Security Enhanced Authentication Protocol for UHF Passive RFID System

Suna Choi, Sangyeon Lee, Heyungsub Lee
RFID Basic Technology Research Team
Electronics and Telecommunications Research Institute (ETRI)
Deajeon, Korea
sunachoi@etri.re.kr, lsyeoun@etri.re.kr, leehs@etri.re.kr

***Abstract*—The passive RFID system was spotlighted as a future technology for automatic identification, but it has a possibility of eavesdropping and leaking of private information. We propose a security enhanced protocol with mutual authentication and data cryptographic mechanism between secure reader and tag for the UHF passive RFID system. We use the OFB-like mode of AES as an effective encryption method. The proposed security enhanced protocol is designed to satisfy the demands of ISO/IEC WD 29167-6, namely the new international standard for the RFID security services. In addition, we present that the proposed security process conforms to the time limitation of the ISO/IEC 18000-6C.**

Keywords-RFID security; AES; OFB-like mode; mutual authentication.

I. INTRODUCTION

The RFID is one of the most important technologies which bring enormous benefits in applications where objects have to be identified automatically. It can be applied various applications including supply chain management, product tracing, building access control, public transportation, airport baggage, express parcel logistics and automatic product checkout, etc [1].

The ISO/IEC 18000-6C is the representative RFID standard for the UHF-band passive RFID system. But it does not provide security mechanism between the tag and reader in wireless environment, so the conventional RFID system has a possibility of eavesdropping and leaking of private information.

Each RFID system consists of a tag which is attached to a product for identification and a reader which can access individual data of tags. An unauthorized RFID reader might access to the tag and steal the private contents, and it could be used to trace the movements of a consumer who has a product with an RFID tag. Furthermore, RFID tags can be forged and abused when it is applied services such as proof of origins. The security problems can threat the development of the RFID system.

The ISO/IEC 18000-6C standard allows the Kill command to protect privacy [2]. But the tag cannot be used anymore after killed, so the applying services can be restricted. As concerns regarding security and privacy issues are raised highly, ISO/IEC JTC 1 SC31 WG7 has been organized. It is a working group for preparing international standard of the security services and file management of RFID by the classified frequency bands. The ISO/IEC 29167-1 defines the architecture for RFID security framework and security service and the ISO/IEC 29167-6 defines the secured air interface and file management for 860 – 960 MHz UHF band.

Many researchers in the standard group have discussed a cryptographic security system which provides the untraceability, secure communication, authentication, and compatibility with the ISO/IEC 18000-6C standard as the requirements.

There are cryptographic primitives using hash-based methods, symmetric encryption methods, etc. Hash–based methods are conceptually simple and considered a good choice for RFID [3]~[5]. But the symmetric encryption method like Advanced Encryption Standard (AES) is suggested as a better choice on RFID tags from the implementation point of view [6]~[8]. Furthermore, AES is largely accepted in industry and actually mentioned as a strong candidate of the security method for standardization.

The response times and link frequencies of a tag and a reader are specified in the ISO/IEC 18000-6C standard and the security protocol should obey them. But it is hard for a cryptographic process to satisfy the specified time, especially the time from reader transmission to tag response (T1 time), because of the limited resources of the passive tags. In other words, the allowed power of a passive tag is approximately less than several tens of uW. As the operating frequency is higher, the processing time of a cryptographic process can be decreased, however, the consuming power of a tag increases. So the operating frequency is limited (generally less than several MHz).

In this paper, we propose a security enhanced protocol with mutual authentication and cryptographic process which conforms to the ISO/IEC 18000-6C and meets the demands of the ISO/IEC 29167-6. In addition, we present the proposed cryptographic process satisfy the time limitation.

The paper is organized as follows. The key generation method and encryption/decryption process of the proposed cryptographic method are described in Section II. The structure of memory and proposed security enhanced protocol are given in Section III. Then, the discussion and

 ISBN: 978-1-61208-140-3

the simulation results showing that the proposed security process satisfies the time limitation of ISO/IEC 18000-6C are presented in Section IV. Finally, conclusion and further works are followed in Section V.

II. PROPOSED CRYPTOGRAPHIC METHOD

The AES algorithm was chosen in 2001 as an encryption standard. It provides strong security and is well suited for hardware implementation [8]. It operates on a symmetric data block with variable key and block length. The key and block length can be specified to 128, 192, 256 bits. In this paper, we applied the AES algorithm using fixed 128 bit data block and key length.

In order to use a cipher to protect the confidentiality or integrity of messages, the mode of operation of a block cipher must be specified [9]. We apply the modified Output Feedback (OFB) mode of AES, named OFB-like mode. Similar to the OFB mode, the AES engine generates key streams and the messages are encrypted or decrypted by means of bitwise XOR with the generated key streams. Because of the symmetry of the XOR operation, the encryption and decryption processes are technically similar and the extra decryption engine is not required. So, it is appropriated to implement a lightweight secure RFID system.

In the OFB-like mode, however, all messages transmitted between a reader and a tag are considered as a long message and a new session key is generated using the previous key instead of the output of bitwise XOR. It reduces the processing time and enables to satisfy the time limitation specified in the ISO/IEC 18000-6C standard.

A. Session key generation method

Figure 1 shows the generation method of the session keys in the AES OFB-like mode.

The encryption engine that generates a session key is initiated by the first data and the master key. The first data is randomly generated by the reader and the tag during security protocols. The RnInt is a random number transmitted from a reader to a tag and the RnTag is a random number transmitted from a tag to a reader. The addition of the RnInt and RnTag becomes the first data. The AES crypto engine generates the first session key and then generates the second session key using the first session key and the master key. The crypto engine takes the previous session key as the next data in every generating routine of a new session key. The crypto engine generates firstly two session keys to prevent the exhaustion of the session key. And then, the crypto engine generates a new session key whenever one session key of the two is exhausted.

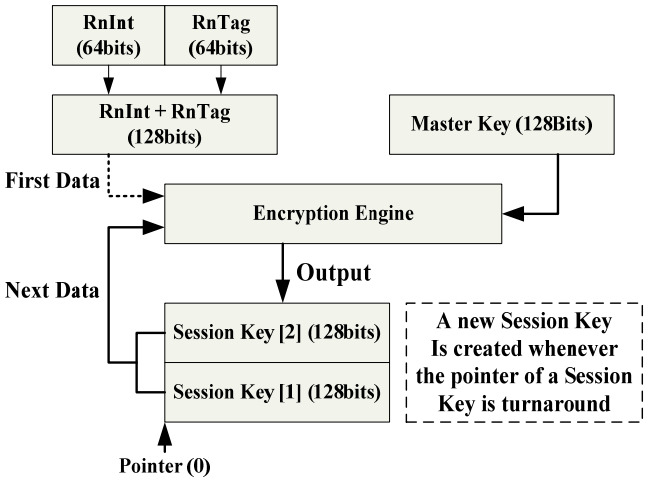

Figure 1. Key generation method in the OFB-like mode

B. Encryption and decryption process

Figures 2 and 3 show the proposed encryption and decryption process.

The encryption process is bitwise XOR operations of the plain data and generated session keys. Sequentially, the command and CRC16 is created and added to the encrypted data. The pointer is moved by a bit as the encryption is performed. And the decryption process is similar to the encryption process. The command and CRC16 is checked and removed and only encrypted data takes the XOR operation with the session key.

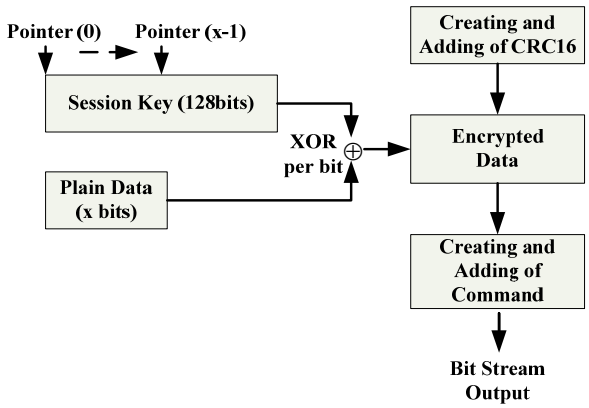

Figure 2. Encryption process

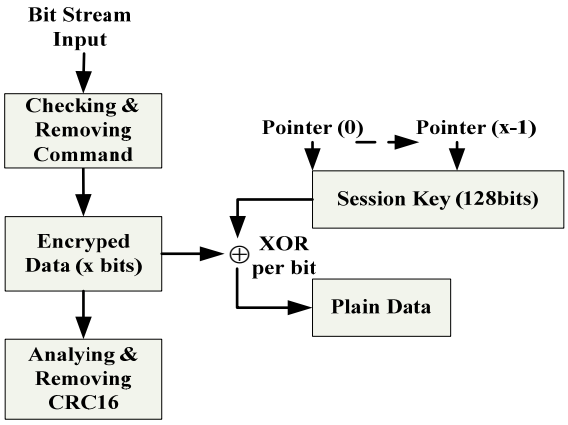

Figure 3. Decryption process

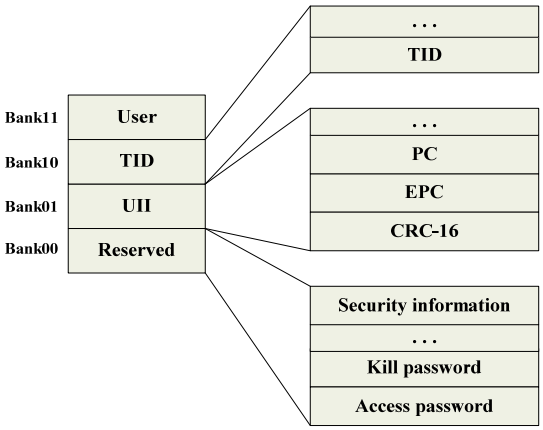

Figure 4. Structure of the RFID tag memory

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
XPC_W1	XEB		MIIM		SA	SS	FS	BM		TC	U	S	RFU	REC[2:0]		
XPC_W2	FMFF						SFF						CSI [3:0] (AES OFB-like)			

Figure 5. XPC in the memory of the secure tag

III. PROPOSED SECURITY ENHANCED PROTOCOL

A. *Memory Map of the Secure Tag*

As shown in Figure 4, a RFID tag has the memory which is logically separated into four distinct banks. They are Reserved bank, Unique Item Identifier (UII) bank, Tag identification (TID) bank, and User bank.

The External Protocol Control (XPC) of the ISO/IEC 18000-6C contains XPC-W1 and XPC-W2 as presented at Figure 5.

If the Extension bit (XEB) is '0', it means that the Tag does not implement an XPC_W2. The XEB value of the proposed secure tag is always '1'.

XPC-W1 of the proposed secure tag has U (Untraced) and S (Secure) flags additionally. The U bit indicates whether the corresponding tag supports the untraced function. When the U bit value is '0', it means that the UII which is transmitted to the reader in the first inventory process is fake. When the U bit value is '1', it means that the UII is true. The S bit indicates whether the corresponding tag supports the security function. When the S bit value is '0', it indicates that the corresponding tag operates as a conventional passive tag. When the S bit value is '1', it indicates that the tag operates as a secure tag supporting the security functions.

XPC-W2 contains 4-bits Crypto-graphic suite identifier (CSI). The CSI indicates the kind of cryptographic algorithm used in the secure tag. The default value of CSI is '1', and it means the proposed AES OFB-like mode is used in the RFID system.

The additional security information stored in the tag memory is depicted at Figure 6. SecParam and key index (KI) and master key are contained in this area.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
SecParam	SM	KS	Num of KI [2:0]			RFU										
KI (16^*N bits)	Key Index [(16*N-1):(16*N-16)]															
	...															
	Key Index [15:0]															
AES Key (128 bits)	AES Key [127:112]															
	...															
	AES Key [15:0]															

Figure 6. Security information in the memory of the secure tag

SecParam is composed of SM, KS, Num of KI and RFU. The functions are presented as the followings:

- SM (Security Mode): 1bit SM represents whether the corresponding tag supports the security functions. When the SM bit value is '0', it indicates that the tag operates as a passive RFID tag according to the ISO/IEC 18000-6C standard and when the SM bit value is '1', it indicates that the tag operates as a secure tag supporting the security functions.
- KS (Key Setting): 1bit KS shows whether the Master key is set in the tag. When the KS bit value is '0', it indicates that the Master key is not in the tag and when the SM bit value is '1', it indicates that the Master key is set in the tag.
- Num of KI: It means the number of Key index. Default value is '1', and it means that 1 word (16bit) of key index is assigned and the size of key pool is 2^{16}. When the value is '0', it means 8 words is assigned. In this case, the size of key pool is 2^{128} as the maximum.
- RFU (Reserved for Future Use): RFU is reserved bits for future use.

For the strong security level, the security RFID reader has a number of AES keys in the key pool. The KI indicates where the AES key is stored in the key pool.

Additionally, 128 bit AES key is stored in the tag memory. The AES key is a private key for generating an output key used for data encryption.

B. *Security enhanced protocol*

We propose the security enhanced protocol with mutual authentication and data cryptographic process. We assume that the secure reader maintains the database of master keys and key index, and the secure tag and the secure reader have the identical master key.

Figure 7 shows the proposed secure protocol.

First, the secure reader sends Select, Query, or Query Rep commands and then the secure tag transmits a RN16 when the slot counter of the tag is '0'. This selection procedure follows the ISO/IEC 18000-6C standard (step 1~4). When receiving an ACK with respect to the RN16 from the secure reader, a secure tag replies PC, XPC and untraced UII.

Because UII has the information of product where the tag is attached, the proposed secure protocol protects the information of UII from the access of illegal readers using the untraced UII, which is a fake UII composed of random

 ISBN: 978-1-61208-140-3

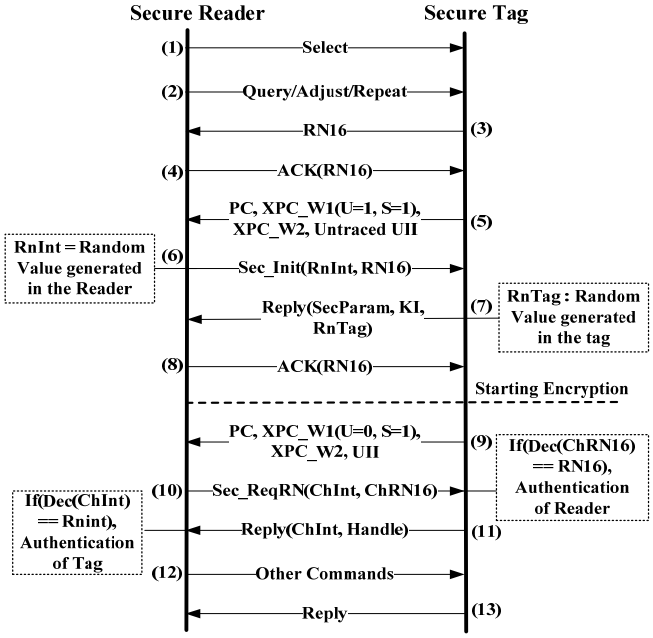

Figure 7. Proposed security protocol

values of the same length with the real UII. The real UII is encrypted and transmitted to the reader in step 9. An attacker can neither get the real UII nor trace the tag (step 5). Subsequently, the secure reader transmits Sec_Init command. It is defined to initialize the encryption engine by sending the RnInt and require the security information of tag. The secure tag creates the RnTag and starts to generate session key using the RnInt and RnTag as the first data (step6). Thereafter, tag replies SecParam, KI, and RnTag (step7). The secure reader generates the session key using the RnInt and RnTag and sends ACK with RN16 (step8).

Afterwards, the commands and replies between secure reader and tag are transmitted after encrypting with the session key. The tag sends encrypted Protocol Control (PC), XPC, UII as a reply and only secure reader which has the Master Key can decrypt the real UII (step 9). When the received PC and XPC are identified as the appropriate value, the secure reader transmits Sec_ReqRN command containing ChInt (encrypted data of RnInt) and ChRN16 (encrypted data of RN16) to the secure tag (step10).

In the proposed protocol, the identical PC, XPC, and RN16 are transmitted as both plain data (step 6, 8) and encrypted data (step 9, 10). Even thought an attacker eavesdrops on the messages, only some bits of session key are exposed by XOR operation of plane text and encrypted data. The session key is changed continuously and other data are encrypted using the other bits of session key, so no more data is exposed.

The secure tag decrypts the received ChRN16 and checks whether the value is matched. If it is successful, the authentication of the reader is completed. When the reader is considered as an authorized secure reader, the secure tag replies re-encrypted ChInt and a new 16 bit random number (Handle) (step11). As the session key value is changed continuously, the re-encrypted ChInt has the different values from the prior ChInt in step10. The secure reader decrypts the reply and checks whether the received ChInt is matched to the RnInt. When they are identical, the secure reader determines that the secure tag is authenticated. Through the process, the secure tag and the secure reader can authenticate each other. When the authentication process is failed, the RFID tag goes to the initial state. When the authentication is completed, encrypted access commands including read/write commands and replies can be transmitted between the secure reader and the secure tag (step12~13).

IV. SIMULATION AND DISCUSSION

Even if an attacker eavesdrops the whole messages between a reader and a tag, the information of the tag can't be recognized. And movements of a consumer who have the tag are untraced. The proposed secure protocol protects the UII from the access of illegal readers by using the untraced UII and encryption of real UII.

In addition, if an illegal reader attempts to fake as legal reader, it can't perform the mutual authentication process because there is no Master Key. Only authorised reader and tag can execute all access commands including read/write commands. When the authentication process is failed, the RFID tag goes to the initial state.

On the other hand, we compare the operating time of crypto engine with allowed time of the security protocol both in the tag and the reader. The results present the proposed security process satisfies the time limitation of the ISO/IEC 18000-6C standard.

As described in the Section II-A, the crypto engine generates firstly two session keys using the RnInt and RnTag, and then generates a new session key whenever one session key of two session keys is exhausted. As shown in Figure 7, the crypto engine of the tag is initiated and starts to generate first session keys when receiving the Sec_Init (step6), and should be completed before sending the encrypted PC, XPC, UII (step9). The same procedure is started when receiving the reply and should be completed before sending Sec_ReqRN in the reader.

The proposed security process is designed following the ISO/IEC 18000-6C standard. The time from reader transmission to tag response is defined as T1 and the time from tag transmission to reader response is defined as T2 in the ISO/IEC 18000-6C standard, and the transmission time of messages is determined by the link frequency.

The simulation condition for analysing the operating time is as follows:

- Link frequency from Reader to tag: 160khz
- Link frequency from tag to reader: 640khz
- Operating frequency of crypto engine: 1.25MHz.

As seen below, the operating time of crypto engine for initialization and generation of first two session keys is less

 ISBN: 978-1-61208-140-3

than the allowed time of the security protocol both in the tag and the reader. The allowed time in the tag and the reader includes the T1 and T2 specified in the ISO/IEC 18000-6C standard.

- Allowed Time in the Tag
  = T1 + T(Reply) + T2 + T(Ack)= 462.875us
- Allowed Time in the Reader
  = T2 + T(Ack) + T1 + T(PC, XPC, UII)
  = 461.3125us
- Simulated Time for Initialization and Generation of first two session keys (256bit)
  = 458us

In the proposed security process, a spare session key is always kept in the tag and reader to prevent from exhausting. In case when the message to encrypt is longer than 128bit, a new session key should be generated during the transmission of the message. As seen below, the time for generating a session key is less than the transmission time in the ISO/IEC 18000-6C standard.

- Transmission Time for 128 bit data
  = 200us
- Simulated Time for generating a session key(128bit)
  = 185us

V. CONCLUSION AND FURTHER WORKS

The proposed secure protocol conceals the UII using untraced UII to protect the information of product where the tag is attached. Also, it provides the mutual authentication process using the encrypted random values generated in the secure reader and tag and the cryptographic process using the AES crypto engine. Only secure reader and tag which share the same master key can authorize each other and decrypt the encrypted messages. In addition, the proposed secure process improves the operating speed using the AES OFB-like mode. Moreover, the proposed secure protocol and encryption process satisfy the requirements of the ISO/IEC 29167-6 and the compatibility with the ISO/IEC 18000-6C standard.

In the future, we plan to implement the RFID security system applying the proposed security protocol. And more detailed analysis will be studied against the specific security risks such as relay attack.

ACKNOWLEDGMENT

This work was supported by the IT and R&D program of MKE/KEIT [10035239, Development of ultralight low-power RFID secure platform].

REFERENCES

[1] K. Finkenzeller, “RFID Handbook : Fundamentals and Application in Contactless Smart Cards and Identification”, 2nd ED, New York :Wiley, 2003

[2] ISO/IEC 18000-6C standard, “Information Technology-Radio frequency identification for item management – Part 6 : Parameters for air interface communications at 860MHz to 960MHz”, July 2007

[3] H. M. Sun and W. C. Ting, “A Gen2-based RFID authentication protocol for security and privacy”, *IEEE transaction on Mpbile Computing*, vol8, no8, pp 1052-1062, 2009

[4] G. Tsudik, “YA-TRAP: Yet Another Trivial RFID Authentication protocol”, *IEEE Annual Conference on Pervasive Computing and Communications*, pp. 640-643, March 2006

[5] S. A. Weis, S. E. Sarma, R. L, Rivest and D. W. Engels, “Security and privacy aspects of low-cost radio frequency identification systems”, *International Conference on Security in Pervasive Computer science*, pp. 201-212, 2004

[6] M. Feldhofer, C. Rechberger, “A Case against Currently used Hash Functions in RFID Protocols”, *OTM 2006 Workshops. LNCS*, vol. 4277, pp. 372-381. Springer, Heidelberg (2006)

[7] M. Kim, J. Ryou, Y. Choi and S. Jun, “Low-cost Cryptographic Circuits for Authentication in Radio Frequency Identification Systems”, *IEEE 10th international symposium on Consumer Electronics*, pp. 1-5, 2006

[8] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, “Strong authentication for RFID systems using the AES algorithm”, *in Proceeding Workshop on Cryptographic Hardware and Embedded System*, vol. 3156, pp. 357-370, 2004

[9] J. Daemanm, V. Rijmen, “The design of Rijndael: AES- the Advanced Encryption Standard”, Springer, 2002

[10] A. Juels, “RFID security and privacy : a research survey” *IEEE Journal on Selected Areas in Communications*, pp. 381-394, Feb, 2006

 ISBN: 978-1-61208-140-3