International Journal of Grid and Distributed Computing
Vol. 11, No. 10 (2018), pp.93-102
http://dx.doi.org/10.14257/ijgdc.2018.11.10.08

# Security Authentication Technique using Hash Code in Wireless RFID Environments

Cheol-seung Lee

*Dept. of Teacher Training & Liberal Arts, Kwangju Women's University, Gwangju, Korea*
*cyberec@kwu.ac.kr*

***Abstract***

*The Fourth Industry Revolution is a computing technology-based environment that provides new industry convergence all around the world. The development of computing technology and networking has provided a ubiquitous environment. In the ubiquitous environment, access and connection to various devices and objects are actively proceeding. RFID, which uses a wireless identification code, is very effectively applied to SCM management by tagging objects, is studying standardization of RFID system in EPCglobal. RFID systems have more security threats than wired solutions by using wireless environment technology. In particular, if it does not provide confidentiality, Indistinguishability, and forward security, it will cause various problems in the era of the fourth industrial revolution. Therefore, this study analyzes RFID security system and various RFID security authentication techniques, proposes an RFID security authentication method using an alternative hash function.*

***Keywords:*** *RFID System, Hash Function, RFID Security*

## 1. Introduction

The Fourth Industrial Revolution has been a hot topic all over the world since the Fourth Industrial Revolution was thrown at the Davos Forum. Among the technologies of the Fourth Industrial Revolution, the ubiquitous computing environment requires a convergence environment of various devices, networks, and software technologies. RFID (Radio Frequency Identification) technology, which identifies objects in the Internet of Things Technology field, is applied to all industries and has a competitive edge.

RFID systems are already used in various fields. Especially, it is very efficient in accurate inventory management and SCM (Supply Chain Management) in distribution and logistics fields. However, due to the indiscreet usage of RFID, there are various security threats owing to leakage of information attached to tag, leakage of unique ID, and attack of attacker, which is a problem to be solved in the future ubiquitous environment.

On account of RFID systems use wireless environments, there are more security threats than wired security problems. In order to construct an RFID security system, the computational complexity of the system must be considered and there are many problems in applying heavy public key cryptosystem with excellent security. Particularly, if it does not provide confidentiality, indistinguishability and forward security, it will cause various problems.

Confidentiality is a security requirement that information must be encrypted and secretly transmitted. In order to ensure confidentiality, a tag must use an authentication protocol that verifies whether it is appropriate information when

Received (June 15, 2018), Review Result (September 28, 2018), Accepted (October 4, 2018)

ISSN: 2005-4262 IJGDC

transmitting identification information to the reader, and a method of transmitting encrypted data only known to the reader.

Indistinguishability means that when a tag sends information to a reader, it is a security requirement that you should not give the same value each time. To ensure Indistinguishability, the tag should not always transmit the same information, and it must transmit the result value after performing the operation equivalent to the random number generation in the tag or transmit the value updated by the legitimate reader outside the tag.

The forward security is to ensure that the attacker does not know the past session key and the current session key generated using the key distribution protocol. In the RFID system, the forward security means that the attacker cannot know the transmission information of the past even if the RFID tag knows the information currently transmitted or the information stored in the tag is exposed.

In this paper, we analyze the RFID standardization system and one - way hash function in Chapter 2, and in Chapter 3, we identify problems in the RFID system security authentication techniques that has been studied. In Chapter 4, we propose a security authentication techniques using a hash function based on a Hash-Lock based ID variant authentication techniques.

## 2. Related Research

### 2.1. RFID System

The RFID system uses the radio frequency to obtain information of the tag by the controller to recognize and analyze. It consists of three components: a reader, a transponder called a tag, a machine that can process data, or a computer. A reader is a device that identifies unique information transmitted from a tag, called a transceiver, tags are classified into active type and passive type according to the power supply type. In a system using a passive tag, when a reader transmits a radio wave to a tag, the tag acquires power from the received low frequency wave, activates it, and transmits its ID information to the reader. The RFID reader sends the read tag ID information to the Savant server to confirm the location of the PML (Project Markup Language) with the object information in the ONS (Object Naming Services), and obtains specific information of the object from the PML server [1].

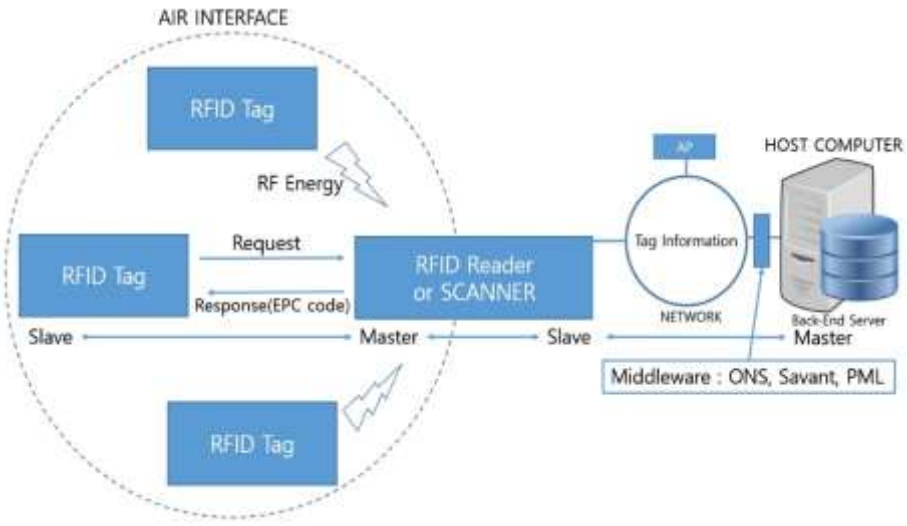


**Figure 1. RFID System Environments**

 

### 2.2. RFID System Standard

RFID system is being standardized in EPCglobal and Ubiquitous ID Center. EPCglobal looked at the EPC (Electronic Product Code) system of GS1(Global Standard Number 1). EPC is performing infrastructure standardization to identify various information of specific products, EPC is aiming at establishing distribution logistics system by standardizing RFID tag technology and information acquisition procedure about products.

In EPCglobal, Class 0 and Class 1, as for the tag, Class 1 Generation 2 of UHF (Ultra High Frequency) band will integrate Class 0/1 and become EPCglobal's RFID Air Interface standard. The EPCglobal code system consists of a back-end server system with middleware including EPC, Savant, ONS and PML, it provides an application service that collects, controls, and manages the data continuously linked with the Internet network. It also needs to be able to ensure interoperability for various types of reader interfaces, various codes, network applications, and various applications [2].

### 2.3. RFID System configuration

In EPCglobal, EPC has been developed as a replacement for bar codes, and individual products can be uniquely identified and authenticated. EPC consists of 4 fields like IPv4 through 64bit or 128bit length ID.

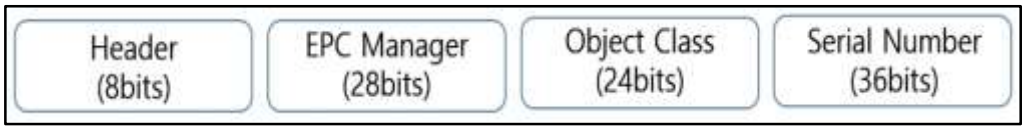


**Figure 2. EPC Code**

The first field in Figure 2 is a header that is compatible with other code version numbers that are already defined and identifies the codes through this header. The second field is an identification code that identifies the vendor's information of 28 bit length. The third field is called the Merchandise object class, and the last field consists of a serial number that identifies each Merchandise.

Savant is a public software installed on the server, which reads RFID tags in the field and provides functions to integrate and control various object information, Savant communicates with the reader through the reader interface and communicates through the application and application interfaces. In Savant's three technologies, the first one is RFID event collection, the second one is the control device function, and the third one is the intermediary for connecting the information network gateway, Savant internal application, and external EPC network.

The EMS (Event Management System) classifies the collected data according to its purpose and places it in the place where the relevant work is handled. The TMS (Task Management System) processes the actual work and plays a role of linking with the existing system. In addition, RFID collects EPC data generated in real time and refers to a real-time information database.

ONS plays the role of converting the EPC to URL (Uniform Resource Locator) on the Internet and finding the IP address. The RFID reader sends the EPC code to Savant, when Savant executes the EPC code to the ONS server, the ONS server switches to the IP address and sends it to Savant.

PML, developed by EPCglobal, is a language that describes the environment related to objects, systems, and objects. The function of the PML is to read information about the product and other information related to the product by the RFID reader through Savant and then to store it in the form of XML (Extensible

 

Markup Language) in the PML server. The main purpose of the PML is to provide information on the products to which the RFID technology is applied in a standard common language and make it available for various tasks and application systems. The PML includes inventory control, automated trading, supply chain tracking and machine control [3-5].

### 2.4. One-way Hash Function

A one-way hash function refers to an encryption method that receives input values of a certain length and maintains a constant output value through a hash function *H()*. The characteristics of the hash function are as follows: *H(H(x))* ..... For a given input value x, a hash table is constructed as shown in Figure 1 to obtain an output value, the input value $H(x_n\text{-}1)$ cannot be obtained in the reverse direction [6].

Typical input lengths of hash functions are 128bit, 160bit, 192bit, and 256bit. Typical one-way hash functions are MD5 and SHA-2, and MD5 [7] is mainly used for the symmetric key block encryption algorithm.

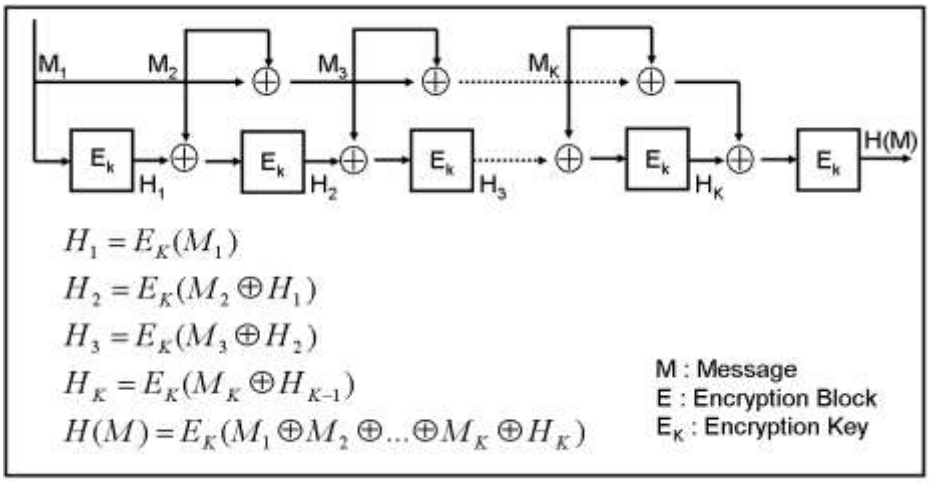


**Figure 3. MD5 Hash Function**

## 3. RFID Systems Security Authentication Technique

The security threats of RFID systems include the leakage of information about the property attached to the tag and there is a security threat from the attacker because a unique ID is leaked between the direct identification information of the tag. In Section 3, we introduce the RFID system security authentication techniques and analyze the problems [8].

### 3.1. Kill Tag Authentication Technique

The Kill Tag security method proposed by EPCglobal refers to a method of converting the tag into the inactivation mode by using 8-bit unique password and Kill command for each tag.

Since the tag has a short circuit inside it, it executes the Kill command, and the once inactive tag becomes impossible to be reused. However, for tags that are designed to be Read / Write, the tag can be reactivated using flag bits, but problems with the 8-bit password in tags can occur, you can abuse the command to get the password by a simple calculation of $2^8$ or so. Therefore, considering the tags to be used for many products, it is necessary to use 128-bit or more code but there are problems and cost to store the RFID tag [9].

 

### 3.2. Re-Encryption Authentication Technique

The Re-Encryption scheme is a technique for re-encrypting the RFID system using a Public key password authentication method. The information stored in the tag rewrites the data transferred from the external unit when the user requests use. The Re-Encryption scheme can guarantee confidentiality by preventing the attacker from intercepting the result of randomly generated tags in the rewriting cycle. However, there is a disadvantage in that it requires cost for public key encryption, it is not possible for an RFID tag to perform a public key cryptographic operation, the reader's information update problem does not guarantee Indistinguishability.

### 3.3. OTP Authentication Technique

OTP (: One Time Password) authentication scheme is a method in which a reader and a tag share a common table of a random key, a key of a recipient is confirmed through a plurality of communications, and a tag that mutually authenticates transmits an ID. After the authentication process, the OTP is updated by the random value, the XOR operation is applied to the RFID to perform the mutual authentication, but the ID of the tag is updated every time, so that it can be practically used. However, there is a problem that there is a problem of separation between the reader and the database, communication between the tag and the reader, and possibility of tapping during the authentication session [10].

### 3.4. Hash-Lock Authentication Technique

The tags of the Hash-Lock authentication scheme are passive and have only a few hundred bits of memory with read functions. ID is the actual data, ID is the random value *key*, and *metaID* is the *metaID = H(key)* generated by the key hash function.

In a Hash-lock authentication scheme, a tag having a hash function as an operation tool stores its own actual data ID by the owner, and stores the temporary *metaID* value required in the authentication process. At this time, the *metaID* is a hash value *metaID = H(key)* of a randomly selected key, and is called a Hash-Lock. After Hash-Lock, *key* and *metaID* are stored in the database securely with RF channel or physical contact for security.

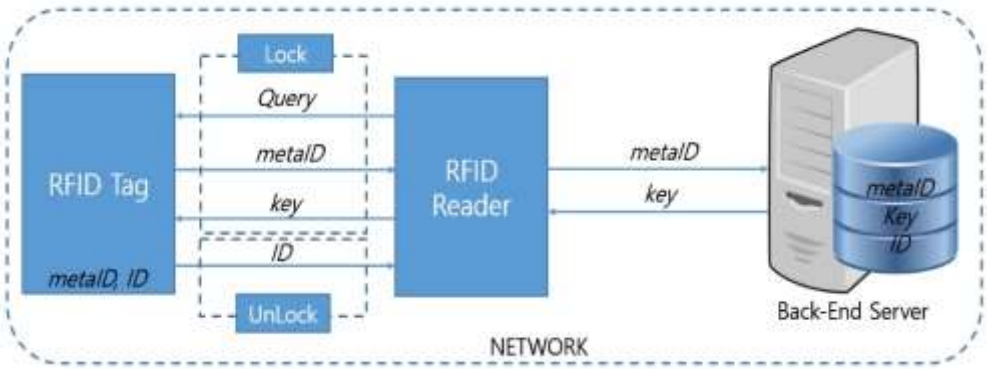


**Figure 4. Hash-Lock Authentication Technique**

Figure 4 shows the authentication process of the Hash-Lock technique. Hash-Lock is divided into lock and unlock. In the locked state, the tag keeps locked until it reaches the unlocked state by responding to the *Query* of all the readers with *metaID*. However, if the hash received from the reader is the same as its own *metaID*, it is judged to be valid information, and is changed to the unlock state and the *ID* is transmitted to the reader.

The Hash-Lock scheme requires a single hash operation on the tag, assuming that the back-end server's database is secure, it manages the keys of all tags. The safety of the Hash-Lock technique is based on a one-way hash function, an attacker cannot impersonate a legitimate leader because it is difficult to know the *key* from the *metaID* if the *key* is not known. Identification information in the tag is only given to an authenticated reader who can access the Back-end server, which ensures confidentiality.

However, after an attacker obtains a *metaID* value, it can spoof attack by obtaining a *key* value through a legitimate reader by pretending to be a legitimate tag. In addition, since the tag in the locked state always transmits the *metaID* value, it cannot satisfy the Indistinguishability, and there may be a problem of tracking the location.

### 3.5. Hash-Lock-based ID Deformed Authentication

The authentication scheme based on the Hash-Lock technique is a technique that assumes that a hash function is included in a tag and that the tag performs the hash operation twice during the protocol execution.

**Table 1. Operational Sign**

| Sign | Description |
|---|---|
| ID | Current ID value |
| HID | The hashed ID value |
| TID | Authentication session number |
| LST | Last successful authentication session number |
| AE | Database entry |
| DATA | User information |
| H() | One-way hash function |
| R | Random number |
| $\oplus$ | Exclusive OR operation |

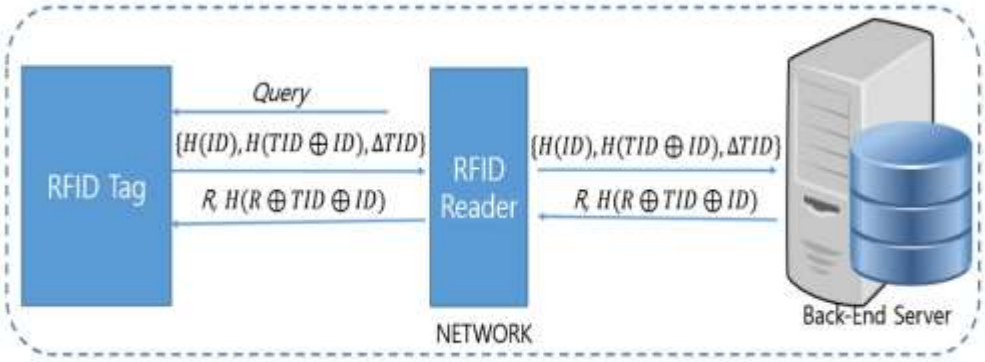


**Figure 5. Hash-Lock-based ID Deformed Authentication**

In Figure 5, after the reader sends a query to the tag, the tag has *H(ID)* hash of the current *ID* value, $\Delta TID$, which is the most recent successful authentication session number LST, And sends $H(TID \oplus ID)$ to the leader. The reader stores the $\{H(ID), H(TID \oplus ID), \Delta TID\}$ value in the back-end server, and the back-end server finds the hash table in which the *H(ID)* value in the database is stored as the *key* value. After checking whether the value is stored in another value and the hash table, random number *R* is generated, and the table value is updated and the new table having the new database *key* value $H(R \oplus ID)$ is updated and stored together.

 

The $R$ value and the $H(R \oplus TID \oplus ID)$ value are then sent to the reader together, and the reader sends the two values to the tag. The tag first XORs the received $R$ value with its own $TID$ value and $ID$, verifies whether the hash value matches the received $H(R \oplus TID \oplus ID)$ value, and changes its $ID$ to $ID = TID \oplus ID$ if it matches.

Hash-Lock-based ID deformation authentication technique guarantees lightness and confidentiality of the back-end server. However, there is a disadvantage that it cannot guarantee disability.

First, the transmission of the same *H(ID)* value can be traced from the attacker to the tag. Since the second $\Delta TID$ value is a constant value, a part of the next response information of the tag can be predicted. If the third arbitrary reader continuously transmits the query to the tag, the value of $\Delta TID$ increases, so that it can be distinguished from other tags. After intercepting the transmission value of the fourth normal reader, if the attacker's intentionally generated *R(= 0)* value and the $H(R \oplus TID \oplus ID)$ value calculated using the *R(= 0)* value are transmitted to the tag, the tag is recognized as a normal protocol, *ID* is changed, but the *R* value is 0, so the original *ID* is maintained. As a result, there is a problem that the information held by the server and the information held by the tag do not coincide with each other, so that the normal authentication procedure cannot be performed. After all, since the transmitted value *H(ID)* of the tag always becomes a fixed value after the attack, the Indistinguishability is broken and the position tracking becomes easier and the forward stability is not ensured.

## 4. Hash Code Security Authentication Technique

RFID security authentication schemes are still challenging. In this paper, we propose RFID authentication method considering confidentiality, indistinguishability, and forward security in order to reduce computation volume and provide strong security. In order to overcome RFID security authentication technique, ID anonymization can be used to prevent related information leakage, tag tracking can be avoided and public key encryption algorithm can be used. However, public key cryptography requires considerable amount of computation This is due to the increased cost of the tag, which is not appropriate for RFID security authentication techniques.

**Table 2. Operational Sign**

| Sign | Description |
|---|---|
| m | Number of tags |
| n | The length of the hash value |
| ID | Identification information of the tag |
| H | One-way hash function |
| $H_n$ | Other hash functions |
| $S_i$ | The hash value of the tag |
| T | Tag |

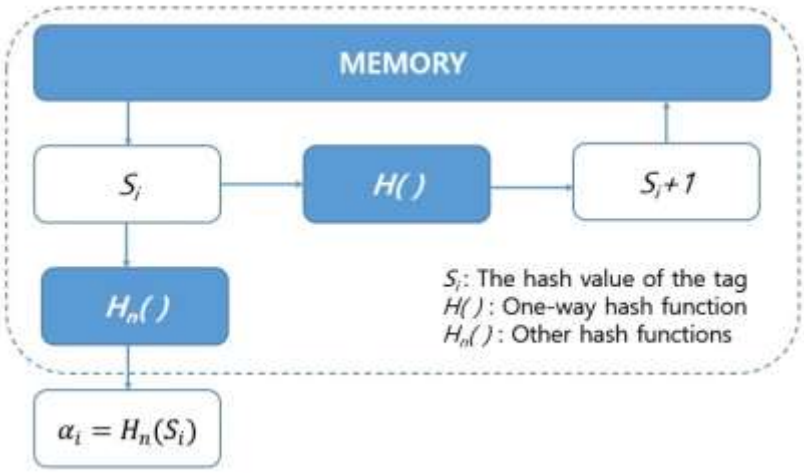


**Figure 6. Internal Structure of Tag**

In Figure 6, we have two hash functions $H( )$, $H_n( )$, the Back-End server stores each identification information ID value for the tag $T$ and the hashed secret value $S_i$ value of the randomly generated tag in the database. It is assumed that each tag has $S_i$. If the value $n$, the number of times the tag is read, is specified, the range of $T$ is $1 <= T <= m$. Each time the reader sends a *Query*, the tag applies its own secret value $S_i$ to the hash function $H_n( )$ and sends $\alpha_i = H_n(S_i)$ to the reader. The tag figures $S_{i+1} = H(S_i)$ to update its own secret value, and the reader sends $\alpha_i = H_n(S_i)$ to the Back-end server.

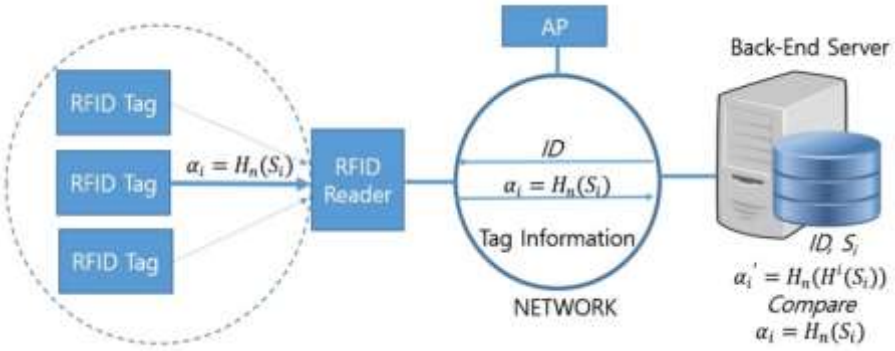


**Figure 7. Authentication Process**

In Figure 7, the Back-end server figures $\alpha_i' = H_n(H^i(S_i))$ for all $1 <= T < m$ and $1 <= i <= n$ to find the Si value that matches the received $\alpha_i$. The *ID* can be found by the value of $S_i$, and the Back-end server sends the *ID* to the reader and then terminates the protocol. Finally, the Back-end server puts all of its secret values into a formula to determine which hash table a particular tag belongs to. Of course, a method of storing the values of all the hash tables can be considered, but it becomes impossible if the number m of the tags increases to some extent.

Since the proposed scheme does not perform authentication protocol on whether the reader is suitable, the protocol is very simple because it gives the reader the value calculated by the hash function $H_n( )$ as the current secret value $S_i$. It is difficult to attack by inputting specific values from the outside.

In addition, the tags themselves update the internal information of the tag, not the tag that renews the internal information of the tags from the outside, thus ensuring confidentiality and Indistinguishability from attack by tapping.

 

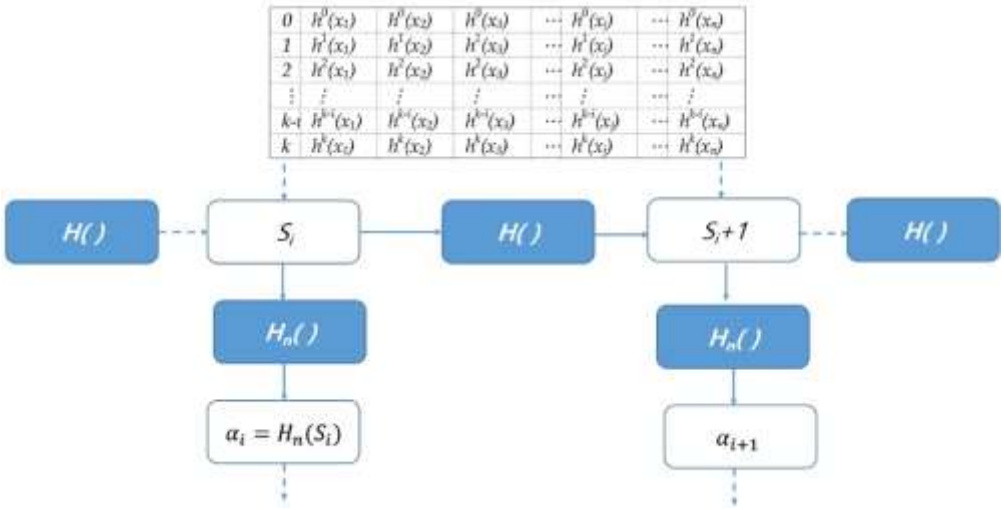


**Figure 8. Hash Table Example**

Also, in Figure 8, the change of the internal information of the tag operation is calculated by using the one-way hash function. Even if internal information is leaked by an attack, the RFID tag can be made at a low price while securing the forward safety to the characteristics of the hash function.

## 5. Conclusion and Future Research

RFID technology, which identifies objects wirelessly in the great paradigm of the Fourth Industrial Revolution, is an identified recognition technology among the things Internet technology, and is applied to all industries and has a competitive edge. However, due to the indiscreet use of RFID, there are security threats due to leakage of information attached to tag, leakage of unique ID, and attack of attacker, which is a problem to be solved in the future ubiquitous environment. In order to construct an RFID security system, it is necessary to consider the amount of computation of the system, and there are many problems to apply a security technique with excellent security and heavy security. In particular, if it does not provide confidentiality, Indistinguishability and omnidirectional safety, it will cause various problems.

In this paper, we analyze RFID standardization system and one - way hash function, we propose a secure authentication scheme using a hash function based on a Hash-Lock-based ID variant authentication scheme.

The proposed authentication scheme is configured to update the internal information of the tag itself by using a simple protocol that reduces the amount of computation using the characteristics of the hash function. This is an authentication technique that ensures confidentiality, Indistinguishability and omnidirectional safety. In the fourth industrial revolution era, it will be necessary to study the extended use of RFID system and various security systems.

## Acknowledgments

This paper is a revised and expanded version of a paper entitled “A Study on Requirements for Wireless RFID System Environments” presented at, C.S. Lee, Hokkaido, Japan, August 23-25 of Proceedings of the 7th International Conference on Next Generation Computer and Information Technology, NGCIT 2018.

This paper was supported (in part) by Research Funds of Kwangju Women's University in 2018 (kwul18-052).

 

## References

[1] R. Weinstein, "A Technical Overview and Its Application to the Enterprise", IT Professional, IEEE Computer Society, vol. 7, no. 3, **(2005)** June, pp. 27-33.
[2] H. Chow, K. Choy, W. Lee and K. Laub, "Design of a RFID case-based Resource Management System for Warehouse Operations", Journal of International Expert System with Applications, vol. 20, no. 4, **(2006)** May, pp. 561-576.
[3] C. Floerkemeier, D. Anarkat, T. Osinski and M. Harrison, "PML Core Specification 1.0", Auto-ID Center Recommendation, **(2003)** September, pp. 5-25.
[4] U. Karthaus, and M. Fischer, "Fully integrated passive UHF RFID transponder IC with 16.7-uW minimum RF input power", IEEE Journal for Solid-state Circuits, vol. 38, no. 10, **(2003)** October, pp. 1602-1608.
[5] H. Yoon, M. Mohaisen, K. Chang, J. Bae and G. Choi, "Performance Analysis of Wireless Communications between Tag and Reader in EPCglobal Gen-2 RFID System", Journal of Korean Institute of Electromagnetic and Engineering and Science, vol. 18, no. 124, **(2007)**, pp. 1047-1056.
[6] C. S. Lee "A Study on Effective Hash Routing in MANET", Proceedings of the 3rd International Conference on Computer, Information and Application, Yeosu, Korea, **(2015)** May, pp. 21-23.
[7] C. S. Lee "A Study on Effective using Security Routing based on Mobile Ad-hoc Networks", International Journal of Security and Its Application, vol. 9, no. 7, **(2015)**, pp. 141-152.
[8] C. S. Lee "A Study on Requirements for Wireless RFID System Environments", Proceedings of the 7th International Conference on Next Generation Computer and Information Technology, NGCIT 2018, Hokkaido, Japan, **(2018)** August, pp. 46-51.
[9] A. Juels, R. Rivest and M. Szydlo, "The blocker tag: Selective Blocking of RFID Tags for Consumer Privacy", 8th ACM Conference on Computer and Communications Security, **(2003)** March, pp. 27-30.
[10] A. Juels, "RFID security and privacy: a research survey", IEEE Journal on Selected Areas in Communications, vol. 24, Issue 2, **(2006)**, February, pp. 381-394.

## Author

**Cheol-seung Lee** is currently an assistant professor at the Teacher Training & Liberal Arts Department at the University of Kwangju women's University in Korea. He received his Ph.D. in Computer Engineering from the University of Chosun, Korea, in 2008.

His recent research activities are focused on MANET, Wireless Network security and Mobile programming and privacy in IOT and smart environments.

 