A Fully Integrated CMOS Security-Enhanced Passive RFID Tag

Suna Choi, Hyunseok Kim, Sangyeon Lee, Kangbok Lee, and Heyungsub Lee

A fully integrated CMOS security-enhanced passive (SEP) tag that compensates the security weakness of ISO/IEC 18000-6C is presented in this paper. For this purpose, we propose a security-enhanced protocol that provides mutual authentication between tag and reader. We show that the proposed protocol meets the security demands of the ongoing international standard for RFID secure systems, ISO/IEC 29167-6. This paper fabricates the SEP tag with a 0.18-µm CMOS technology and suggests the optimal operating frequency of the CMOS SEP tag to comply with ISO/IEC 18000-6C. Furthermore, we measure the SEP tag under a wireless environment. The measured results show that communications between the SEP tag and reader are successfully executed in both conventional passive and SEP modes, which follow ISO/IEC 18000-6C and the proposed security enhanced protocol, respectively. In particular, this paper shows that the SEP tag satisfies the timing link requirement specified in ISO/IEC 18000-6C.

Keywords: RFID, security-enhanced passive tag, AES, ISO/IEC 29167-6, ISO/IEC 18000-6C.

I. Introduction

RFID is one of the most important technologies for applications in which objects have to be identified automatically. RFID can be applied in various fields, including supply chain management, product tracing, building access control, and public transportation [1]. ISO/IEC 18000-6C is the representative RFID standard for a UHF-band passive RFID system. However, it does not provide a cryptographic mechanism between the tag and reader and thus allows the possibility of eavesdropping on or leaking of private information [1]-[3]. Although the revised ISO/IEC 18000-6C standard allows a KILL command and recommission function for reusing a tag after it is killed, this is still not considered sufficient for enhancing RFID security [4].

As concerns regarding security and privacy issues have frequently been raised, a working group called ISO/IEC JTC 1 SC31 WG7 has been organized to prepare an international standard for the security services and file management of RFID systems [5]. The new standard, ISO/IEC 29167, is classified into seven parts based on the frequency bands. ISO/IEC 29167-1 defines the overall architecture for the RFID security framework and security service, whereas ISO/IEC 29167-6, which we are interested in, defines the secure air interface and file management for the 860 MHz to 960 MHz UHF-band. There has been a recent movement to combine ISO/IEC 29167-6 into a sub-standard of ISO/IEC 18000-6. Therefore, the new security standard should obey the physical layer requirement in ISO/IEC 18000-6C, such as the modulation scheme, link timing, and state-diagram. Moreover, since 2009, many members in the standard group have been discussing cryptographic security systems as being untraceable and having secure communication and authentication.

Manuscript received Oct. 22, 2012; revised June 18, 2013; accepted July 23, 2013.

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

Suna Choi (phone: +82 10 7182 4431, sunachoi@etri.re.kr) is with the Broadcasting & Telecommunications Media Research Laboratory, ETRI, Daejeon, Rep. of Korea.

Hyunseok Kim (corresponding author, hyunseok@etri.re.kr), Sangyeon Lee (lsyeoun@etri.re.kr), Kangbok Lee (kblee@etri.re.kr), Heyungsub Lee (leehs@etri.re.kr) are with the IT Convergence Technology Research Laboratory, ETRI, Daejeon, Rep. of Korea.

Among the security methods available, the Advanced Encryption Standard (AES) has been mentioned as a strong candidate [6]. The AES algorithm was chosen in 2001 as an international encryption standard. It provides strong security and is well suited for low-cost low-power RFID tag implementation. Furthermore, it is largely accepted within the industry [7], [8]. Several researchers have suggested security tag implementations using the AES algorithm [9]-[13]. Some suggest implementing only digital processors without an analog front end or memory [9]-[12]. One suggests implementing security tags including an analog front end and a digital processor without memory [13]. Based on the above-mentioned research, it is clear that the AES algorithm is one of the best choices for the RFID tag. However, installing the AES algorithm into a CMOS RFID tag demands great attention. In this paper, we focus on the operating frequency and operating time of an AES engine. If the operating frequency is lower, the consuming power of the tag decreases, while the communication distance of the tag increases; however, the tag requires a long processing time for encryption and decryption. As the receive-to-transmit turn-around time regarding a tag, called T_1, is a particularly small value, the tag is forced to adopt a high operating frequency and satisfy T_1. Nevertheless, if the operating frequency increases, the operating time of the tag decreases; however, the consuming power of the tag increases, which leads to a greater burden for a battery-less security tag. Because it is hard for a security tag to satisfy the specified link timing, no research on security tags compatible with ISO/IEC 18000-6C has yet been published.

In this paper, we propose a fully integrated CMOS SEP tag, which comprises an analog front end, a digital processor, and non-volatile memory (NVM). The CMOS SEP tag provides both conventional passive mode, following ISO/IEC 18000-6C, and SEP mode, following the proposed security-enhanced protocol using an AES security engine. The proposed protocol provides mutual authentication and a cryptographic process as recommended by ISO/IEC 29167-6 [14]. Through simulation and measurements, this paper shows that the implemented CMOS SEP tag satisfies the time limitation specified in ISO/IEC 18000-6C.

The remainder of this paper is organized as follows. The proposed cryptographic method and security-enhanced protocol are described in sections II and III, respectively. Next, the operating time for the cryptographic process is explained in section IV. Section V shows the details of the CMOS SEP tag design including the security engine. The implementation and measured results are then presented in section VI. A comparison with other achievements is discussed in section VII. Finally, some concluding remarks are given in section VIII.

II. Proposed Cryptographic Method

1. AES OFB-like Mode

The AES algorithm operates on a symmetric data block with a variable key and block length. The key and block length can be specified as 64 bits, 128 bits, 192 bits, and so on. In this paper, we apply the AES algorithm using a fixed 128 bits for the data block and key length and a modified output feedback (OFB) mode of the AES, called the OFB-like mode. Similar to the OFB mode, the AES security engine generates a session key first, and then the messages are encrypted and decrypted by means of bitwise exclusive OR (XOR) with the key streams [10]. Owing to the symmetry of the XOR operation, the encryption and decryption processes are technically similar, and an extra decryption engine is not required. The OFB-like mode reduces the operating time and enables us to satisfy the time limitation specified in the ISO/IEC 18000-6C standard, which we will prove in section VI. [0]Therefore, the OFB-like mode of the AES is appropriate to implement a lightweight secure tag.

2. Initialization and Encryption/Decryption

The security engine based on the AES OFB-like mode is initiated using initial data and a master key and then generates streams of session keys [14]. Initial data is the concatenation of *RnInt* and *RnTag*, which are random numbers transmitted from a tag to a reader and from a reader to a tag, respectively. After initialization, the security engine first generates two session keys to prevent temporary exhaustion of the session key. Whenever one of the two session keys is exhausted, a new session key is generated. The generated session key is then used as data in every generating routine of the session keys.

The encryption process is performed using bitwise XOR operations of the plain data and the generated session keys [14]. Sequentially, the header data and *CRC*16 are created and added to the encrypted data. The pointer is moved by one bit as each encryption is performed. The decryption process is similar to the encryption process. The header data and *CRC*16 are checked and removed, and only encrypted data takes an XOR operation with the session keys.

III. Proposed Security-Enhanced Protocol

A protocol in which the security level is enhanced is proposed in this section. This protocol basically has two features. One is to provide untraceability by hiding *UII*, and the other is to perform mutual authentication using the AES cryptographic engine, which was explained in the previous section. This protocol, which was already shown in [14], is

ETRI Journal, Volume 36, Number 1, February 2014
http://dx.doi.org/10.4218/etrij.14.0112.0674

explained in detail with notations in Table 1 and is evaluated regarding security analysis.

1. Proposed Security-Enhanced Protocol

With information described in Table 1, the proposed security-enhanced protocol with a mutual authentication and data cryptographic process is explained. We assume that the SEP reader maintains a database of master keys and key indices, and the SEP tag and reader have an identical master key. The proposed security-enhanced protocol is shown in Fig. 1, and the details of each step are explained as follows.

Steps 1 through 4. These steps show an initial inventory process between an SEP reader and an SEP tag. *RN*16′ returned to the tag plays the role of connecting the SEP reader to the SEP tag.

Step 5. The SEP tag, which is initialized as *U*=1, replies with *PC*, *XPC*, and untraced *UII*. The proposed security-enhanced protocol protects the information of *UII* from illegal readers. An untraced *UII* means a fake *UII* composed of random values with the same length as the real *UII*. The real *UII* will be provided to the SEP reader with encrypted type after changing to *U*=0.

Step 6. After generating *RnInt*#1, the SEP reader transmits the Sec_Init command to initialize the secure engine. Basically, *RnInt* and *RnTag* are required for initialization. To be distinguished from *RnInt* in Step 11, the index of #1 is used.

Step 7. The SEP tag saves the received *RnInt*#1 and then creates *RnTag*. With *RnInt*#1 and *RnTag*, the secure engine in the SEP tag is initialized. This initialization process should be finished before the SEP tag receives the ACK command.

Step 8. The SEP tag receives the ACK command. Thereafter, the SEP tag replies with a *SecParam*, *KI*, and *RnTag*. Because the SEP reader generates a session key with them, the SEP reader and tag will have the same session key.

Step 9. Because the SEP tag is ready to show its own *UII* to the corresponding SEP reader, *U*=1 changes to *U*=0. The tag sends an encrypted *PC*, *XPC*, and *UII* as a reply.

Step 10. Only the SEP reader that has the same session key as that in the SEP tag can extract a real *UII* after decryption. The SEP reader transmits a Sec_ReqRN command containing *ChInt* and *ChRN*16 to authenticate the reader. The SEP tag decrypts the received *ChRN*16 and checks whether the value matches the *RN*16. If they are identical, the authentication of the reader is completed.

Step 11. When a reader is considered to be an authorized SEP reader, the SEP tag replies with a re-encrypted *RnInt*#2 and a new 16-bit random number (*Handle*). As the session key value is changed, *ChInt* has different values from the prior one. The SEP reader decrypts the reply and checks whether the received *RnInt*#2′ matches *RnInt*#2. When they are identical, the SEP reader determines that the SEP tag is authenticated. Through Steps 10 and 11, the SEP tag and SEP reader can authenticate each other. When the authentication process fails, the SEP tag returns to the ready state it was in prior to Step 1.

Table 1. Notation.

Name	Description
*RN*16	16-bit random number generating in tag If it is stored in reader, dash is put into next
*XPC_W*1	Extended protocol control Part 1 *XEB*, *U*, and *S* are included in this part Refer to Fig. 4 in [14]
XEB	Extension bit in *XPC_X*1 [0] bit in *XPC_W*1
U	Untraced indicator bit in *XPC_X*1 When reader requests to show *UII*, tag shows random number if *U*=1 and real *UII* if *U*=0
S	Secure indicator bit in *XPC_X*1 Tag works as conventional general passive tag if *S*=0, but tag supports secure-enhanced protocol if *S*=1 In this case, all commands can be encrypted or not according to status of *U*
*XPC_W*2	Extended protocol control Part 2 If cryptographic engine is implemented in passive tag, this part should be located in *XPC* and has type of cryptographic engine Refer to Fig. 4 in [14]
RnInt#1	First 64-bit random number generated in reader *RnInt* as one piece of initial data for encryption engine #1 is added to be distinguished from *RnInt* in Step 10
RnInt#2	Second random number generated in reader Random number generated for reader authentication #2 is added to be distinguished from *RnInt* in Step 6
RnTag	64-bit random number generated in tag *RnTag* as one piece of initial data for encryption engine
SecParam	Parameter for supporting secure-enhanced protocol Includes whether tag supports security mode or not, whether tag owns master key or not, and how many key indices tag has Refer to Fig. 5 in [14]
KI	Key index, which means numbering of key set When one reader manages many tags, one more master key per tag can be arranged In this case, reader assigns all keys to number
K	Session key
EK( )	Encryption with session key *K*
DK( )	Decryption with session key *K*
ChInt	Encrypted value of *RnInt*#2
*ChRN*16	Encrypted value of *RN*16
ChHandle	Encrypted value of *Handle*

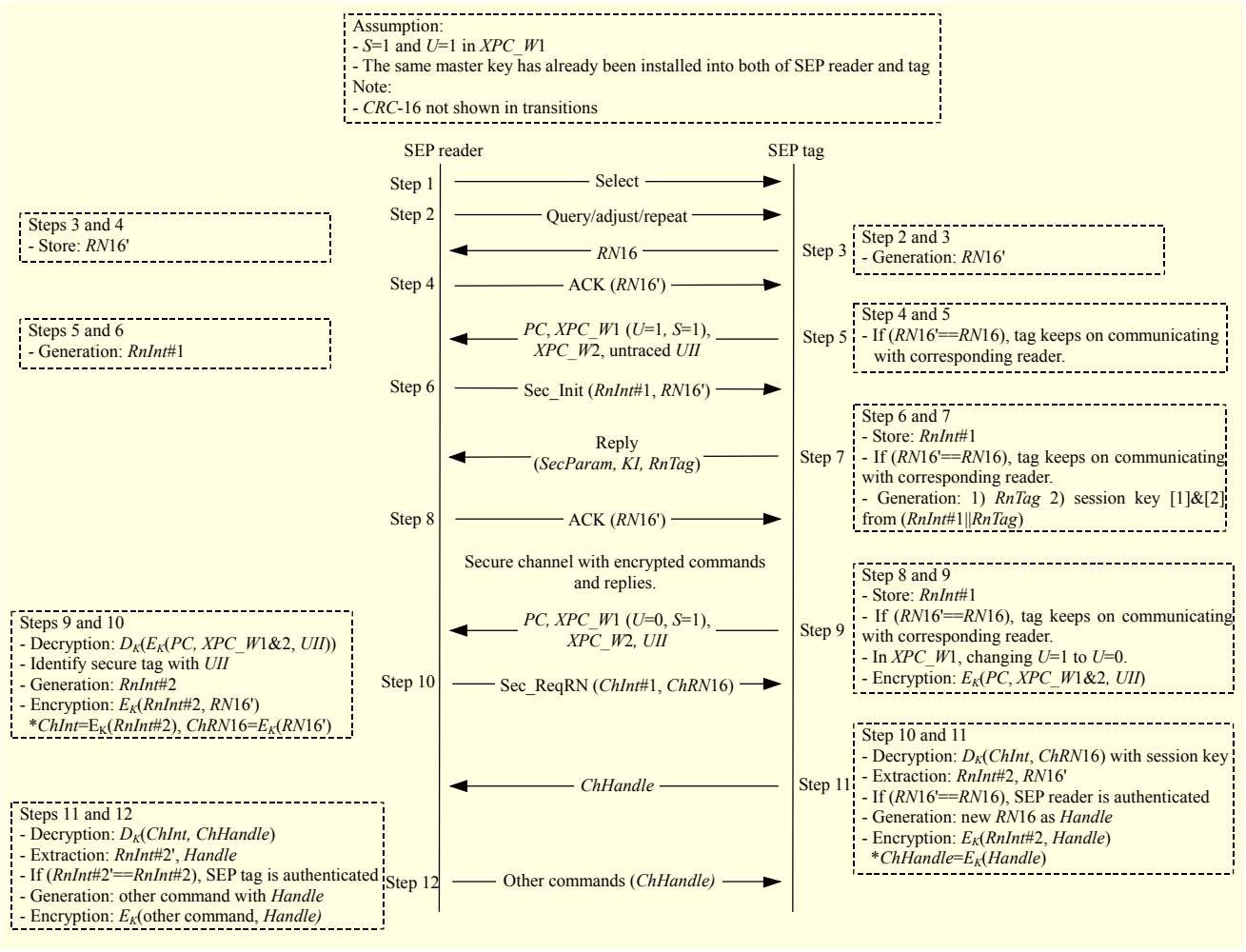


Fig. 1. Proposed security-enhanced protocol.

Steps 12 and 13. When the authentication is complete, encrypted access commands, including read/write and replies, are transmitted between the SEP reader and SEP tag.

2. Security Analysis

A. Data Confidentiality

The SEP tag is initially set up to send untraced *UII* when *U*=1. Before building a secure channel between the SEP reader and tag, no attacker can identify the SEP tag. Although an attacker eavesdrops on a message in Step 9, this message is meaningless to the attacker because this message is encrypted. The encrypted messages, which provide the security robustness of meaningful data, will not be compromised.

B. Tag Tracking and Tracing

The conventional tag is designed to have a unique number that can be tracked in the range of any reader. However, in our proposed protocol, the tag does not provide the real *UII* before the secure channel is built. Because the untraced *UII*, which is composed simply of a random number, is provided instead, an unauthenticated reader cannot get the real *UII*. Consequently, unwanted tracking by an unauthenticated reader is impossible.

C. Tag Anonymity

After Step 8, all messages between the SEP reader and tag are encrypted as cipher text. Since new session keys are used sequentially in every message transition, even the same messages have different values from one another. Thus, tag anonymity is guaranteed.

D. Man-in-the-Middle Attack Prevention

The adversative reader or tag can impersonate the valid one to intercept, change, and obtain the messages going between the parties. However, each party should have the initial master key to generate the session key, which means the adversary

cannot have an authorized session key. Because only a valid reader or tag has the session key to decrypt this cipher text, the man-in-the-middle attack can be avoided.

E. Replay Attack Prevention

In replay attack, adversaries try to eavesdrop on the transmission messages for the purpose of duplicating the valid messages and then repeating them. However, the session keys are sequentially generated and used to encrypt the messages between the SEP tag and reader. This leads to the fact that the encrypted data is changed in every transmission cycle. Thus, the attackers cannot deceive the authorized reader or tag using the former data.

F. Mutual Authentication

Our protocol provides a mutual authentication process using the encrypted random values generated in the SEP reader/tag and the cryptographic process using the AES security engine. Only the SEP reader and SEP tag, which share an identical master key, can recognize the encrypted messages and authorize each other. Therefore, the proposed protocol satisfies the security demands of ISO/IEC 29167-6.

IV. Operating Time for Cryptographic Process

This section calculates the allowed time for the cryptographic process in both the SEP tag and SEP reader. As explained in section II, the security engines of the SEP tag and SEP reader are initiated with the initial data and the master key. Two session keys are then generated before starting the encryption to prevent the exhaustion of the session key. The time allowed for the process is determined by the flow of the security-enhanced protocol, which was explained in section III, as well as by the transmission times of the messages between the SEP tag and reader.

As shown in Fig. 2, the security engine of the SEP tag initializes its processing while receiving an *RnInt* and should finish the generation of the first two session keys before completely receiving the ACK command since the messages of the SEP tag are encrypted by the XOR operation with the session key and are transmitted to the SEP reader from Step 9. The security engine of the SEP reader, meanwhile, initializes its processing when receiving the *RnTag* and should complete the generation process before receiving the *PC*, *XPC,* and untraced *UII* since the messages of the SEP reader are encrypted and transmitted to the SEP tag in Step 10.

Therefore, the calculation formulas of the time allowed for initializing and generating the first two session keys in the tag and reader are drawn as follows:

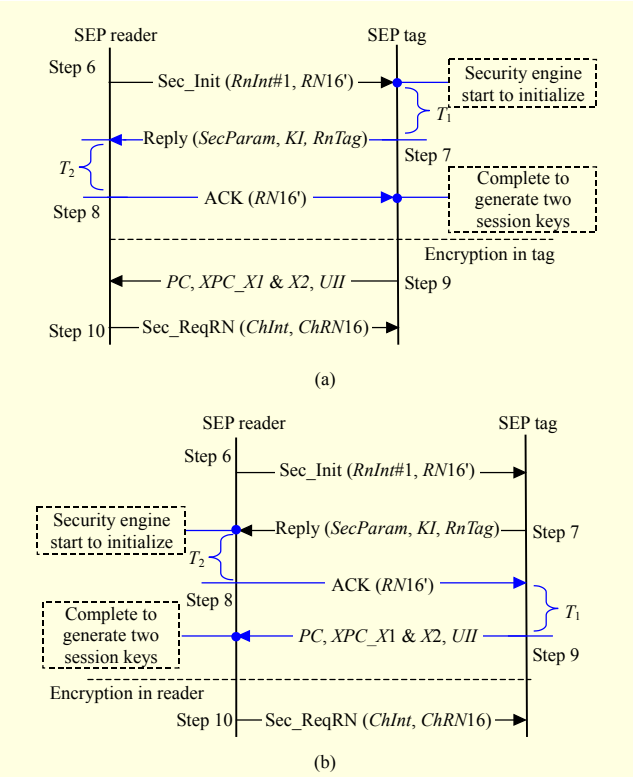


Fig. 2. Operations of security engine in SEP mode: (a) in SEP tag; (b) in SEP Reader.

$$\text{Allowed time in SEC tag} = T_1 + T(\text{tag reply to a Sec\_Init}) + T_2 + T(\text{ACK}), \quad (1)$$

$$\text{Allowed time in reader} = T_2 + T(\text{ACK}) + T_1 + T(\text{tag reply to an ACK}). \quad (2)$$

The security engine of the SEP tag should obey the link frequencies and response times to provide compatibility with ISO/IEC 18000-6C. In (1) and (2), T_1 denotes the time from reader transmission to tag response, while T_2 represents the time from tag transmission to reader response, as specified in ISO/IEC 18000-6C. Additionally, T(messages) represents the time duration for processing the messages. T(messages) is determined by the length of the messages and the link frequency. The link frequency from reader to tag and from tag to reader denoted in ISO/IEC 18000-6C is 40 kHz to 160 kHz and 40 kHz to 640 kHz, respectively.

We calculate the values of T_1, T_2, and T (messages) and then add the values together based on the variation of link frequencies between the reader and tag. Figure 3 shows the calculated results of (1) and (2). We can see that the allowed times for the SEP tag and SEP reader decrease as the link frequency increases. When the link frequency from the reader to the tag is 160 kHz and the link frequency from the tag to the reader is 640 kHz, the time allowed for the cryptographic

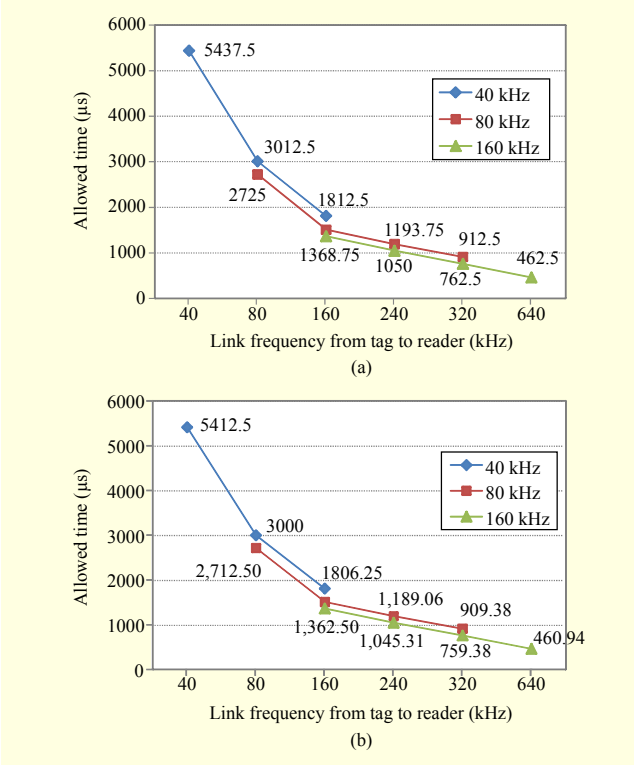


Fig. 3. Time allowed for cryptographic process: (a) in SEP tag; (b) in SEP reader.

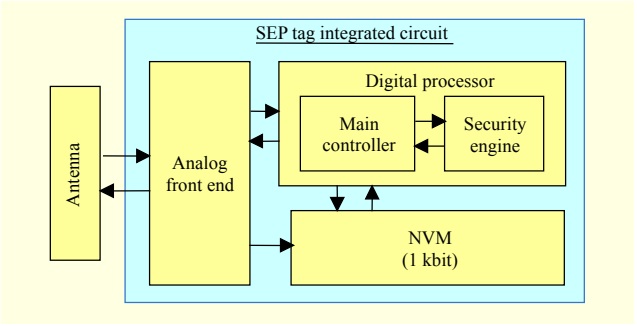


Fig. 4. Block diagram of SEP tag.

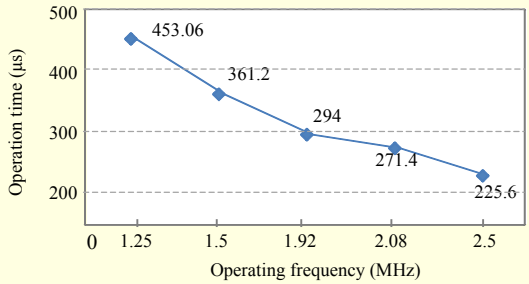


Fig. 5. Operating time for initializing and generating first two session keys.

process is 462.5 μs and 460.94 μs, respectively (that is, the smallest value for an SEP tag and for an SEP reader, respectively). For security-enhanced communication complying with ISO/IEC 18000-6C, the operating times of the implemented SEP tag and reader should be less than the smallest times allowed.

V. Design of CMOS SEP Tag

A fully integrated CMOS SEP tag supporting the proposed security-enhanced protocol is designed. The CMOS SEP tag consists of a digital processor, an analog front end, and NVM, as shown in Fig. 4.

1. Digital Processor

The digital processor handles the instructions from the reader and exchanges data with the NVM. To communicate with the reader, it consists of a reader-to-tag (RT) decoder, a command decoder, an execution processor, a reply controller, and a tag-to-reader (TR) encoder [17]. It also includes the security engine, which executes the cryptographic process.

The entire AES cryptographic process is performed through a repetition of mixing the columns, substituting bytes, and shifting the rows. The security engine is a power-hungry block, and it is therefore important to determine the operating frequency of the security engine. As the operating frequency is lower, the consuming power of the security engine is decreased. Additionally, the operating times for initializing and generating the first two session keys should be less than the smallest allowed times of 462.5 μs and 460.94 μs in the SEP tag and reader, respectively, as explained in section IV.

For this purpose, we simulate the operating times for initializing and generating the first two session keys according to the variation of the operating frequency of the security engine. Figure 5 shows the simulation results of the operating time for this process.

We compare the allowed times with the simulated operating time of the initialization and generation of the first two session keys. As the operating frequency of the security engine increases from 1.25 MHz to 2.5 MHz, the operation time decreases gradually. When the operating frequency of the security engine is 1.25 MHz, the operating time is 453.06 μs, and the value is less than the allowed time in both the SEP tag and SEP reader. Therefore, we choose 1.25 MHz as the operating frequency for the security engine.

2. Analog Front End and NVM

The analog front end for CMOS SEP tag consists of a voltage multiplier, a voltage regulator, a clock generator, a

modulator/demodulator, and a power-on-reset [15]. An eight-stage rectifier generates the power supply for the CMOS SEP tag using low-threshold N-type MOS devices. Regulators stabilize the output of the supply voltage generator and support constant DC voltage to the other circuits [16].

The clock generator provides the main clock for driving a digital processor. As the operating frequency is higher, the operating time decreases; however, the consuming power of the tag increases. Therefore, an appropriate frequency should be selected. Moreover, there are additional conditions for conforming to ISO/IEC 18000-6C.

First, the main frequency of the SEP tag should be a multiple of the highest link frequency from tag to reader (that is, 640 kHz) for the data processing. Although the optimal value has been debated in several papers, it has been deduced that 1.92 MHz or greater is needed to fully support ISO/IEC 18000-6C [17]. Second, the main frequency of the SEP tag should be a multiple of the operating frequency of the security engine. For an efficient consuming power, the main frequency clock is divided by 2^x and is provided separately to the other blocks. We choose 1.25 MHz as the minimum operating frequency of the security engine, the reason for which was explained in subsection V.1. To satisfy the above two additional conditions, we select a 2.56-MHz main clock frequency.

We design 1-kbit NVM to support the security process and preserve a large amount of user memory for additional future functions. The NVM for the SEP tag consists of an asynchronous memory controller and a C-flash memory cell array [18], [19].

VI. Implementation

We fabricate a CMOS SEP tag using a 0.18-μm logic CMOS process from Tower Semiconductor, Inc. A photograph of the tag is shown in Fig. 6. The tag contains an analog front end, a baseband processor with a security engine, and NVM. Two pads are conventionally sufficient to connect an antenna to a CMOS tag. Additional pads are used for the experimental test. The CMOS SEP tag occupies an area of 1.78 mm^2 (1.33 mm × 1.337 mm) without the test pads. The measured results of the consuming current of the CMOS SEP tag are listed in Table 2. The digital processor, including the security engine, as a power-hungry block, occupies 70% to 85% of the total power consumption.

For wireless communication of the fabricated CMOS SEP tag, an antenna is assembled as shown in Fig. 7. The SEP reader as a counterpart of the SEP tag is made using the proposed cryptographic method and security-enhanced protocol, as explained in sections II and III.

Figure 8 shows the measured communication waveforms

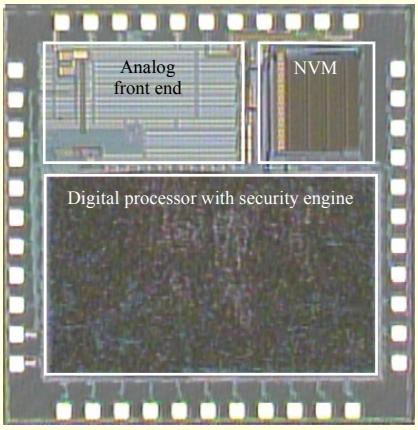


Fig. 6. Photograph of CMOS SEP tag.

Table 2. Consuming current of CMOS SEP tag.

Feature	Consuming current
Analog front end	12 μA
Digital processor with security engine	125 μA
NVM	10 μA (read) - 33 μA (write)
Total	147 μA - 170 μA

Fig. 7. Antenna assembled SEP tag.

between the SEP tag and reader when a transmission power of 30 dBm and an antenna gain of 6 dBi are applied to the reader. In conventional passive mode, communications between the SEP tag and reader follow ISO/IEC 18000-6C. For measurement in SEP mode, we implement and use an SEP reader, which follows the proposed security-enhanced protocol explained in section III. Successful communication between the assembled SEP tag and SEP reader is executed within a frequency range of 860 MHz through 960 MHz, and the SEP tag achieves a communication distance of 1 m in a wireless environment. Each of the commands and replies of the SEP tag and reader is labeled.

To verify the time requirement, the operating time of the cryptographic process is measured using two test signals: AES_Init and AES_Done. The operating time is expressed as follows:

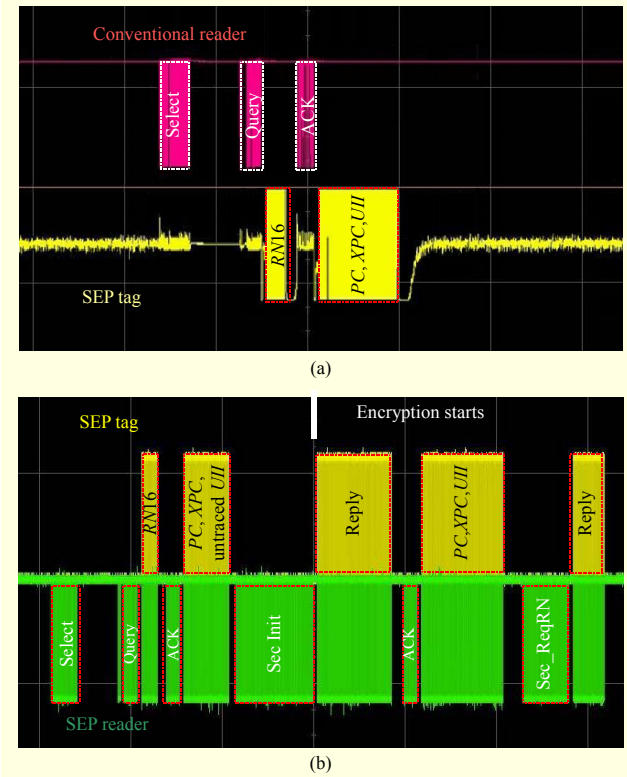


Fig. 8. Measured communication waveforms: (a) conventional passive mode; (b) SEP mode.

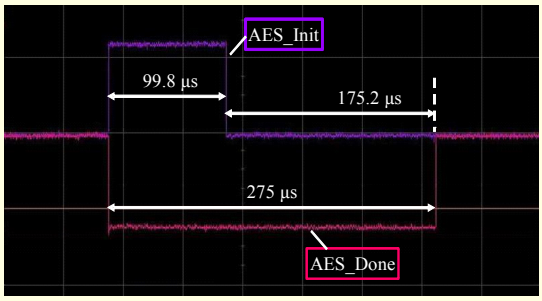


Fig. 9. Measured operating signals of security engine.

Operating time of cryptographic process
= time for initialization
+ time for generating two session keys, (3)

Time for initialization = duration of AES_Init, (4)

Time for generating two session keys
= 2 *(rising of AES_Done – falling of AES_Init). (5)

Figure 9 shows the measured results of the AES_Init and AES_Done signals when the operating frequency of the security engine is 1.25 MHz. The AES_Init signal is high when the security engine starts to initialize, and then it decreases significantly when the initialization process (setting of initial data and AES key) is completed. The AES_Done signal is high when the generation of the session key is completed.

Table 3. Measured results of security engine.

Operation	Time (µs)
Initialization	99.8
Generating one session key	175.2
Generating two session keys	350.4
Cryptographic process	450.2

Table 4. Comparison of time allowed in SEP tag and reader and operating time of cryptographic process.

Allowed time in SEP tag	Allowed time in reader	Operation time of cryptographic process
462.5 µs	460.9 µs	450.2 µs (less than the allowed times)

The measured results for the different operating times are listed in Table 3, while Table 4 summarizes a comparison of the allowed times in the SEP tag and SEP reader, as well as the measured operating time of the cryptographic process. As shown in Table 4, the measured result is less than the allowed time in the SEP tag and SEP reader. This shows that the fabricated CMOS SEP tag satisfies the time limitation of ISO/IEC 18000-6C.

VII. Discussion

To evaluate its performance, our implementation is analyzed against existing achievements. This paper is focused on compliance with T_1 under ISO/IEC 18000-6C, and the operating time of the proposed AES engine is thus a key issue. However, it is difficult to make a direct comparison among the operating times of AES engines since existing AES engines operate using diverse clock frequencies. Thus, the clock cycles for AES engines and the regulated clock frequency of each AES engine to be finished by T_1 (460.94 µs) are compared. Next, the current consumption values of the AES engines based on the regulated clock frequencies are estimated. For this estimation, we assume that the current consumption is proportional to the operating frequency. Furthermore, the chip sizes of the AES engines, which are directly connected to the price, are compared.

Table 5 summarizes and compares the performance of the proposed AES engines with that of existing works. As shown

ETRI Journal, Volume 36, Number 1, February 2014
http://dx.doi.org/10.4218/etrij.14.0112.0674

Table 5. Comparison of performance of AES engine in an SEP tag.

	[9]	[10]	[12]	This work
Process	Philips 0.35 μm CMOS	0.25 μm CMOS	TSMC 0.18 μm CMOS	Tower 0.18 μm CMOS
AES area	0.5 mm × 0.5 mm	N/A	0.37 mm × 0.45 mm	0.4 mm × 0.4 mm
Secure engine	AES-128	AES-128	AES-128	AES-128
Standard	N/A	N/A	ISO/IEC 18000-6C	ISO/IEC 18000-6C
Clock cycles for AES engine	1,032	870	N/A	563
Clock frequency for AES engine	100 kHz	10 MHz	N/A	1.25 MHz
Current consumption of AES engine	3.0 μA (at 100 kHz)	N/A	N/A	6.0 μA (at 1.25 MHz)
Current consumption to finish AES engine within 460.92 μs	67.2 μA (at 2.2389 MHz)	N/A	N/A	6 μA (at 1.25 MHz)
Simulation or measurement	Simulation	Simulation	Simulation	Measurement

in this table, our work has the smallest chip area and shortest clock cycles for an AES engine. Unfortunately, the clock cycles for an AES engine in [12] and the current consumption values of an AES engine in [10] are not mentioned. Therefore, the operating frequencies used in [9] and [10] are regulated, and only the consumption current from [9] is estimated and compared with our work. Faster clocks are required to finish the AES engines in [9] and [10] within 460.94 μs, and the current consumption of [9] is estimated to be 67.2 μA, which is much higher than the 6 μA achieved in our work.

It should be noted that our proposed AES engine achieves the best possible performance compatible to ISO/IEC 18000-6C, based not only on a simulation but also on our measurement results.

VIII. Conclusion

A fully integrated CMOS SEP tag operating in the UHF band was designed and implemented. To overcome the security weakness of ISO/IEC 18000-6C, a security-enhanced protocol was proposed and implemented into a CMOS SEP tag in a 0.18-μm CMOS process. The proposed protocol provides mutual authentication and encrypted data transmission, which satisfies the demands of ISO/IEC 29167-6. Furthermore, we suggested an optimal operating frequency for the CMOS SEP tag that efficiently complies with ISO/IEC 18000-6C. The measured results show that the CMOS SEP tag operates well in both conventional passive mode and SEP mode. Also, the measured operating time for the cryptographic process satisfies the time allowance limitation. Therefore, our CMOS SEP tag satisfies both the timing link specifications of ISO/IEC 18000-6C and the security demands of ISO/IEC 29167-6.

References

[1] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed., New York: John Wiley & Sons, Inc., 2003.

[2] A. Juels, "RFID Security and Privacy: A Research Survey," *IEEE J. Sel. Areas Comm.*, vol. 24, no. 2, Feb. 2006, pp. 381-394.

[3] J. Bae et al., "Design of Reader Baseband Receiver Structure for Demodulating Backscattered Tag Signal in a Passive RFID Environment," *ETRI J.*, vol. 34, no. 2, Apr. 2012, pp.147-158.

[4] ISO/IEC 18000-6, *Radio Frequency Identification for Item Management — Part 6: Parameters for Air Interface Communications at 860 MHz to 960 MHz*, 2010.

[5] Y.S. Kang et al., "Comments on an Improved RFID Security Protocol for ISO/IEC WD 29167-6," *ETRI J.*, vol. 35, no. 1, Feb. 2013, pp. 170-172.

[6] NIST, *Specification for the Advanced Encryption Standard (AES) Technical Report*, FIPS Pubs 197, 2001.

[7] M. Feldhofer and C. Rechberger, "A Case against Currently used Hash Functions in RFID Protocols," *OTM Workshops*, *LNCS*, vol. 4277, 2006, pp. 372-381.

[8] M. Feldhofer and J. Wolkerstorfer, "Strong Crypto for RFID Tags: A Comparison of Low Power Hardware Implementations," *Proc. IEEE ISCAS*, May 2007, pp. 1839-1842.

[9] M. Feldhofer et al., "AES Implementation on a Grain of Sand," *IEE Proc. Info. Security*, vol. 152, 2005, pp. 13-20.

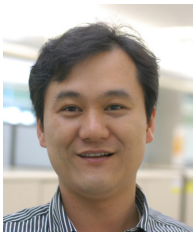
[10] M. Kim et al., "Low-Cost Cryptographic Circuits for Authentication in Radio Frequency Identification Systems," *IEEE 10th Int. Symp. Consum. Electron.*, 2006, pp. 1-5.

[11] Y. Qi et al., "Design and Implementation of a Security-Enhanced Baseband System for UHF RFID Tag," *IEEE 8th Int. Conf. ASIC*, Changsha, Hunan, Oct. 20-23, 2009, pp. 999-1002.

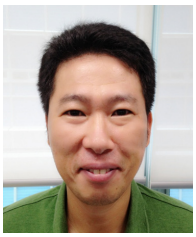
[12] A.S.W. Man et al., "Low Power VLSI Design for a RFID Passive Tag Baseband System Enhanced with an AES Crytography

Engine," *RFID Eurasia*, 2007, pp. 1-6.
[13] X. Feng et al., "An UHF RFID Transponder with Novel Demodulator and Security Algorithm," *3rd Int. Conf. Anti-counterfeiting, Security, Identification Commun.*, Hong Kong, China, Aug. 20-22, 2009, pp. 254-257.
[14] S. Choi et al., "Security Enhanced Authentication Protocol for UHF Passive RFID System," *7th Int. Conf. Wireless Mobile Comm.*, Luxembourg City, Luxembourg, June 19, 2011, pp. 307-311.
[15] U. Karthaus and M. Fischer, "Fully Integrated Passive UHF RFID Transponder IC with 16.7-μm Minimum RF Input Power," *IEEE J. Solid-State Circuits*, vol. 38, no. 10, Oct. 2003, pp. 1602-1608.
[16] P.R. Gray et al., *Analysis and Design of Analog Integrated Circuits*, 4th ed., New York: John Wiley & Sons, Inc., 2001.
[17] Q. Luo et al., "A Low-Power Dual-Clock Strategy for Digital Circuits of EPC Gen2 RFID Tag," *IEEE Int. Conf. RFID*, Orlando, FL, USA, Apr. 27-28, 2008, pp. 7-14.
[18] Y. Roizin et al., "C-Flash: An Ultra-Low Power Single Poly Logic NVM," *Int. Conf. Memory Tech. Design*, Opio, France, May 18-22, 2008, pp. 90-92.
[19] L. Jin et al.,"Design of 512-Bit Logic Process-Based Single Poly EEPROM IP," *J. Central South Univ. Technol.*, vol. 18, no. 6, Dec. 2011, pp. 2036-2044.

Suna Choi received her BS and MS in electronics engineering from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Rep. of Korea, in 2001 and 2004, respectively. In 2004, she joined the Magnachip Co., Rep. of Korea. Since 2006, she has been with ETRI, Daejeon, Rep. of Korea. Her research interests include RFID systems, communication systems, and system on chip.

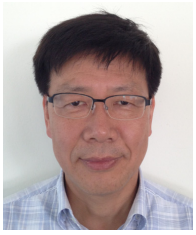


Hyunseok Kim received his BS degree (*summa cum laude*) in control and instrumentation engineering and his MS degree in biomedical engineering from Chonbuk National University, Jeonju, Rep. of Korea, in 1995 and 1997, respectively. He received his PhD degree in electrical engineering from Arizona State University (ASU), Tempe, AZ, USA, in 2006. From 2002 to 2006, he worked as a research assistant in the electrical engineering department at ASU. Since 2006, he has been with ETRI, Rep. of Korea. He has been engaged in the research and development of CMOS RFID tag chips. His research interests are the design of UHF CMOS RFID tag chips, CMOS temperature sensors, and RF/analog and mixed-signal CMOS circuits. Since 2012, he has been serving as an *ETRI Journal* editor.



Sangyeoun Lee received his BS and MS degrees in electronics engineering from Kangwon National University, Rep. of Korea, in 1996 and 1998, respectively. He joined ETRI in October 2000 and has been engaged in the research and development of high-speed router systems, EPON/GPON OLT systems, RFID sensor tag and reader systems, and RFID security tag and reader systems. Now, he is a principal member of the engineering staff in the IoT Convergence Research Department. His current research interests are the technology development and implementation of RFID systems.

Kangbok Lee received his BS in electronics engineering from Kyungpook National University, Daegu, Rep. of Korea, and his MS in information and communication engineering from Chungbuk National University, Cheongju, Rep. of Korea, in 1993 and 2000, respectively. From 1993 to 2000, he was with the LG Semiconductor Co., Cheongju, Rep. of Korea, where he worked on MCU design. In 2000, he joined ETRI, Daejeon, Rep. of Korea, where he has worked on the Development of SoC design, such as network processors, communication controllers, and RFID. His research interests include communication circuits, communication systems, RFID/NFC devices, and system on chip (SoC).



Heyungsub Lee received his BS, MS, and PhD degrees in electronics engineering from Chungnam National University, Rep. of Korea, in 1985, 1994, and 2002, respectively. He joined Samsung Electronics in 1985 and was engaged in the research and development of SRAM until August 1990. He joined ETRI in September 1990 and has been engaged in the research and development of SDH-based transmission systems, high-speed router systems, optical premise network systems, RFID systems, and so on. Now, he is a principal member of the engineering staff in the IoT Convergence Research Department. His current research interests are the technology development and service implementation of IoT.

ETRI Journal, Volume 36, Number 1, February 2014
http://dx.doi.org/10.4218/etrij.14.0112.0674