International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.225-234
http://dx.doi.org/10.14257/ijsia.2014.8.6.20

A Strong Lightweight Authentication Protocol for Low-cost RFID Systems

Zhicai Shi[1,2], Josef Pieprzyk[2,3], Christophe Doche[2], Yongxiang Xia[1], Yu Zhang[4] and Jian Dai[1]

[1] *School of Electronic & Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, P. R. China*
{szc1964, x-free}@163.com, 1101196001@qq.com
[2] *The Department of Computing, Macquarie University, Sydney 2109, Australia*
Josef.pieprzyk@qut.edu.au, Christophe.doche@mq.edu.au
[3] *School of Electrical Engineering and Computer Science, Queensland University of Technology, Brisbane 4000, Australia*
[4] *Sino-Korean School of Multi-media, Shanghai University of Engineering Science, Shanghai 201620, P. R. China*
zhangyu43321@163.com

Abstract

RFID is an important technology that can be used to create the ubiquitous society. But an RFID system uses open radio frequency signal to transfer information and this leads to pose many serious threats to its privacy and security. In general, the computing and storage resources in an RFID tag are very limited and this makes it difficult to solve its secure and private problems, especially for low-cost RFID tags. In order to ensure the security and privacy of low-cost RFID systems we propose a lightweight authentication protocol based on Hash function. This protocol can ensure forward security and prevent information leakage, location tracing, eavesdropping, replay attack and spoofing. This protocol completes the strong authentication of the reader to the tag by twice authenticating and it only transfers part information of the encrypted tag's identifier for each session so it is difficult for an adversary to intercept the whole identifier of a tag. This protocol is simple and it takes less computing and storage resources, it is very suitable to some low-cost RFID systems.

Keywords: *RFID, Authentication protocol, Hash function, Privacy, Security*

1. Introduction

With the development of the Internet of Things, Radio Frequency Identification (RFID) technique gets the broad attention. RFID is a pervasive technology deployed in everyday life in order to identify objects using radio-waves, without visible light. It is considered as a supplementary or replacement technology for traditional barcode technology to identify, track, and trace items automatically. RFID may be viewed as a means of explicitly labeling objects to facilitate their "perception" by computing devices[l]. Today, RFID systems have been successfully applied to manufacturing, supply chain, agriculture, transportation, healthcare, e-payment and other fields [2, 3]. But, the wide applications of RFID into modern society may make the security and privacy of consumers exposed to threats and risks. For example, businesses may have many malicious competitors to collect unprotected RFID information, use forgery tags to provide some wrong information, or even launch denial of

ISSN: 1738-9976 IJSIA

service attacks against RFID systems. On the other hand, as a consumer, it is naturally preferred that the information of his RFID-tagged products should be private and secure. However, a tag reader can read the content of an un-protected tag, tracing the tagged product and even identifying the person carrying the tagged product. To protect the private information on the RFID tags, some special techniques can be used to prevent some malicious readers from accessing the tags. One of the most effective techniques is RFID authentication. Up to now, many authentication protocols have been proposed. Some protocols use the complicated encryption algorithms and they are not suitable for RFID systems with very limited computing and storage resources. Some other protocols use Hash function to complete the authentication for RFID systems, but they have some flaws which cannot ensure the security and privacy of RFID systems. It is very necessary to design a simple and feasible lightweight authentication protocol for the RFID systems, especially for low-cost RFID systems.

2. The RFID System and its Security

A RFID system consists of three components: Radio Frequency (RF) tags, RF readers and a backend server [4], as shown in Figure 1. A tag is basically a silicon chip with antenna and a small memory that stores its unique identifier known as EPC (Electronic Product Code). A reader is a device capable of sending and receiving data in the form of radio frequency signal. This device is basically used to read EPC from the tag. A backend server is used to store the information about the tagged objects and cooperates with readers to finish some complicated functions.

The basic working procedure for an RFID system is that the objects are tagged with a tag. The tag store some related data about the tagged objects. The tag receives the query from the reader and transmits data stored in it to the reader. The reader transfers these data to the backend server through wired or wireless networks. The reader could be fixed as well as mobile. The server processes the request from the reader and sends the related information about the tagged objects to the reader.

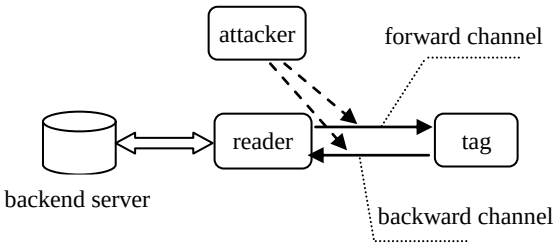

Figure 1. The Components of an RFID System

For an RFID system, a tag is a special device. Its computing and storage resource is very limited. There are two main types of tags: active tag and passive tag. Active tags include miniature batteries used to power the tags and they are capable to transmit data over longer distance. The other is passive tag which does not have any battery, it needs to be activated by the RF signal beamed from the reader. Passive tags are smaller, less expensive and used for a shorter range. Because of their priority this kind of tags are applied widely. Our researches mainly focus on the secure and private problems on this kind of low-cost Tags. We also note that since well-designed conventional cryptographic protocols can be effectively implemented on resource-abundant backend servers and readers, it is usually assumed that the channels between backend servers and readers are secure. However, because of the limited resource in

tags and the open wireless communication approach between tags and readers it has to assume that the channel between tags and readers is insecure. Readers have electric power enough to transmit signals over longer distance and tags only have limited electric energy to transmit signals over shorter distance. So the communication channels between readers and tags are asymmetric. We call the channel from readers to tags as forward channel and the channel from tags to readers as backward channel. These two channels are open and insecure. Most secure problems of RFID systems are resulted from these insecure channels.

For an RFID system, there exist many factors which threat to its security and privacy. The main secure and private problems are information leakage, eavesdropping, location tracing, forward security, desynchronization, replay attack, and spoofing [5].

• Information leakage: A tag stores its secret and private information. The information should not leak to any un-authorized or un-authenticated users. So the messages between tags and readers are usually encrypted so that illegal users cannot get any meaning information from the messages which they have gotten.

• Eavesdropping: This is one of the most basic threats to RFID systems. For this threat, eavesdroppers could impersonate a legitimate target tag to collect some information about the tag or the reader. Then they can conclude some security or privacy about the tag from the information which they have gotten.

• Location tracing or tracking: Some identity information stored in a tag can be used to trace the tag's holder by an adversary. When the transferred messages between tags and readers keep invariable it is easy to trace the location of a tag from these messages or to get the information of the tag's holder.

• Forward security: This security means that although attackers get the true messages of current sessions it is difficult and even impossible for an adversary to reveal any useful information of previous sessions.

• Desynchronization: The identity information of a tag is usually stored in the tag and the backend server simultaneously. To avoid being traced it is necessary to renew the identity information of the tags after each authentication. If the identity information in the backend server is renewed, the identity information in the tag is not renewed so that the identity information in the tag is not identical to the identity information in the backend server, which will compromise the next authentication.

• Replay attack: An attacker gets the messages from previous sessions during authenticating and retransmits them so as to disturb the next normal authentication process.

• Spoofing: This attack means that an attacker successfully impersonates a legitimate tag or reader to communicate with another one, so it can obtain illegal profit.

3. The Related Works

Authentication is the process of ensuring that the users are the persons whom they claim to be. Therefore, the goal of authentication is that the tag authenticates the reader before it is accessed and the authenticated readers can get the content of the valid tags. Moreover, private information would not be leaked to un-authorized or un-authenticated entities.

An RFID authentication protocol is a special cryptographic protocol where resource-limited RFID tags are involved. This kind of protocol is called as the lightweight authentication protocol. For this case, conventional authentication protocols that concern symmetric key computations or even public key computations are not applicable.

Many research works have been done for RFID authentication. Some authentication protocols use Hash function trying to solve the secure and private problems of RFID systems by using the one-way property of Hash function. But most of them have serious security

problems. Some classical authentication protocols based on Hash function are Hash-Lock protocol, Randomized Hash-Lock Protocol, Hash-chain protocol, and so on.

Based on the difficulty of inverting to solve a one-way hash function, S. A. Weis and S. E. Sarma, *et al.*, proposed Hash-Lock protocol which attempts to provide mutual authentication between tags and readers [6]. The protocol uses the metaID to replace the actual tag's ID to ensure its privacy. During the authenticating process the plaintext of the tag's ID is transferred between tags and readers, and metaID is fixed. So an adversary easily compromises mutual authentication by simply eavesdropping and replaying these exchanged messages between tags and readers. Moreover, the tag's holder is easily traced by an adversary by the fixed metaID.

In order to overcome the flaws of Hash-Lock protocol, S. A. Weis and S. E. Sarma, *et al.*, proposed randomized Hash-Lock protocol [6]. This protocol uses the pseudorandom number generator (PRNG) to randomize the transferred messages between tags and readers. Tags respond to reader's queries by generating a random value, r, then hashing its ID concatenated with r, and sending both values to the reader. A legitimate reader identifies one of its tags by performing a brute-force search of its known IDs. Then the reader sends the identified tag's ID to the tag by plaintext. It is easy for an adversary to eavesdrop and obtain the identity information of the tag. Hence, it is vulnerable to spoofing and replay attack. In addition, the tag's holder is easily traced and this protocol cannot satisfy the forward security.

M. Ohkubo et al. proposed Hash-chain protocol [7, 8]. It uses two different Hash functions H( ) and G( ). This protocol only provides one-way authentication, namely, the reader authenticates the tag while the tag does not authenticate the reader. To achieve forward security, this protocol uses the hash chain technique to renew the secret information stored in the tag. But it is vulnerable to spoofing and replay attack. Another similar scheme was provided by Sang-Soo Yeo, *et al.*, [9]. The scheme gave a conceptually simple but elegant solution to defeat the tracing problem and to ensure forward security. This scheme requires each tag to support 2 Hash functions. When the tag is queried by a reader, it sends the hash value of its current identifier by a Hash function, G( ), and then renews its identity information using another different hash function, H( ). These protocols use two different Hash functions and this makes it not suitable to low-cost RFID systems.

Yong Ki Lee, *et al.*, proposed a secure and low-cost authentication protocol for the RFID system, Semi-Randomized Access Control (SRAC) [10]. It also uses a pseudonym, MetaID to replace the tag's ID like Hash-Lock protocol. It provides mutual authentication and forward security. It can protect RFID systems from many attacks, such as tracing, cloning and denial of service. However, it is vulnerable to replay attack. The adversary can simply eavesdrop and reuse the MetaID to be authenticated successfully. Later, Su Mi Lee, *et al.*, proposed a low-cost RFID authentication protocol (LCAP) using a challenge-response method [11]. This protocol provides mutual authentication and guarantees the location privacy of tag's holder. It also provides untraceability by changing tag's identification dynamically. Nevertheless, it does not provide forward security, namely, an adversary infers previous information about tags after it obtains the present messages.

Jung-Sik Cho, *et al.*, [12, 13] proposed a new Hash-based authentication protocol to solve the secure and private problems for RFID systems. However, Hyunsung Kim [14] demonstrated that this protocol is vulnerable to DOS attack. He pointed out that Jung-Sik Cho, *et al.*, protocol is vulnerable to traffic analysis and tag/reader impersonation attacks. More precisely, an adversary can impersonate a valid tag or reader with probability 1/4. Finally, an adversary can obtain some information about the secret values of the tag in the next session with probability 3/4. Walid I. Khedr [15] pointed out that an adversary can perform a desynchronization attack by intercepting and tampering the transferred message in

step 5. Further, he justified that Jung-Sik Cho, *et al.*, protocol cannot ensure the forward security.

J. H. Ha and S. J. Moon, *et al.*, [16] proposed an RFID security protocol using the hash-based functions and proved that their protocol can provide forward privacy. However, Da-Zhi Sun and Ji-Dong Zhong [17] pointed out that an attacker can track a target tag by observing unsuccessful previous session of the tag. They justified that J. H. Ha, *et al.*, protocol fails to provide forward privacy as they claimed and then they proposed another hash-based authentication functions to overcome the weaknesses of J. H. Ha *et al.*, protocol. But all these protocols use two different hash functions and they are not suitable for low-cost RFID systems.

Liu Yang, Peng Yu, *et al.*, proposed an RFID secure authenticated protocol based on Hash function [18]. Their protocol ensures the privacy of information and realizes three party mutual authentications among tag, reader and backend database. But for each authenticating process of the protocol, the tag and the reader call Hash function over five times respectively. So their proposed protocol is so complicated that it is not suitable to low-cost RFID systems.

Except Hash function and other encryption functions, a pseudorandom generator and bitwise operations are often used to construct authentication protocols for RFID systems. But as soon as these protocols are proposed they were pointed out by other researchers that they did not solve all problems about the security and privacy of RFID systems, and they had some flaws to be improved, especially for low-cost RFID systems.

4. A Strong Lightweight FRID Authentication Protocol based on Hash Function

In the following parts, we propose a lightweight authentication protocol for low-cost RFID systems. This authentication protocol utilizes the one-way property of Hash function to encrypt the transferred messages between readers and tags so as to ensure the privacy and security of the RFID system. At the same time, a pseudorandom generator is used to ensure the freshness of the exchanged messages to prevent the RFID system to be traced. The used symbols during the authenticating process are listed in Table 1.

Supposed a tag is uniquely identified by an identifier, *ID*, which includes 2m bits. The backend server share the same Hash function with the tags and their shared secret key is *k*. Under the initial state, *ID* and *ID_index* are stored in each tag and the backend database, *ID_index* is the Hash value of the tag's *ID*. The tag and the backend server have two functions respectively. One is a 2m-bit Hash function, $H_k(\ )$, and another is a m-bit pseudorandom generator, *PRNG*( ).

The mutual authentication procedure between a reader and a tag is shown as Figure 2 and this protocol is described as follows:

Table 1. The Related Symbols for the RFID Authentication Protocol

Notation	Description
ID	the unique identifier of a tag
ID-index	the index of a tag
k	the secret key of the Hash function
$H_k()$	the Hash function with the secret key *k*
Rr	the pseudorandom number generated by a reader
Rt	the pseudorandom number generated by a tag
PRNG()	the pseudorandom generator
$F_l(x)$	the function to get the left half of *x*
$F_r(x)$	the function to get the right half of *x*
$\oplus$	XOR operator
$\|\|$	concatenation operator

- Step1: reader→tag

The reader generates a query for the tag and calls *PRNG*() to generate a pseudorandom number, *Rr*, then the reader sends query|| *Rr* to the tag.

- Step2: tag→reader

The tag calls *PRNG*() to generate another pseudorandom number, *Rt*, then the tag calls $H_k()$ to calculate $ID\_index \oplus H_k(Rt||Rr)$ and $H_k(ID \oplus (Rt||Rr))$, and forms the message $m1 = ID\_index \oplus H_k(Rt||Rr)$, $m2 = F_l(H_k(ID \oplus (Rt||Rr)))$, $m3 = F_r(H_k(ID \oplus (Rt||Rr)))$, and the tag sends *m1*, *m2* and *Rt* to the reader.

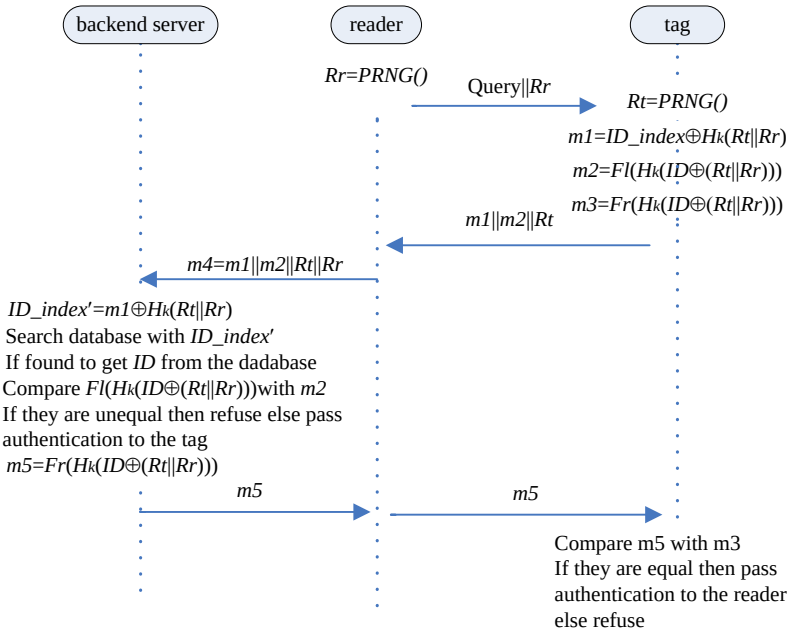

Figure 2. The Diagram of the Authentication Protocol based on Hash Function

- Step3: reader→backend server

The reader uses the received message *m1*, *m2* and *Rt* to generate the message $m4=(m1||m2||Rt||Rr)$, and sends *m4* to the backend server.

- Step4: backend server→reader

The backend server gets *Rt* and *Rr* from the message *m4*, and it uses the Hash function $H_k()$ to calculate $H_k(Rt||Rr)$, then get $ID\_index'=m1\oplus H_k(Rt||Rr)$. The backend server searches its database with *ID_index'*. If the backend server does not find the corresponding record in its database it notifies the reader that the tag is illegal. Otherwise it finds the corresponding record and uses the *ID* in this record to calculate $H_k(ID\oplus(Rt||Rr))$. Then the backend server compares *m2* with $F_l(H_k(ID\oplus(Rt||Rr)))$. If they are not equal the backend server notifies the reader that the tag is illegal. Otherwise the tag is legitimate. Then the backend server generates the message $m5= F_r(H_k(ID\oplus(Rt||Rr)))$ and sends *m5* to the reader. This step finishes the strong authentication of the reader to the tag by using the messages *m1* and *m2* simultaneously.

- Step5: reader→tag

The reader sends *m5* to the tag. Then the tag compares *m5* with *m3*. If they are equal the tag knows this reader is legal, otherwise the tag refuse to be accessed by this reader. This finishes the authentication of the tag to the reader.

5. The Analysis of the Strong Lightweight FRID Authentication Protocol

During the authenticating process described above, the tag and the backend server call Hash operation two times to hide the tag's private information. Therefore it is very difficult for an adversary to tamper or reveal the tag's identity information. The tag and the reader call one pseudorandom generating operation to ensure the freshness of the transferred messages between tags and readers in order to prevent to be traced. This ensures the forward security of the proposed protocol also. Suppose that there are *N* tags in total and the backend server maybe finish *N* comparison operations at most for a successful authentication. For the tag it only needs Hash function and pseudorandom number generating operation. Now we analyze the security and privacy of the proposed authentication protocol.

- Eavesdropping: During the authenticating process, all transferred messages between tags and readers are encrypted by Hash function and attackers do not know anything about the tag from their acquired messages. Eavesdropping to the communication between tags and readers is invalid. The privacy of the RFID system is protected.
- Location detection or tracing: One of the most serious privacy problems for the RFID system is that if an invariable value is exposed for each authentication, the privacy of the user's location may be encroached upon. To prevent this type of attack, a pseudorandom number generator is used to ensure each session between tags and readers is different so as to make attackers not to know where their received data is sent from.
- Replay attack: This type of attack means to re-sends data acquired by eavesdropping to compromise the RFID system. When identical or fixed values from the tag are exposed during the re-sending process, tracing problems may arise and privacy may be encroached upon. In order to prevent replay attack the content of each session between tags and readers should be different by randomizing and Hash operations. If an attacker re-sends its received message later this message has not any meanings because each new session generates a new random number and the corresponding messages.
- Forward security: For each authenticating process, readers and tags generate a pair of new random numbers that there are not any relationships with the last authentication. These

random numbers randomize all transferred messages between tags and readers. Attackers cannot infer any useful information of the previous authentication from the present received messages, and attackers cannot guess the tag's or reader's past behaviors.

• Spoofing: The protocol ensures user anonymity and privacy by hashing all exchanged messages between readers and tags. Only part information of the tag's *ID* (*e.g.*, *m2* and *m3*) is transferred each time during the authenticating procedure. An attacker cannot get the whole identity information of a tag, so an adversary cannot impersonate a valid tag to spoof the RFID system.

By analyzing above, it is observed clearly that all transferred messages between tags and readers are randomized and they are variable during the authenticating procedure, although *ID* and *ID-index* of each tag is invariable. The tag's *ID* is not changed so that the proposed authentication protocol can be used to the distribution computing environment. At the same time, it is seen obviously that each transferred message between tags and readers only includes part information of the tag's *ID* during the authenticating procedure so that it is difficult for the adversary to acquire the whole information about the tag's *ID*. On the other hand, the messages *m1* and *m2* are simultaneously used by the backend server to complete twice strong authentication to the tag. The comparison of our proposed protocol with some typical Hash-based authentication protocols is listed in Table 2.

Table 2. The Comparison of the Different Authentication Protocols

Protocol type	Eaves-dropping	Location tracing	Replay attack	Forward security	Spoofing
Hash-Lock protocol	x	x	x	x	x
Randomized Hash-Lock protocol	x	x	x	x	x
Hash-chain protocol	√	√	x	√	x
SRAC protocol	√	√	x	√	x
Our proposed protocol	√	√	√	√	√

6. Conclusions

It is generally admitted that the security and privacy protection of the tag play an important role in determining the cost and performance of an RFID system. To solve the secure and private problems of the RFID system with low-cost tags, we have proposed a lightweight mutual authentication protocol based on Hash function and this protocol completes the mutual authentication between tags and readers. Superior to other similar protocols, our proposed protocol can ensure forward security and prevent information leakage, location tracing, eavesdropping, replay attack, and spoofing. The proposed protocol is simple and secure. The backend server only needs twice Hash operations and it can finish the strong authentication to tags. The tag only needs twice Hash calculations and one random generating operation. It only stores the shared secret key *k*, its identifier *ID* and its index *ID-index*. It is obvious that our proposed protocol needs less computing and storage resource, and it can be used in low-cost RFID systems.

Acknowledgements

We are grateful for the anonymous reviewers who made constructive comments so that we can improve and refine our paper. The relative work about this paper is supported by National Natural Science Foundation of China (No. 61272097), and the Course Construction Project of Shanghai University of Engineering Science (No. K201302002).

References

[1] A. N. Nambiar, "RFID Technology: a Review of its Applications". Proceedings of the World Congress on Engineering and Computer Science, **(2009)** October 20-22, San Francisco, USA.
[2] S.-Y. Kang, D.-G. Lee and I.-Y. Lee, "A Study on Secure RFID Mutual Authentication Scheme in Pervasive Computing Environment". Computer Communications, vol. 31, **(2008)**, pp. 4248-4254.
[3] A. Stephen, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", The First International Conference on Security in Pervasive Computing, **(2003)** March 12-14, Boppard, Germany.
[4] S. E. Sarma, S. A. Weis and D. W. Engels, "RFID Systems and Security and Privacy Implications". Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems, **(2002)** August 13-15, CA, USA.
[5] S. E. Sarma, S. A. Weis and D. W. Engels, "Radio-frequency Identification: Secure Risks and Challenges". RSA Laboratories Cryptobytes, vol. 6, no. 1, **(2003)**, pp. 2-9.
[6] S. A. Weis, S. E. Sarma, R. L. Rivest and D. W. Engels, "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems", Proceedings of the 1st International Conference on Security in Pervasive Computing, **(2003)** March 12-14, Boppard, Germany.
[7] M. Ohkubo, K. Suzuki and S. Kinoshita, "Cryptographic Approach to "Privacy-Friendly" Tags" RFID Privacy Workshop, MIT Press, Cambridge, **(2003)**.
[8] M. Ohkubo, K. Suzuki and S. Kinoshita, "Hash-chain Based Forward Secure Privacy Protection Scheme for Low-cost RFID", Proceedings of the 2004 Symposium on Cryptography and Formation Security, **(2004)** January 27-30, Sendai, Japan.
[9] S.-S. Yeo and S.-K. Kim, "Scalable and Flexible Privacy Protection Scheme for RFID Systems", European Workshop on Security and Privacy in Ad hoc and Sensor Networks ESAS'05, **(2005)** July 13-14, Visegrad, Hungary.
[10] Y. K. Lee and I. Verbauwhede, "Secure and Low-cost RFID Authentication Protocols", Proceedings of the 2nd IEEE Workshop on Adaptive Wireless Networks, **(2005)** November 28-December 1, St. Louis, USA.
[11] S. M. Lee, Y. J. Hwang, D. H. Lee and J. I. Lim, "Efficient Authentication for Low-Cost RFID Systems", LNCS, vol. 3480, **(2005)**, pp. 619-627.
[12] J.-S. Cho, S. S. Yeo and S. K. Kim, "Securing against Brute-force Attack: a Hash-based RFID Mutual Authentication Protocol Using a Secret Value", Computer Communications, vol. 34, **(2011)**, pp. 391-397.
[13] J.-S. Cho, Y.-S. Jeong and O.-P. Sang, "Consideration on the Brute-force Attack Cost and Retrieval Cost: a Hash-based Radio-frequency Identification (RFID) Tag Mutual Authentication Protocol", Computers and Mathematics with Applications, vol. 3, **(2012)**, pp. 1-8.
[14] H. Kim, "Desynchronization Attack on Hash-based RFID Mutual Authentication Protocol", Journal of Security Engineering, vol. 9, no. 4, **(2012)**, pp. 357-365.
[15] W. I. Khedr, "SRFID: a Hash-based Secure Scheme for Low Cost RFID Systems", Egyptian Informatics Journal, vol. 14, **(2013)**, pp. 89-98.
[16] J. H. Ha, S. J. Moon, J. Y. Zhou and J. C. Ha, "A New Formal Proof Model for RFID Location Privacy", Proceedings of the 13th European Symposium on Research in Computer Security–ESORICS'08, **(2008)** October 6-8, Malaya, Spain.
[17] D.-Z. Sun and J.-D. Zhong, "A Hash-Based RFID Security Protocol for Strong Privacy Protection", IEEE Transactions on Consumer Electronics, vol. 58, no. 4, **(2012)**, pp. 1246-1252.
[18] L. Yang, P. Yu, W. Bailing, Q. Yun, B. Xuefeng, Y. Xinling and Y. zelong, "Hash-based RFID Mutual Authentication Protocol", International Journal of Security and Its Applications, vol. 7, no. 3, **(2013)**, pp. 183-194.

Authors

Zhicai Shi, he received his Ph.D. degree from Zhejiang University. He is currently the Professor of School of Electronic & Electrical Engineering, Shanghai University of Engineering Science, China. His research aims to create new technologies for network analysis and RFID authentication. In recent years, based on granular computing he proposed some information-fused methods to reduce the attributes of big data so as to improve the performance of network analysis. At the same time he proposed some innovative authentication methods for RFID systems. He is the author of 6 books, more than 70 publications in journals and conferences.

Josef Pieprzyk, he received his Ph.D. degree from Polish Academy of Sciences. He is currently the Professor of School of Electrical Engineering and Computer Science, Queensland University of Technology, Australia. His main research interest is Cryptology and Computer Security, and includes design and analysis of cryptographic algorithms, secure multiparty computations, and cryptographic protocols. He published more than 200 papers in refereed journals and refereed international conferences.

Christophe Doche, he received his Ph.D. degree from University of Bordeaux. He is currently the head of Computing Department of Macquarie University, Australia. His main research interests are Cryptology, Analytic number theory, Computation and algorithms in finite fields. Since 2000, he published 3 books and more than 20 papers in refereed journals and refereed international conferences.

Yongxiang Xia, he received his M.S. degree from Donghua University. He is currently the Lecture of School of Electronic & Electrical Engineering, Shanghai University of Engineering Science, China. His research interest is network and information security. He is the author of 4 books, more than 20 publications in journals and conferences.