A One Round-Trip Ultralightweight Security Protocol for Low-Cost RFID Tags

Wissam Razouk and Abderrahim Sekkaki

Mathematics and Computer Science Department, Faculty of Science, Hassan II University, Maarif, B.P. 5366, 20000 Casablanca, Morocco; e-mail: {wissam.razouk, abderrahim.sekkaki}@etude.univcasa.ma

Received 15 February 2013; Accepted 27 March 2013

Abstract

Radio Frequency Identification systems are already used in many sensitive areas, and are likely to be adopted almost everywhere. But their massive deployment implies several security and privacy issues. Moreover, low cost RFID tags have very limited storage and computational capabilities and cannot afford classic cryptographic primitives, which makes them vulnerable to several attacks. In this paper, we introduce some novelties in the field of low-cost security protocols such as the utilization of only two messages to fully complete the authentication and identification of the reader-tag. Additionally, the implementation of the pseudo random number generator (PRNG) on the server side reduces the storage and computation requirements on the tag. Furthermore, the proposed scheme protects the user's privacy and resists several attacks like malicious traceability, replay and impersonation attacks. And most importantly our protocol relies on simple bitwise operations and does not require computationally expensive cryptographic mechanisms.

Keywords: RFID security, low-cost RFID, lightweight cryptography, mutual authentication, un-traceability, privacy, confidentiality.

Journal of Green Engineering, Vol. 3, 261–272.

1 Introduction

RFID tags are wireless microchips that help to identify objects and people as well. They are already used nowadays in a variety of applications like medical implants, public transportation, aviation security and homeland security, etc. [27]. They are also significantly popular in areas such as authentication, e-payment, access control, and more importantly in supply chain management, retail inventory control and product tracking [24]. This success is mainly due to the fact that RFID tags allow a very effective remote identification of a great number of tagged items simultaneously and without visual or physical contact.

Usually the tags and readers are the main components of a RFID system. The reader is generally connected to a database on a server that stores the information associated with the tags. However, the shared radio medium allows easy eavesdropping on the communication between the tag and the reader. Furthermore, the tag can also be queried without authorization. Indeed, although security is essential for many RFID systems, numerous applications may suffer from multiple vulnerabilities like information leakage, traceability, impersonation or denial of service.

In general, RFID tags can be categorized into different types, depending on power source, memory size or tag price. If we take the price as a criterion, we can divide RFID tags into high-cost and low-cost RFID tags. We will focus in the rest of this document on the last type, as for massive deployment the price has to be kept low. Indeed, due to market consideration, low-cost RFIDs are estimated to be the best choice, and are more likely to be widely deployed.

Unfortunately low-cost RFID tags are very constrained devices and lack resources for performing classic cryptographic primitives. These systems can store no more than hundreds of bits and have only 5–10 K logic gates [18]. Moreover, only 250-3 K can be used for security reasons.

Many proposals have been published for this purpose; nevertheless, obtaining a maximum security with very few resources is still considered as a real challenge [3].

In this paper we propose an efficient ultralightweight security protocol for low-cost RFID tags. Furthermore, the proposed scheme resists several attacks, provides mutual authentication and protects the user's privacy.

The rest of this paper is organized as follows: First, we give a detailed description of the proposed scheme in Section 4. Next, we present the security

analysis and performance evaluation in Section 5. Finally, conclusions are given in Section 6.

2 Related Work

In 2006 three ultralightweight security protocols called UMAP family were proposed; Peris-Lopez et al. presented first M2AP [18], followed by EMAP [22] and LMAP [19]. Although considered as an interesting advance in lightweight cryptography, many security issues were highlighted using active and passive attacks [2, 4, 5, 8, 15–17].

Then in 2007 Chien released a proposal named SASI (strong authentication and strong integrity) [7]. The protocol shares the same structure with the UMAP family; it was designed to avoid some of the previous issues. But several security analyses have demonstrated de-synchronization attacks, and many weaknesses have been published [6, 9, 10, 13, 25].

Next, in 2008 Gossamer [21] was proposed to further develop the UMAP family and SASI protocol; however, other papers were published highlighting certain weaknesses of this scheme [28] [26]. Similarly, other protocols were presented later [11, 14, 29], but are also considered insecure according to many articles [12, 20, 23].

3 Our Contributions

- In the related works overviewed above, the protocols have a minimum of four and up to six exchanged messages. This type of protocols requires a number of operations on the reader side that is linear in the number of tags in the system, which might be impracticable since RFID systems can consist of a great number of tags. Our protocol needs only two message exchanges to fully complete the mutual authentication process.
- In all the protocols in Section 2 the tag keeps sending the same pseudo-dynamic index (IDS) as long as the reader has not been authenticated, which might make the protocol vulnerable to malicious traceability. In our scheme the tag does not send any message unless the reader is authenticated. Moreover all the exchange messages are randomized thanks to the nonce generated by the reader.
- It is not easy for low-cost RFID tags to install a PRNG, and hackers can also easily attack a system if PRNGs are not well designed. That is why we choose to implement the pseudo random number generator

(PRNG) on the server side to enhance security, and also to reduce the computation and storage requirements on the tag side.
- Unlike previous protocols in the state-of-art our protocol is not vulnerable to desynchronization attacks, as no updates are needed. Instead we use the nonce generated by the reader as a one-time-use authentication key.
- The proposed protocol relies on simple bitwise operations and does not involve computationally expensive cryptographic operations to provide protection against several attacks.

4 Description of the Proposed Scheme

4.1 Preliminaries and Notations

Three entities are involved in this scheme: the tag, the reader, and the backend server. Each tag stores the identifier IDT and the timestamp value t_i of the last authentication session to prevent replay attacks. Whereas the pseudo random number generator (PRNG) is only installed on the sever, therefore the tag needs only simple bitwise operations like XOR ($\oplus$) and left rotation ($Rot(A, B)$). Finally, the key K is shared between both tags and readers. We consider the length of the key and identifier is equal to 96-bits, which is compliant with EPCGlobal standard [1].We also assume that the communication between the reader and the back-end database is secure. On the contrary, the channel between the tag and the reader is considered insecure due to its open nature. The notations used throughout this paper are as follows:

- IDT: the identifier of the tag.
- K: a shared secret key
- R_i: a random integer
- $\oplus$: a bitwise XOR operation
- $Rot(A, B)$: a circular shift on A, $(B \bmod N)$ positions to the left for a given value of N (in our case 96).
- t_i: the timestamp of the current session, typically giving date and time of day, this sequence of encoded information is used in order to identify when the communication has been initiated. This data is usually obtainable in a consistent format, allowing for easy comparison of two different records and tracking progress over time.

For the sake of clarity, we denote both the server and the reader as reader. The messages exchanged in the protocol are described below:

Step 1 *The reader sends a request message to the tag.*
The reader generates a random integer R_i, then computes A_i, B_i and C_i by

$$A_i = Rot(Rot(R_i, K) \oplus K, K) \tag{1}$$

$$B_i = Rot(Rot(K \oplus R_i, R_i), R_i) \tag{2}$$

$$C_i = Rot(Rot(t_i, K) \oplus R_i, R_i) \tag{3}$$

$A_i||B_i||C_i$ are sent along with the request message to the tag.

Step 2 *The tag authenticates the reader.*
Upon receiving $A_i||B_i||C_i$ as a query, the tag extracts R_i of A_i by

$$R_i = Rot^{-1}(Rot^{-1}(A_i, K') \oplus K', K') \tag{4}$$

Next, the tag verifies if K equals K' stored in its memory using R_i and B_i as follows:

$$K = Rot^{-1}(Rot^{-1}(B_i, R_i), R_i) \oplus R_i) \tag{5}$$

Finally, the tag obtains t_i from C_i, and verifies if t_i is superior to t_i' stored during the last communication. The reader is authenticated if the message $A_i||B_i||C_i$ contains the right key K and the right timestamp t_i. The tag replaces then t_i' by the new t_i and computes $D_i||E_i$ to send it as a response by

$$D_i = Rot(Rot(K \oplus R_i, R_i), R_i) \tag{6}$$

$$E_i = Rot(Rot(IDT \oplus R_i, R_i), R_i) \tag{7}$$

Step 3 *The reader authenticates the tag.*
After receiving the response $D_i||E_i$, the reader computes D_i' by

$$D_i' = Rot(Rot(K \oplus R_i, R_i), R_i) \tag{8}$$

The reader will authenticate the tag if $D_i' = D_i$. Next the IDT is retrieved using

$$IDT = Rot^{-1}(Rot^{-1}(E_i, R_i), R_i) \oplus R_i \tag{9}$$

At this point, both the reader and the tag are mutually authenticated. The proposed ultralightweight RFID authentication protocol can be easily understood by looking at Figure 1.

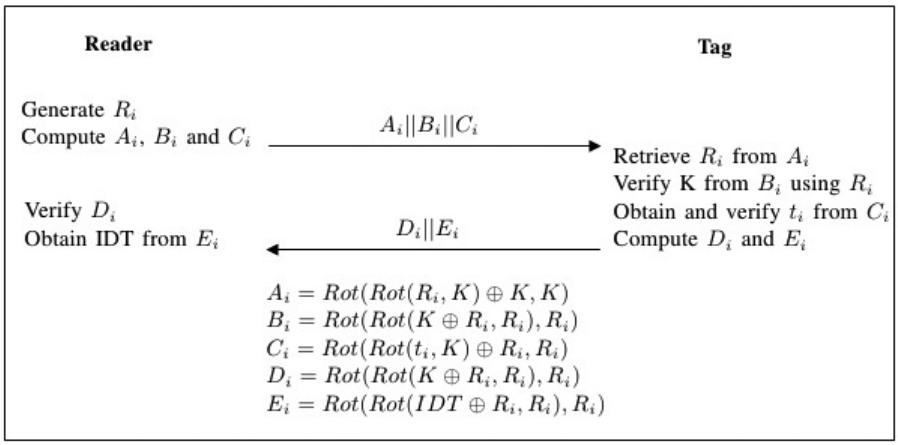

Figure 1 An ultralightweight security protocol for low-cost RFID tags.

5 Security Analysis and Performance Evaluation

The proposed protocol provides mutual authentication, the user's privacy protection and the resistance against various attacks such as impersonation and replay attacks. Moreover, the computational cost is quite low since only bitwise and rotation operations are used. A comparison of the relevant protocols in Section 1 is listed in Table 1.

5.1 Security Analysis

5.1.1 User's Privacy Protection

Traceability is one of the most difficult problems to solve. Indeed, malicious traceability allows recognizing and tracing an object or a person in different times and places. For instance, an attacker could identify important user's personal belongings in order to steal them, or track an important political person etc. Unlike the previous proposed protocols presented in Section 1, the tag does not send any message in our proposal, unless the reader is authenticated. Moreover, the double rotation provides a solid wrapping for the identity of the tag. In addition, all forward messages contain a random number which is different for each session. Therefore, it is difficult for an adversary to identify or trace a tag.

Table 1 Comparison of ultralightweight authentication protocols.

Protocols	UMAP Family [18, 19, 22]	SASI [7]	Gossamer [21]	This work
Total message exchanges	4	4	4	2
Resist de-synchronization attacks	×	×	×	√
Resist disclosure attacks	×	×	√	√
Required memory on the tag[1]	6L	7L	7L	3L
User's privacy protection	×	×	√	√
Forward secrecy	×	×	√	√
Mutual authentication	×	√	√	√
Operations in the tag	$\wedge, \vee, \oplus, +$	$\wedge, \vee, \oplus, +, Rot$	$\wedge, \vee, \oplus, +, Rot, MixBits$[2]	$\oplus, Rot$

[1] L denotes the bit length of the secret information.

[2] MixBits is a lightweight pseudo random number generator.

5.1.2 Mutual Authentication

This feature is important for many applications, such as e-bank payments. Indeed, the proposed protocol provides mutual authentication; thus, only a legitimate reader possessing the key K can build a valid message $A_i||B_i||C_i$. Similarly, only a genuine tag can derive the random number R_i from $A_i||B_i||C_i$, and then compute message $D_i||E_i$. Also the exchanged messages involve secret values K and R_i that allow data integrity to be checked.

5.1.3 Forward Secrecy

Forward security feature guarantees the security of past communications, even if the tag is compromised later. In fact, even if current messages are exposed, the random numbers used to create all the exchanged information are different and unknown, which prevents from inferring any secrets from previous sessions. Thus, this protocol obtains forward secrecy, and reduces the chances of using previous sessions to compromise the communication between the reader and the tag.

5.1.4 Resist Impersonation Attack

For example, an attacker can try to be authenticated as someone else, and gain access to restricted areas without being authorized to do so. Also, an expensive object can be disguised into a cheap one. Thus, in the proposed scheme, if an adversary wants to deceive a tag, and pretends to be a legal reader, the attack would not be successful, because the secret key K is unknown and therefore A_i, B_i and C_i cannot be found. In the same way, an attacker would fail to deceive the reader since both R_i and K are unknown; thus, D_i and E_i cannot be forged to pass the authentication.

5.1.5 Resist Peplay Attack

The proposed protocol is designed to counter replay attacks. To our best knowledge, this is the first time that a timestamp information is included in the request messages to prevent this type of attacks in low-cost RFIDs. For example, an eavesdropper could try to impersonate the reader and replay the request $A_i||B_i||C_i$; however, the message would not be validated as it will not pass the verification of K and t_i. Similarly, if an adversary tries to replay the response $D_i||E_i$, the reader will detect the attack, because different random numbers are used in each session. Therefore, our protocol resists replay attacks.

5.2 Performance Evaluation

5.2.1 Low Computation Cost

Low-cost RFID tags cannot afford to use classic cryptographic primitives, mainly because hash functions and standard cryptographic algorithms have a very high computational cost and need large memory space. Consequently, these methods are not suitable for very constrained devices like low-cost RFIDs.

The protocol we have proposed only requires left rotation and simple bitwise XOR. The computational cost of these operations is quite low and can be implemented in hardware efficiently.

5.2.2 Communication Cost

All the protocols described in Section 2 have a minimum of four and up to six exchanged messages. This type of protocols may be impractical, since it requires a number of operations on the reader side that is linear in the number of tags in the system, and might be considered unfeasible since RFID systems are usually composed of a great number of tags. However, in the proposed protocol, the mutual authentication and the integrity protection are fully realized with only two messages.

5.2.3 Storage Requirement

Each tag needs to store only two records in ROM. The identity IDT and the key K are considered to have 96-bit length, which is compliant with all encoding schemes (i.e. GID, SGTIN, SSCC) defined by EPCGlobal standard [1]. The timestamp t_i is stored in a rewritable memory because it needs updates. Again, this is considered very low compared with the previous protocols described in Section 1.

6 Conclusion

The Radio Frequency Identification technology is nowadays used in many sensitive areas, but due to market considerations, the price has to be kept low. However, low-cost RFIDs are very constrained devices, and cannot support classic cryptographic primitives.

In this paper, we presented an ultralightweight protocol suitable for low-cost RFID tags. Furthermore, the proposed protocol resists several attacks such as malicious traceability and replay attacks. Also, the protocol needs only two forward messages to fully complete the authentication and identi-

fication process. Indeed, it is highly unlikely that the communication would be compromised, even though the key is shared. In fact, the double rotation offers a solid wrapping for the key; furthermore, all the messages are completely different thanks to the random number. As a result, the forward messages are not fixed; so an attacker cannot trace or identify a tag. Finally, the timestamp is used to provide a double security check and protects the tag from replay attacks.

References

[1] EPC Global Standard Class-1 Generation 2. `http://www.epcglobalinc.org/standards/`.

[2] B. Alomair, L. Lazos, and R. Poovendran. Passive attacks on a class of authentication protocols for rfid. In Proceedings of the 10th International Conference on Information Security and Cryptology, pages 102–115. Springer-Verlag, 2007.

[3] G. Avoine, X. Carpent, and B. Martin. Privacy-friendly synchronized ultralightweight authentication protocols in the storm. Journal of Network and Computer Applications, 2011.

[4] M. Bárász, B. Boros, P. Ligeti, K. Lója, and D. Nagy. Breaking LMAP. Proc. of RFIDSec, 7:11–16, 2007.

[5] M. Bárász, B. Boros, P. Ligeti, K. Lója, and D. Nagy. Passive attack against the M2AP mutual authentication protocol for RFID tags. In Proceedings of First International EURASIP Workshop on RFID Technology, 2007.

[6] 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.

[7] 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.

[8] H. Y. Chien and C. W. Huang. Security of ultra-lightweight rfid authentication protocols and its improvements. ACM SIGOPS Operating Systems Review, 41(4):83–86, 2007.

[9] P. D'Arco and A. De Santis. From weaknesses to secret disclosure in a recent ultralightweight rfid authentication protocol. Technical Report, Cryptology ePrint Archive. `http://eprint.iacr.org/2008/470`, 2008.

[10] P. D'Arco and A. De Santis. On ultralightweight RFID authentication protocols. IEEE Transactions on Dependable and Secure Computing, 8(4):548–563, 2011.

[11] M. David and N. R. Prasad. Providing strong security and high privacy in low-cost RFID networks. In Security and Privacy in Mobile Information and Communication Systems, pages 172–179, 2009.

[12] J. Hernandez-Castro, P. Peris-Lopez, R. Phan, and J. Tapiador. Cryptanalysis of the David–Prasad RFID ultralightweight authentication protocol. In Radio Frequency Identification: Security and Privacy Issues, pages 22–34, 2010.

[13] J. C. Hernandez-Castro, J. M. E. Tapiador, P. Peris-Lopez, and J. J. Quisquater. Cryptanalysis of the sasi ultralightweight RFID authentication protocol with modular rotations. In ArXiv e-prints, 2008.

[14] Y. C. Lee, Y. C. Hsieh, P. S. You, and T. C. Chen. A new ultralightweight RFID protocol with mutual authentication. In Proceedings of WASE International Conference on Information Engineering (ICIE'09), volume 2, pages 58–61. IEEE, 2009.

[15] T. Li and R. Deng. Vulnerability analysis of EMAP – An efficient RFID mutual authentication protocol. In Proceedings of the Second International Conference on Availability, Reliability and Security (ARES2007), pages 238–245. IEEE, 2007.

[16] T. Li and G. Wang. Security analysis of two ultra-lightweight RFID authentication protocols. In New Approaches for Security, Privacy and Trust in Complex Environments, pages 109–120, 2007.

[17] T. Li, G. Wang, and R. H. Deng. Security analysis on a family of ultra-lightweight RFID authentication protocols. Journal of Software, 3(3):1–10, 2008.

[18] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda. Emap: An efficient mutual-authentication protocol for low-cost RFID tags. In Proceedings of OTM 2006 Workshops on the Move to Meaningful Internet Systems, pages 352–361. Springer, 2006.

[19] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda. M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags. In Ubiquitous Intelligence and Computing, pages 912–923, 2006.

[20] P. Peris-Lopez, J. Hernandez-Castro, R. Phan, J. Tapiador, and T. Li. Quasi-linear cryptanalysis of a secure RFID ultralightweight authentication protocol. In Information Security and Cryptology, pages 427–442. Springer, 2011.

[21] P. Peris-Lopez, J. Hernandez-Castro, J. Tapiador, and A. Ribagorda. Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In Information Security Applications, pages 56–68, 2009.

[22] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estévez-Tapiador, and A. Ribagorda. LMAP: A real lightweight mutual authentication protocol for low-cost rfid tags. In Proceedings of 2nd Workshop on RFID Security, page 6, 2006.

[23] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. E. Tapiador, and J. C. A. van der Lubbe. Security flaws in a recent ultralightweight RFID protocol. Arxiv preprint arXiv:0910.2115, 2009.

[24] C.M. Roberts. Radio frequency identification (RFID). Computers & Security, 25(1):18–26, 2006.

[25] H. M. Sun, W. C. Ting, and K. H. Wang. On the security of Chien's ultralightweight RFID authentication protocol. IEEE Transactions on Dependable and Secure Computing, 8(2):315–317, 2011.

[26] D. Tagra, M. Rahman, and S. Sampalli. Technique for preventing dos attacks on RFID systems. In Proceedings of International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pages 6–10. IEEE, 2010.

[27] R. Weinstein. RFID: A technical overview and its application to the enterprise. IT professional, 7(3):27–33, 2005.

[28] K. H. Yeh and N. W. Lo. Improvement of two lightweight rfid authentication protocols. Information Assurance and Security Letters, 1:6–11, 2010.

[29] K. H. Yeh, N. W. Lo, and E. Winata. An efficient ultralightweight authentication protocol for RFID systems. Proceedings of RFIDSec Asia, 10:49–60, 2010.

Biographies

Wissam Razouk received her B.Sc and M.Sc degrees from Hassan II Universiy, Casablanca, Morocco. She is currently a PhD student in the Mathematics and Computer Science Department, in the same university. Her primary research interests are RFID security protocols and formal verifications.

Abderrahim Sekkaki received his D.Sc. in the Network Management domain from the "Paul Sabatier" University, France, 1991. He received a Dr. of State Degree from Hassan II University, Morocco in 2002 and is presently a computer science professor at the same university. His research interests include distributed systems, policies based network management, and security.