Mutual authentication between RFID tag and reader using Elliptic curve cryptography

Nguyen Ngoc Hoa*, Dang Thu Hien, Tran Thuy Trang

College of Technology, Vietnam National University, Hanoi
144 Xuan Thuy, Ha Noi, Vietnam

Received 15 November 2007

Abstract. This paper presents an approach related to authenticate mutually a RFID (Radio Frequency Identification) tag from a RFID reader by using the cryptography based on Elliptic curve. Our proposal mutual authentication lies on the Elliptic curve discrete logarithm problem, which is considered the core in order to fight against all of attacks like replay attack, forgery attack and man-in-the-middle attack. Scientifically, we prove not only the accuracy and the security of our approach, but also its performance in the mutual authentication between a RFID tag and a reader. The obtained result of our approach is considered a good step toward the enhancement of safety/security of biometric passport.

Keywords: RFID, elliptic curve cryptography, mutual authentication.

1. Introduction

Actually, RFID (stands for radio-frequency identification) is considered as a novel technology dedicated to system for automated identification of both objects and people. In reality, human beings are very skilful at identifying objects under a variety of circumstances. For example, a bleary-eyed person can easily pick out a pen on a desk while working. However, computer vision performs such tasks poorly. Thus, RFID may be viewed as a means of explicitly labelling objects/people in order to facilitate their "perception" by computing devices [1].

An RFID device – frequently just called an RFID tag – is a small microchip designed for twice objectives: wireless data transmission and identification by using an attached antenna in a package resembling an ordinary adhesive sticker. The microchip itself can be as small as a grain of sand, some 0.4mm^2 [2]. An RFID tag transmits data over the air, in response to interrogation by an RFID reader. For low cost, RFID tags adhere to a minimalist design. They carry little data in on-board memory. The unique index of an RFID tag, known as an RFID code, includes information like that in an ordinary barcode, but serves also as a pointer to database records for the tag. An RFID code today can be up to 96 bits in length [3]. Moreover, small and inexpensive RFID tags are *passive* in general. They have no on-board power source; they derive their transmission

* Corresponding. Tel: 84-4-7547813.
E-mail: hoa.nguyen@vnu.edu.vn

power from the signal of an interrogating reader by using a specific material [4]. Passive tags have practical read distances ranging from about 10cm (ISO 14443) up to a few meters (Electronic Product Code (EPC) and ISO 18000-6), depending on the chosen radio frequency and antenna design/size.

Today, RFID tags can be used in many fields as smart appliances, shopping, interactive objects, medication compliance, transport payments, etc. [5]. Standards for RFID passports are also proposed and determined by the International Civil Aviation Organization (ICAO)[16]. ICAO refers to the ISO 14443 RFID chips in e-passports as "contactless integrated circuits". ICAO standards provide for e-passports to be identifiable by a standard e-passport logo on the front cover. RFID tags are included in new United Kingdom and some new United States passports, beginning in 2006. The chips will store the same information that is printed within the passport and will also include a digital picture of the owner. The passports will incorporate a thin metal lining to make it more difficult for unauthorized readers to "skim" information when the passport is closed.

The widespread adoption and deployment of RFID technology by both corporate and government interests, poses several privacy-related concerns for consumers and organizations alike. The first concern focuses on the need to maintain secure user/location privacy (anonymity and untraceability). Passive eavesdroppers and active intruders should not successfully identify or track tags (objects/users). Researchers have proposed many solutions [6] such as tag "killing", frequent renaming of tags over time using an encrypted identifier, audit systems for RFID privacy, blocker tags preventing unwanted scanning [7], etc. The second issue is related to those attacks that attempt to disrupt the functionality of RFID tags. Electively this type of attack can be defended against by cleverly incorporating authentication techniques as RFID tags and readers exchange messages. Such attacks as denial of service and counterfeiting can be combated if authentication is successful.

In this paper, we focus on a proposed approach aimed to authenticate mutually an RFID tag and a reader. The main idea of our approach is based on the recent results of the Elliptic Curve Cryptography. In the rest of this paper, we first introduce some related works and then the fundamental theory concerning our approach. The mutual authentication and its evaluation will be presented in the section four and five respectively.

2. Related works

Realizing the urgent need to propose a new suitable scheme to solve the security problem with the use of RFID tags, many protocols have been recommended that claim either to achieve secure authentication or to prevent unauthorized traceability. Most of these protocols only apply for weak adversary model [8-10]. All of these protocols, which rely on a trusted third party as a back-end server with an insecure channel between the server and the reader, are vulnerable to man–in-the-middle attack.

Furthermore, there are other more reasonable solutions proposed afterward such as Weis-Sarma-Rivest-Engels [11]. However, Weis-Sarma-Rivest-Engels also unfortunately meets two problems: the heavy workload for server to solve the traceability and irresistible to impersonate attack. Henrici and Muller were proved to be insecure under the man-in-the-middle attack and other ones by Dimitriou [12].

Recently, YA-TRAP scheme was suggested by Gene Tsudik[10]. But Tsudik also pointed out that one drawback in his scheme is susceptible to DOS (Deny of Service) attack.

Thus, our research is therefore focused on the way of proposing a new scheme to enhance the security of a RFID tag. Our proposed scheme is based on the recent result of the Elliptic Curve cryptography in response to authenticate the both machine (reader) providing a service to user and his RFID tag.

3. Fundamental theory

Before detailing our proposed approach, we present, in this section, the fundamental theory related to the Elliptic Curve cryptography (ECC).

ECC is a relatively new cryptosystem, suggested independently in 1986 by Miller [13] and Koblitz [14]. ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The detailed description of ECC and its implementation can be found in [15]. We present here only the algorithms specific for our approach.

3.1. Elliptic curve

An elliptic curve E over a field F is the set of solutions (x;y) which satisfy the Weierstrass equation:

$$E: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$
$$(a_i \in F)$$

Let $E(F)$ be the set of points $(x,y) \in F^2$ satisfying Weierstrass equation with the *point at the infinity O*.

The equation above is applied for any curves over arbitrary fields. In cryptography, we only consider curves over finite fields. Two well-known fields are F_p with a prime p and F_{q^m} with $q = p^r$. With p = 2, all operators can be easily carried out on the devices. Operation over curves includes addition of 2 points on an elliptic curve and scalar multiplication between an integer and a point on an elliptic curve [16].

3.2. Elliptic curve over finite field F_q

Elliptic curve can be defined over finite field F_q with $q = p$ or $q = 2^m$, that m and p are a prime:

- *With q=p* $Y^2 = X^3 + aX + b \ (a, b \in F_p)$
- *With q=2^m* $Y^2 + XY = X^3 + aX^2 + b \ (a, b \in F_{2^m})$

Then, there are a finite number of points on the elliptic curve satisfying equations above. In addition, this number is called *the order of the elliptic curve*.

We can construct an Abel group from all points on the elliptic curve. Firstly, we have to define the addition operator and scalar multiplication operator. The Abel group is defined as $< E(F_q), + >$, with the following properties:

- *Closure* : $P + Q \in E(F_q), \quad \forall P, Q \in E(F_q)$
- *Associativity*:

$$P + (Q + R) = (P + Q) + R, \quad \forall P, Q, R \in E(F_q)$$

- *Neutral element*: ***O*** (also called Zero element or point at infinity)

$$P + O = O + P = P, \quad \forall P \in E(F_q)$$
(1)

- *Inverse elements*: For any $P(x, y) \in E(F_q)$, exists an inverse element $P'(x, -y)$:

$$\forall P \in E(F_q), \exists P' \in E(F_q) : P + P' = P' + P = O$$

- *Commutativity*:

$$P + Q = Q + P, \quad \forall P, Q \in E(F_q)$$

From all above properties, $E(F_q)$ is an Abel group.

3.3. Elliptic curve discrete logarithm problem (ECDLP)

Before presenting this problem, we define several following notions:

- Oder of a point P : Order of a point $P \in E(F_q)$ is the smallest integer r such that $r * P = \infty$
- Base point G is the element G $\in E(F_q)$ that has the smallest order.

Let E be an elliptic curve over a finite field F_q, and G $\in E(F_q)$ a point of order n and Q $\in E(F_q)$. Given E, P, Q, the elliptic curve discrete logarithm problem is to find the unique integer k, $0 \le k \le n-1$ such that $Q = kG$, if such an integer exists.

The assumed hardness of several problems related to the discrete logarithm in the subgroup of allows cryptographic use of elliptic curves.

4. Mutual authentication between RFID tag and reader

By using the ECDLP, we propose a mutual authentication between a RFID tag and a reader. This scheme involves four entities: *RFID user*, *RFID tag*, *registration server* (called RS) and *authentication server* (called AS). Before using a RFID tag, the user has to register it with the RS. Thus, the authentication process are taken place between AS and user in order to validate this tag. Therefore, our authentication scheme includes the three main phases: setup, registration and mutual authentication.

4.1. Setup phase

Suppose that the system parameters for an Elliptic curve over finite field F_p or F_2^m as follows:

- *T = <q, FR, a, b, G, n ,h>*
- *q : prime p or 2m decides a finite field*
- *FR: the field representation*
- *a, b: the curve coefficients*
- *P1, P2: Two points of order n on the curve*
- *n : order of P1, P2. N = #E(Fq) is divisible by n*
- *h*: $\#E(F_q)/n$

We assume that the ECDLP problem is hard to solve under defined elliptic curve above. We have $H : \{0,1\}^* \rightarrow Z_q^*$ is a hash

Registration server RS picks up an secret key (s_1,s_2) with $s_i \in Z_n$ $i=1,2$ and computes public key $Z = -s_1P_1-s_2P_2$ and transfers public key Z to authentication server AS.

Authentication server chooses a secret key (a_1, a_2) with $a_i \in Z_n$ $i=1,2$ and computes public key $AS_{PUB} = -a_1P_1-a_2P_2$ and transfers public key A to registration server RS.

4.2. Registration phase

This phase contains two following steps:

- *Step 1*: identify user's parameters for the RFID tags; it can be his biometric such as fingerprint, iris, face, or even a password.
- *Step* 2: After receiving request from user U_i, the RS compute P_{ID} corresponding to user's parameters and update his RFID tag with the parameters ID_i, P_{ID}, secret keys (s_1,s_2), AS_{PUB}, *H*() and issues it to the user U_i in the secure manner.

4.3. Mutual authentication

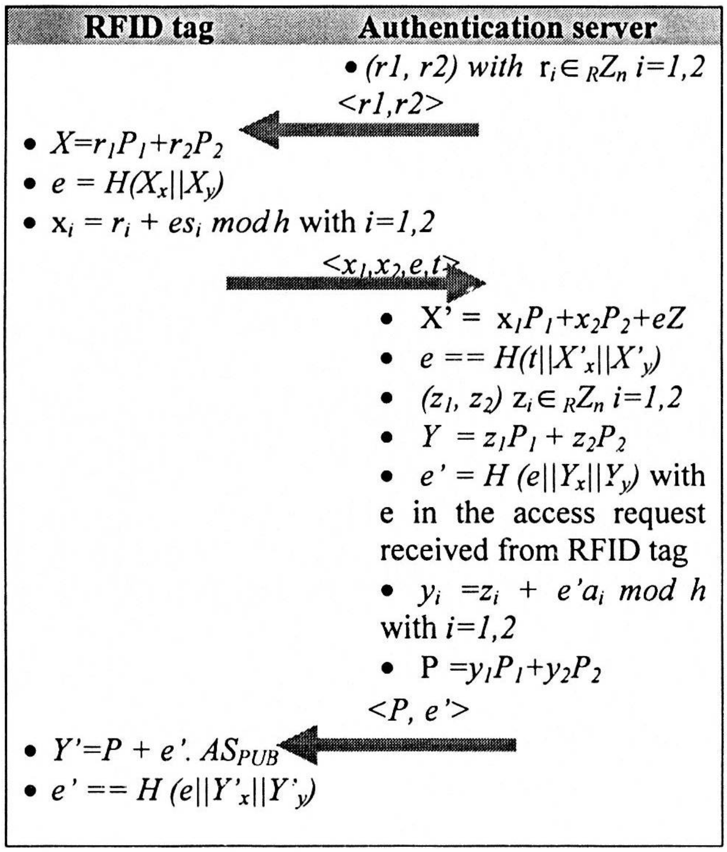
Whenever the user wants to log into a server to access its services, this phase is executed to authenticate user's identity and server's identity.

This phase is divided into 3 sub phases

- Login phase: User requests authentication
- User authentication phase : authenticates user to authentication server
- Server authentication phase : authenticates authentication server to user

4.3.1. Login phase

• Authenticate user to the RFID tag by P_{ID} through password, fingerprint and other biological data.



RFID tag **Authentication server**

• *(r1, r2) with* $r_i \in_R Z_n$ $i=1,2$

<*r1,r2*>

• $X=r_1P_1+r_2P_2$

• $e = H(X_x||X_y)$

• $x_i = r_i + es_i \; mod\, h$ with $i=1,2$

<x_1,x_2,e,t>

• $X' = x_1P_1+x_2P_2+eZ$

• $e == H(t||X'_x||X'_y)$

• (z_1, z_2) $z_i \in_R Z_n$ $i=1,2$

• $Y = z_1P_1 + z_2P_2$

• $e' = H(e||Y_x||Y_y)$ with e in the access request received from RFID tag

• $y_i = z_i + e'a_i \; mod\; h$ with $i=1,2$

• $P = y_1P_1+y_2P_2$

<*P, e'*>

• $Y'=P + e'.\, AS_{PUB}$

• $e' == H(e||Y'_x||Y'_y)$

• Authenticate server randomly chooses a pair of numbers *(r1, r2)* with $r_i \in Z_n$ $i=1,2$. and sends to RFID tags

On receiving, RFID tags processes:

• Computes $X=r_1P_1+r_2P_2$

• Computes $e = H(X_x||X_y)$

• Computes $x_i = r_i + es_i \; mod\, h$ with $i=1,2$

• Sends access request <x_1, x_2, e> to authentication server AS over public channel

4.3.2. User authentication phase

After receiving request <x_1, x_2, e>, authentication server AS processes the following steps:

• Computes $X' = x_1P_1+x_2P_2+eZ$

• Checks whether $e == H(X'_x||X'_y)$. If it holds, the authentication server AS authenticates RFID tag's identity; otherwise, rejects it.

4.3.3. Server authentication phase

• Server picks up a random pair of numbers (z_1, z_2) with $z_i \in Z_n$ $i=1,2$.

• Computes $Y = z_1P_1 + z_2P_2$

• Computes $e' = H(e||Y_x||Y_y)$ with e in the access request received from RFID tag

• Computes $y_i = z_i + e'a_i \; mod\, h$ with $i=1,2$

• Computes $P = y_1P_1+y_2P_2$

• Sends <P, e'> to RFID

On receiving <P, e'>, RFID tag processes following tasks:

• Computes $Y'=P + e'.\, AS_{PUB}$

• Compares $e' == H(e||Y'_x||Y'_y)$. If it holds, RFID authenticates authentication server AS

5. Evaluation

The evaluation of our authentication scheme is manifested by three aspects: its accuracy, security and performance.

5.1. Accuracy

The accuracy of the proposed authentication scheme is proven by the verifying the identicalness between X' and X, Y' and Y. Indeed, we have:

$$X' = x_1P_1 + x_2P_2 + eZ$$

$= (r_1+es_1)P_1 + (r_2+ es_2)P_2 + e'(-s_1P_1- s_2P_2)$

$= r_1P_1 + r_2P_2 = \mathbf{X}$

Similarly, we also have

$Y'= P + e'. AS_{PUB}$

$= y_1P_1+ y_2P_2 + e'. AS_{PUB}$

$= (z_1+e'a_1)P_1+ (z_2+ e'a_2)P_2 + e'(-a_1P_1- a_2P_2)$

$=z_1P_1 + z_2P_2 =\mathbf{Y}$

Thus, the mutual authentication based on ECC guarantees the accuracy totally.

5.2. Security

In order to prove the security of this scheme, we consider the following possible attack scenarios:

- **Replay attack**

The adversary cannot perform a replay attack because the authentication server generates different pair of numbers (r_1,r_2) at the beginning of different authentication process.

- **Forgery attack**

To imitate a valid RFID tag, in a possible period of time, the adversary have to construct a valid sequence $<x_1',x_2', e'>$. Therefore, we have:

$$x_1'P_1+x_2'P_2+e'Z = X \text{ and } e' = H (X_x||X_y)$$

We have:

$$x_1'P_1+x_2'P_2+e'(-s_1P_1-s_2P_2) = X$$
$$(x_1'-e's_1)P_1 - (x_2'-e's_2)P_2 = X$$

Suppose that the user with the secret key chose 2 numbers

$r_1 = x_1'-e's_1 \text{ mod } h \text{ and } r_2 = x_2'-e's_2 \text{ mod} h$ (1)

So e $= H (X_x||X_y) \neq e' H (X_x||X_y)$
And $x_1 = r_1+es_1 \text{mod } h$ and $x_2=r_2+ es_2 \text{mod } h$ (2)

From (1) and (2), we have equations

$x_1' = r_1 + e's_1 \text{ mod} h \qquad x_2' = r_2 + e's_2 \text{mod} h$
$x_1 = r_1 + es_1 \text{ mod} h \qquad x_2 = r_2 + es_2 \text{mod} h$

From this, we can compute (s_1,s_2):

$(s_1,s_2) = ((x_1-x_1')/(e-e')) \text{ mod } h,$
$(x_2-x_2')/(e-e')) \text{ mod } h)$ (3)

We have equation Z = $-s_1P_1-s_2P_2$ has n solutions (s_1,s_2) if given $<x_1',x_2', e'>$. We suppose to have two different solutions (s_1,s_2) and (s_1^*,s_2^*) both satisfying $Z=-s_1P_1-s_2P_2$. Choose $r_1^* = r_1+e(s_1 - s_1^*)$ mod h and $r_2^* = r_2+e(s_2-s_2^*)$ mod h, we have 3 equations:

$$Z = - s_1P_1 - s_2P_2 =-s_1^*P_1 - s_2^*P_2$$
$$x_1 =r_1 + es_1 = r_1^* + es_1^* \text{ mod } h$$
$$x_2=r_2 + es_2 = r_2^* + es_2^* \text{ mod } h$$

All three above equations satisfying the given sequence $<x_1, x_2, e>$. Therefore, we cannot determine which (s_1,s_2) is the accurate secret pair generating the sequence $<x_1, x_2, e>$ and because (r_1,r_2) và (r_1^*,r_2^*) have the same probability of being chosen (because of random choosing) , the probability of the solution (s_1,s_2) of equation (3) different from original (s_1,s_2) is $(n-1)/n$. We call it (s_1^*,s_2^*). Then, we have:

$$-s_1P_1 - s_2P_2 =-s_1^*P_1 - s_2^*P_2$$
$$P_1(s_1-s_1^*)= P_2(s_2-s_2^*)$$

By this reasoning, in a possible period of time, with the probability of $(n-1)/n$, we can solve the ECDLP problem with 2 points P_1 and P_2. That is illogical and denies the assumptions of ECDLP. That is why the forgery attacks are impossible in our authentication scheme.

- **Man-in-the-middle Attack**

The adversary cannot make any modification in the sequence $<x_1,x_2, e, t>$ due to the strict relationship between the parameters. Therefore, the man-in-middle attach is also blocked in our authentication scheme.

5.3. Effectiveness

This authentication mechanism is designed for RFID therefore the number of operations is restricted so as the computing of RFID is secure and fast. However, our approach requires very little operations as shown in the table 1.

Table 1. Number of operations for each phase

	Add two point of EC	Scalar multiple an integer with a point of EC
Access phase	1	2
Tag authentication phase	0	0
Server authentication phase	1	1

Thus, during an authentication, the calculations in a RFID tag are suitable and acceptable. That validates not only the possibility of implementing this mechanism in order to authenticate a RFID tag and its reader, but also the performance of our proposed approach.

6. Conclusion

This work provides evidence that ECC could be used in response to requirement for authentication of both RFID tag and the reader. In this paper, we present our proposed scheme for such mutual authentication. This mechanism has been proven avoiding the replay, forgery and man-in-the-middle attacks. In the near future, we will implement this scheme in the framework of constructing the e-passport system in Vietnam.

Acknowledgments: *This work is supported by the research project N°. QC.06.03 granted by Vietnam National University, Hanoi, Vietnam.*

References

[1] Juels, R. Pappu, S. Garfinkel, RFID Privacy: An Overview of Problems and Proposed Solutions, in *IEEE Security & Privacy*, vol. 3 (2005) 34.

[2] K. Takaragi, M. Usami, R. Imura, R. Itsuki, and T. Satoh, *An ultra small individual recognition security chip*. IEEE Micro, vol. 21, issues 6 (2001) 43.

[3] EPC global Inc., *EPCTM generation 1 tag data standards*, version 1.1 revision 1.27, Technical report, 2005.

[4] T. Lohmann, M. Schneider, C. Ruland, Analysis of power constraints for cryptographic algorithms in mid-cost RFID tags, *Smart Card Research and Advanced Applications*, vol. 3928, Springer (2006) 278.

[5] M. Baard, *RFID invades the capital*. Wired News, 07/2005, www.wired.com/news/privacy/0,1848,66801,00.html.

[6] M. Bellare, R. Canetti and H. Krawczyk, Pseudorandom functions revisited: The cascade construction and its concrete security, *Proceedings of the 37th Symposium on Foundations of Computer Science*, IEEE (1996) 512.

[7] A. Juels, R. Rivest, Michael Szydlo, The blocker tag: Selective blocking of RFID tags for consumer privacy. Conference *on Computer and Communications Security* – ACM (2003) 103.

[8] H. Gilbert, M. Robshaw and H. Sibert, An active attack against HB+ - a provably secure lightweight protocol, *IEEE Letters*, vol 41 issue 21 (2005) 1169.

[9] T. Dimitriou, A secure and efficient RFID protocol that can make big brother obsolete, *International Conference on Pervasive Computing and Communications*, IEEE (2006) 269.

[10] G. Tsudik, Yet Another Trivial RFID Authentication Protocol, 4th *IEEE conference on Pervasive Computing and Communications* (2006) 640.

[11] S. Weis, S. Sarma, R. Rivest, D. Engels, Security and Privacy Aspects of Low-Cost Radio Frequency Indentification Systems, *Proc. of the 1st Security in Pervasive Computing*, LNCS (2004) 201.

[12] D. Henrici and P. Muller, Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers, *IEEE Pervasive Computing and Communications Workshops* (2004) 149.

[13] N. Koblitz, Elliptic Curve Cryptosystems. *Mathematics of Computation*, vol. 48 (1987) 203.

[14] V. S. Miller, *Use of elliptic curves in cryptography*. In H. C. Williams, editor, Advances in cryptology | CRYPTO '85, Berlin, Germany, vol 218 of LNCS (1986) 417.

[15] D. Hankerson, A. J. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*. Springer-Verlag Inc., Germany, 2004.

[16] International Civil Aviation Organization, *Document 9303*, Part 1, Volumes 1 and 2, 6th edition, 2006.

Xác thực hai chiều giữa thẻ RFID và đầu đọc sử dụng hệ mật dựa trên đường cong Elliptic

Nguyễn Ngọc Hoá, Đặng Thu Hiền, Trần Thuỳ Trang

Khoa Công nghệ Thông tin, Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
144 Xuân Thuỷ, Hà Nội, Việt Nam

Bài báo này trình bày một phương pháp xác thực hai chiều cho thẻ RFID (Radio Frequency Identification) và đầu đọc nhờ sử dụng mã hoá dựa trên đường cong Elliptic. Cơ chế do chúng tôi đề xuất được xây dựng dựa trên bài toán logarit rời rạc của đường cong Elliptic, có khả năng chống lại các kiểu tấn công lặp lại, tấn công giả mạo và tấn công man-in-the-middle. Không chỉ chứng tỏ tính chính xác và an toàn, chúng tôi còn chỉ ra hiệu suất tính toán cao của phương pháp này trong việc xác thực hai chiều giữa thẻ RFID và đầu đọc. Những kết quả thu được là một bước đi quan trọng trong bài toán đảm bảo an toàn thông tin cho hộ chiếu sinh trắc học điện tử.