On the security of another CRC based ultralightweight RFID authentication protocol

Seyed Farhad Aghili and Hamid Mala

Department of Information Technology Engineering, Faculty of Computer Engineering, University of Isfahan, Hezar Jerib St., Isfahan 81746-73441, Iran

{sf.aghili@eng, h.mala@eng}.ui.ac.ir

Abstract. Design of ultra-lightweight authentication protocols for RFID systems conformed with the EPC Class-1 Generation-2 standard is still a challenging issue in RFID security. Recently, Maurya *et al.* have proposed a CRC based authentication protocol and claimed that their protocol can resist against all known attacks in RFID systems. However, in this paper we show that their protocol is vulnerable to tag impersonation attack. Moreover, we show that how an attacker can easily trace a target RFID tag. Our analyses show that the success probability of our attacks is “1” while the complexity is only one session eavesdropping, two XORs and one CRC computation.

keywords: RFID, EPC-C1G2, Cyclic Redundancy Code, Ultra-lightweight, Authentication, Impersonation Attack, Traceability Attack.

1 Introduction

The Electronic Product Code Class-1 Generation-2 specification (EPC-C1G2 in short) specification is a standard [1] for RFID protocols, which only supports an on-chip 16-bit Pseudo-random Number Generator (PRNG) and a 16-bit Cyclic Redundancy Code (CRC). In this standard, tags are assumed to be passive and communicate at the UHF band (800- 960 MHz), and their communication range is from 2 to 10 meters. A brief analysis of the EPC-C1G2 standard reveals serious security problems. Authentication is one of the main topics of research in the RFID security field, where a tag and a reader must identify each other and ensure the legitimacy of each other. Several authentication protocols conformed with EPC-C1G2 standard have been published, but most of them suffer from various security vulnerabilities [12, 14, 15, 19, 27, 34, 35, 3].

In the recent decade, several ultra-lightweight authentication protocols have been proposed for RFID systems which are designed for EPC-C1G2 standard. In these schemes, some designers have used CRC and PRNG [14, 15] and some others have designed their schemes based on bitwise operations like AND, XOR and OR [25, 26, 20]. Although these protocols are ultra-lightweight and conformed with EPC-C1G2 standard, they are vulnerable against attacks such as tag and reader impersonation, secret disclosure, tag traceability and de-synchronization attacks. Moreover, some schemes have proposed in the literatures which use simple operations such as bitwise XOR, modular addition and also shift operation [17, 16, 13, 28]. However, these protocols are vulnerable to several attacks such as secret disclosure and impersonation attacks [2, 4, 10, 8].

Recently, Maurya *et al.* proposed a coding theory based ultra-lightweight RFID authentication protocol with CRC [23]. They claimed that their protocol is ultra-lightweight and owned the security properties necessary for RFID systems. In this paper, we show that this protocol has serious vulnerabilities.

The rest of this paper is organized as follows. Section 2 briefly introduces the related work. Notations and preliminaries used in the paper are introduced in Section 3. We describe Maurya *et al.* [23] authentication protocol in Section 4. In Section 5, we analyze the security of Mauryar *et al.* protocol and propose two important attacks against this protocol. Finally, in Section 6 we present the conclusion.

2 Related Work

So far, many authentication protocols conformed to EPC-C1G2 standard have been proposed in the literature [9, 12, 14, 15, 19, 18, 22, 27, 34, 35] but most of them cannot provide security robustness and suffer from various security vulnerabilities [12, 14, 15, 19, 27, 34, 35]. In this section, we briefly review some recent ultra-lightweight RFID authentication protocols compatible to the EPC-C1G2 standard.

In 2007, Chien proposed the first ultra-lightweight protocol called *SASI* [13] which is based on bit-wise functions such as XOR and rotation operations. However, Cao *et al.* [10] showed that this protocol has several vulnerabilities such as denial-of-service and traceability based on a compromised tag.

In 2009, another ultra-lightweight protocol was proposed called *Gossamer* [28]. This protocol was designed to improve the security weaknesses of previous ultra-lightweight protocols. Later, in [8] the authors showed that *Gossamer* protocol is also vulnerable to several attacks.

Duc *et al.* published a mutual authentication scheme for EPC-C1G2 RFID tag, their protocol is based on CRC and PRNG functions, which supports EPC-C1G2 RFID tags [15]. However, due to the lack of forward security, Chien and Chen proposed a new method to solve these problems [14]. They claimed that their scheme is secure against known attacks to RFID systems. But later cryptanalysis of their scheme by Peris-Lopez *et al.* showed that it cannot guarantee forward secrecy and location privacy of tags and it does not resist against tag and back-end database impersonation attacks [24].

In 2012, Tian *et al.* [32] used bitwise XOR, left rotation and a very lightweight permutation function to propose an ultra-lightweight protocol called *RAPP*. Although that function was ultra-lightweight, the scheme was vulnerable to traceability, secret disclosure, and de-synchronization attacks [5, 6, 30, 7].

In 2016, Tewari and Gupta [31] proposed an RFID authentication protocol and claimed that their protocol is robust against de-synchronization, secret disclosure and traceability attacks. But later, secret disclosure attack was presented against it [29, 33]. Moreover, Fan *et al.* [17] presented a protocol called $ULRMAPC$ and claimed that their protocol has strong security compared with other existing protocols. However, the authors in [2] showed that $ULRMAPC$ protocol is vulnerable against denial of service (DoS), impersonation and de-synchronization attacks.

Recently, Maurya *et al.* [23] proposed an ultra-lightweight authentication protocol. They used CRC and PRNG functions and claimed that their protocol is conformed with the EPC-C1G2 standard and robust against most attacks presented in RFID systems. In this paper, the security of this protocol is investigated and several weaknesses are presented against it.

3 Notation and Preliminaries

In this section we describe the preliminaries and notations used in this paper. The notations used in the paper are depicted in Table 1.

Definition 1: syndrome decoding The syndrome decoding is an error correction method of coding theory. In this theory, a linear code C of length n and dimension k over F_2 by distance d of the code C is called $[n,k,d]-$binary linear code, in which F_2^n is a binary linear code C of length n over F_2 and F_2 is a binary field with two elements 0 and 1. The Hamming weight of c, denoted by $wt(c)$ is the number of non-zero elements in c, where c is a codeword in C.

A matrix G is the generator of the binary linear code C whose rows form a basis of C. A matrix H is a parity-check matrix of the linear code C which is a generator matrix of the dual code $C^{\perp}$. The coset leader $u \in F_2^n$ is in the code C if and only if the rank of $G' = \begin{pmatrix} G \\ u \end{pmatrix}$ is k.

For any $w \in F_2^n$, the word $S(w) = wH^T \in F_2^{n-k}$ is the syndrome of w with respect to the parity-check matrix H. Constructing a syndrome look-up table is as follow.

- List all cosets for the code C, choose a word of least weight as coset leader u from each coset;
- Use the parity-check matrix H for the code C, and calculate its syndrome $S(u) = uH^T$ for each coset leader u.

(For more details, the reader can refer to [21]).

Definition 2: Cyclic Redundancy Code (CRC) A Cyclic Redundancy Code (CRC) is a checksum algorithm and is completely linear. The EPC-C1G2 standard supports on-chip 16-bit CRC. This code has a linear property which can be discribed as follows. For any binary strings a, b, c, d, e and f, it holds that [24]:

$$CRC(a\|b\|c) \oplus CRC(d\|e\|f) = CRC(a \oplus d\|b \oplus e\|c \oplus f) \tag{1}$$

Table 1. Notation

Notation	**Description**
C	The binary code generated by G
c	A codeword of the code C
n	The bit-length of each parameter
$wt(c)$	The hamming weight of the codeword c
G	The generator matrix of the code C
k	The dimension of the code C
d	The hamming distance of the code C
t	The error correction capability of the code C
R_T	Random numbers generated by the tag
R_r	Random numbers generated by the reader
ID_i	The identity of the ith tag
K	The secret key shared between the reader and the tag
$\oplus$	Exclusive OR operation
$\|\|$	Concatenation operation

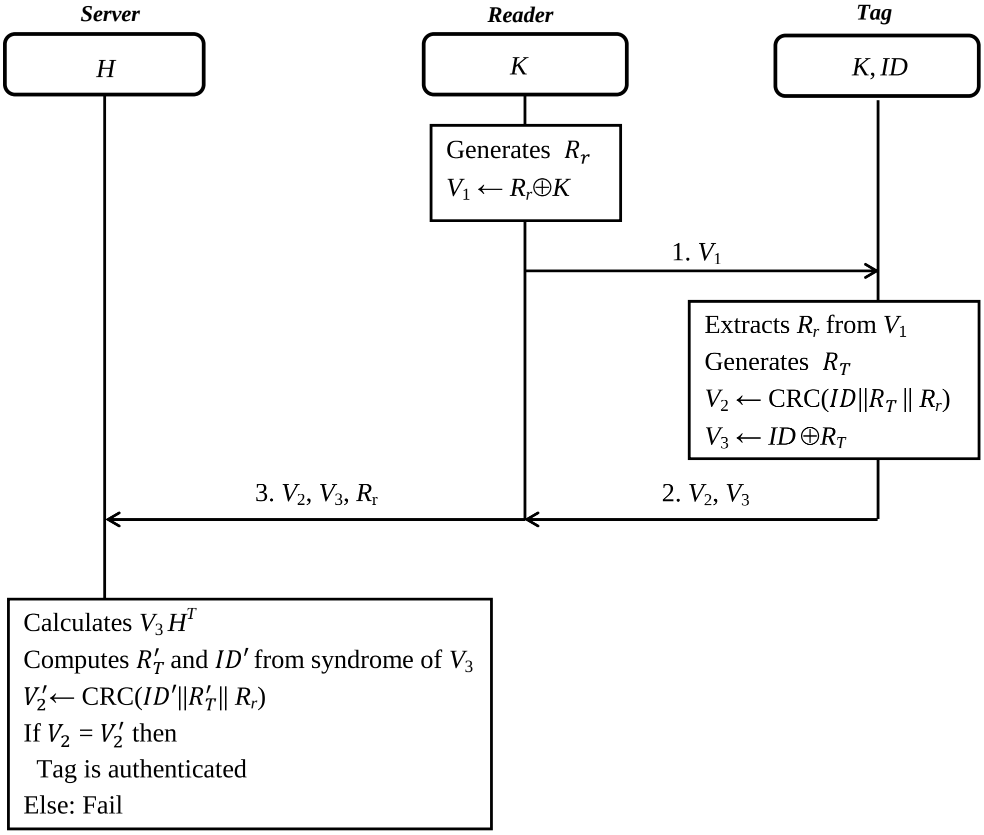
Server
H
Reader
K
Tag
K, ID
Generates R_r
$V_1 \leftarrow R_r \oplus K$
1. V_1
Extracts R_r from V_1
Generates R_T
$V_2 \leftarrow \mathrm{CRC}(ID \| R_T \| R_r)$
$V_3 \leftarrow ID \oplus R_T$
3. V_2, V_3, R_r
2. V_2, V_3
Calculates $V_3 H^T$
Computes R'_T and ID' from syndrome of V_3
$V'_2 \leftarrow \mathrm{CRC}(ID' \| R'_T \| R_r)$
If $V_2 = V'_2$ then
Tag is authenticated
Else: Fail

Fig. 1. Maurya *et al.* authentication protocol

In this paper we use Eq. (1) and show that Maurya *et al.* [23] authentication protocol is vulnerable to tag impersonation attack. Moreover, we show that how an attacker can easily trace a target RFID tag.

4 Maurya *et al.* Authentication Protocol

Maurya *et al.* in [23] have proposed an ultra-lighweit authentication protocol conformed to the EPC-C1G2 standard. This protocol employs a syndrome decoding, a CRC which is a lightweight permutation function and a 16-bit PRNG. In this section we briefly review this protocol which has two phases.

4.1 Phase 1: Initialization

In this phase, a binary linear code C with a generator matrix G of order $k \times n$ with a minimum distance d and the corresponding parity-check matrix H are stored to a legitimate server. The initiator uses the generator matrix to generate 2^k codewords as unique identification numbers for all tags. (Note: In this scheme, maximum number of the tags are 2^k). The initiator also shares a secret key K between any legitimate tag and the legitimate reader. Finally, the server stores all syndromes and corresponding coset leaders on its database.

4.2 Phase 2: Authentication

The authentication protocol, as shown in Fig. 1, runs as below:

1. The reader generates a random number R_r and uses the stored secret key K to compute $V_1 = R_r \oplus K$ and then starts the protocol by sending V_1 to the target tag;
2. Once the tag received V_1 does as follow:
   - Generates a random number R_T, $(wt(R_T) \leq t)$;
   - Extracts $R_r = V_1 \oplus K$;
   - Computes $V_2 = CRC(ID \| R_T \| R_r)$ and $V_3 = ID \oplus R_T$;
   - Forwards V_2 and V_3 to the reader.
3. The reader forwards the tuple (V_2, V_3, R_r) to the server.
4. Once the server received the tuple (V_2, V_3, R_r), it acts as follow:
   - Calculates the syndrome of V_3 by using the equation $S(V_3) = V_3 H^T$;
   - Uses the stored syndrome $V_3 H^T$ and finds the corresponding coset leader R_T;
   - Computes $ID = V_3 \oplus R_T$;
   - Computes $V_2' = CRC(ID \| R_T \| R_r)$;
   - If $V_2' = V_2$ then it authenticates the expected tag, otherwise the authentication fails.

5 Security Analysis of the Maurya *et al.* Protocol

In this section, we show how Maurya *et al.* authentication protocol suffers from tag impersonation and tag traceability attacks. In this scheme the authors use the CRC function that has the property presented in Section 3 (Eq. (1)). Therefore, the adversary uses this linear property to execute his/her attacks. (Note: In these attacks the superscript j shows the jth run of protocol, $j = 1, 2$). In addition, in Maurya *et al.* protocol the values of ID and K are constant and neither tag nor server/reader update these important secret parameters.

5.1 Tag Impersonation Attack

In this attack, an adversary can cheat the reader to authenticate him/her as a legitimate tag. This attack consists of two phases: learning phase and execution phase which is described as follow:

1. Learning Phase: In this phase, an adversary stores required information by eavesdropping only one run of the protocol as below.
   - The adversary eavesdrops one complete run of the protocol;
   - The adversary stores $V_1^1 = R_r^1 \oplus K$, $V_2^1 = CRC(ID \| R_T^1 \| R_r^1)$ and $V_3^1 = ID \oplus R_T^1$.
2. Execution Phase: In this phase, an adversary uses the information stored in learning phase and executes the attack as below.
   - The reader generates a random number R_r and computes $V_1^2 = R_r^2 \oplus K$ and starts another run of the protocol by sending V_1^2 to the target tag which now is the adversary;
   - Once the adversary received V_1^2 does as follow:
     - Computes $V_1 = V_1^1 \oplus V_1^2 = R_r^1 \oplus R_r^2$;
     - Computes $V_2 = V_2^1 \oplus CRC(0 \| 0 \| V_1) = CRC(ID \| R_T^1 \| R_r^2)$;
     - Forwards V_2 and V_3^1 to the reader.
   - The reader forwards the tuple (V_2, V_3^1, R_r^2) to the server.
   - Once the server received the tuple (V_2, V_3^1, R_r^2), it acts as follow:
     - Calculates the syndrome of V_3^1 by using the equation $S(V_3^1) = V_3^1 H^T$;
     - Uses the stored syndrome $V_3^1 H^T$ and finds the corresponding coset leader R_T^1;
     - Computes $ID = V_3^1 \oplus R_T^1$;
     - Computes $V_2' = CRC(ID \| R_T^1 \| R_r^2)$;
     - Now the checking process $V_2' = V_2$ is passed and it authenticates the adversary as an expected tag.

Hence, following the given attack the tag is impersonated by the adversary. The success probability of this attack is “1" while the complexity is only “2" runs of protocol.

5.2 Tag Traceability Attack

In this attack, an adversary is trying to trace the target tag. This attack consists of two phases: learning phase and decision phase which is described as follow:

1. Learning Phase: In this phase, an adversary stores required information by eavesdropping one runs of protocol as below.
   - The adversary eavesdrops the messages transmitted between the tag and the reader in one run of the protocol;
   - The adversary stores $V_1^1 = R_r^1 \oplus K$, $V_2^1 = CRC(ID \| R_T^1 \| R_r^1)$ and $V_3^1 = ID \oplus R_T^1$.
2. Decision Phase: In this phase, an adversary uses the information stored in the learning phase and executes the attack as below.
   - When the reader computes the message $V_1^2 = R_r^2 \oplus K$ and sends V_1^2 to the target tag, the adversary eavesdrops this message;
   - According to the sequence of the protocol, once the tag received V_1^2, it does as follow:
     - Computes $V_1^2 = R_r^2 \oplus K$;
     - Computes $V_2^2 = CRC(ID \| R_T^2 \| R_r^2)$ and $V_3^2 = ID \oplus R_T^2$;
     - Forwards V_2^2 and V_3^2 to the reader.
   - Now, the adversary eavesdrops messages V_2^2 and V_3^2 and acts as follow:
     - Computes $V_1 = V_1^1 \oplus V_1^2 = R_r^1 \oplus R_r^2$;
     - Computes $V_3 = V_3^1 \oplus V_3^2 = R_T^1 \oplus R_T^2$;
     - Now, if the checking process $V_2^1 \oplus V_2^2 = CRC(0 \| V_3 \| V_1)$ is passed, it concludes the current tag is the one in the learning phase. This checking process is passed as below by considering Eq. (1).

$$\begin{aligned} V_2^1 \oplus V_2^2 &= CRC(ID \| R_T^1 \| R_r^1) \oplus CRC(ID \| R_T^2 \| R_r^2) \\ &= CRC(ID \oplus ID \| R_T^1 \oplus R_T^2 \| R_r^1 \oplus R_r^2) \\ &= CRC(0 \| R_T^1 \oplus R_T^2 \| R_r^1 \oplus R_r^2) \\ &= CRC(0 \| V_3 \| V_1) \end{aligned}$$

One can see that the adversary can trace the target tag with probability “1” and with the complexity of only one session eavesdropping, two XORs and one CRC computation.

In this paper, we showed that all the security weaknesses of Maurya *et al.* protocol are related to the use of the 16-bit CRC. It cannot be solved by using larger CRCs and it is because of the bad (linear) properties of CRC functions. So, we pass up to propose an improved version of this protocol and we suggest to look for another alternative solutions.

In Table 2, we lists some CRC based RFID protocols. These protocols cannot provide any basic security features. In this table, the symbol "*Yes*" represents that the scheme prevents attack and the symbol "*No*" represents that the scheme does not resist against that. We denote resistance against server/reader impersonation attack by *RRI*, resistance against tag impersonation attack by *RTI*, forward security by *FS*, resistance against replay attack by *RR*, resistance against denial of service attack by *RD*, resistance against traceability attack by *RT* and finally resistance against secret disclosure attack by *RS*.

Table 2. Security features of some CRC based RFID protocols

Protocol	RRI	RTI	FS	RR	RD	RT	RS
Duc *et al.* [15]	Yes	Yes	No	No	No	Yes	Yes
Chien and Chen [14]	No	No	No	Yes	Yes	No	Yes
Chen and Chien [11]	Yes	No	Yes	Yes	Yes	No	No
Maurya *et al.* [23]	Yes	No	Yes	Yes	Yes	No	Yes

6 Conclusion

In this article, we investigated the security of the Maurya *et al.* authentication protocol. This CRC based protocol was recently proposed for ultra-lightweight RFID systems. We showed that Maurya *et al.* protocol is vulnerable to tag impersonation and tag traceability attacks. Our attacks are based on the linear property of CRC function. The success probability of presented attacks is "1" while the complexity is only one session eavesdropping, two XORs and one CRC computation.

References

1. EPCglobal Inc. Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.09. *Available online at http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2. Last access 2013/12/14.*
2. S. F. Aghili, M. Ashouri-Talouki, and H. Mala. DoS, impersonation and de-synchronization attacks against an ultra-lightweight RFID mutual authentication protocol for IoT. *The Journal of Supercomputing*, pages 1–17, 2017.
3. S. F. Aghili, N. Bagheri, P. Gauravaram, M. Safkhani, and S. K. Sanadhya. On the Security of Two RFID Mutual Authentication Protocols. In M. Hutter and J.-M. Schmidt, editors, *RFIDSec*, volume 8262 of *Lecture Notes in Computer Science*, pages 86–99. Springer, 2013.

4. S. F. Aghili and H. Mala. Security Analysis of an Ultra-lightweight RFID Authentication Protocol for M-commerce. *IACR Cryptology ePrint Archive*, 2017:547, 2017.
5. Z. Ahmadian, M. Salmasizadeh, and M. R. Aref. Desynchronization attack on RAPP ultralightweight authentication protocol. *Information processing letters*, 113(7):205–209, 2013.
6. G. Avoine and X. Carpent. Yet Another Ultralightweight Authentication Protocol That Is Broken. *RFIDSec*, 7739:20–30, 2012.
7. N. Bagheri, M. Safkhani, P. Peris-Lopez, and J. E. Tapiador. Weaknesses in a new ultralightweight RFID authentication protocol with permutationâĂŤRAPP. *Security and Communication Networks*, 7(6):945–949, 2014.
8. Z. Bilal, A. Masood, and F. Kausar. Security analysis of ultra-lightweight cryptographic protocol for low-cost RFID tags: Gossamer protocol. In *Network-Based Information Systems, 2009. NBIS'09. International Conference on*, pages 260–267. IEEE, 2009.
9. M. Burmester and B. de Medeiros. The Security of EPC Gen2 Compliant RFID Protocols. In S. M. Bellovin, R. Gennaro, A. D. Keromytis, and M. Yung, editors, *ACNS*, volume 5037 of *Lecture Notes in Computer Science*, pages 490–506, 2008.
10. T. Cao, E. Bertino, and H. Lei. Security analysis of the SASI protocol. *IEEE Transactions on Dependable and secure Computing*, 6(1):73–77, 2009.
11. C.-L. Chen and C.-F. Chien. An ownership transfer scheme using mobile rfids. *Wireless personal communications*, 68(3):1093–1119, 2013.
12. C.-L. Chen and Y.-Y. Deng. Conformation of EPC Class 1 Generation 2 standards RFID system with mutual authentication and privacy protection. *Eng. Appl. of AI*, 22(8):1284–1291, 2009.
13. H.-Y. Chien. SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing*, 4(4):337–340, 2007.
14. H.-Y. Chien and C.-H. Chen. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. *Computer Standards & Interfaces*, 29(2):254–259, 2007.
15. D. N. Duc, J. Park, H. Lee, and K. Kim. Enhancing security of EPCglobal GEN-2 RFID tag against traceability and cloning. *in Proceedings of the Symposium on Cryptography and Information Security*, pages 17–20, 2006.
16. K. Fan, N. Ge, Y. Gong, H. Li, R. Su, and Y. Yang. An ultra-lightweight RFID authentication scheme for mobile commerce. *Peer-to-Peer Networking and Applications*, pages 1–9, 2016.
17. K. Fan, Y. Gong, C. Liang, H. Li, and Y. Yang. Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. *Security and Communication Networks*, 9(16):3095–3104, 2015.
18. D. Han and D. Kwon. Vulnerability of an RFID authentication protocol conforming to EPC Class 1 Generation 2 Standards. *Computer Standards & Interfaces*, 31(4):648–652, 2009.

19. S. Karthikeyan and M. Nesterenko. RFID security without extensive cryptography. In V. Atluri, P. Ning, and W. Du, editors, *SASN*, pages 63–67. ACM, 2005. Proceedings of the 3rd ACM Workshop on Security of ad hoc and Sensor Networks, SASN 2005, Alexandria, VA, USA, November 7, 2005.
20. T. Li. Employing Lightweight Primitives on Low-Cost RFID Tags for Authentication. In *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*, pages 1–5. IEEE, 2008.
21. S. Ling and C. Xing. *Coding theory: a first course*. Cambridge University Press, 2004.
22. N.-W. Lo and K.-H. Yeh. An Efficient Mutual Authentication Scheme for EPCglobal Class-1 Generation-2 RFID System. In M. K. Denko, C.-S. Shih, K.-C. Li, S.-L. Tsao, Q.-A. Zeng, S.-H. Park, Y.-B. Ko, S.-H. Hung, and J. H. Park, editors, *EUC Workshops*, volume 4809 of *Lecture Notes in Computer Science*, pages 43–56. Springer, 2007.
23. P. K. Maurya, J. Pal, and S. Bagchi. A Coding Theory Based Ultralightweight RFID Authentication Protocol with CRC. *Wireless Personal Communications*, pages 1–10.
24. P. Peris-Lopez, J. C. H. Castro, J. M. Estévez-Tapiador, and A. Ribagorda. Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard. *Computer Standards & Interfaces*, 31(2):372–380, 2009.
25. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. EMAP: an efficient mutual-authentication protocol for low-cost RFID tags. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pages 352–361. Springer, 2006.
26. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. M^{2}AP: A minimalist mutual-authentication protocol for low-cost RFID tags. In *International Conference on Ubiquitous Intelligence and Computing*, pages 912–923. Springer, 2006.
27. P. Peris-Lopez, J. C. Hernandez-Castro, J. E. Tapiador, and J. C. A. van der Lubbe. Cryptanalysis of an EPC Class-1 Generation-2 standard compliant authentication protocol. *Eng. Appl. of AI*, 24(6):1061–1069, 2011.
28. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Tapiador, and A. Ribagorda. Advances in ultra-lightweight cryptography for low-cost RFID tags: Gossamer protocol. In *International Workshop on Information Security Applications*, pages 56–68. Springer, 2008.
29. M. Safkhani and N. Bagheri. Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things. *The Journal of Supercomputing*, pages 1–7, 2016.
30. W. Shao-hui, H. Zhijie, L. Sujuan, and C. Dan-wei. Security analysis of RAPP an RFID authentication protocol based on permutation. *College of computer, Nanjing University of Posts and Telecommunications, Nanjing*, 210046, 2012.
31. A. Tewari and B. Gupta. Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *The Journal of Supercomputing*, 73(3):1085–1102, 2016.
32. Y. Tian, G. Chen, and J. Li. A new ultralightweight RFID authentication protocol with permutation. *IEEE Communications Letters*, 16(5):702–705, 2012.

33. K.-H. Wang, C.-M. Chen, W. Fang, and T.-Y. Wu. On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. *The Journal of Supercomputing*, pages 1–6, 2017.

34. T.-C. Yeh, Y.-J. Wang, T.-C. Kuo, and S.-S. Wang. Securing RFID systems conforming to EPC Class 1 Generation 2 standard. *Expert Syst. Appl.*, 37(12):7678–7683, 2010.

35. E.-J. Yoon. Improvement of the securing RFID systems conforming to EPC Class 1 Generation 2 standard. *Expert Syst. Appl.*, 39(1):1589–1594, 2012.