RFID Security Protocol by Lightweight ECC Algorithm

SungJin Kim[*], YoungSoo Kim[*], SeokCheon Park[*]
[*]*College of Software, Kyungwon Univ.*
scpark@kyungwon.ac.kr

Abstract

A radio-frequency identification (RFID) system has been gradually expending its application areas.

However, RFID had a serious security problem like as attacker's tracing and spoofing. Especially, Low-cost RFID tags are weak device and have limited computing power. Therefore, an RFID security protocol has been light weighted.

In this paper, we design a lightweight RFID security protocol based on the ID Blind Scheme and ECC (Elliptic Curve Cryptography). Our protocol offers enhanced security feature in RFID security with respect to user privacy against tag cloning allowing an additional ECC modular operation.

1. Introduction

Radio Frequency Identification (RFID) technology can be used in lots of industries such as supply chain, manufacturing, inventory, storage, etc.

RFID system will be more widely used in various industry then optical barcode technology if the RFID device-frequently just called an RFID tag is cheaper (below $5 cent) and more secure against eavesdropping.

RFID system consists of three basic components, namely the tag, the reader and the database.

Between reader and database is secure range in transmit. But, tag and reader range is insecure because of tag's limited computer power and memory capacity especially passive tag.

The tag uniquely identifies the item to which it is affixed and communicates with the reader via radio signals. The reader then converts the radio signals into data that can be passed onto the middleware (which determines what the specific RFID system does) to trigger further actions, based on the identifying information.

Usually RFID technology have security problems inherently due to the tag offer no access-control and tamper-resistance mechanisms. It can induce the eavesdropping of the data stored in the tag will be of any great threat since everyone can observe the specific information. For example, an adversary may try to monitor someone by tracking, he get information of products, which an individual user carries or trace a user.

Even though there are many cryptographic primitives for RFID security. They cannot be applied to RFID system because of limited computing power of low-cost tag.

Therefore, we propose a protocol that can be realized in a low-cost tag and protect from tracing and spoofing. Our proposed protocol using ECC (Elliptic Curve Cryptography) elements for strengthen protocol and blind factor for downsizing the tag memory and gates.

The unusual design constraints places on embedded devices require a new, highly efficient, easy to deploy cryptography scheme that provides high levels of security while minimizing memory, execution speed requirements and power requirements. ECC id an essential methodology for meeting these requirements of embedded designs.

We will show our protocol offers the most improved security feature which involves ECC downsizing function in tag and more strengthen encryption in reader and database.

This paper is organized as follow: In section 2, we describe RFID previous work. In section 3, we introduce our idea of security and lightweight. In section 4, we explain process of our protocol. And finally, we make analysis of our protocol about security and performance aspect.

In the final section, we provide a summary of our work and future work.

2. Related Works

There are many papers about authenticated encryption scheme [1, 2, 3, 4, 5] based on various difficulties such as discrete logarithm, factoring, or

0-7695-2930-5/07 $25.00 © 2007 IEEE
DOI 10.1109/ALPIT.2007.103

elliptic curve, etc. Several savants also armed at the linkages of a huge message or the message linkages for message flows to design a suitable algorithm with the concept of authenticated encryption scheme [6, 7, 8, 9, 10]. According to the group of verifiers, many papers have been proposed to suit the requirements of an authenticated encryption scheme with (t, n) shared verification such as [11, 12, 13].

Actually, there are some subjects should be down in the future. The future works can be described as the below items [14].

1) In practical implement, when signer cannot sign message, the proxy behavior will happen.

2) In a mobile environment, short response time and efficient computation are very important. When a user requests a service to a provider with payment way, he will considerably care about the transmitted time and cost. Since it costs quite much of the computation of authentication encryption schemes more efforts should be made to improve the efficiency.

3) Actually, the other cryptosystem is developing gradually recently, Elliptic curve cryptosystem. It can pro-vide more efficient performance, and keeps the same security as the traditional public cryptosystems.

In this paper, we make mention of the encryption schemes. We suggest new security protocol which is regard to elliptic curve cryptography for provide more efficient and more security.

3. Idea of Our Protocol

In this chapter, we explain idea of our proposal. Main idea of our protocol is minimize the tag memory size by downsizing the ECC security function and transmit bit length and strengthen RFID system security by modify the origin ECC algorithm.

3.1 Using Elliptic Curve Cryptography

ECC is an asymmetric cryptographic approach (also known as public key cryptography) that applies different keys for encryption and decryption

Among ECC, We use finite field F_2^m type Elliptic Curve because of (Menezes and Vanstone [15] have noted that) arithmetic in the finite field F_2^m is especially suitable for hardware implementation. An arithmetic processor efficiently designed to compute in F_2^m could readily apply to implementations of elliptic curve cryptosystems over the same field. Hence, it is worth examining some of the properties of the field F_2^m.

Looking at F_2^m as a vector space of dimension m over F_2, the elements of F_2^m can be represented as binary vectors (or strings) of length m, given a suitable basis of this vector space. This makes it easy to store data in tag (ideally in shift registers of length m).

Addition F_2^m can be performed in one clock cycle by bitwise XORing the operands like as squaring an element in F_2^m is merely a matter of rotating its vector representation, which can be done in one clock cycle.

The security of ECC relies on the hardness of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP), which states that given *P* and *Q* = *kP*, it is hard to find *k*. While a brute-force approach is to compute all multiples of *P* until *Q* is found, *k* would be so large in a real cryptographic application that it would be infeasible to determine *k* in this way.

Besides the curve equation, an important elliptic curve parameter is the *base point* , *G*, which is fixed for each curve. In the Elliptic Curve Cryptosystem, the large random integer *k* is kept private and forms the secret key, while the result *Q* of multiplying the the private key *k* with the curve' s base point *G* serves as the corresponding public key. Not every elliptic curve offers strong security properties and for some curves the ECDLP may be solved efficiently. Also, 193 bits cryptograph key of elliptic curve cryptograph base is secured by 2020. In the case of calculating using an Intel Pentium PC 450MHz, it makes for a strong basis of information protection [16] as it will take 6.54 x 1011 years of computational processing for a cryptographic attack.

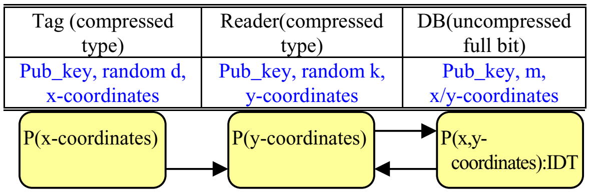
3.2 Principle of our Protocol

Main idea of our protocol is using ECC elements for strengthen RFID security and blind factor(x-coordinate value of P) for downsizing the tag capacity. Especially, we use Finite field F_2^m, it has limited elements and no round-off error and fast computing. Therefore it's appropriate in our security protocol.

We design bit length of tag is limited below 64bit for downsizing the tag capacity less then around 3,000 gates. Therefore, total amount of cost the RFID tag could be less then 5 cents.

Figure 1 illustrates our idea and key parameter for security. Tag compute x-coordinate value(r) of P point and send to Reader. Reader adds on y-coordinate value(s) of P point to x-coordinate. DB is received x,y-coordinates values(r, s) from Reader and then verify and check correctness of coordinates.

And, operation of RFID elements is restricted as blow; especially tag's operation function is only bitwise-XOR, and nonce generation. Therefore, we will expect to downsize the tag gates.



Tag (compressed type)	Reader(compressed type)	DB(uncompressed full bit)
Pub_key, random d, x-coordinates	Pub_key, random k, y-coordinates	Pub_key, m, x/y-coordinates

Figure 1. Main Idea of Our protocol

4. Design of Our Protocol

In this chapter, we describe the process of our security protocol as four phases. First phase is domain parameter generation, second phase is key pair generation, third phase is key verification, and fourth is Signature generation and fifth is Signature verification phase. Multi-step procedure of our protocol is below as figure 2. Our protocol security is based on ID blind. The original ID retrieves on the secure channel between Reader, Database and ID table is regularly updates.

Even though attacker gets information in insecure channel between R and T, they cannot get ID without reader's y-coordinates value(s) and database's IDT. IDT value is only shared in D and R. D updates regularly and therefore ID blind is possible. D and R update scheme is depend on tag type. For example, If T is used in human's resource like passport, ID card then update short time term(update interval is short), and other case update long term or rare.

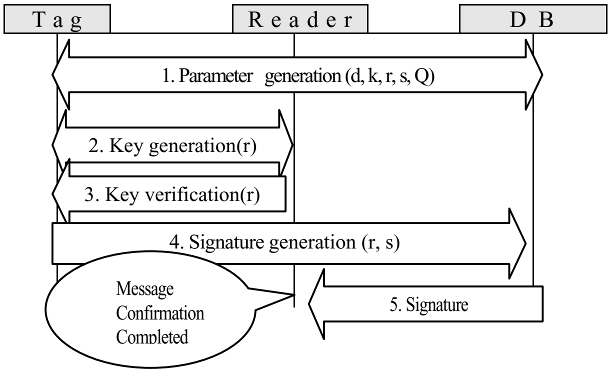

Tag
Reader
DB
1. Parameter generation (d, k, r, s, Q)
2. Key generation(r)
3. Key verification(r)
4. Signature generation (r, s)
Message Confirmation Completed
5. Signature

Figure 2. The procedure of our protocol

4.1 Parameter generation

In this step, D can make regularly update strategy of RFID system and modify Elliptic Curve type and key parameter. This regular updating can make strength of RFID security. We assume that D first define elliptic curve finite filed GF(p) and Tag has his unique key pair G_0 (x_0, y_0) of compressed form, and Reader have group key pair G's(compressed form) as (G_0~G_n), and D have more group values(as G, H, I ….) and mapped IDT values($m_{0\sim n}$; $G_{0\sim n}$)

We also use the notations for entities and operations as summarized in Table 1 to simplify description throughout the paper.

Table 1. Notations

Symbol	Quantity
T	RFID tag
R	RFID reader
D	Back-end server, which has a database
A	An adversary
h()	Encryption function.
PRNG	Pseudo-Random Number Generator
IDT	ID table, each ID is mapping with each P coordinates
a, b	Elements of F_q that define an elliptic curve E over F_q
G	A distinguished point on an elliptic curve called the base point or generating point, we design each tag has its owns G point.
n	The order of filed
Q	Elliptic Curve public key, same as dP = (x_q, y_q)
p	An odd prime number
P	An EC point, ID Mapping coordinates
E	Elliptic Curve over the field $F2^m$ defined by a and b
k	Reader's private key
d	Tag's private key
r, x_p	The x-coordinate of a point P, r = $x_1$mod n
s, y_p	The y-coordinate of a point P, s ≡ k^{-1}{e- dr) mod n
Y_p	The representation of the y-coordinate of a point P when compression is used
m	Tag Identification

4.2 Key pair generation

In this step, R select a random private key(k ∈GF(q)) and compute private key(Qr = kG), and send message(k, Qr) to T, then T select a random private key (d ∈GF(q)) and compute public key Q = kdG = (x_q, y_q) and send it to R for verification. Reader's key pair generation scheme is as figure 3.

Let G be a set of fixed points (base points), we assume this fixed point is already inserted in each tag for optimization.

```
Input:tag base coordinates set G; #of needed signatures k;
Output: key[kn, Qr]
for each tag g∈ G do
    for i = 1 to |G| do
        for c = 1 to n do
            Key[$k_n$, Qr] = {PRNG(), $k_n$($G_i$)}
        end
    end
end
```

Figure 3. Reader's Key pair generation

And, let k be the random number of signatures a reader needs to produce, n denote an order of field (tag's counter). For each tag has each fixed point $G(G_{tag} \in G_{reader})$, and $1 \leq i \leq n$.

The coordinates for public key $[k_n, q_r]$ is = [PRNG( ), $k_n(G_i)$].

4.3 Key verification

R is received public key (Q= dkG= (x_q, y_q)) then check Q is lies on the elliptic curve ($F2^m$). If Q is in $F2^m$ then Q is valid and goes to next step, else re-keying (4.2).

4.4 Signature generation

If Q is valid then T compute x-coordinates value ($r = x_q \bmod n$) and then r is valid ($r \neq 0$). Tag's signature generation is as figure 4.

```
Input: Public Key Q; # of PRNG(length) n
Output: tag's private-key : x-coordinates r;
for each Q  do
   for i = 1 to n-1 do
      if (r = 0) then
            reject
      else
            r = $x_q$ % n
   end
end
```

Figure 4. Tag's signature generation

4.5 Signature verification

In this step, DB received coordinates pair(r, s) from R and then, uncompresses and checks parameters.

If parameter is valid then search message among IDT which is related to coordinated pair(r, s).

Finally, send a message (m) to R. Figure 5 illustrates ID find scheme which is repeat until IDT length to find original message (m).

```
Input: tag identifiers coordinates P(x, y); # of
needed IDT (length);
Output: Message m;
for each P(r, s)  do
   for i = 1 to |IDT| do
      if (r , s ∈ IDT )  ID(r, s) =  m
   end
end
```

Figure 5. ID find scheme

5. Analysis

In this chapter, we make analysis of our protocol in security and Performance aspect.

5.1 Security analysis

In this section, we analyze the security of our protocol respect to data confidentiality, authentication, Traceability.

5.1.1 Data confidentiality

Our protocol is used blind factor r(x-coordinates) in insecure ranges (T-R) and original tag's ID is can find in D after Signature verification step. And If T, R's parameter is valid then ID is transfer in secure range(R-D). And our security scheme is based in ECC, so secret key r is almost infeasible to fine in restricted time (In our scheme, our ideal is that downsizing bit length and regularly update parameter, our scheme is regularly update IDT in this limited time).

As an example, if 10,000 computers each rated at 1,000 MIPS are available, and $n \approx 2^{160}$, then an elliptic curve discrete logarithm can be computed in 96,000 years. Andrew Odlyzko [18] has estimated that if 0.1% of the world's computer power were available for one year to work on a collaborative effort to break some challenge cipher, then the computing power available would be 108 MIPS years in 2004 and 1010 to 1011 MIPS years in 2014.

5.1.2 Data authentication

In Our protocol, tag generate parameters (private key d, and public key Q) and sends it to R. then R and D make variation 2 times like as Figure 6. if parameters is invalid then reject, so our protocol is verify that the inventoried tag had been issued by the entities authorized by the parameters.

5.1.3 Traceability

Our protocol provide location privacy by using random values d (in tag), k (in reader) in each session. Since output of tag parameter(r) is totally difference. Even if malicious attacker replays the parameter, tag transmits the values to R, R verify the values and reject.

5.2 Performance Analysis

In this section, we can estimate our protocol and above proposed scheme which are introduce in section

2. For the convenience, we use abbreviation to represent every proposed scheme as table 2[14].

Table 2. Abbreviation of protocol

Abbreviation	Protocol
HMP_DL	Horster et al.'s scheme[2]
WH_DL	Wu and Hus's scheme [5]
TH_ECC	Tzeng and Hwang [18] proposed a signature scheme with elliptic curve cryptosystem
HCY_ML	Hwang et al.'s scheme [7]
TSE_ML	Tseng et al. proposed a scheme [9] that is authenticated encryption scheme with message
TSE_MF	another scheme of TSE ML according to the requirements of the type of the message flow scheme
HW_T	the Hsu and Wu [11] proposed a (t, n) threshold authenticated encryption scheme
SJ_ECC	Our proposed protocol

5.2.1 Performance Analysis

In efficiency property, we will focus on the performance of our scheme and to analyze the efficiency. For convenience, we first define some notations to denote the performance factor as table 3.

We mainly consider those T_h, T_{exp}, T_{mul}, T_{inv} time as it make a computational heavily cost. And, In order to differentiate the computational complexity between the elliptic curve cryptosystem and the general discrete logarithm cryptosystem, we define the other notations to evaluate the performance of the authenticated encryption scheme based on ECDLP.

Also, we define some notion to denote the total size of the transmitted message. For the communication cost of the various schemes, we define some notation to denote the total size of the transmitted message.

We could dispute the computational cost over two phases, signature generation and message recovery phase.

In our protocol, generation and recovery phase summery as table 4. The signature generation phase of ours SJ_ECC protocol requires $T_{mul} + T_{ec\_mul}$ in tag, and $2T_{ec\_mul} + T_h + 2T_{exp}$ in reader, the message recovery phase needs $(T_{inv} + T_{exp}) + loop|IDT|$. And our protocol send x or y coordinates between T, R, so communication cost can be ≈ $((n + 1)|p|)/2 + |h|$.

Table 3. Abbreviation of performance time

Abbreviation	Protocol
T_{mul}	The time for multiplication
T_h	The time for executing hash function
T_{exp}	The time for exponentiation with modulo P
T_{inv}	The time for inversion modulo P
T_{ec_mul}	The time for multiplying a number by a point on the elliptic curve
T_{ec_add}	The time for the adding one point to another on the elliptic curve
T_loop	In our protocol, the time for mapping ID finding time
ML	Message linkage
MF	Massage flows
$\vert p\vert$	A bit length of a prime number p
$\vert q\vert$	A bit length of a prime number q.
$\vert h\vert$	A bit length of a hashing value.
$\vert IDT\vert$	Our ID table size
[n/c]	A set of signature blocks is (ri, si, ri1, · · · , ric) for each segment i, i = 1, · · · , [n/c]
t	t verifiers of a group of m verifiers such like that is defined in Hsu and Wu [11]

In our signature generation phase, we reduced tag capacity for tag lightweight. It is focus on practical implementation for row-cost tag. Table 5 is illustrates the comparisons of our protocol performance analysis with other.

Table 4. Our protocol (SJ_ECC) phase

signature generation phase	message recovery phase
Tag 1) Randomly select a value d 2) Compute q, r Q= dkG= (x_q, y_q) Reader 3) Randomly select a value k 4) Compute r, s $r = x_q \mathrm{mod}\ n$ $s = k^{-1}(e- dr) \mathrm{mod}\ n$.	DB 5) Computes x_q, v, r, s $x_q' = inv(x_q)$ $v = x_q' \mathrm{mod}\ n$ 6) Do { ID-find loop } while(IDT(r,s) = m)

Table 5. Performance analysis

Protocol	ML	MF	Comm. cost	Signature generation	Message recovery
HMP_DL	N	N	$\vert p\vert + \vert q\vert$	$T_{exp} + T_{inv} + 2T_{mul} + T_h$	$2T_{exp} + T_h + 3T_{mul}$
WH_DL	N	N	$\vert p\vert + 2\vert q\vert$	$3T_h + T_{inv} + 2T_{mul} + 2T_{exp}$	$3T_h + T_{inv} + 3T_{exp}$
TH_ECC	Y	N	$(n + 1)\vert p\vert + \vert h\vert$	$2T_{ec\_mul} + T_{ec\_add+}T_{mul} + (n + 1)T_h$	$4T_{ec\ mul} + 2T_{ec\ add} + (n + 1)T_h$
HCY_ML	Y	Y	$N\vert p\vert + n\vert q\vert$	$n(T_h + T_{inv})+n(T_{exp} + T_{mul})$	$n(T_h + 3T_{mul})+(2n + 1)T_{exp}$
TSE_ML	Y	N	$N\vert p\vert + \vert q\vert + \vert h\vert$	$(n + 1)(T_h + T_{mul})+T_{exp}$	$(n + 1)(T_h + T_{mul})+Texp +3T_{exp} + nT_{inv}$
TSE_MF	Y	Y	$[n/c](t\vert p\vert+\vert q\vert)+dn/ce(\vert h\vert)$	$[n/c](T_{exp}+(t + 1)(T_h + T_{mul}))$	$[n/c](n + 1)(3T_{exp} + tTinv+(t + 1)(T_h + T_{mul}))$
HW_T	N	N	$(t + 2)\vert p\vert+2\vert q\vert$	$3T_{exp} + T_{mul}$	$3T_{exp} + (2t + 1)T_{mul}+(t -1)T_{inv}$
SJ_ECC	Y	Y	$((n + 1)\vert p\vert)/2 + \vert h\vert$	T a g : $T_{mul}+T_{ec\_mul}$ Reader : $2T_{ec\_mul} +T_h+ 2T_{exp}$	$(T_{inv} + T_{exp}) + loop\vert IDT\vert$

6. Conclusion and Future task

In this paper, we proposed a robust and lightweight protocol that has security function using blind factor and ECC scheme. Our tag lightweight protocol may solve several problems as practical implement, short response time and efficient computation and the strength of RFID system. There is a trade-off between cost and security in RFID authentication protocol; therefore, many literatures did not suggest a protocol which guarantees cost and security together. However, in this paper, we propose a strength security and practical protocol for tag downsizing. As future work, we will propose a protocol that is efficient in totally communication cost.

References

[1] S. Araki, S. Uehara and K. Imamura, “The limited verifier signature and its application,” *IEICE Transactions on Fundamentals, vol. E82-A, no. 1, pp. 63–68,* 1999.

[2] P. Horster, M. Michels, and H. Petersen, “Authenticated encryption schemes with low communication costs,” *IEEE Electronics Letters, vol. 30, no. 15, pp. 1212–1213,* 1994.

[3] W. B. Lee and C. C. Chang., “Authenticated encryption scheme without using a one way function,” *IEEE Electronics Letters, vol. 31, no. 19, pp. 1656–1657,* 1995.

[4] C. Ma and K. Cheng, “Publicly verifiable authenticated encryption,” *IEEE Electronics Letters, vol. 39, no. 3, pp. 281–282,* 2003.

[5] T. S. Wu and C. L. Hsu, “Convertible authenticated encryption scheme,” *The journal of Systems and Software, vol. 39, no. 3, pp. 281–282,* 2002.

[6] B. H. Chen, “Improvement of authenticated encryption schemes with message linkages for message flows,” *Computers and Electrical Engineering, vol. 30, no. 7, pp. 465–469,* 2004.

[7] C. L. Hsu, T. S. Wu, and T. C. Wu, “Improvements of generalization of threshold signature and authenticated encryption for group communications,” *Information Processing Lettes, vol. 81, no. 1, pp. 41–45,* 2002.

[8] W. B. Lee and C. C. Chang, “Authenticated encryption schemes with linkage between message blocks,” *Information Processing Letters, vol. 63, no. 5, pp. 247–250,* 1997.

[9] Y. M. Tseng, J. K. Jan, and H. Y. Chien, “Authenticated encryption schemes with message linkages for message flows,” *International Journal of Computers & Electrical Engineering, vol. 29, no. 1, pp. 101–109,* 2003.

[10] Z. Zhang, S. Araki and G. Xiao, “Improvement of tseng et al.’s authenticated encryption schemes with message linkages,” *Computers and Electrical Engineering, vol. 162, no. 3, pp. 1475–1483,* 2005.

[11] C. L. Hsu and T. C. Wu, “Authenticated encryption scheme with (t, n) shared verification,” *IEE Proceedings 20, 1998. Computers and Digital Techniques, vol. 145,no. 2, pp. 117–120,* 1998.

[12] J. Z. Lu and H. Y. Chen, “Improvement of authenticated encryption scheme with (t, n) shared verification,” *in Computer Software and Applications Con-ference, 2000. COMPSAC 2000. The 24th Annual International, pp. 445–448,* Oct. 2000.

[13] C. T. Wang, C. C. Chang, and C. H. Lin, “Generalization of threshold signature and authenticated encryption for group communications,” *IEICE Trans. Fundamentals, vol. E83-A, no. 6, pp. 1228–1237,* 2000.

[14] Min-Shiang Hwang and Chi-Yu Liu, “Authenticated Encryption Schemes: Current Status and Key Issues,“ *International Journal of Network Security, Vol.1, No.2, PP.61–73,* Sep. 2005 (http://isrc.nchu.edu.tw/ijns/)

[15] A. Menezes, and S. Vanstone, “Elliptic Curve Cryptosystems and Their Implementation,” *Journal of Cryptology, pp. 209~224,* 1993.

[16] D. Johnson, “ECC, Future Resiliency and High Security Systems,” *Certicom White Paper,* March 1999.

[17] Andrew Odlyzko. The future of integer factorization. Cryptobytes, 1(2):5–12, 1995.

[18] S. F. Tzeng and M. S. Hwang, “Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem,” *Computer Standards & Interface, vol. 26, no.2, pp.61-71,* 2004.