Wireless Pers Commun (2017) 97:967–976
DOI 10.1007/s11277-017-4546-z

A Coding Theory Based Ultralightweight RFID Authentication Protocol with CRC

Pramod Kumar Maurya[1] · **Joydeb Pal**[1] · **Satya Bagchi**[1]

Published online: 29 May 2017

Abstract Radio frequency identification (RFID) is a fast growing technology for automatically identification in various industries. However, RFID system arises many security and privacy problems. Due to resource constraints in RFID tags, ultralightweight authentication schemes are an effective way to avoid these problems. In this paper, we present an ultralightweight authentication scheme which integrates cyclic redundancy check and syndrome decoding mechanism to enhance the security and privacy functionality without increasing any computation cost. In the proposed scheme, the server needs to store a generator matrix and corresponding parity-check matrix of a linear code for tag matching and authentication. Also, tags need to store only a codeword of the linear code as a unique identification number and a secret key. Our security analysis shows that the scheme provides higher security to prevent existing possible attacks. Performance evaluation illustrates that the scheme uses very less resources on tags in terms of computational operations and memory storage.

Keywords RFID system · Syndrome decoding · Authentication protocol · Security · Privacy

✉ Satya Bagchi
satya5050@gmail.com

Pramod Kumar Maurya
pramod_kumar22490@hotmail.com

Joydeb Pal
joydebpal77@gmail.com

[1] Department of Mathematics, National Institute of Technology Durgapur, Burdwan, India

1 Introduction

Radio Frequency Identification (RFID) is a system which uses radio signal to automatically identify objects. This technology was first introduced in second world war to identify friend and foe planes. Nowadays, RFID is used widespread in various commercial industries like supply-chain management, sales management, passports, libraries, human implantation, etc [7].

Generally, RFID system contains three components: tag (transponder), reader (interrogator), and back-end server. RFID tag is a small microchip that is embedded with objects to track or identify. Peoples see RFID as a successor of optical bar-code because of no need to line-of-sight contact to read RFID tags. Nowadays, Electronic Product Code (EPC) tags are deployed in many automatically identifying applications which are standardized by EPCglobal Inc.. Each EPC tag stores a unique identification number which is known as an EPC code in on-board memory. An EPC Gen-2 tag contains a pseudo-random number generator [5, 12]. Length of an EPC code is upto 96-bit. RFID reader, radio frequency (RF) emitter, which uses RF to interrogate tags when a tag comes into the reader's read range. Back-end server manages database containing information associated with tags. In context of power source, RFID tags are divided into two types: active and passive. Active tag has its own power source for data transmission and computational process while passive tag has no internal power source. Passive tag harvests power from the signal of an interrogator.

RFID system operates in several frequency bands. Lower frequency (LF) RFID system operates at 124–135 kHz, having read range upto half a meter. High frequency (HF) system operates on 13.56 MHz, which can read upto a meter or more. Ultra high frequency (UHF) operates at 860–960 MHz, having read range upto 10 m.

RFID technology provides many benefits in various commercial industries and consumers. However, this technology arises many privacy and security issues. Because of RFID technology is based on wireless communication which suffers with numerous possible threats and eavesdropping, RFID system violates privacy in two general forms: reveal personal information and location privacy. Privacy and security threats create serious problem when a tag is combined with sensitive personal information. Due to limitation of memory, power sources and computational resource, RFID system can not bear traditional cryptographic algorithms. A simple way to protect RFID system from security and privacy threats is to use an ultralightweight authentication protocol which has less computational work with higher security.

In this paper, we propose an ultralightweight authentication protocol which is based on syndrome decoding, an error correction method of coding theory [3, 10] and cyclic redundancy check (CRC), an efficient checksum algorithm to protect message integrity.

Let $\mathbb{F}_2$ be a binary field with two elements 0 and 1. A binary linear code C of length n over $\mathbb{F}_2$ is a subspace of $\mathbb{F}_2^n$. A linear code C of length n and dimension k over $\mathbb{F}_2$ is called a binary linear $[n, k]$-code. If the distance d of the code C is known, it is also referred as $[n, k, d]$-binary linear code. Let c be a codeword in C. The (Hamming) weight of c, denoted by $wt(c)$, is defined to be the number of nonzero positions in c.

A generator matrix G of the binary linear code C is a matrix whose rows form a basis of C. A parity-check matrix H of the linear code C is a generator matrix of the dual code $C^{\perp}$. Let $u \in \mathbb{F}_2^n$, then u is in the code C if and only if rank of $G' = \begin{pmatrix} G \\ u \end{pmatrix}$ is k.

For any $w \in \mathbb{F}_2^n$, the syndrome of w with respect to the parity-check matrix H is the word $S(w) = wH^T \in \mathbb{F}_2^{n-k}$, where H^T is the transpose of H. Steps to construct a syndrome look-up table are following.

Step 1 List all cosets for the code C, choose from each coset a word of least weight as coset leader u.

Step 2 Take the parity-check matrix H for the code C, and for each coset leader u, calculate its syndrome $S(u) = uH^T$.

This paper is organized as follows. We summarize the previous work in Sect. 2. In Sect. 3, we propose our scheme. We analyze security and privacy parameters of our proposed protocol in Sect. 4. In Sect. 5, we compare our proposed scheme with some other authentication protocols under the various parameters. Finally, we present conclusion in Sect. 6.

2 Past Works

In this section, we will review some selected protocols and discuss their approaches, advantages and drawbacks. In 2003, Weis et al. [14] introduced a hash-lock based authentication scheme. The main advantage of the scheme is that a tag responds to a reader's query with a masked ID known as metaID = $h(K)$ to hide the real ID of the tag, where K is secret key shared between server and the tag and $h()$ is a one-way hash function. Although this scheme provides certain level of reliability at low-cost, an adversary can easily track the tag by its metaID which is unique image of the real ID. Also, the adversary can eavesdrop the communication channel to get the tag's secret key which is sent in plaintext to break the privacy properties of the scheme.

In 2004, Henrici and Muller [6] proposed another hash-based scheme to provide mutual authentication properties. In this scheme, the authors use a random number, called transaction identifier *TID*, to refresh the tag identifier dynamically. The *TID* increases in every successful authentication session so that the scheme resists replay attack. This scheme makes the tag's ID randomized in every session so that the scheme defends against location attack. Unfortunately, this scheme is vulnerable under man-in-the-middle attack and desynchronization attack [5].

In 2006, Lopez et al. [11] proposed a minimalist ultralightweight mutual authentication protocol, called M^2AP, for low-cost RFID tags. This protocol utilize simple operations such as *XOR*, *AND*, *OR*, and addition modulo. Although, this protocol works very well under the resource's limitation of RFID tags but this scheme is vulnerable under desynchronization attack and disclosure attack [2, 9].

In 2007, Chien [4] proposed a new ultralightweight RFID authentication protocol known as SASI. The scheme utilizes simple operations such as *XOR*, *AND*, *OR*, and bitwise rotation. SASI provides strong data integrity and tag anonymity. However, desynchronization attack is possible which is investigated by Sun et al. [12].

A new ultralightweight authentication protocol with permutation known as *RAPP* is introduced by Tian et al. [13] in 2012. This scheme introduced a new permutation operation to mix order of bits. *RAPP* uses fewer resources of tags in terms of computational operations and storage cost. Unfortunately, this scheme is vulnerable under desynchronization attack [1].

Recently, Khan and Moessner [8] proposed low cost authentication protocol (*LCAP*) that uses timestamp as a counter and in each authentication session, the counter is

incremented. This protocol introduced a classful structure for key classes to reduce computational load. This protocol is vulnerable under distributed denial-of-service (DDoS) attack because a number of adversaries cooperate to interrogate the tag to increase its counter for overflow.

3 Proposed Scheme

We propose an ultralightweight authentication protocol for RFID system with syndrome decoding and CRC. Notations used in this protocol is defined in Table 1, and our proposed protocol is shown in Fig. 1.

3.1 Assumptions

The proposed protocol works under the following assumptions.

1. Every tag and legitimate reader have a pseduo random number generator (PRNG).
2. Every tag can generate a random number with length n and $wt(R_T) \leq t$.
3. Communication channel between server and reader is secure.
4. Communication channel between Reader and tag is insecure and their communications are subject to eavesdropping.

3.2 Initialization

1. An initiator (manufacturer) chooses a binary linear code C with generator matrix G of order $k \times n$ with minimum distance d and corresponding a fixed parity-check matrix H, assigns to a legitimate server.
2. The initiator chooses a CRC function and assigns to each tag and the server.

Table 1 Notations and symbols are used in the proposed scheme

Notation	Description
C	Binary code generated by G.
c	A codeword of the code C.
n	Number of bits in bit-string of each parameter.
$wt(c)$	Weight of the codeword c (number of 1's of the binary codeword c).
G	Generator matrix of the code C.
k	Dimension of the code C.
d	Hamming distance of the code C.
t	Error correction capability of the code C.
R_T	Random number generated by a tag with the length n, and $wt(R_T) \leq t$.
R_r	Random number generated by a reader.
ID_i	ID of ith tag $(i \leq 2^k)$.
K	Secret key shared between legitimate tags and legitimate readers.
$\|$	Concatenation operation.
$\oplus$	Exclusive-or operation.

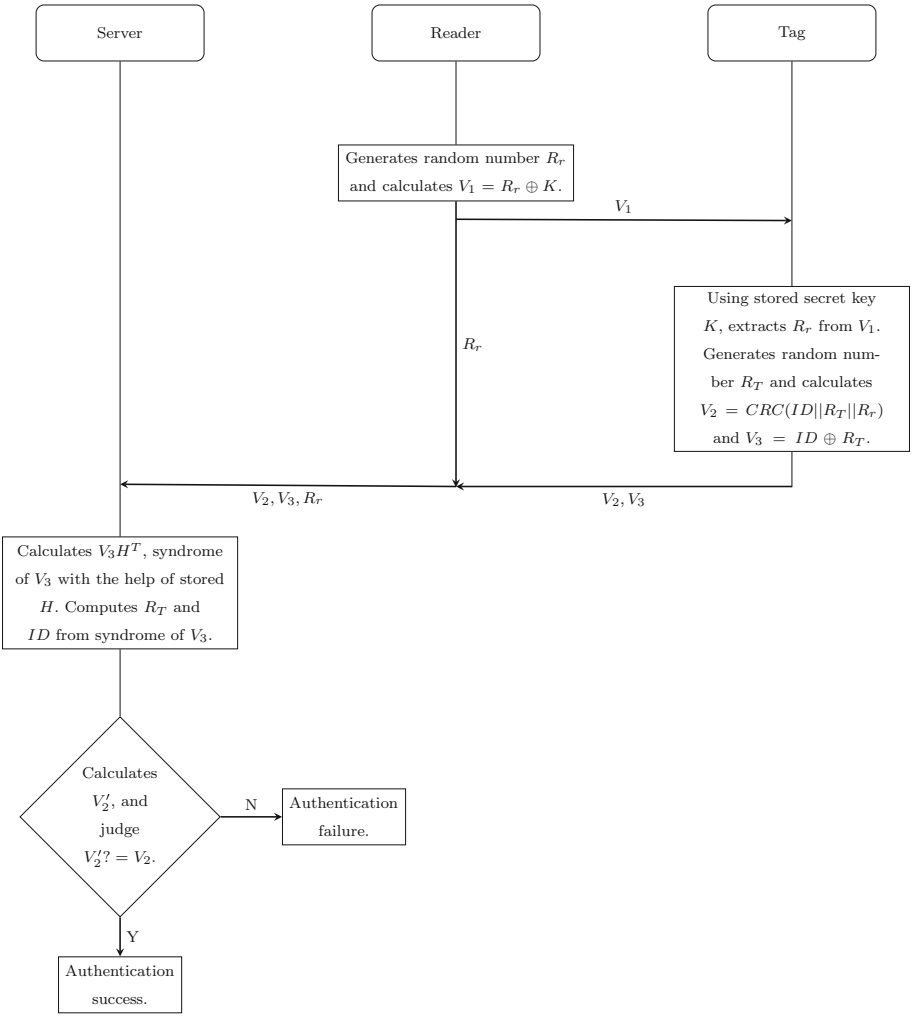

Fig. 1 Proposed authentication protocol

3. The generator matrix generates 2^k codewords.
4. The initiator assigns to each tag an unique identification number *ID*, chosen from these 2^k codewords.
5. The initiator assigns a secret key K shared between legitimate tags and legitimate readers.
6. The server stores the other information of the tags in its own database.
7. The server stores all syndromes and corresponding coset leaders.

3.3 Process

The proposed authentication protocol works as follows.

Phase 1 Reader generates a random number R_r and computes $V_1 = R_r \oplus K$ using stored secret key K and transmits V_1 to a tag.
Phase 2 After receiving V_1, the tag generates a random number R_T, $(wt(R_T) \leq t)$ and computes response message as follows:

- Calculates $R_r = V_1 \oplus K$.
- Computes $V_2 = CRC(ID \| R_T \| R_r)$ and $V_3 = ID \oplus R_T$.

Phase 3 The tag transmits V_2, V_3 to the reader.
Phase 4 The reader sends V_2, V_3 with R_r to the server.
Phase 5 After receiving V_2, V_3 and R_r from the reader, the server authenticates the tag as follows:

- Calculates $V_3 H^T$, the syndrome of V_3.
- Find the corresponding coset leader u $(= R_T)$ from the stored syndrome $V_3 H^T$.
- So $ID = V_3 \oplus u$.
- Computes $V_2^{'} = CRC(ID \| R_T \| R_r)$
- If $V_2^{'} = V_2$ then the tag is authorized otherwise not.

4 Security and Privacy Analysis

4.1 Tag Location Privacy

Communication between tag and reader is wireless which is an insecure channel. Adversaries can eavesdrop and collect data transmitted between reader and tag. If tag's response is static in each session, adversaries can track the tag with the help of a number of unauthorized readers. In the proposed protocol, the tag's response message (V_2, V_3) contains random numbers which are generated by legitimate reader and the tag in each authentication session, so V_2 and V_3 behave like a random number in each session. Therefore, for an adversary, it is not possible to track the position of the tag.

4.2 Impersonation Attack

Suppose an adversary eavesdrops a session and collects data V_1, V_2 and V_3. In the next session, when reader queries the tag by sending current $V_1^{'}$, which contains updated random number, the adversary can not impersonate the tag using V_1, V_2, V_3 and current $V_1^{'}$ because here each contains different random number. So the scheme is secure against impersonation attack.

4.3 Disclosure Attack

In each authentication session, the tag masks its unique identity *ID* with random number and also reader's random number is masked with secret key K shared among legitimate readers and legitimate tags. So it is hard to disclose *ID* and R_r without knowing K and R_T. Therefore, our proposed scheme prevents disclosure attack.

4.4 Replay Attack

An adversary can collect data from an authentication session and use these data to authenticate as a legitimate tag. In our proposed protocol, tag's response V_2 and V_3 are randomized in each authentication session. Suppose an adversary eavesdrops and collects tag's response V_2 and V_3 of the previous session. When a legitimate reader interrogates the tag by sending current session's $V_1^{'}$, the adversary transmits previous session's V_2 and V_3 as the tag to the reader. After receiving V_2 and V_3, the reader transmits it with current session's $R_r^{'}$ to the server. The server computes ID from V_3 with the help of G and H. The server computes $V_2^{'}$ using ID, R_T and current $R_r^{'}$. But the reader's random number stored in V_2 and the current $R_r^{'}$ are different, so $V_2^{'} \neq V_2$. Hence the server can not authenticate the tag.

4.5 De-synchronization Attack

In the proposed scheme, there is no secret share among tags and the server. So here no need to update any value in each authentication session which cause de-synchronization problem. So, our scheme is fully protected from de-synchronization attack.

We compare security features of various popular ultralightweight authentication protocols with our proposed protocol in Table 2. It shows that proposed scheme provides better security with respect to others [8, 11, 13].

5 Cost Performance Comparison

For RFID system, an authentication protocol is better if it provides reasonable security with less computational cost. Computational cost means required memory, operations computation load and communication round (data send by tag in one authentication session). Reader and server have no limitation whereas RFID tag has limited memory to store static data and computational resources to perform computational work. So it is important for an authentication protocol to be easily implemented in low-cost tags.

In Table 3, we compare computational cost of various ultralightweight authentication protocols [8, 11, 13] with our proposed scheme in terms of required memory, communication round, and operations. In the table, we denote m as number of tags stored in the

Table 2 Security performance comparision

Protocol → Attack ↓	M^2AP [11]	RAPP [13]	LCAP [8]	Proposed protocol
De-synchronization attack	✔	✔	✔	×
Tracking attack	✔	✔	×	×
Disclosure attack	✔	✔	×	×
Impersonation attack	✔	×	×	×
Mutual authentication	✔	✔	×	×

Table 3 Computation cost performance comparison

Protocol	Entity	M^2AP [11]	RAPP [13]	LCAP [8]	Proposed protocol
Matrix multiplications/ CRC permutations /cipher computations	T	×	11 (Permutation)	2 (cipher)	1 (CRC)
	S	×	11 (Permutation)	2 (cipher)	1 (matrix multiplication), 1 (CRC)
No. of PRNG	T	×	×	1	1
	R+S	2	2	1	1
No. of basic operations	T	19	19	4	3
No. of authentication steps		5	5	4	4
Required memory	T	$6n$	$4n$	$6.5n$	$2n$
	S	6 nm	8 nm	6.5 nm	$n^2 + (2n - k).2^{n-k}$

database, T as tag-side, R as reader-side and S as server-side to show overall performance of the RFID system.

6 Conclusion

In this paper, we have shown some overview of RFID system. We review various types of authentication scheme with benefits and drawbacks. We have proposed a novel authentication protocol which uses only CRC and syndrome decoding for authentication. Then we analyze its security and privacy under various parameters. In Tables 2 and 3, we compare its security and computational cost with some other well-known ultralightweight authentication schemes [8, 11, 13]. It works under the limitation of passive tags. Finally, we conclude that proposed scheme provides better security with very less amount of computational cost.

Acknowledgements The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper.

Conflict of interest The authors P. K. Maurya thanks the Institute NIT Durgapur and J. Pal thanks to DST-INSPIRE, India, for financial support of their research works.

References

1. Ahmadian, Z., Salmasizadeh, M., & Aref, M. R. (2013). Desynchronization attack on RAPP ultralightweight authentication protocol. *Information Processing Letters*, *113*(7), 205–209.
2. Alomair, B., Lazos, L., & Poovendran, R. (2007). *Passive attacks on a class of authentication protocols for RFID*. Berlin: Springer.
3. Basu, M., Rahaman, M., & Bagchi, S. (2009). On a new code, $[2^n - 1, n, 2^{n-1}]$. *Discrete Applied Mathematics*, *157*(2), 402–405.
4. Chien, H. Y. (2007). SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing*, *4*(4), 337–340.
5. Gao, L., Ma, M., Shu, Y., & Wei, Y. (2013). A security protocol resistant to intermittent position trace attacks and desynchronization attacks in RFID systems. *Wireless Personal Communications*, *68*(4), 1943–1959.

6. Henrici, D., & Muller, P. (2004). Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In *Proceedings of the second IEEE annual conference on pervasive computing and communications workshops, 2004* (pp. 149–153).
7. Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, *24*(2), 381–394.
8. Khan, G., & Moessner, M. (2015). Low-cost authentication protocol for passive, computation capable RFID tags. *Wireless Networks*, *21*(2), 565–580.
9. Li, T., & Wang, G. (2007). *Security analysis of two ultra-lightweight RFID authentication protocols*. Berlin: Springer.
10. Ling, S., & Xing, C. (2004). *Coding theory*. Cambridge: Cambridge University Press.
11. Peris-Lopez, P., Hernandez-Castro, J., Estevez-Tapiador, J., & Ribagorda, A. (2006). M^2 AP : A minimalist mutual-authentication protocol for low-cost RFID tags. In *Ubiquitous intelligence and computing: Third international conference, UIC 2006, Wuhan, China, September 3–6, 2006. Proceedings* (Vol. 4159, pp. 912–923).
12. Sun, H. M., & Ting, W. C. (2009). A gen2-based RFID authentication protocol for security and privacy. *IEEE Transactions on Mobile Computing*, *8*(8), 1052–1062.
13. Tian, Y., Chen, G., & Li, J. (2012). A new ultralightweight RFID authentication protocol with permutation. *IEEE Communications Letters*, *16*(5), 702–705.
14. Weis, S., Sarma, S., Rivest, R., & Engels, D. (2004). Security and privacy aspects of low-cost radio frequency identification systems. *Security in Pervasive Computing*, *2802*, 201–212.

Pramod Kumar Maurya received his M.Sc. in Mathematics from University of Allahabad, India, 2011. He has completed M.Tech. in Computer Science and Data Processing from IIT KHARAGPUR, India, 2014. He is currently a research scholar in the Department of Mathematics at NIT DURGAPUR, India. His research interests include identity authentication, RFID security, and information security.

Joydeb Pal received the B.Sc. and M.Sc. Degrees in Mathematics from the University of Calcutta, West Bengal, India, in 2011 and 2013, respectively. He is pursuing Ph.D. in the Department of Mathematics at NIT Durgapur, India. His research interests include RFID security and coding theory.

Satya Bagchi received the B.Sc. and M.Sc. Degrees in Mathematics from the University of Kalyani, West Bengal, India, in 2002 and 2004, respectively. He received Ph.D. degree in Mathematics from the same university in 2013. From 2006 to 2007 he was a lecturer, Department of Mathematics, A B N Seal College, Cooch Behar, West Bengal, India. He is currently an Assistant Professor, Department of Mathematics, National Institute of Technology, Durgapur, India. His current research interests are in RFID security protocol design, cryptography and coding theory. Dr. Bagchi is a life member of the Cryptology Research Society of India (CRSI).