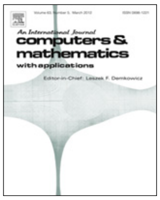
Computers and Mathematics with Applications 69 (2015) 58–65

Contents lists available at ScienceDirect

Computers and Mathematics with Applications

journal homepage: www.elsevier.com/locate/camwa



Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol[☆]

Jung-Sik Cho[a], Young-Sik Jeong[b], Sang Oh Park[a,*]

[a] Chung-Ang University, Republic of Korea

[b] Dongguk University, Republic of Korea

ARTICLE INFO

Article history:
Available online 9 March 2012

Keywords:
RFID
Hash
Mutual authentication

ABSTRACT

A radio-frequency identification (RFID) system is a promising automatic identification technology that uses communication via radio waves to identify and track moving objects. RFID systems are expected to replace bar-code systems in object identification fields in the future, but various security problems are obstructing their diffusion. The most important problem of RFID system is that an attacker can access the tag information, which raises privacy infringement and forgery problems. This paper proposes a hash-based RFID tag mutual authentication protocol to solve these security problems of RFID systems. The proposed protocol is designed to demand high cost of acquiring the tag information for attackers.

1. Introduction

Radio-frequency identification (RFID) systems are automatic identification systems using radio frequencies, and they consist of RFID tags, RFID readers, and a back-end server [1]. Tags store the unique identification information of objects and are attached to the objects to be identified. The reader requests unique identification information from a tag using a radio frequency and the tag returns the stored identification information using the radio frequency sent from the reader. The reader then sends the identification information received from the tag to the back-end server. The back-end server manages in its database (DB) the information of objects with attached tags and the unique identification information of the objects, and supplies the information of the objects when a reader requests it [1,2].

The advantages of RFID system are that the RFID tag is small and low-cost; massive RFID tags are recognizable simultaneously with radio frequency [1,2]. Therefore, RFID systems are expected to replace the current bar-code systems used in supply chain management [1,3,4].

Typical security problems that RFID systems must solve are privacy infringement and forgery. These security problems originate from the objects (tags, readers, back-end server) of the RFID system and information leakage during the communication process [3]. These may be solved easily if a proper cryptographic algorithm is applied in the communication between the tag and the reader [5–8]. But, as the tag is small and low-cost, the hardware resources are limited. Therefore, it is difficult to apply ordinary cryptographic algorithms to RFID systems, and this is blocking the widespread use of RFID systems [3].

[☆] This paper was originally submitted to the special issue "Advanced Information Security".

[*] Correspondence to: Chung-Ang University, 221 Huksuk-Dong, DongJak-Ku, 156-756 Seoul, Republic of Korea.
E-mail addresses: mfg@alg.cse.cau.ac.kr (J.-S. Cho), ysjeong2k@gmail.com (Y.-S. Jeong), sj1st@cs.cau.ac.kr (S.O. Park).

0898-1221/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2012.02.025

Much research is being conducted to address these security problems of RFID systems, largely divided into research on the blocking of the tag identification itself [3] and research on the use of tag authentication protocols [3,5,4,9]. Blocking the tag identification itself presents the potential loss of usefulness and management efficiency and may be abused by attackers. On the other hand, the tag authentication protocols allow the components of the RFID system to authenticate tags by processing and exchanging information in accordance with the defined procedure through cryptographic primitives. As only the valid components can generate and confirm information, the participation of invalid components is restricted and information leakage is prevented. This technique is most actively researched in diverse directions because it enables many variations.

This paper proposes a hash-based mutual authentication protocol to solve the privacy infringement and forgery problems. There have been many difficulties in applying hash functions to low-priced tags, but, as with much other research on hash-based techniques, this paper also assumes that hash functions will be able to be applied to tags in the near future.

The remainder of this paper is arranged as follows. We briefly review the properties of an RFID system and define attack models of an attacker causing privacy infringement and forgery problems. The necessary security requirements to complement an RFID system are described in Section 2, and the characteristics and problems of related works will be analyzed in Section 3. We present the hash-based mutual authentication protocol in Section 4 and analyze the security issues of the proposed protocol in terms of the privacy and forgery problems in Section 5.

2. RFID system security

RFID is identified a passive tag and an active tag according to the existence of own battery. An active tag that has its own power can compute high-level processes and its transmission range is wide. A passive tag, in contrast, has a limited transmission range and computation power for sending back radio waves received from a reader. Low-cost passive tags have played a leading role in popularizing RFID systems recently. Thus, the tag described in this paper is based on a passive tag.

The primary reason that RFID systems cause security problems is the limited resources of tags. Tags do not have their own power source, but consist of a small microchip and an antenna. When a reader makes a request in accordance with a predefined procedure, the tag returns the stored unique identification information to the reader. The tag generates power using the radio frequency delivered through the reader's request and performs limited operations before returning the unique identification information stored in the microchip to the reader. In this process, the communication between tag and the reader has the following characteristics [3,5,6,8].

- The unique identification information of the tag is transmitted to the reader via radio frequency without any processing.
- The tag transmits its own unique identification information at existence of query in any reader.
- Communication between the back-end server and the reader is secure; otherwise, communication between the reader and the tag is insecure because it uses radio frequency.

Due to inherent characteristics in RFID technology such as the special architecture of RFID systems and tag identification, RFID systems are subject to various attacks and can cause serious information leakage [2]. RFID systems are deployed in many industrial fields and possible privacy infringement and forgery problems in RFID applications might lead to the detriment of the RFID system owner [5].

Privacy infringement is divided into user privacy infringement and location privacy infringement. In user privacy infringement, an attacker gains the tag's ID through various attacks and analyzes it to obtain the information about the RFID-tagged objects, such as product price and personal interests and tastes. In location privacy infringement, an attacker traces the location of people and objects via the illicit tracking of RFID tags. Privacy infringement in RFID systems is a serious security risk because sensitive information is read directly from the tag without the knowledge or acknowledgment of the tag holder.

Forgery, a primary security concern in RFID systems along with privacy infringement, is a type of malicious act that obtains authentication information by masquerading as a legitimate reader or tag. An attacker impersonating a legitimate reader or tag in the system counterfeits behaviors of a tag or a reader or falsifies tag contents to gain an illegitimate advantage [4]. In general, RFID readers suffer mostly from forgery attacks. For example, a reader unknowingly communicates with an adversary who mimics an authentic tag or receives tag information that has been altered by unauthorized or unknown means.

Types of attacks by these attackers include attacks for privacy infringement such as eavesdropping, traffic analysis, and location tracking, and attacks for tag forgery such as replay attack, spoofing attack, and physical attack [9]. The following is a definition of an attack model.

- Eavesdropping [10,11]
  As the communication between the tag and the reader uses radio frequency, anyone can eavesdrop the communication between the tag and the reader. The attacker can acquire the secret information of the user through eavesdropping or make another attack by using the eavesdropped message.
- Traffic analysis (brute-force attack) [6,10,11]
  Traffic analysis is an attacking method to analyze the secret information necessary for the authentication protocol by using the messages eavesdropped from the communication between the reader and tag. Through the analysis of tag information, the attacker can acquire the information to connect the tag and the identity of tag owner. An attacker performs brute-force attacks with traffic analysis tools.

- Location tracking [6,11]
  With a malicious reader, the adversary can acquire the information of the tag and estimate which tag this information belongs to. When attacking, the attacker transmits the query continuously to the tag to be traced. Through this, the location of the tag owner is exposed and privacy can be violated.
- Replay attack [7,11]
  This is an attack in which an attacker transmits a message obtained by eavesdropping a regular communication between a reader and a tag to a verifier to be authenticated.
- Man-in-the-middle attack [4]
  This is similar to a replay attack. It is an attack in which an attacker impersonates as a legitimate tag by transmitting a response message that is obtained from the tag by the attacker impersonating a legitimate reader.
- Physical attack [12]
  The tag has a fatal defect that it is weak to physical attack. After an attacker has obtained a tag and physically acquired the information in it, the attacker can counterfeit the tag or alter it.

Many techniques for security of RFID systems are being proposed, and the security level of these techniques is evaluated by measuring the satisfaction of the security requirements in general. The security requirements mentioned here are defined as confidentiality, indistinguishability, forward security, and mutual authentication [3,5]. The security requirements are defined as follows.

- Confidentiality [5,10]
  Confidentiality is a security requirement that all the information should be secretly transmitted in every communication. If a tag transmits information without authentication or encryption, an attacker can identify the tag and infringe the privacy of its owner. Therefore, for confidentiality, it is necessary to authenticate the reader when the tag transmits the identification information to the reader, or to transmit encrypted information in order only for the legitimate reader to read it.
- Indistinguishability [5,10]
  This is the requirement that the transmitted information of the tag should not be the same, expectable, or distinguishable from the transmission information of other tag. If the transmitted information of the tag cannot satisfy indistinguishability, an attacker with a similar reader can continuously trace the owner of a specific tag or detect the real-time location of the tag owner by using the readers dispersed in several places.
- Forward security [5,10]
  This is the requirement that the previously transmitted information should not be traced with the present transmission information of the tag. If the past location of the specific tag owner can be traced with the present information, this will be a serious privacy infringement.
- Mutual authentication [7]
  Mutual authentication is the requirement that authentication should be given between the objects composing the RFID system. That is, mutual authentication should be made between the tag and the reader, the reader and the back-end server, and the tag and the back-end server.

When an RFID security scheme satisfies confidentiality, indistinguishability, and forward security, it is considered "resilient to privacy infringement". If the scheme satisfies mutual authentication, it is considered "resilient to forgery".

3. Reviews on related works

RFID security schemes can be grouped into two categories: schemes that interrupt tag recognition itself and those that utilize tag authentication protocols. Schemes in the first category can resist privacy infringement attacks to some extent, but they decrease RFID systems' efficiency and applicability. In addition, attackers can exploit schemes in the first category for malicious use [13–15]. In the second category, tag authentication schemes can be categorized according to the employed cryptographic primitive. Factors that one must consider in choosing a cryptographic primitive are security, efficiency, and applicability (practical implementation). When priority is given to efficiency and applicability, tag authentication schemes use lightweight operations like bit or mod operations as cryptographic primitives. Not surprisingly, tag authentication protocols employing lightweight cryptographic primitives provide high efficiency and applicability, but they are weak in terms of security. When security is very important, tag authentication protocols use traditional cryptographic operations such as symmetric or asymmetric key algorithms and hash algorithms. An assumption here is that such traditional cryptographic algorithms are operable in tags or that they will be operable in the near future if they are beyond the computational capabilities of current low-cost tags [16,17].

This paper is focusing on hash function-based scheme. A scheme based on the hash function is a technique in which the identification information of the tag is protected from the attacker through the one-way property of the hash function. Hash-based schemes have differences in accordance with how the secret value is used and managed. The methods of using and managing the secret value are determined by considering the characteristics and security requirements of the tag. Existing proposed protocols have improved and modified the use and management of the secret value.

Table 1
Notation.

Notation	Description
R	This represents a random number. R^r is a random number generated by a reader, and R^t is a random number generated by a tag.
ID^k, $DATA^k$	ID^k is the unique identification information (ID) stored in tag k. $DATA^k$ is the information of the object associated with the tag k.
s	This is the secret value shared by the back-end server and the tags. Each tag has two secret values: s^s and s^t
$h()$, α	$h()$ is the hash function and α is the hashed value.
$F_y^x(z)$, RID	$F_y^x(z)$ is a function that has z as an argument and performs an operation based on x; y is the communication session information. RID is the resulting value.

Among RFID security techniques, hash-based techniques offer a high level of security. However, they are regarded as impractical because, as the security level becomes higher, both the implementation and performance of tags get more unrealistic and the efficiency of the back-end server drops. As a typical example, the technique proposed by Ohkubo [6] has high a level of security, but the cost of searching tags by the back-end server is very inefficient. On the other hand, the hash lock technique [18] is sufficiently practical in terms of tag implementation and efficiency of the back-end server, but it has many weaknesses in security. This technique is particularly vulnerable to indistinguishability. Many modifications of these two techniques have been proposed. However, they share common problems in their basic forms. When attackers make specific formats of requests or meaningless requests to tags, the tags make the same response or their information is easily leaked [18]. Synchronization is another problem that needs to be solved, but techniques addressing this problem also show security vulnerability [19,20]. It seems that this problem originates from the use of random numbers which are used to satisfy the security requirements of RFID systems [9]. Therefore, this paper proposes a technique to solve this problem.

4. Proposed technique

Most RFID tag authentication techniques use random numbers for authentication by readers and protection of tag information. These random numbers, however, are easily exposed, because they are transmitted through radio frequencies without any processing. Thus, attackers can obtain them with simple means such as eavesdropping, and can use them to obtain the information that they want. To address this problem, this paper proposes a technique to prevent the exposure of tag information by processing the random numbers of readers and tags.

4.1. Notation and arithmetic operations

In the proposed protocol, the communication between the reader and the back-end server is secure, while the communication between each tag and the reader is insecure. The notation used in the proposed technique is defined in Table 1. The size of each value is assumed to be 96 bits.

Among the above notation, it is necessary to explain the method of generating RID and the role of s. First of all, RID is generated as follows:

$$F_i^s(R) = (R - R \bmod s + 1)(0:47) \parallel (R + s - R \bmod s)(48:95) = RID_i. \tag{1}$$

The argument in Eq. (1) is a random number. The random numbers are grouped on the basis of the secret value s, and the MSB 48 bit of the minimum value and the LSB 48 bit of the maximum value of each group are combined. The role of the secret value s is to define the range of each group when random numbers, which have been entered as the argument, are grouped. The secret value s can be equal for every tag. That is, it is not unique for each tag.

Tags have two secret values: s^t and s^r. The secret values used in Eq. (1) are determined by the following equations, depending on the random numbers that are entered as the argument.

$$F_i^{s^r}(R^r) = RID_i^r \tag{2}$$

$$F_i^{s^t}(R^t) = RID_i^t. \tag{3}$$

Secret values do not have ‘0’ and ‘1’. This is to consider the grouping of random numbers.

4.2. Proposed protocol

The proposed technique proposes the protocol as shown in Fig. 1. Each step of this protocol is described below.

Phase 0: *Information sharing between back-end server and tags*

- The back-end server and the tag decide and share the message-composing method for authentication and operating function.
- The tag has its own random number generator.
- The reader has a random number generator solely for itself.

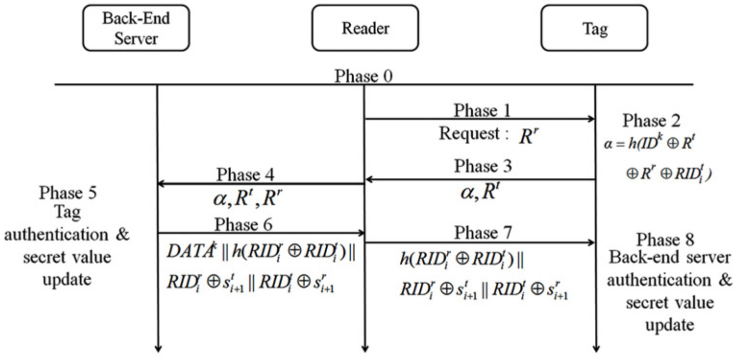

Back-End Server
Reader
Tag
Phase 0
Phase 1
Request : R^r
Phase 2
$\alpha = h(ID^k \oplus R^t \oplus R^r \oplus RID_i^t)$
Phase 3
α, R^t
Phase 4
α, R^t, R^r
Phase 5
Tag authentication & secret value update
Phase 6
$DATA^k \parallel h(RID_i^r \oplus RID_i^t) \parallel RID_i^r \oplus s_{i+1}^t \parallel RID_i^t \oplus s_{i+1}^r$
Phase 7
$h(RID_i^r \oplus RID_i^t) \parallel RID_i^r \oplus s_{i+1}^t \parallel RID_i^t \oplus s_{i+1}^r$
Phase 8
Back-end server authentication & secret value update

Fig. 1. Proposed protocol.

- The back-end server stores and manages the following tag information in the DB:

ID	S_i^t	S_i^r	S_{i-1}^t	S_{i-1}^r	$DATA$

■ *DATA*: Information of the tagged object.
■ *ID*: Unique identification information of the tag.
■ S_i^t, S_i^r: Secret values currently shared by the tag and the back-end server.
■ S_{i-1}^t, S_{i-1}^r: Secret values of the previous session shared by the tag and the back-end server.

Phase 1: *Reader's request*

- The reader generates a random number (R^r) in the session and requests tag information using this number.

Phase 2: *Generation of response message*

- The tag generates a random number (R^t) and also generates RID_i^t using Eq. (3).
- The response message is created using the hash function as follows:

$$\alpha = h(ID^k \oplus R^t \oplus R^r \oplus RID_i^t). \tag{4}$$

Phases 3 *and* 4: *Transmission of response*

- The tag sends the response message (α) generated from Eq. (4) and the random number (R^t) to the reader.
- The reader sends the response message received from the tag and the random number generated in the current session to the back-end server.

Phase 5: *Tag authentication and secret value update*

- The back-end server searches the tag in the DB based on the information received from the reader.
  I. The back-end server performs the following, based on the saved information of each tag.
    (1) It extracts the ID and the s_i^t and s_i^r values of a tag in the table.
    (2) It calculates the group ID ($RID_i^{t'}$) with s_i^t and R^t.
    (3) It generates α' with R^r from the reader, the calculated $RID_i^{t'}$, R^t, and the extracted ID.
    (4) The back-end server repeats steps (1)–(3) until α' is the same as α.
- When the tag is found, the back-end server updates the secret values of the tag. The secret values of this session are stored in S_{i-1}^t and S_{i-1}^r, and the newly updated secret values are stored in S_i^t and S_i^r.
- If the back-end server fails to find the tag, it searches again using the secret values (S_{i-1}^t, S_{i-1}^r) of the previous session. If no tag is found, it is judged an abnormal authentication message and the session is terminated.
- When the tag searching, authentication, and updating of secret values are completed, a message is generated as follows:

$$DATA^k \parallel h(RID_i^r \oplus RID_i^t) \parallel RID_i^r \oplus S_{i+1}^t \parallel RID_i^t \oplus S_{i+1}^r. \tag{5}$$

- The components of Eq. (5) are as follows.
  ■ Information of the tagged object ($DATA^k$) to be sent to the reader.
  ■ A message to provide authentication of the back-end server to the tag ($h(RID_i^r \oplus RID_i^t)$).
  ■ A message to provide authentication of the back-end server to the tag ($h(RID_i^r \oplus RID_i^t)$).
  ■ A message to safely deliver the newly updated secret values to the tag ($RID_i^r \oplus S_{i+1}^t \parallel RID_i^t \oplus S_{i+1}^r$).

Table 2
Performance comparisons.

Protocol	Computational cost		Communication rounds
	Tag	Back-end server (worst case)	
Dimitriou's protocol [4]	$\mathrm{H} + 3\mathrm{H_K} + \mathrm{RNG}$	$O(\log n)$	5
Yang's protocol [7]	2H	$O(2n)$	5
Ours protocol	$2\mathrm{H} + 4\mathrm{MOD} + \mathrm{RNG}$	$O(2n)$	5

H: hash operation; $\mathrm{H_K}$: keyed hash operation; RNG: random number generator; MOD: modular operation.

Phases 6 *and* 7: *Delivery of message generated by the back-end server*

- The back-end server delivers the message generated through Eq. (5) to the reader.
- The reader acquires the information of the tagged object from the message received from the back-end server and sends the remaining message to the tag.

Phase 8: *Back-end server authentication and secret value update*

- The tag authenticates the back-end server based on the message received from the reader.
  - ■ The tag generates RID_i^r by calculating Eq. (2) with the random number (R^r) received from the reader.
  - ■ The tag performs a hash operation using RID_i^t and RID_i^r that have been generated.
  - ■ The tag authenticates the back-end server by confirming that the hashed value is identical to $h(RID_i^r \oplus RID_i^t)$ that it received from the reader.
- When the back-end server authentication is completed, it expels the updated secret values from $RID_i^r \oplus S_{i+1}^t \parallel RID_i^t \oplus S_{i+1}^r$ and updates the secret values.
- If back-end server authentication fails, the secret values are not updated.

5. Analysis

This section analyzes the security level of the proposed technique. Attackers can perform wiretapping to the proposed technique. Information leakage through eavesdropping occurs when the reader and the tag exchange messages through a radio frequency in phases 1, 3, and 7. However, attackers cannot get any tag information just by eavesdropping. Even with eavesdropping in multiple sessions, attackers cannot get any information of tags and cannot even identify them, because tag information is processed through hash operation, random numbers, and Eq. (1).

Now we will calculate the cost of an attack when an attacker performs an analysis attack of the communication content to acquire tag information from the message obtained through eavesdropping. If the attacker obtained α, R^r, R^t by eavesdropping in phases 1 and 3, he/she will try to estimate the ID and secret values of the tag. At this time, the attacker will perform a brute-force attack and the cost has complexity 2^{192}. If the attacker additionally performed eavesdropping in phase 7, the cost of finding the two secret values also has complexity 2^{192}. This is a very high cost compared to the highest cost 2^{96} when the attacker performs a brute-force attack on existing protocols.

By requiring a high cost of acquiring tag information from attackers, the proposed technique satisfies all the security requirements for RFID systems as described below.

- Confidentiality: The proposed technique protects the ID of tags based on a hash operation, and the attacker must find the secret values to get it, but cannot find them due to high complexity.
- Indistinguishability: The proposed technique uses random numbers and grouping of them to make it impossible to predict the message generated by tags in each session.
- Forward security: To ensure forward security, the proposed technique is designed in such a way that, when the tag information is updated, the back-end server will generate it randomly.
- Mutual authentication: The proposed technique provides authentication between the back-end server and tags based on secret values, and provides reader authentication based on random numbers generated by the reader.

The proposed technique solves the user privacy infringement and forgery problems by satisfying all the security requirements as shown above.

The proposed protocol did not involve greater increase in computational cost or did rather require less cost. Existing protocols basically require more than two hash computations and some of them additionally perform random number generation. In the proposed protocol, the tag performs two hash computations, four modular computations, and one random number generation. When costs for the back-end server to retrieve all tags are taken into account, existing protocols generally perform hash computation n times. However, when synchronization problems occur, $2n$ hash computations have to be performed. In the worst case, the proposed protocol has to perform $2n$ hash and modular computations as well for the back-end server to retrieve a tag. Most protocols based on the hash function have to basically perform five rounds of communication for tag authentication and back-end server authentication. The proposed protocol also performs five rounds of communication. Table 2 shows a comparison to the existing protocols.

The proposed protocol was designed by using the framework of existing protocols. Thus, the structure and cost are not very different. However, existing protocols have serious vulnerability to location tracking and brute-force attack. The proposed protocol involves minimal cost increase and structural change to solve the drawbacks in existing protocols.

6. Future work

RFID security schemes should be designed to prevent security threats while maintaining the efficiency of the RFID systems. RFID systems require the back-end server to retrieve all tags in the system in order to identify a single tag, and an ideal goal is that they have constant-time tag retrieval complexity. However, most of the existing RFID tag authentication schemes have linear-time tag retrieval complexity, and it is very hard to reduce the retrieval complexity to be logarithmic in the number of tags, or even to be constant. As tag retrieval complexity decreases, it is easier for an attacker to gain access to tag information.

To build a security scheme that provides high security and efficiency, the hash operation for tag retrieval at the back-end server is replaced with a more lightweight operation. This does not allow constant-time tag retrieval but its tag retrieval accelerates compared to the tag retrieval made using the hash operation. In such a scheme, when the tag creates response messages, it produces messages for tag retrieval and authentication separately. Messages for retrieval are processed using an operation that is lighter than the hash operation, whereas messages for authentication are processed using the hash operation. This enables the back-end server to perform the computationally expensive hash operation only once.

7. Conclusion

An RFID system is a low-priced non-contact automatic identification technology. Due to the most basic characteristics of using radio frequency with small chip tags, however, RFID systems has user privacy infringement and forgery issues. To solve these problems, the present paper has proposed a hash-based RFID tag mutual authentication protocol.

The basic feature of the proposed protocol is grouping of random numbers to address the problem of the exposure of random numbers which are used to protect tag information and provide anonymity, resulting in acquisition of the random numbers by attackers through eavesdropping or other means to access tag information. As a result, the proposed technique demands a high cost of brute-force attack from attackers.

The proposed technique solves the user privacy infringement and forgery problems by satisfying all the security requirements for RFID systems. Future studies will need to find ways to provide higher efficiency of RFID systems.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2011-0014394) and by the IT R&D Program of MKE/KEIT [10035708, "The Development of CPS (Cyber-Physical Systems) Core Technologies for High Confidential Autonomic Control Software"].

References

[1] K. Finkenzeller, RFID Handbook, second ed., Wiley & Sons, 2002.

[2] EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860–960 MHz Version 1.2.0. EPCglobal Inc. (2008).

[3] A. Juels, RFID security and privacy: a research survey, Selected Areas in Communications 24 (2) (2006) 381–394.

[4] T. Dimitriou, A lightweight RFID protocol to protect against traceability and cloning attack, in: Proc. of SECURECOMM'05, 2005.

[5] S. Yeo, S. Kim, Scalable and flexible privacy protection scheme for RFID systems, in: European Workshop on Security and Privacy in Ad hoc and Sensor Networks—ESAS'05, in: LNCS, vol. 3813, Springer, Heidelberg, 2005, pp. 153–163.

[6] Miyako Ohkubo, Koutarou Suzuki, Shingo Kinoshita, Cryptographic approach to privacy-friendly tag, in: RFID Privacy Workshop, MIT, MA, USA, 2003.

[7] J. Yang, J. Park, H. Lee, K. Ren, K. Kim, Mutual authentication protocol for low-cost RFID, in: Proceedings of the Workshop on RFID and Lightweight Cryptography, July 2005, pp. 17–24.

[8] S.A. Sarma, S.E. Weis, D.W. Engels, RFID systems and security and privacy implications, in: Cryptographic Hardware and Embedded Systems- –CHES 2002, in: LNCS, vol. 2523, Springer, 2002, pp. 454–469.

[9] Jung-Sik Cho, Soo-Cheol Kim, Sang-Soo Yeo, RFID system security analysis, response strategies and research directions, in: Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops, IEEE Computer Society, 2011, pp. 371–376.

[10] S. Yu, K. Ren, W. Lou, A privacy-preserving lightweight authentication protocol for low-cost RFID tags, in: IEEE MILCOM 2007, October 2007, pp. 1–7.

[11] Y.-C. Lee, Y.-C. Hsieh, P.-S. You, T.-C. Chen, An improvement on RFID authentication protocol with privacy protection, in: Third International Conference on Convergence and Hybrid Information Technology—ICCIT 2008, vol. 2, November 2008, pp. 569–573.

[12] Srinivas Devadas, G. Edward Suh, Sid Praal, Richard Sowell, Thomas Ziola, Vivek Khandelwal, Design and implementation of PUF-based "Unclonable" RFID ICs for anti-counterfeiting and security applications, in: Proceedings of the IEEE International Conference on RFID, April 2008, pp. 58–64.

[13] A. Mitrokotsa, M.R. Rieback, A.S. Tanenbaum, Classification of RFID attacks, in: Proceedings of the 2nd International Workshop on RFID Technology, 2008.

[14] M. Langheinrich, A Survey of RFID privacy approaches, in: Personal and Ubiquitous Computing, 2009.

[15] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, RFID systems: a survey on security threats and proposed solutions, in: PWC 2006, LNCS, vol. 4217, pp. 159–170.

[16] M. Feldhofer, An authentication protocol in a security layer for RFID smart tags, in: The 12th IEEE Mediterranean Electrotechnical Conference–MELECON 2004, vol. 2, May 2004, pp. 759–762.

[17] I. Vajda, L. Buttyan, Lightweight authentication protocols for low-cost RFID tags, in: Second Workshop on Security in Ubiquitous Computing—Ubicomp 2003, October 2003.

[18] S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels, Security and privacy aspects of low-cost radio frequency identification systems, Security in Pervasive Computing (2003) 201–212.

[19] Bing Liang, Security and performance analysis for RFID protocols, in: Dissertations and Theses Collection, Paper 52. http://ink.library.smu.edu.sg/etd_coll/52.

[20] Ehsan Vahedi, Rabab Ward, Ian Blake, Security analysis and complexity comparison of some recent lightweight RFID protocols, Computational Intelligence in Security for Information Systems (2011).