HB-MP^{++} Protocol: An Ultra Light-weight Authentication Protocol for RFID System

Bongno Yoon,[1,2] Man Young Sung,[1,a] *Member, IEEE*
[1]Department of Electrical Engineering, Korea University,
Anam-Dong, Sungbuk-Gu, Seoul 136-701 Korea
[2]Telecommunication R&D center, Samsung Electronics,
Maetan-Dong, Suwon-Si, Gyeonggi-Do, 443-742, Korea
[a]semicad@korea.ac.kr
byoon17@{korea.ac.kr, samsung.com}

Sujin Yeon,[2] Hyun S. Oh,[2]
Yoonjoo Kwon,[2] Chuljin Kim,[2] and
Kyung-Ho Kim,[2] *Senior Member, IEEE*
[2]Telecommunication R&D center, Samsung Electronics,
Maetan-Dong, Suwon-Si, Gyeonggi-Do, 443-742, Korea
{sujin.yeon, hs910.oh, namgae, cjkim65, kyungkim}
@samsung.com

***Abstract* – Since Hopper and Blum suggested the HB protocol which is based on the conjectured hardness of the LPN (Learning Parity in the Presence of Noise) problem in 2001, a family of light-weight authentication protocols has been developed for RFID (Radio Frequency Identification) system by many engineers. It was found that each algorithm had own weakness against new attacks so that more advanced protocols have been expanded in order to overcome the attacks. In this paper, we enhance the HB-MP and HB-MP^{+} protocol, called HB-MP^{++}. Ultra low-weight and concrete function will be used to eliminate vulnerability of the conventional methods. We also provide the security and performance analysis of the proposed protocol.**

Keywords-components; RFID, Authentication, HB protocol

I. INTRODUCTION

A Radio-Frequency IDentification (RFID) is one of the fastest growing and most beneficial technologies being adopted by various businesses today. Implementation of this technology which is automated identification of objects and people has recently been fueled by the establishment of key standards, retailer and government mandates [1, 2]. A typical RFID system generally consists of readers, also known as interrogators, and tags, also named as transponders. A reader transmits information to a tag by modulating an RF signal in the 860MHz~960MHz frequency range. The tag receives both information and operating energy from this RF signal. Tags are passive, meaning that they receive all of their operating energy from the reader's RF waveform. The reader transmits a continuous wave to tags for acquiring their ID or information [3]. Fig. 1 presents the basic RFID system. The fact that tags and reader communicate using a wireless radio frequency link could explain the inevitability of which there are security issues in RFID system. Simply eavesdropping the messages that transmitted on the wireless channel, dishonest person can illegally collect private information, such as personal credit or medical records [4]. Another important privacy concern is the tracking of individuals by RFID tags. A reader at a fixed location could track RFID-labeled clothes or banknotes carried by people passing by. Correlating data from multiple tags, attacker could find the tag's movement, social interactions and financial transactions [5]. The issue of authentication is also a critical topic in using RFID. The data authenticity means that any transmitted data between RFID system's participants should be authenticable. That is, messages communicated between reader and tags should be checked if they come from honest entity or not [6]. If we would not have strong methods to demonstrate data authentication, malicious person would attempt to counterfeit themselves to the honest entities by embezzling the previously obtained messages. It is needless to say the foundation of RFID system's security would collapse if we were not to succeed in authenticating the messages. The RFID topology mentioned before is mainly determined by the low-cost of the tags, and consequently by their limited functionality, directly affecting the security of the system. Since we already know the cost of RFID tags are supposed to be a biggest impediments to widespread application, the resource of RFID tags are absolutely required to be limited. Even though the security algorithm and protocol are limited to a low cost and low weight implementation, cryptographic services needed by RFID system should be basically same as other system, such as authentication, confidentiality, un-traceability and availability [7, 8]. Focusing on authentication

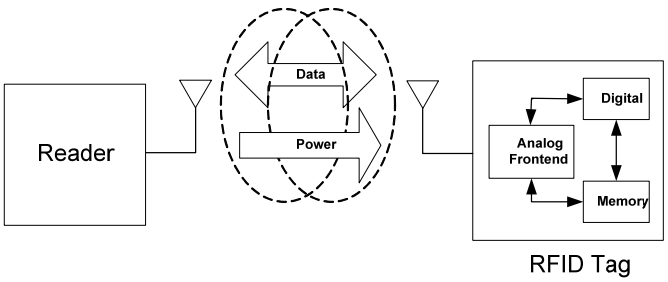

Fig. 1. Basic RFID reader and tag system

features, many engineers have mentioned efficient algorithms and protocols. Modern authentication protocols are generally likely to be categorized by two kinds of technologies. One is hash function based security protocol. Weis et al. gave a concept about hash lock protocol and randomized hash lock protocol in 2003 [9, 10]. In their work, when the reader attempts to identify the tag, a reader querying the RFID tag will receive a metaID, i.e. *metaID* ← *hash(key)*. The reader forwards this *metaID* to the backend server in order to seek the unlocking key ID with the received hashed value because the tag could unlock itself only when the reader sends the unlocking key. Based on the difficulty of inverting a one-way hash function, this scheme prevents unauthorized readers from reading tag contents. However, this creates the matter of privacy because an adversary can track the movements of a tag by repeatedly querying and comparing *metaID* values. To protect the tracking of individuals, the authors proposed the randomized hash lock scheme. That is, the tags respond to reader queries with the pair (r, $h(ID||r)$), where r is chosen uniformly at random. Since every new reader query results in a different reply due to the randomized generation of r, the adversary is unable to track the tag. Afterwards, some modified protocols which are based on hash function are suggested, so called "hash based ID variation protocol" and "hash chain protocol". But, the hash based protocol not only has a flaw in data security but also gives great burden to the database for single tag authentication, so recent research tendency for RFID authentication is a exclusive OR (XOR) based security protocol. With the light-weight binary operation, Hopper and Blum firstly developed an innovative security scheme, named HB [11]. Now that the HB protocol requires only the implementation of dot products and XOR logic, it seems to be suitable for RFID taking into account light-weight aspects. In 2005, Juels and Weis proved that HB is only effective in passive attacks and specified a modified protocol to resist the active attack, HB$^+$ [12]. Later, Katz et al. and Gilbert et al. found new attack algorithm to break the security of the HB$^+$ [13, 14]. In early 2007, Munilla and Peinado offer a new authentication protocol, named HB-MP, derived from HB$^+$, providing more efficient performance and resistance against various active attacks applied to HB and HB$^+$ [8]. Owing to security imperfection of the HB-MP protocol, Leng and Mayes strengthen the HB-MP algorithm by randomizing the rotation of the secret key, which eliminates the vulnerabilities [15]. However, the HB-MP$^+$ does not have real function for rotating secret key to defend against sophisticated active attack nor strong methods for preventing tracking problem due to the same bit size of tag's response. In this paper, we made a progress in a noble RFID authentication protocol which is based on HB for secure and ultra light-weight function. Using k-stage Linear Feedback Shifter Register (LFSR), we could obtain more concrete function to intensify the security and performance for RFID system. This paper is organized as follows: In section 2, we summarize the previous works and their security problems. We describe our new protocol in detail in section 3. There will be security and performance analysis of our protocol in section 4. Finally, conclusions are addressed in the last section.

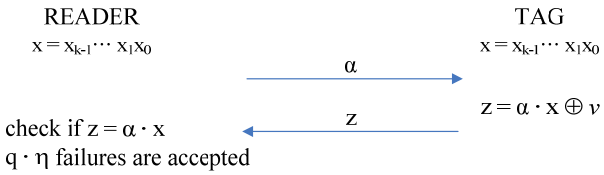

Fig. 2. A single round of HB protocol

II. RELATED WORK

A. HB protocol with LPN problem

We begin by reviewing Hopper and Blum's secure human authentication protocol, which we refer to the HB protocol [11]. The HB protocol is based on the hardness of complexity of the computational Learning Parity with Noise (LPN) problem. Simply speaking, the LPN problem requires an attacker to recover a k-bit secret key x after being given several equations of the form $\beta_i = \alpha_i \cdot x \oplus v_i$, with unknowns x and the v_i's. Here v_i is a noise bit equal to 1 with a probability $\eta \in [0,1/2]$. Throughout we denote the Hamming Weight of a vector x by $|x|$.

Definition. Let $\boldsymbol{A}$ be a random $q \times k$ binary matrix, let $\mathbf{x}$ be a random k-bit vector, let $\eta \in [0,1/2]$ be a constant noise parameter, and let v be a random q-bit vector such that $|v| < \eta q$. Given $\boldsymbol{A}$, η, and $z = (\boldsymbol{A} \cdot \mathbf{x}) \oplus v$, find a k-bit vector $\mathbf{x'}$ such that $|(\boldsymbol{A} \cdot \mathbf{x'}) \oplus z| < \eta q$.

We first introduce some notations to explain the HB algorithm in detail.

Table 1. Notations for HB protocol

k	length of the secret key shared by reader and tag
x	k-bit secret key shared by reader and tag
α	random k-bit binary vector
v	noise bit; $v = 1$ with probability $\eta \in [0,1/2]$
•	denotes scalar product
⊕	denotes XOR operation

This protocol is composed of q rounds, one of depicted in Fig. 2, and described as follows:

Step1. The reader generates at random a challenge α and sends it to the tag

Step2. The tag computes z as follows

$z = \alpha \cdot x \oplus v$

and sends the response to the reader

Step3. The reader checks $z = \alpha \cdot x$

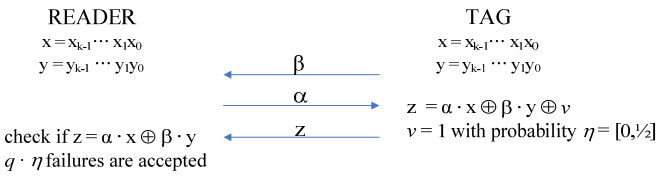

Fig. 3. A Single round of HB$^+$ protocol

The round described in Fig. 2 is repeated q times. The tag is authenticated if the checking procedure fails at most $q\eta$ times. In 2005, Juels and Weis proved HB is only resistant to passive attacks [12], meaning it is not secure against active attacks. Since v is strictly less than 1/2, $\alpha \cdot x$ will be revealed by challenging the tag with some chosen α several times. Gaussian elimination will therefore give x once k equations with linearly independent α's have been retrieved.

B. HB$^+$ protocol against active attacks

As commented above, Juels and Weis not only found the deficiencies of HB but also modified the HB to be secure against active attacks. Comparing to HB protocol, reader and tag share an additional k-bit secret β. To keep a hostile reader from extracting the secrets of tag, tag first selects a random k-bit blinding factor and sends it to reader. This blinding factor can effectively eliminate the threat of losing tag's secret to corrupt reader. Like HB protocol, the reader authenticates a tag after q rounds if the tag's response is incorrect in less than $q\eta$ times. All notations are almost same with the case of HB except adding the y and β.

Table 2. Notations for HB$^+$ protocol

x, y	k-bit secret key shared by reader and tag
α, β	random k-bit binary vector

This protocol also consists of q rounds, one of which is illustrated in Fig. 3, and described as follows:

Step1. The tag chooses at random a k-bit binary vector β and sends it the reader
Step2. The reader generates at random a challenge α. The challenge is sent to the tag
Step3. The tag computes α as follows
$z = \alpha \cdot x \oplus \beta \cdot y \oplus v$
and sends it to the reader
Step4. The reader checks
$z = \alpha \cdot x \oplus \beta \cdot y$

Although HB$^+$ is resistant against the active attacks applied to HB, Gilbert et al. showed a very efficient man-in-the middle attack that could allow an attacker to discover the secret x and y [15, 16]. In this case, the adversary retransmits the random vector β without any modification, but modifies the vector α such that $\alpha' = \alpha \oplus \delta$ is sent to the tag, where δ is a fixed value.

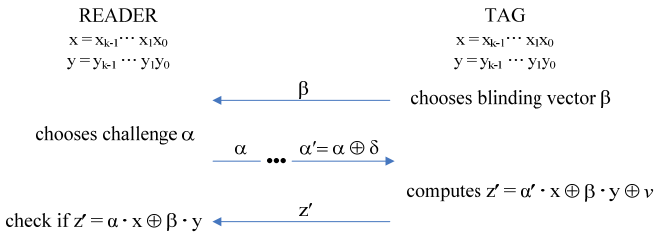

Fig. 4. General concept of man-in-the-middle attack

If the tag is finally accepted by the reader, the attacker concludes that $\delta \cdot x = 0$. Otherwise, he concludes that $\delta \cdot x = 1$. This allows him to obtain the secret key x. For instance if $\delta = 00\ldots01$ and the tag is accepted, with high probability $\delta \cdot x = 0$ and it would mean the Least Significant Bit (LSB) of x equals 0; changing δ, the adversary can recover x bit after bit. A similar process can be applied on β to obtain the secret key y. Fig. 4 shows simple concept of the man-in-the middle attack. Another obvious problem in HB$^+$ is the transmission cost of the q rounds communication. In each round, a pack of three k-bit messages have to be transmitted. This requires the exchange of $2k + 1$ bits per round and $2qk + q$ bits in total, which is unacceptably high for RFID system [17].

C. HB-MP protocol against man-in-the-middle attack

A new authentication protocol has been designed by Munilla and Peinado in 2007 [8]. The evolved scheme that is named as HB-MP has some modification of the HB$^+$ protocol in order to resist active attacks as well as the man-in-the-middle attack applied to HB and HB$^+$. Newly hired notations in HB-MP are shown in table 3. One of the rounds is depicted in Fig. 5 and described as follows.

Step1. The reader chooses at random a m-bit binary vector α and sends it to the tag
Step2. The tag computes $x = Rot(x, y_i)$, where y_i is the ith bit of the key y
Step3. The tag computes z as follows
$z = \alpha \cdot xm \oplus v$
and looks for a k-bit binary vector β such that $\beta \cdot xm = z$
Step4. The tag sends β to the reader
Step5. The reader computes the x in the ith round as $x = Rot(x, y_i)$, where y_i is the ith bit of the key y
Step6. The reader checks if
$\alpha \cdot xm = \beta \cdot xm$

Table 3. Notations for HB-MP protocol

α, β	random m-bit binary vector
m	length of the message exchanged between the parties
xm	m-bit binary vector considering of the m LSB of x
Rot(p,u)	bitwise left rotate operator. The operand p is rotated u position

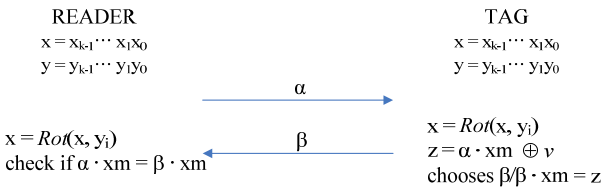

Fig. 5. A single round of HB-MP protocol

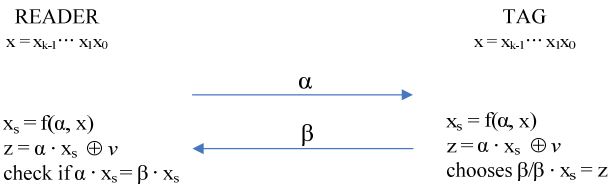

Fig. 6. A single round of HB-MP$^+$ protocol

The kernel parts of HB-MP are that the response of tag is provided by not z but β and the response depends on the dot product of α and xm which is modified at every round. Though HB-MP is supposed to be resistant against the man-in-the middle attack thanks to the randomness of response, the rotation of xm has its own weak points. Since $x = Rot(x, y_i)$, so xm in the first round of all authentication sessions should be the same. The reason why the value of xm should be same is the synchronization issue. New entities may not be able to verify each other unless the values of x in the tag and reader are same. This synchronization issue may arise due to predictable rotation of xm. So, if the attacker pretends to be a valid reader, he can initiate repetitive authentication sessions, initially restricted to the first round. The technique used in last session can be exploited to reveal the tag's first round xm. If the attacker observes the *i*th round, he is able to reveal xm used in the *i*th round.

D. HB-MP$^+$ protocol

To overcome the fragility resulting from the predictable repetition of xm, Leng et al. use some additional random bits generated by the reader to randomize the rotation [15]. The essence of HB-MP$^+$ is to use a random secret in each round, namely a round key. The notations are the same with HB-MP except a one way function f(.) and the round key.

Table 4. Notations for HB-MP$^+$ Protocol

x_s	random secret key in each round, $x_s = f(\alpha, x)$
f(.)	one-way non-linear function

The HB-MP$^+$ protocol they made is shown in Fig. 6 and explained like follows.

Step1. The reader chooses at random a *m*-bit binary vector α and sends it the tag

Step2. The reader and tag computes the round key $x_s = f(\alpha, x)$. f(.) is the one-way function

Step3. The tag computes z as follows
$z = \alpha \cdot x_s \oplus v$
and looks for a *m*-bit binary vector β such that
$\beta \cdot x_s = z$

Step4. The tag sends β to the reader

Step5. The reader computes the $x_s = f(\alpha, x)$, using the secret x and random number α

Step6. The reader checks if $\alpha \cdot x_s = \beta \cdot x_s$

The round key x_s is generated by a random number α and shared secret x. There is no need for another secret y and because the x is not changed. We don't have to concern about synchronization problems between tag and reader. However, the non-linear one-way function used in HB-MP$^+$ is abstract, so we are not able to prove the function is appropriate for RFID system in the aspect of light-weight. Moreover, as the tag's response has the same number of bits, HB-MP$^+$ still has a vulnerability of traceability.

III. PROPOSED PROTOCOL

A. Linear Shift Feedback Register

We will use the LSFR that consists of consecutive two-stage memory or storage stage and feedback logic [18, 19]. Pseudorandom Noise (PN) sequences are generated by combining the outputs of feedback shift registers. PN sequences are shifted through the shift register in response to clock pulses. The initial contents of the stages and feedback logic determine the successive contents of the stages. A feedback shift register and its output are called linear when the feedback logic consists of entirely of modulo-2 adders. Fig. 7 shows n-stage LSFR. The main reason why we use the LSFR in our proposed protocol is that the output of LSFR (PN sequences) has a useful property, which is called "run property". With the "run property", we are able to provide a more efficient resistance against the man-in-the-middle attacks by adding more randomness. A "run" is defined as a sequence of a single type of binary digits. The length of the "run" is the number of same digits in the PN sequences. For example, if we have 16-bit PN sequence, 0001001101011110, the followings are easily calculated as "run length" by counter.

r_1:3, r_2:1, r_3:2, r_4:2, r_5:1, r_6:1, r_7:1, r_8:4, r_9:1,r_{10}:3, …

After counting the "run length" as above, we will use them as the parameter in the function of "Rotation" and "Truncation"

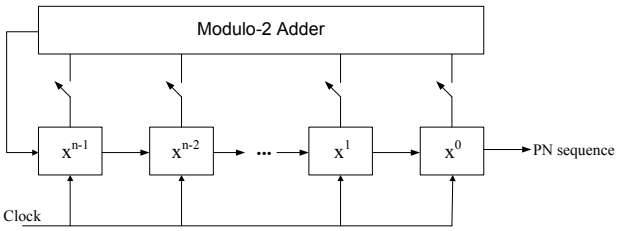

Fig. 7. *n*-stage linear feedback shift register

that will be explained next section. LFSR is also so easy and light to implement that it is very useful in the secure RFID system [20].

B. Description of HB-MP^{++}

The essential idea of HB-MP^{++} protocol we indicate in this paper is to implement the concrete as well as ultra light-weight functions in order to rotate the secret key x in each round. These functions will bring about unpredictable randomness to overcome the weakness of HB-MP^{+}. All notations used in HB-MP^{++} are introduced in table 5.

Table 5. Notations for HB-MP^{++} Protocol

k	length of the secret key shared by reader and tag
x	k-bit secret key shared by reader and tag
x'	denotes $Rot(x, r_n)$
x_s	denotes $Trun(x', r_n)$
α	random k-bit binary vector
α'	denotes $\alpha \oplus x$
α_s	denotes $Trun(\alpha', r_n)$
r_n	number of run of PN sequence
Rot(p,u)	bitwise left rotate operator. The operand p is rotated u position
Trun(p,u)	truncate operator. The operand p is truncated u-LSB bits.

The protocol HB-MP^{++} is composed of q rounds like other protocols, one of which is illustrated in Fig. 8, and described as follows.

Step1. The reader chooses a k-bit binary vector α and sent it to the tag
Step2. The tag and reader compute $\alpha' = \alpha \oplus x$
Step3. The tag and reader generate PN sequence from LFSR using α' as initial value
Step4. The tag and reader calculate the length of "run" of the PN sequence
Step5. The tag and reader compute $x = Rot(x, r_n)$ and $x_s = Trun(x, r_n)$ and $\alpha_s = Trun(\alpha', r_n)$
Step6. The tag computes z as follows:
$z = \alpha_s \bullet x_s \oplus v$
and looks for a random-bit($<k$) binary vector β such that $z = \beta \bullet x_s$
Step7. The tag sends β to the reader
Step8. The reader checks if
$\alpha_s \bullet x_s = \beta \bullet x_s$

XOR function can enhance the unpredictability of α in step 2. Even though offender eavesdrops α illegally, he never has the information about α' thanks to XORing between the k-bit binary vector α and secret key x. We make use of α' for the initial value of LFSR and generate the PN noise sequence. Using the length of the PN sequence's "run", r_n, the secret key x is left-rotated r_n position, which is adding randomness

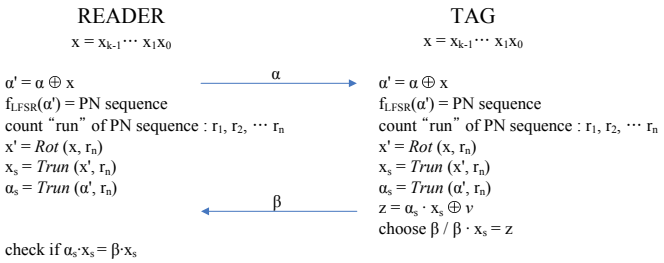

Fig. 8. A single round of HB-MP^{++} protocol

on the secret key ($x = Rot(x, r_n)$). The r_n is also utilized in the function of bit-truncation. If the value of r_n is u, α' is truncated by u-less significant bit ($\alpha_s = Trun(\alpha', r_n)$). Because the value of u varies in each stage, the bit number of α_s is continuously supposed to be changed. As a consequence, as we choose β which has same bit number with α_s, the bit number's change of tag's response (β) make this advanced protocol become resistant to traceability. In the example of last section, the secret key x is left-rotated 3 positions and α' is truncated by 3-less significant bit at the first round. So, the tag's response has the 13(16-3) bit. Then, the x will be rotated 1 position and β has the 15 bit in the 2nd round.

IV. SECURITY and PERFORMANCE ANALYSIS

Since the HB-MP^{++} is also based on the LPN, a passive attacker has to solve the LPN problem to reveal the secret key of x. As the protocol is also designed to have round keys which are rotated at random, the security is updated in each round and synchronization problem will be solved. This improved algorithm is able to intensify security with the ultra-simple 4-step functions, XOR, LFSR, Rotate and Truncate. So, the unauthorized user who tries to get the information about secret key and trace the movement of tag illegally never accomplish the intention as long as he does not know the structure of functions and initial values in each step. The main shortcoming of HB-MP and HB-MP^{+} is that the tag's response β has always same bit size (m: the length of message). By repeatedly staring the bit size of tag's response, a spying reader will be able to have more chance to track the movement of the tag. Compared to the two protocols, the protocol discussed in this paper has a different size of tag's response continuously. That's the reason HB-MP^{++} is also strongly resistant to traceability. Another advantage of this protocol comes from the fact that HB-MP^{++} has only one secret key instead of two kinds of secret key in the case of HB-MP, which may contribute to simple structure of the protocol. Unless the non-linear function has light-weight, we may not adopt the algorithm for the RFID system. In the HB-MP^{++}, we don't have to concern the weight of protocol because all functions (LFSR, XOR, Rotate, Truncate) which used in this protocol have been proved to have ultra light-weight and be easy to implement.

V. CONCLUSIONS

RFID tags are small, wireless devices that help identity objects and people. Authentication protocols for RFID tag and reader are important both for secure implementation as well as for allaying consumer's concerns with regard to their privacy and security. In this work, we make a concrete and light-weight function that will be very useful in RFID system. Our protocol, named HB-MP^{++}, provides a powerful method against passive as well as any active attacks. The new algorithm presents better increased security and un-traceability. This new protocol also gives better performance and efficiency rather than those of the more recent protocols derived from HB family group.

REFERENCES

[1] J. Banks, D. Hanny, M.A. Pachano, and L.G. Thompson, RFID Applied, John Wiley & Sons, Inc., Hoboken, NJ, 2007

[2] A. Juels, RFID Security and Privacy: A Research Survey, *Invited Paper*, IEEE Journal on Selected Areas in Communications, Vol.24, No.2. Feb., 2006

[3] H.B. Kang, S.K, Hong, H.C. Park, H.Y. Chang, K.W. Park, J.H. Ahn, J.S, Kih, M.Y. Sung, Y.K. Sung, A Ferroelectric Based Passive RFID Tag for UHF(860-960MHz) Band, Integrated Ferroelectrics, 89:94-105, 2007

[4] K. Finkenzeller, RFID Handbook, John Wiley & Sons, Inc., 2003

[5] C.C. Tan, B. Sheng, Q. Li, Secure and Serverless RFID Authentication and Search Protocols, IEEE Transactions on Wireless Communications, Vol. 7, No. 4, April, 2008

[6] J. H. Oh, H.S Kim, J.Y. Choi, A Light-weight Security Protocol for RFID System, International Federation for Information Processing, Personal Wireless Communication Vol. 245, 2007

[7] G. Avoine, Adversary Model for Radio Frequency Identification, Technical Report LASEC-REPORT-2005-001, EPFL, Lausanne, Switzerland, Sep. 2005

[8] [8] J. Munilla, A. Peinado, HB-MP: A Further Step in the HB-Family of Light-weight Authentication Protocols, Computer Network, 51(2007), 2262-2267

[9] S.Weis, S. Sarma, R.Rivest, D. Engels, Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems, International Conference on Security in Pervasive Computing, March 2003

[10] S.Weis, Security and Privacy in Radio Frequency Identification Devices, Massachusetts Institute of Technology, 2003

[11] N.J. Hopper, M.Blum, Secure Human Identification Protocols. Advanced in Cryptology-ASIACRYPT2001, Lecture Notes in Computer Science, Vol.2248, Springer, 2001

[12] A. Juels, S. Weis, Authenticating Pervasive Devices with Human Protocols, Advanced in Cryptology-Crypto2005, Lecture Notes in Computer Science, Vol. 3621, Springer 2005, pp.293-308

[13] H.Gibert, M.Robshaw, H.Silbert, An Active attack against HB^{+} - A Provable Secure Light-weight Authentication Protocol, Cryptology ePrint Archive, Report 2005/237, 2005

[14] J. Katz, J.S. Shin, Parallel and Concurrent Security of the HB and HB^{+} protocols, Cryptology ePrint Archive, Report, 2005/461, 2005

[15] X, Leng, K. Mayes, K, Markantonakis, HB-MP^{+} Protocol: An Improvement on the HB-MP Protocol, 2008 IEEE International Conference on RFID, April, 2008

[16] D.N Due, K.Kim, Securing HB+ against GRS Man-in-the-Middle Attack, 2007 Symposium on Cryptography and Information Security, Jan., 2007

[17] H.Gilbert, J. Matthew, B. Robshaw, Y. Seurin, HB$^{\#}$: Increasing the Security and Efficiency of HB^{+}, Eurocrypt 2008

[18] N. Weste, D. Harris, CMOS VLSI Design, Addison & Wesley, 2005

[19] V. K. Garg, IS-95 CDMA and cdma2000, Prentice Hall, 2000

[20] S. Mukhopadhyay, P. Sarkar, Application of LFSRs for Parallel Sequence, Lectural Notes in Computer Science, Springer, Vol. 3982/2006