Send Orders for Reprints to reprints@benthamscience.ae

An ID-Based RFID Privacy Protocol with Weil-Pairing

Xie Yumin*

Nanjing Institute of Technology, Jiangning District, Nanjing, China

Abstract: Identification is a very important usage case of RFID. This kind of usage can be subverted by a specific type of attack, such as counterfeiting, sniffing, tracking and so on. From a certain point of view, to protect an RFID tag's privacy or security is to keep its ID hidden from an illegal reader. In this paper, we proposed an ID-based privacy protect protocol for an RFID-based smart card. This protocol is a bilinear pairings-based one, which is a lightweight public-key cryptosystem on ECC. Security attributes of the protocol are presented.

Keywords: ID-Based, RFID, Privacy, Weil-Pairing, ECC.

1. INTRODUCTION

Radio Frequency Identification (RFID) is an emerging technology that has been already applied to existing applications such as supply-chain management and inventory control [1]. An RFID tag is composed of a tiny microchip that is attached to an antenna. While these tags are stuck onto objects, they can be identified and tracked by readers over an electromagnetic field. RFID tags facilitate the process and the management of products during their life cycle [2].

The simplest form of an RFID system is the automatic identification of items. In general, an RFID tag will reply any well-formed reader request with their full ID. This ID can be resoled to a special issue, supply information, a product manufacturer and even a serial number [3]. If the request reader is illegal, those tags disclose the possession of certain sensitive items to them. For example, when the European Central Bank considered the use of RFID tags in Banknotes, criminal scenarios quickly surfaced in which clever robbers would screen their victims first in order to assess the amount of cash carried [4-6].

The other use case of RFID include monitoring, authentication, alerting. Due to the recent development of RFID tag technology, RFID tags can manufactured inexpensively and in non-conspicuous miniature sizes, so that they can be integrated into products during the manufacturing process of the products, rather than being attached to the packaging of the products. And at the same time RFID-tag readers are increasingly easy and inexpensive to buy. So once a specific tag has been associated with a particular item, the mere presence of this tag in a particular reader field already implies a location disclosure. Let one reader can scan a tag and let others cannot find (only presence of the tag) it is a hard difficulty.

In this paper, we proposed an ID-based privacy protect protocol for an RFID-based smart card.

The rest of the paper is organized as follows. Section 2 introduces the security problem in RFID applications. Section 3 gives basic knowledge of Weil Pairing. In section 4 we proposed our new scheme. The security of our new scheme is discussed in section 5. Section 6 concludes the paper and proposes an open problem.

2. PROBLEM

Typical RFID systems are composed of three elements, the RFID tag, the RFID reader and the back-end database associates records with tag data collected by readers. Unlike the cable-based communications, when the wireless tags communicate with a legal reader, any unexpected readers nearby can listen their talks in almost insensible way. This may create new threats to the security and privacy of individuals or organizations which hire the RFID application systems [10]. So some security or privacy mechanisms must be taken into consideration.

Different applications need different methods to protect their information, and further more, different RFID based systems must taken corresponding mechanisms. For example, [7] the low cost demanded for RFID tags causes them to be very resource limited. Generally speaking, these kind tags can only store hundreds of bits, and their logic gate number is often between 5000 and 10000. Within this gate counting, only between 250 and 3000 gates can be used to security functions [7]. In this paper, we take our attention on another kind of RFID based smart card. Even we think that the RFID tag maybe attached on cell phones. If so, the limited storage and computing power on tags will be greatly improved.

Now, we give a chart to explain the idea of our algorithm. As shown in Fig. (**1**). Suppose a target (We call it C) equips with an RFID based smart card. It will log in a system at A and log out the system at B. ID_C is the identity of C. We want to use this identity to log in, but do not let or A B know the true value of it.

1874-4443/14

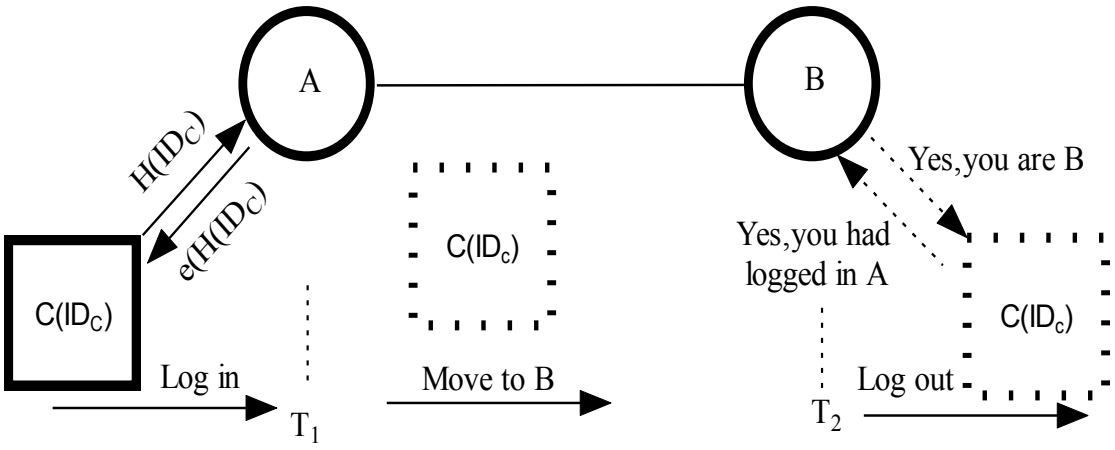

Fig. (1). The main idea of our algorithm.

After C log out the system from B, it can clear all information which get from A, and A or B know nothing about the true value of ID_C during this process.

3. BASIC KNOWLEDGE OF WEIL PAIRING

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and let e: $G_1 \times G_1 \to G_2$ be a paring which satisfies the following conditions [11]:

A: Bilinear $e(P_1+P_2,Q)=e(P_1,Q)e(P_2,Q)$ and $e(P,Q_1+Q_2)=e(P,Q_1)e(P,Q_2)$;

B: Non-degenerate, there exists $P \in G_1$ and $Q \in G_1$ such that $e(P,Q) \neq 1$

C: Computability, there is an efficient algorithm to compute function e.

The m-torsion subgroup of E ($m \in Z$, E is an elliptic curve), denoted by $E[m]$, is the set of points of order m in $E: E[m] := \{P \in E \mid mP = O\}$

$P \in E[m]$ is called an m-torsion point. Usually we choose m as a prime divisor of $\#E(F_P)$.

Lemma 1: Suppose $E[m]$ is an m-torsion subgroup on an elliptic curve E, and m is a prime. For any $P \in E[m]$ and $P \neq O$,there exists $2P \neq O$ and $P/2 \neq O$.

Proof: if there exists an element $P \in E[m]$ and $P \neq O$, which satisfies $2P = O$, then we can find the generator of $E[m]$ is not P. Suppose the generator is Q, then there is a number $z \in Z$, and we can get $P = zQ$ and then $2P = 2zQ = O$, finally we get a contradiction $2z = m$.

Now we define a function $f(P) = 2P$ ($P \neq O$). For any $P_1, P_2 \in E[m] \setminus \{O\}$ and $P_1 \neq P_2$, there exists:

$f(P_1) \neq f(P_2)$

$f(P_1) \neq O$

$f(P_2) \neq O$

So f is a one to one function on $E[m] \setminus \{O\}$, and according to f^{-1} we can get $P/2 \neq O$.

Lemma 2: Suppose $E[m]$ is an m-torsion subgroup on an elliptic curve E, and m is a prime. For any $P,Q \in E[m] \setminus \{O\}$, there exists:

$e(2P,Q/2) = e(P,Q)$

Obviously,

$e(2P,Q/2)$

$= e(P,Q/2)e(P,Q/2) = e(P,Q/2+Q/2)$

$= e(P,Q)$

4. ID-BASED PRIVACY PROTECT PROTOCOL

General ID-based cryptography includes four algorithms: Setup, Extract, Encrypt, Decrypt. Our protocol is slightly different from general one. It includes four algorithms named Setup, Extract, Log in and Log out. Our protocol works as follows:

Setup Begin

Let P be a generator of G_1: Remember that G_1 is an additive group of prime order q and the bilinear pairing is given by $e: G_1 \times G_1 \to G_2$. Define two cryptographic hash functions:

$H: \{0,1\}^* \to Z_q$

$H_1: \{0,1\}^* \to G$.

Key Generation Center(KGC) [6] chooses a random number $s \in Z_q^*$ and set $P_{Pub} = sP$. Then it publishes system parameters:

$\{G, q, P, P_{Pub}, H, H_1\}$.

KGC keeps s as the master-key, which is known only by itself.

Setup End

Extract Begin

Users, such as A, B, C send following IDs information to KGC.

$Q_A = H_1(ID_A)$,

$Q_B = H_1(ID_B)$,

$Q_C = H_1(ID_C)$

KGC send the following messages to A, B, C respectively.

$S_A = sQ_A$,

$S_B = sQ_B$,

$S_C = sQ_C$

If two readers, such as A, B ,would to be construct a system, one acts as a log in reader, the other acts as a log out reader, they should do the following works:

$A: P_A = aP$,

$P_A^{'} = a^{'}P$

$T_{Ha} = H(P_A, P_A^{'})$

$T_{Ae} = e(P_A, P_A^{'})$

B: $P_B = bP$,

$P_B^{'} = b^{'}P$,

$T_{Hb} = H(P_B, P_B^{'})$,

$T_{Be} = e(P_B, P_B^{'})$

$B \rightarrow A: T_{Hb}, T_{Be}$

$A \rightarrow B: T_{Ha}, T_{Ae}$

Extract End

C log in A Begin

$C \rightarrow A: Q_C$ (A stores Q_C into its DB)

$A: P_C = cP_A$

$P_C^{'} = c^{'}P_A^{'}$

$T_{Pc} = cP_C^{'}$

$P_A = 2P_A$

$P_A^{'} = P_A^{'} / 2$

$T_{La} = e(H(P_A, P_A^{'})Q_A, P_{Pub})T_{Ae}e(P_C, P_C^{'})$

$T_A = H(P_A, P_A^{'})S_A \oplus aP_A^{'}$

$T_{Xa} = (e(H(P_A, P_A^{'})Q_A +$

$T_{Hb}Q_B, P_{Pub})T_{Ae}T_{Be}) \oplus T_{Be}$

$A \rightarrow C: P_C, P_C^{'}, T_{Pc}, T_{La}, T_A, T_{Xa}$

$C: P_C = kP_C$

$P_C^{'} = P_C^{'} / k$

$T_{Lc} = T_{La}e(H(P_C, P_C^{'})Q_C, P_{Pub})$

$T_C = H(P_C, P_C^{'})S_C \oplus T_{Pc}$

C log in A End

C log out B Begin

$C \rightarrow B: T_A$

$B \rightarrow C$: if ((T_A is not included in DB of B) sends $e(T_A + T_B, P) \oplus T_{Be}$ to C

$C: if\,(e(T_A + T_B, P) \oplus T_{Be} == T_{Xa})$ sends T_C, T_{Lc} to B

B: $if\,(e(T_A + T_C, P) == T_{Lc}))$ accepts C and adds T_A to the DB of B.

C log out B End

5. ANALYSIS OF THE PROTOCOL

In fact, in our protocol we take advantage of the main idea of [8]. In this paper, the authors present a new ID-based one round authenticated tripartite key agreement protocol with pairings. Now we list its main idea as follows:

Let A, B and C be the three entities who are going to agree to some session keys. After they finish the Extract step as the general ID-based one does, they do the following woks:

$$A \to B,C : P_A = aP, P_A^{'} = a^{'}P$$

$$T_A = H(P_A, P_A^{'})S_A + aP_A^{'}$$

$$B \to A,C : P_B = bP, P_B^{'} = b^{'}P$$

$$T_B = H(P_B, P_B^{'})S_B + bP_B^{'}$$

$$C \to A,B : P_C = cP, P_C^{'} = c^{'}P$$

$$T_C = H(P_C, P_C^{'})S_C + T_{Pc}$$

A verifies:

$$e(T_B + T_C, P) = e(H(P_B, P_B^{'})Q_B + H(P_C, P_C^{'})Q_C, P_{Pub})e(P_B, P_B^{'})e(P_C, P_C^{'})$$

B verifies:

$$e(T_A + T_C, P) = e(H(P_A, P_A^{'})Q_A + H(P_C, P_C^{'})Q_C, P_{Pub})e(P_A, P_A^{'})e(P_C, P_C^{'})$$

C verifies:

$$e(T_A + T_B, P) = e(H(P_A, P_A^{'})Q_A + H(P_B, P_B^{'})Q_B, P_{Pub})e(P_A, P_A^{'})e(P_B, P_B^{'})$$

If the above equations hold, A,B,C can compute eight secret session keys respectively. Such as A:

$$K_A^1 = e(P_B, P_C)^a (= K_B^1 = K_C^1),$$

$$K_A^2 = e(P_B, P_C^{'})^a (= K_B^2 = K_C^2),$$

●●●

$$K_A^8 = e(P_B^{'}, P_C^{'})^{a^{'}} (= K_B^8 = K_C^8)$$

Now we give a definition first, then use this definition to analyze the security properties of out giving protocol.

Definition: The Bilinear Diffie-Hellman (BDH) Problem for a bilinear paring e: $e : G_1 \times G_1 \to G_2$ is defined as follows: given $P, aP, a^{'}P \in G$, compute $e(aP, a^{'}P)$,where $a, a^{'} \in Z_q^{*}$. An algorithm is said to solve this problem with an advantage of ε if

$$Pr[\Re(P, aP, a^{'}P) = e(aP, a^{'}P)] \geq \varepsilon$$

We know that only from P, aP to get a is a hard problem. We assume that BDH problem is hard [8]. And in this paper, we call these two hard problems as BDH problem.

In above protocol, after C log in the system, only T_A, $e(T_A + T_B, P) \oplus T_{Be}$, T_C, T_{Lc} are transferred under insecurity air channels.

5.1. T_A

At the extract stage, A chooses random ephemeral keys $a, a^{'}$ from Z_q^{*}, and set $P_A = aP$, $P_A^{'} = a^{'}P$. When an entity C log in to the system, A set T_A as follows:

$$P_A = 2P_A, P_A^{'} = P_A^{'} / 2$$

$$T_A = H(P_A, P_A^{'})S_A \oplus aa^{'}P$$

So after a series of entities $C_1, C_2, \cdots, C_n$ logged out the system, an illegal reader may get T_{Ai} as:

$$T_{Ai} = H(2iP_A, P_A^{'} / 2i)S_A \oplus aa^{'}P \quad \text{(i=1,2,…,n)}$$

Now change

$$T_{Ai} = H_i sP_G \oplus aa^{'}P \text{ where:}$$

$$H_i = H(2iP_A, P_A / 2i),$$

$$P_G = Q(ID_A) \in G$$

$H_i, s, P_G, a, a^{'}$ are all keep as private values by A according to our protocol. So obviously, if only know finite numbers T_{Ai}, computing $a, a^{'}$ is a BHD problem.

5.2. $e(T_A + T_B, P) \oplus T_{Be}$

$$e(T_A + T_B, P) \oplus T_{Be} =$$

$$e(T_A, P)e(T_B, P) \oplus T_{Be}$$

T_{Be} is keep as private values by A and B, T_B is keep as private values by B according to our protocol. So according to the analysis of 4.1, if only know finite numbers T_{Ai}, computing T_{Be} or T_B is a BHD problem.

5.3. T_C, T_{Lc}

T_C, T_{Lc} are used only once after C find that B is the exact one it will log out. After C send the two values to entity B, it will be accepted by B if those values are legal. Then the values are no usage any more.

5.4. A Precondition

Following conditions should be satisfied when A selects $a, a^{'}, c, c^{'}$ and B selects $b, b^{'}$ from Z_q^{*}:

$$e(aP, a^{'}P) \neq 1$$

$e(bP, b'P) \neq 1$ and

$e(cP, c'P) \neq 1$.

$H_1 : \{0,1\}^* \rightarrow G$ can be easily converted into a normal version by using a function :

$f(m) \rightarrow h(m)P$ [6].

CONCLUSION AND OPEN PROBLEM

ID-based public key cryptosystem can be an alternative for certificate-based public key infrastructures. For key management problem, the former is more convenient then the later. In this paper, we proposed an ID-based privacy protect protocol. We suppose an RFID smart card with an identity ID would to log in and log out a system. We want to protect the card privacy while using ID as its identity to interact with the system. With our protocol, identity's ID information like the value of ID can be protected to some extent. But there still exists open problems. For example, although an adversary doesn't know the exact IDs value with an RFID card, but it can trace the value T_A which the card attached with. So there exists *I don't know who are you, but I can track you* problem. In addition, like general ID-based system, there are still exist Key Escrow Problem in our protocol [9].

CONFLICT OF INTEREST

The author confirms that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] B. Alomair, L. Lazos, and R. Poovendran, "Passive attacks on a class of authentication protocols for RFID", In: *Information Security and Cryptology-ICISC 2007*. Springer: Berlin Heidelberg, pp. 102-115, 2007.

[2] M. Hutter , Rfid Authentication Protocols Based on Elliptic Curves, *Proceeding of 2009 International Conference on Security and Cryptography,* pp.101-110, 2009.

[3] M. Langheinrich, "A survey of RFID privacy approaches", *Personal and Ubiquitous Computing,* vol. 13, no. 6, pp. 413-421, 2009.

[4] M. Langheinrich, "A survey of RFID privac approaches", *Personal and Ubiquitous Computing,* vol. 13*,* no. 6*,* pp. 413-421, 2009.

[5] S. Vaudenay, "On privacy models for RFID". In: *Advances in Cryptology–Asiacrypt,* Springer: Berlin Heidelberg, pp. 68-87, 2007.

[6] V. N. Lakshmi, I. Rameshbabu, D. L. Bhaskari, "A Security Mechanism for library management system using low cost RFID tags", *Journal of Systemics, Cybernetics and Informatics,* vol. 5, no. 1, pp. 92-96, 2007.

[7] P. P. Lopez, J. C. Hernandez-Castro, and J. M. Tapiador, A. Ribagorda, "RFID systems: A survey on security threats and proposed solutions", *Personal Wireless Communications,* pp. 159-170, 2006.

[8] F. Zhang, S. Liu, K. Kim, "ID-based one round authenticated tripartite key agreement protocol with pairings", *Cryptology ePrint Archive, Report* 2002/122, 2002.

[9] J. Baek, J. Newmarch, R. S. Naini, and W. Susilo, "A survey of identity-based cryptography", *Proc. of Australian Unix Users Group Annual Conference,* pp. 95-102, 2004.

[10] M. Kis, **a**nd E. Kalayci, "RFID Infrastructures and AI Approachs For Security", In: *RFID Eurasia, 1st Annual,* pp. 1-6. 2007.

[11] X. Chen, f. Zhang, D. M. Konidala, and K. Kim, "New ID-based threshold signature scheme from bilinear pairings", In: *Progress in Cryptology-INDOCRYPT ,* pp. 371-383, 2005.

Received: November 10, 2014 Revised: January 07, 2015 Accepted: January 19, 2015