |
| <i>Info</i> | Any data relevant to a session about the tag             |
| $E()$       | A symmetric encryption function in the reader            |
| $D()$       | A symmetric decryption function in the reader            |
| $K_2$       | The private key of $E()$ and $D()$                       |
| $PRNG()$    | A secure one-way pseudo-random number generator function |
| $ID/PRN$    | A random number generated by $PRNG()$                    |
| $N_R$       | A random number generated by a reader                    |
| $N_T$       | A random number generated by a tag                       |
|             | The concatenation operation                              |

To facilitate the subsequent analysis, a reasonable attack model about system security in this paper is shown as follows:

- The frontend communication is unsafe. A reader and a tag use a radio channel for communication on which an attacker can easily eavesdrop, tamper, delete and replay the messages.
- In backward channel, readers and the cloud will communicate through VPN connections. As [1] said, since the VPN agency can offer a reader a random virtual IP address in each login, the malicious can not link the same reader from different access sessions based on the source IP address in IP packets. So in network layer, we think the VPN can protect the readers' anonymity and we do not consider an adversary to intercept, block, and resend TCP/IP packets in this layer.
- The cloud provider is not trusted and may be malicious or vulnerable. Therefore, the protocol needs to provide anonymous access and confidentiality for a tag.
- Before the authentication step, there exists a procedure that the tags are securely enrolled in this RFID system. So the RFID reader can share the authentication key  $K_1$  with each enrolled tags, and the tags' original information  $(ID_i, E_{K_2}(Info_{origin}))$  will be stored in the cloud server.

### 3.2 Description of Our Protocol

The architecture of our protocol is depicted in Fig. 1. On the backward channel, similar to [1], mobile or fixed readers anonymously access the cloud through wireless or wired VPN connections, and an encrypted PRN table which is similar to the Encrypted Hashed Table in [1] is constructed. The index is a random number generated by PRNG() function, and the record indexed by the random number is the  $E_{K_2}(info)$ , it is a cipher text using a reader-defined encryption algorithm with a reader-managed key  $K_2$ . So all of the data in cloud are encrypted by reader-self to prevent tags secrets from revealing to the cloud. While on the frontend communication, a distance bounding technology is utilized between a reader and a tag for distance detection to resist Mafia attacks.

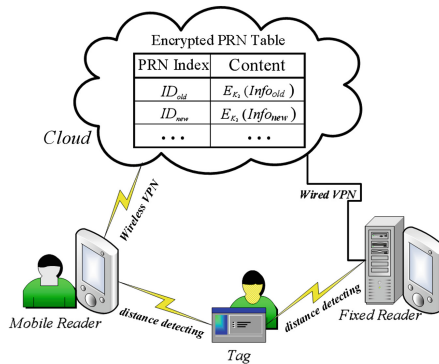


Fig. 1. A security architecture for cloud-based RFID authentication

As illustrated in Fig. 2, the proposed cloud-based RFID authentication protocol can be logically split into three stages: the distance-bounding stage, the mutual authentication stage and the data-updating stage.

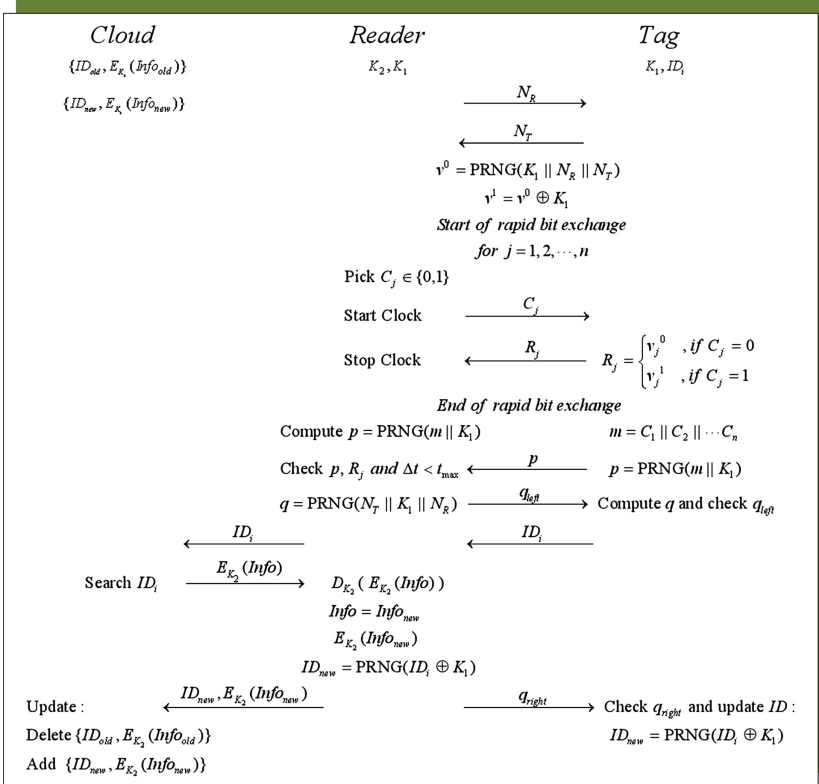


Fig. 2. The proposed protocol

**Distance-Bounding.** The reader and the tag first generate a random number  $N_R$ ,  $N_T$  respectively and send to each other. Then they both calculate  $v^0 = PRNG(K_1 || N_R || N_T)$  and  $v^1 = v^0 \oplus K_1$  to prepare for rapid bit exchange. During each round of the n-round rapid bit exchange, the reader chooses a random timing bit  $C_j$  to challenge the tag and the tag immediately responds  $R_j$  on receiving  $C_j$ .  $R_j$  is jointly determined by  $j$ ,  $v^0$ ,  $v^1$  and  $C_j$ . That is, if  $C_j = 0$ , the value of  $R_j$  is taken from the j-th bit of  $v^0$ , else, it is from  $v^1$ . The timing of each round starts when the reader sends  $C_j$  and stops on receiving  $R_j$ . After the rapid bit exchange, the reader checks  $R_j$  and  $\Delta t$ .

**Mutual Authentication.** Both the reader and the tag take bits  $C_j$ s and concatenate them to an  $m$ , and then compute  $p = PRNG(m || K_1)$ . Then the tag

sends  $p$ . Upon receiving  $p$ , the reader checks its correctness and rejects the tag if false. Else, the reader calculates  $q = PRNG(N_T || K_1 || N_R)$  and sends its left half part  $q_{left}$  to the tag. The tag also computes  $q$ , and then checks the receiving  $q_{left}$ . If it fails, the tag terminates the protocol; else, it continues.

**Data-Updating.** The tag sends data to the reader, and the reader forwards it to the cloud. Then the cloud looks up the corresponding record (current record) using this pseudo-random number index, and returns the cipher texts of the tag to the reader. The reader will then decrypt, data process, encrypt into cipher texts, and update  $ID_{new} = PRNG(ID_i \oplus K_1)$ . At last, the reader sends back the new record to the cloud and notify the tag to update  $ID$  with the right half part  $q_{right}$ . After receiving the new record, the cloud keeps the current record, deletes other old records and adds the new record. Simultaneously, if  $q_{right}$  is correct, the tag then computes  $PRNG(ID_i \oplus K_1)$  as the new index  $ID_{new}$ .

## 4 Security Analysis

The following part will analyze and evaluate how our protocol performs against these attacks.

**Anonymity and Confidentiality Against the Cloud.** Since all the records in the cloud are encrypted by readers with a symmetric algorithm  $E_{K_2}$  and only these readers possess the key  $K_2$ , so the confidentiality is achieved. Using pseudo random number indexes not only can accelerate the searching speed and achieved scalability, which is conducive to support large-scale applications, but can also guarantee an anonymous access for a tag. In addition, as said in the assumption in attack model, we ensure that the VPN technology on the backward channel can ensure the security of communication between readers and the cloud.

**Impersonation Attack Resistance.** The protocol supports distance detection and more importantly, mutual authentication between a reader and a tag, therefore the authenticity of both parties is achieved.

**Mafia Attack Resistance.** As shown in background, the Mafia Fraud can be achieved by pre-ask or postask strategy. If consider the rapid bit exchange only, the adversary therefore has a  $3/4$  probability of replying correctly for each challenge bit and hence  $(3/4)^n$  for the  $n$ -round rapid bit exchange. However, as a matter of fact, in the mutual authentication phase the presence of  $p$  could provide the reader with the list of challenges received by the genuine tag and adds a line of defense to a mafia attacker. The premise of generating  $p$  is to obtain all the random challenge bits. Therefore, the security of  $p$  relies on the security of function  $PRNG()$ . According to the EPC Class 1 Generation 2 standards, the pseudo-random function  $PRNG()$  is a one-way function similar to a hash function, i.e. it is nearly impossible (a probability less than 0.025% [14]) to deduce



the seed parameter in parentheses using the pseudo random number generated by this function, namely  $m||K_1$ . When the length of  $p$  is 1, the probability that the adversary guesses correctly shall be  $(1/2)^l$ . Hence, the maximum success probability of a mafia attack is  $(3/4)^n \times (1/2)^l$ , the actual probability depends on the length of  $PRNG()$ , but if the length  $l$  is long enough, the probability is less than  $(1/2)^n$  which is the maximum resistance to Mafia Fraud in academic circles [7–9] while  $(3/4)^n$  in most cases.

**Terrorist Attack Resistance.** In our protocol, the dishonest tag cannot provide the registers  $v^0$  and  $v^1$  to the adversary since the adversary can determine the key  $K_1 = v^0 \oplus v^1$ . So tags cannot help the attacker without any leakage on the long term key  $K_1$ . Therefore, the protocol is resistant to Terrorist Fraud.

**Desynchronizing Attack Resistance.** Consider the attack in [20], an adversary intercepts or manipulates the last message  $q_{right}$  the reader sends to the tag. In fact, the tag will not update  $ID$  either way due to check failure. When the tag communicates with the reader next time, the cloud can still retrieve a record of the tag.

**Tracking Attack Resistance.** Assuming that an attacker obtains the index  $ID$  after eavesdropping on the exchanges between a reader and a tag, when attacker eavesdrops next time, it cannot track the tag for the  $ID$  has been updated. Supposing that the attacker counterfeits a reader to cheat the tag, because the tag needs to check  $q_{left}$  before it transmits  $ID$ , the attacker would ultimately be unable to provide  $q_{left}$  and cannot get  $ID$ .

Table 2 shows a comparison between our protocol and [1]. In terms of performance, the computation complexity for the cloud to verify a tag are both  $O(1)$ . In our protocol, the tag only needs to execute PRNG functions while it needs to execute 4 Hash functions in [1], which is not supported by the EPC-C1 G2 standards.

**Table 2.** Comparison of cloud-based authentication protocols

| Protocol     | Complexity to verify a tag | Mafia | Terrorist | tracking | EPC-C1 G2 compliant |
|--------------|----------------------------|-------|-----------|----------|---------------------|
| Xie [1]      | $O(1)$                     | No    | No        | No       | No                  |
| Our protocol | $O(1)$                     | Yes   | Yes       | Yes      | Yes                 |

In summary, our protocol can provide anonymity and confidentiality protection for a tag against the cloud and effectively resist impersonating reader attacks, impersonating tag attacks, Mafia attacks, Terrorist attacks, desynchronizing attacks and tracking attacks. Compared with the protocol in literature [1],

it keeps the high efficiency of verifying a tag for the cloud, further strengthens the security of a cloud-base RFID system, and makes the system be compatible with current mature EPC-C1 G2 standards.

## 5 Conclusions

In this paper, two main security challenges of a cloud-based RFID system have been considered, i.e. the untrustworthy cloud provider and the insecure backward communication. Most current RFID authentication protocols did not fully consider the above security challenges and therefore inapplicable to cloud-based applications. Besides, they are not compatible with the prevailing EPC Class 1 Generation 2 standards. Moreover, many RFID authentication protocols are threatened by Mafia Frauds and Terrorist Frauds. A distance bounding protocol, as a possible measure, is not yet efficient enough to resist. Motivated by the above, the first EPC-C1 G2 standards compliant cloud-based RFID authentication protocol has been purposed, which can preserve tags users privacy from leaking to the cloud and defend against various attacks. Besides, we improved the distance-bounding technology and it can effectively reduce the success probability of a Mafia attack.

Future works include that we keep on improving the distance-bounding technology, design a more lightweight authentication protocol in accordance with the EPC-C1 G2 standards and solve the problem of insecure communications between the cloud and readers in cloud-based RFID.

**Acknowledgments.** This work was supported by ZTE Corporation and University Joint Research Project.

## References

1. Xie, W., Xie, L., Zhang, C., et al.: Cloud-based RFID authentication. In: IEEE International Conference on RFID 2013, pp. 168–175 (2013)
2. Van Tilborg, H.C.A., Jajodia, S. (eds.): *Encyclopedia of Cryptography and Security*. Springer Science & Business Media, Heidelberg (2014)
3. Avoine, G., Bingol, M.A., Kardas, S., Lauradoux, C., Martin, B.: A framework for analyzing RFID distance bounding protocols. *J. Comput. Secur.* **19**(2), 289–317 (2009)
4. Desmedt, Y., Goutier, C., Bengio, S.: Special uses and abuses of the fiat-shamir passport protocol (extended abstract). In: Pomerance, C. (ed.) *CRYPTO 1987*. LNCS, vol. 293, pp. 21–39. Springer, Heidelberg (1988). [https://doi.org/10.1007/3-540-48184-2\\_3](https://doi.org/10.1007/3-540-48184-2_3)
5. Brands, S., Chaum, D.: Distance-bounding protocols. In: Helleseth, T. (ed.) *EUROCRYPT 1993*. LNCS, vol. 765, pp. 344–359. Springer, Heidelberg (1994). [https://doi.org/10.1007/3-540-48285-7\\_30](https://doi.org/10.1007/3-540-48285-7_30)
6. Hancke, G.P., Kuhn, M.G.: An RFID distance bounding protocol. In: 2005 SECURECOMM (2005)

7. Gambs, S., Onete, C., Robert, J.M.: Prover anonymous and deniable distance-bounding authentication. In: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, AsiaCCS 2014, pp. 501–506 (2014)
8. Trujillo-Rasua, R., Martin, B., Avoine, G.: Distance-bounding facing both mafia and distance frauds. *IEEE Trans. Wireless Commun.* **13**(10), 5690–5698 (2014)
9. Jeon, I.-S., Yoon, E.-J.: An ultra-lightweight RFID distance bounding protocol. *Int. J. Math. Anal.* **8**(46), 2265–2275 (2014)
10. Kiraz, M.S., Bingl, M.A., Karda, S., et al.: Anonymous RFID authentication for cloud services. *Int. J. Inf. Secur. Sci.* **1**(2), 32–42 (2012)
11. Karda, S., Celik, S., Bingl, M.A., et al.: A new security and privacy framework for RFID in cloud computing. In: 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, vol. 1, pp. 171–176. IEEE (2013)
12. Jobe, S., Venifa Mini, G., Celin, J.J.A.: Efficient RFID authentication in cloud computing. *Int. J. Sci. Eng. Technol. Res. (IJSETR)* **2**(4), 954–958 (2013)
13. Chen, S.-M., Wu, M.-E., Sun, H.-M., et al.: CRFID: an RFID system with a cloud database as a back-end server. *Future Gener. Comput. Syst.* **30**, 155–161 (2014)
14. UHF Class 1 Gen 2 Standard v. 2.0.0 [S], GS1/EPCglobal (2013)
15. Chien, H., Chen, C.: Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. *Comput. Stand. Interfaces* **29**, 254–259 (2007)
16. Chen, C.-L., Huang, Y.-C., Shih, T.-F.: A novel mutual authentication scheme for RFID conforming EPCglobal Class 1 Generation 2 standards. *Inf. Technol. Control* **41**(3), 220–228 (2012)
17. Pang, L., Li, H., He, L., Alramadhan, A., et al.: Secure and efficient lightweight RFID authentication protocol based on fast tag indexing. *Int. J. Commun. Syst.* **27**, 3244–3254 (2014)
18. Gao, L., Ma, M., Shu, Y., Wei, Y.: An ultra-lightweight RFID authentication protocol with CRC and permutation. *J. Netw. Comput. Appl.* **41**, 37–46 (2014)
19. Han, D., Kwon, D.: Vulnerability of an RFID authentication protocol conforming to EPC Class 1 Generation 2 standards. *Comput. Stand. Interfaces* **31**, 648–652 (2009)
20. Safkhani, M., Bagheri, N.: For an EPC-C1G2 RFID compliant Protocol, CRC with Concatenation: No; PRNG with Concatenation: Yes. *Cryptology ePrint Archive, Report 2013/490* (2013)
21. Akg, M., Caglayan, M.U.: On the security of recently proposed RFID protocols. *IACR Cryptology ePrint Archive, 2013/820* (2013)
22. Zahra, S.B., Mahdi, R.A., Aref, M.R.: Formal cryptanalysis of a CRC-based RFID authentication protocol. In: 2014 22nd Iranian Conference on Electrical Engineering (ICEE), Shahid Beheshti University, pp. 1642–1647 (2014)