An Identity-based Cryptography Scheme Based on FullIdent Algorithm

Xie Yumin[1], Muhammad Kamran[2]
[1]Nanjing Institute of Technology, Nanjing 210000, China
Email: xxyymm3721@126.com
[2]Department of Electrical Engineering, University of Engineering and Technology, Lahore KSK Campus Pakista
Email: kamran.uet@gmail.com

***Abstract*— FullIdent is an identity-based cryptography (IBC) algorithm which is proposed by Boneh and Franklin. In this paper, we give a new identity-based cryptography scheme based on FullIdent. Comparing to FullIdent, our new one concludes three improvements. First, there is no IDMapToPoint function when a sender encrypt message with our scheme. Second, there is no paring operation calculating works during encrypt phase in our scheme. Third, using our new scheme, it is easy to construct an identity-based cryptography system without key escrow problem (KEP). In contrast with existing solutions for KEP, our scheme only employs two independent private key generators (PKG). In addition, our scheme for KEP is very simple because all values are transferred with plaintext.**

***Index Terms*— ID-Based Cryptography, Weil-Pairing, ECC, Key Escrow Problem, FullIdent**

I. INTRODUCTION

The concept of identity-based cryptography was first proposed by Shamir [1]in 1984. With this new idea of cryptography, user's identifier information such as IP or home address can be used as a public key to encrypt a message, or to verify the user's signature. IBC can greatly reduce the system complexity and the cost because no public key management is needed by using IBC. So some Public Key Infrastructure (PKI) can be greatly simplified [2]. In his paper [1], Shamir expresses the main idea of IBC as shown in Fig.1.

IBC includes identity-based signature (IBS) scheme and identity-based encryption (IBE) scheme. It seems that IBS is easer than IBE. For example, when Shamir just proposed the concept of IBC, he immediately used the existing RSA function to construct an IBS scheme, but he was unable to give an (IBE) scheme at the same time. The later became a long-lasting open problem until 2001, Boneh and Franklin [3] and Cocks [4] proposed two schemes independently for the IBE. From then on, many IBE schemes have been proposed and IBC is now flourishing within the research community [2].

The purpose of IBC is to help the administrator of a PKI center. In addtion, with special structure design IBC can be used to simplify the key revocation. For example, surpose a company set an email address 'service.xcop@hotmail.com' as its after-sale service contact information. The company after-sale service team includes Bob,Alice,Tom,Kate and Jack.Each member will be on duty a day every week. As shown in Fig.2, Jack will be on duty every Fridy, he has and only has the responsibility to open, to read, and to reply an email which comes from a user of company on fridy. Jack can log in after-sale email server the day other than Fridy, but he can't open, read, and reply those emails which be received the day other than Fridy. User may send an email to company on Saturday or Sundy, and those emials should be treated with as soon as possible. So arrnging a member who is in turn on Monday to deal with those emails seems suitable. In Fig.2, the suitable member is Bob. Once a company set such an arragement like as shown in Fig.2, anther unreasonable treatment will happen to the special memeber such as Jack, beacaue he will have to deal more emails than other member who is in turn on duty from Tuesday to Fridy. So it is necessary to change the member who will be on duty for the first work day every week.For example, if Bob treats user's email on Monday this week, he will not on duty next monday, and so on. So, it needs a private key alteration arragement for the after-sale service team member. IBE scheme can satisfy this requirement.For example, the PKG can notify users to send their emails by using 'service.xcop@hotmail.com ‖current-day' as encrypting public key. PGK will renew email sysytem private key every week,and sends those new keys to appropriate member of the after-sale service team members.

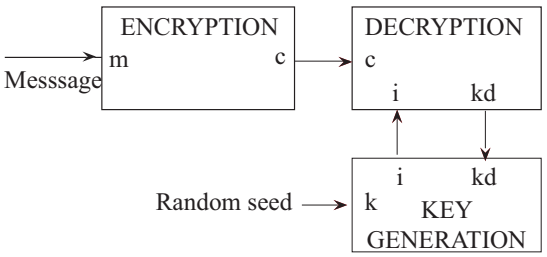

Figure 1. The main idea of Shamir's IBC system

Another IBE application is delegation [3] . Suppose a

doi:10.4304/jcp.9.11.2691-2696

Figure 2. After-sevice team member duty arragement

manager has several assistants and each of them can use the manager email system to deal with a fixed subject responsibility. For example, there are five subjects and they are market, received payments, advert,delivery, customer service.Then the manager can authorize the corresponding private key to each assistent. Every assistent can and only can read emails within his responsible subject.

In fact, although IBE and IBS are two branches of IBC application scheme, there are many deffrences between them. For IBE, the main puppose for a system is to take it as a key management infrastructure.For this puppose IBE can greatly reduce the key mangement works for the sysytem administrator. This kind of property may become more important because in IBS systems there are more memeber roles than it is in IBE systems. For example, from Fig.3 and Fig.4 we can know that in IBS system a user will interact with a signer to sign a message, and this message and its signatrue will be verified by many verifiers.

Now we give an example that uses IBC to reduce the key manegement in a special application-wireless sensor networks(WSN). As we know WSN often comprises with small sensor nodes which only include limited resources in it. Those nodes mostly are deployed in open envirments and such that the communications between them are insecure. Due to limited resoures of the nodes, only symmetric cryptosystems can be used in such kind systems. Olivera [5] proposed a scheme called TinyTate. According to TinyTate, node can exchange a symmetric key with each of its neighboring nodes by using an IBE scheme. We list the main idea of TinyTate in Table I .

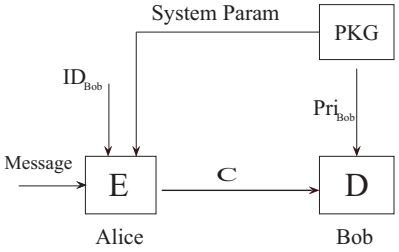

Figure 3. The structure of IBE scheme

In this paper, we proposed a new IBC scheme which based on FullIdent algorithm.With FullIdent, a user must do IDMapToPoint function one time when the user want to encrypt a mesaage.In our new scheme, this function will be done once and for all.In addition,with our new

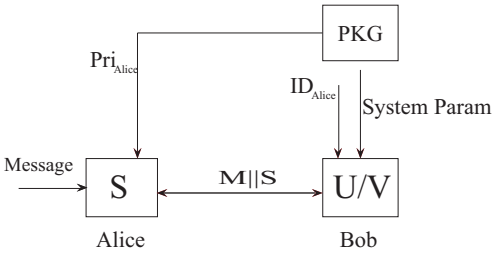

Figure 4. The structure of IBS scheme

TABLE I.
THE MAIN IDEA OF TINYTAPE

Step1	$A \Rightarrow g_a : ID_A, r$ $B \Rightarrow g_b : ID_B, r$ ...
Step2	$M \Rightarrow A : ID_a, enc_{p_a}(ID_m \Vert ID_a \Vert K_{ma} \Vert r)$ $N \Rightarrow B : ID_b, enc_{p_b}(ID_n \Vert ID_b \Vert K_{nb} \Vert r)$ ...
Step3	$A \Rightarrow M : ID_a, ID_m, m, mac_{k_{ma}}(ID_a \Vert ID_m \Vert m \Vert r^{'})$ $N \Rightarrow B : ID_n, ID_b, m, mac_{k_{nb}}(ID_n \Vert ID_b \Vert m \Vert r^{'})$ ...

scheme, one can easy to construct an IBC scheme without KEP.

The rest of the paper is organized as follows. Section 2 introduces the basic concept of pairings.Section 3 presents the detail of FullIdent algorithm. In section 4 we proposed our new scheme. The secrity of our new scheme are discussed in section 5. Section 6 gives an application of our new scheme. It is a solution for KEP with IBC schemes, and we discuss the security of this solution in section 7. Section 8 concludes the paper.

II. BASIC CONCEPTS

Suppose G_1, G_2 are two groups which hold cyclic property with order q for a large prime number. The FuulIdent is implemented by Weil pairing which possesses the following three good properties.

A. Bilinear: For all $Q, P \in G_q$ and for $x, y \in Z$ we have $e(xQ, yP) = e(Q, P)^{xy}$.

B. Non degenerate: For all $P \in G_q$ and $P \neq O$ we have $e(P, P) \neq 1$.

C. Computable: For all $P_1, P_2 \in G_q$, the value $e(P_1, P_2)$ is easy to compute.

Bilinear pairing, which includes Weil pairing and Tape pairing can be broadly used in many applications. Encryption, signature and key management are its three

fundamental fields. Table II includes several examples of those usages.

TABLE II.
DIFFERENT USAGES OF BILINEAR PAIRING

Item	Applications or Advantages	Comments or Shortcomings
Encrypt	1.Good for ID-based schemes 2.Simplity and Privacy	Key escrow problem with ID based-scheme
Signature	Short signature, Blind signature, Ring signature, Group signature, Unique signature, etc.	
Key Agree-ment	Tree-party one-round key agreement	Conference keying
Threshold	A PKG plays the trusted dealer	
Threshold	A PKG plays the trusted dealer	
Others	Chameleon hash, Signcryption	

When we talk about the security of a bilinear pairing scheme, a definite assumption must be given first. For IBE schemes it usually is bilinear diffie hellman problem and for IBS schemes it usually is computational diffie hellman problem.

Bilinear Diffie-Hellman(BDH) problem: For given P, xP, yP, zP with $x, y, z \in Z_q^*$, to compute $e(P,P)^{xyz}$ is a hard problem.

Computational Diffie-Hellman(CDH) problem: For given P, xP, yP with $x, y \in Z_q^*$, to compute xyP is a hard problem.

Beside BDH and CDH problems, there are many other assumptions and we list some of them in talbe III.

III. RELATED WORKS

Like a general IBE scheme, the algorithm named FullIdent [3] includes four steps which named Setup,Extract, Encrypt and Decrypt respectively. We list the main contents of them as follows:

Setup:

Step 1: Pick large *k*-bit prime number *p* which satisfies $p = 2mod3$ and $p = 6q - 1$ for some prime $p > 3$. Suppose E is an elliptic curve which defined by $y^2 = x^3 + 1$ over F_p. Pich an enlement $P \in E/F_p$ of order q.

Step 2: Pick hash functions $H : F_{p^2} \to \{0,1\}^n$, $H_1 : \{0,1\}^n \times \{0,1\}^n \to F_q$ and $G_1 : \{0,1\}^n \to \{0,1\}^n$

TABLE III.
SOME ASSUPTIONS ON DIFFERENT IBC SCHEMES

Assumption	Application Schemes
ECDLP	The basic standard for pairing schemes
DBDH	HIBE, Boneh,etc [6];NIBS [7]
DHBDH	EJPMPKA,Barua,etc [8]
kDBDH	IBESWRO,Boneh,etc [6]
DDH	BLS [9];MS [10]
WDH	IBSP,Hess,etc [11]
kSDH	SSSWRO [12]
CCDH	BLS,Boneh,etc [9]

Step 3: Choose random $s \in Z_q^*$, set $P_{pub} = sP$ .Pick a hash function $G : \{0,1\}^n \to F_q$.

After finashing the above steps,we can get the following infomations about the scheme.

$$\begin{cases} M \in \{0,1\}^n & Message\ space; \\ \{p, n, P, P_{pub}, G, H, H_1, G_1\} & Parameters; \\ s \in Z_q^* & PKG's\ master\ key \end{cases}$$

Extract:

Suppose a user's identifier is string, and suppose ID is the value of this string, then the user's private key can be build by PKG as follows:

Step.1 $Q_{ID} = MapToPoint_G(ID)$

(For more information about $MapToPoint_G$ we can see [3])

Step.2 Set the user's private key $d_{ID} = sQ_{ID}$.

Encrypt:

A user encrypts a massage and then sends it to another user with ID as identifier.We use the following steps to finish this procedure:

Step1: $Q_{ID} = MapToPoint_G(ID)$

Step2: Pick a random $\sigma \in \{0,1\}^n$

Step3: Compute $r = H_1(\sigma, M)$

Step4: The ciphertext $C =< U, V, W >$ where

$$\begin{cases} U = rP \\ V = \sigma \oplus H(g_{ID}^r) \quad g = e(Q_{ID}, P_pub) \\ W = M \oplus G_1(\sigma) \end{cases}$$

Decrypt:

For a ciphertext $C =< U, V, W >$ which is encrypted by the public key ID, if $U \in E/F_p$ isn't a point of oder q, reject the message C, else decrypt C as following steps with d_{ID}:

Step1: $H(e(d_{ID}, U) \oplus V) = \sigma$

Step2: $G_1(\sigma) \oplus W = M$

Step3: $r = H_1(\sigma, M)$. If eqution $rP = U$ holds, accept the ciphertext and goto next step, else reject it.

Step4: Take M as the description of message C.

In the algorithm FullIdent, function MapToPoint works as follows [3]:

Step1: Set $x_0 = (y_0^2 - 1)^{(2p-1)/3}$ and $y_0 = G(ID)$.

Step2: Suppose $Q_0 = (x_0, y_0)$ and $Q_0 \in E/F_p$. Compute $Q_{ID} = 6Q_0$

So there are 5 values of $y_0 \in E/F_p$ which satisfies $6Q_0 = O$. As soon as the select value of $G(ID)$ hit one of those 5 values, it will not have order with q. Now we give anthoer example for this situation.

There is a function called MapToGroup in [9], and this function works as follows:

Step1: For a message space $M \in \{0,1\}^n$, set j=0.

Step2: Compute $h(j||M) \to (x, b)$

Step3: If $f(x)$ [9] is a suitable value in F_{p^l}, do the map operations, else, increament j.

Step4: If j reaches 2^l, return failre.

The failure probability of above function is about $j/2^{2^l}$ [9]

IV. SIMFULLIDENT

Based on FullIdent, we give a new scheme called SimFullIdent. SimFullIdent also includes Setup,Extract, Encrypt and Decrypt four steps.

Setup:

Step1: As in the FullIdent scheme.

Step2: As in the FullIdent scheme. In addition, choose a hash function $H_2 : \{0,1\}^* \to \{0,1\}^n$

Step3: Pick two randoms $s, s_1 \in Z_q^*$ and set $P_s = sP, M_{s_1} = e(s_1 P, s^2 P)$.

After finashing the above steps,we can get the following infomations about the scheme.

$$\begin{cases} M \in \{0,1\}^n & Message\ space; \\ \{p, n, P, P_s, M_{s_1}, H, H_1, H_2, G_1\} & Parameters; \\ s, s_1 \in Z_q^* & PKG's\ master\ keys \end{cases}$$

Extract:

For a request user with identifier ID , the user's private key can be build by PKG as follows:

Step1: The user chooses a random $u \in Z_q^*$, sets $P_u = H_2(ID)uP$, then sends P_u to PKG.

Step2: PKG sets $P_u^{'} = ss_1 P_u, P_u^{''} = ss_1 H_2(ID)P$, sends $P_u^{'}, P_u^{''}$ to the user.

The final $d_{ID} = \{P_u^{'}, P_u^{''}, u\}$.

Encrypt:

A sender can encrypt a message M under the public key with the receiver's ID as follows:

Step1: Pick a random $\sigma \in \{0,1\}^n$

Step2: Compute $r = H_1(\sigma, M)$

Step3: The ciphertext $C = < rP_s, \sigma \oplus H(M_{s_1}^{rH_2(ID)}, M \oplus G_1(\sigma) >$

Decrypt:

A receiver can decrypt messsage $C =< U, V, W >$ as following steps:

Step1: Compute $\sigma = V \oplus H(e(U, P_u^{'})e(U, P_u^{''})^{1-u})$

Step2: $W \oplus G_1(\sigma) = M$

Step3: $r = H_1(\sigma, M)$, test if $U = rP_s$ hold. If not, reject C, else take M as result.

V. THE SECURITY OF SIMFULLIDENT

From [3] we know that FullIdent is a chosen ciphertext secure IBC algorithm. In fact, our new scheme only changes in some action sequence. For example, we transform IDMapToPoint into relation as $d_{ID} = \{ss_1 P_u, ss_1 H_2(ID)P, u\}$. So our new scheme has the same security property as FullIdent.

We can simply verify correctness of our new scheme by the following equations.

$$\begin{aligned} & V \oplus H(e(U, P_u^{'})e(U, P_u^{''})^{1-u} \\ &= V \oplus H(e(rP_s, ss_1 H_2(ID)uP) \\ &\qquad e(rP_s, ss_1 H_2(ID)P)^{1-u} \\ &= V \oplus H(e(rP_s, ss_1 P)^{H_2(ID)u} \\ &\qquad e(rP_s, ss_1 P^{1-u})^{H_2(ID)(1-u)} \\ &= V \oplus H(e(rP_s, ss_1 P)^{H_2(ID)u + H_2(ID)(1-u)} \\ &= V \oplus H(e(rP_s, ss_1 P)^{H_2(ID)} \\ &= \sigma \oplus H(M_{s_1}^{rH_2(ID)} \oplus \\ &\qquad H(e(rP_s, ss_1 P)^{H_2(ID)} \\ &= \sigma \oplus H(e(s^2 P, s_1 P)^{rH_2(ID)}) \oplus \\ &\qquad H(e(rsP, ss_1 P)^{H_2(ID)} \\ &= \sigma \oplus H(e(P, P)^{s^2 S_1 r H_2(ID)}) \oplus \\ &\qquad H(e(P, P)^{s^2 S_1 r H_2(ID)} \end{aligned}$$

From the above equations, we can know that although the PKG doesn't know the user's private value, but it can decrypt any messages if the PKG knows the user's ID as the following shows:

For the message $C =< U, V, W >$ and user's ID, the PKG does:

$$\begin{aligned} & V \oplus H(e(U, ss_1 H_2(ID)P)) \\ &\quad = V \oplus H(e(U, ss_1 H_2(ID)P)) \\ &\quad = V \oplus H(e(rP_s, ss_1 H_2(ID)P)) \\ &\quad = \sigma \oplus H(e(p,p)^{s^2 s_1 r H_2(ID)}) \oplus \\ &\qquad H(e(p,p)^{s^2 s_1 r H_2(ID)}) \end{aligned}$$

$= \sigma$

So like general IBC schemes, our scheme also has a key escrow property. We will give a new solution for this problem in the next section.

VI. Application of SimFullIdent

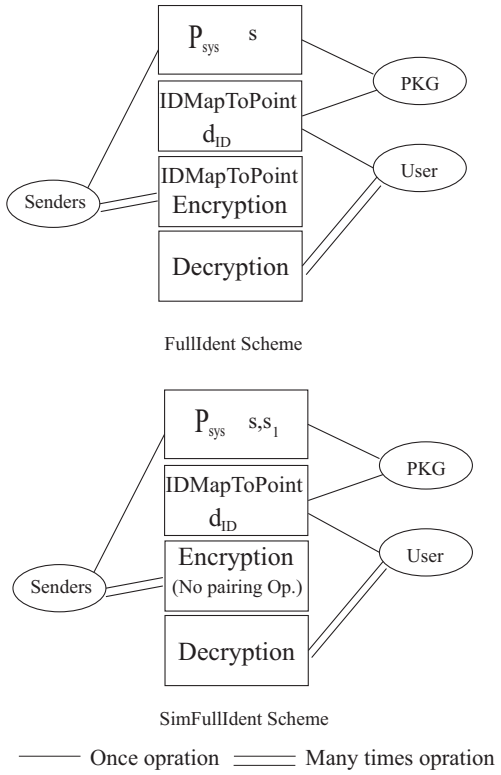

Figure 5. Comparison of FullIdent and SimpFullIdent

Among the following characteristics which SimpFullIdent possess, we think that the third is the most ipmortant because it can solve the open problem which IBC prossess. Datiails comparison of FullIdent and SimpFullIdent be listed in Fig.5.

A. There is no IDMapToPoint function in SimFullIdent scheme.

B. Comparing to FullIdent, there is no paring operation calculating works during encrypt phase in SimFullIdent.

C. Using SimFullIdent we can construct a scheme which can solve the Key Escrow Problem [3].

IBC schemes have a weakness which is the PKG can decrypt or sign any messages using any user infomation. In order to prevent this situation, many reseachers suggested that the master key of the PKG should to be generated by a set number of PKGs. This will impose a heavy load on users.

With the simplicity of SimFullIdent scheme, we can give a very simple scheme which can solve the key escrow problem of identity-based cryptographic. In this scheme only two PKGs are needed. Now we give the algorithm as follows:

Setup:

There are two independent PKGs.They are PKG_A and PKG_B respectively.

PKG_A Pick a random $s_1 \in Z_q^*$ and set $M_{s_1} = e(s_1P, P)$. Send M_{s_1} to PKG_B

PKG_B Pick two randoms $s, s_2 \in Z_q^*$,and set $P_s = sP, M_{s_1} = M_{s_1}^{s_2 s^2}$

The system parameters can be list as follows:

$$\begin{cases} \{p, n, P, P_s, M_{s_1}, H, H_1, H_2, G_1\} & Parameters \\ s, s_1, s_2 \in Z_q^* & PKG's\ master\ keys \end{cases}$$

Extract:

For a given user with ID as indentity, the corresponding private key can be build as follows:

Step1: User picks a random $u \in Z_q^*$ and set $P_u = uH_2(ID)P$. Sends P_u to PKG_B.

Step2: PKG_B set $P_B = ss_2P_u.P_B^{'} = ss_2H_2(ID)P$. Sends $P_B, P_B^{'}$to PKG_A .

Step3: PKG_A set $P_A = s_1P_B, P_A^{'} = s_1P_B^{'}$.Sends $P_A, P_A^{'}$to the user.

Step4: The user set $d_{ID} = \{P_A, P_A^{'}, u\}$.

We call above algorithm as IDWithOutKEP. According to the extract action in IDWithOutKEP, a user gets his final private key:

$$d_{ID} = \{ss_1s_2H_2(ID)uP, ss_1s_2H_2(ID)P, u\}$$

VII. The Security of IDWithOutKEP

Elliptic curve discrete logarithm problem (ECDLP) is the basic concept for which IDWithOutKEP algorithm relies on. There are many detail of ECDLP or bilinear parings security in [7], [11], [13], [14].

We can simply define ECDLP as follows: let P, Q be two points on an elliptic curve E and $Q = kP$, where k is an integer. Solving ECDLP means, according to P and Q one can find out the integer k. Generally speaking, for most of ECDLPs there is no sub-exponent algorithm to solve it.

First we list different roles in Table IV.Those roles often appear within an IDWithOutKEP system. There are four deferent roles as shown in Table IV.

TABLE IV.
Four Roles within an IDWithOutKEP system

Role	User	PKG_A	PKG_B	Intruder
Known	u	s_1	s, s_2	
Public known	$ID, P_{sys}, P_B, P_B^{'}, P_A, P_A^{'}$ ($P_{sys} =< p, n, P, P_s, M_{s_1}, H, H_1, H_2 >$)			
Unkn.	s_1, s_2	s_2, u	s_1, u	s_1, s_2, u
Diffi.	ECDLP	ECDLP	ECDLP	ECDLP

For a user, PKG_B or an intruder, he or she knows P_B and P_A , from relation $P_A = s_1P_B$ or $P_A^{'} = S_1P_B^{'}$, we say that finding out s_1 is an ECDLP.

For a user, PKG_A or an intruder, he or she knows $P_B, P_u, H_2(ID), P_B^{'}$, from relation $P_B = ss_2P_u$ or $P_B^{'} = ss_2H_2(ID)P$, we say that finding out s_2 is an ECDLP.

For PKG_A, PKG_B or an intruder, he or she knows P_u, ID, from relation $P_u = uH_2(ID)P$, we say that finding out u is an ECDLP.

So nobody can get the whole security set $\{s_1, s_2, u_{ID}\}$, IDWithOutKEP is secure under ECDLP.

VIII. Conclusion and Open Problem

ID-based public key cryptosystem can be taken as an alternative solution for certificate-based public key infrastructures, especially when efficient key management and moderate security are required. In this paper, based on FullIdent algorithm we give a new IBC protocol called SimFullIdent. In contrast with FullIdent there are three improvements with SimFullIdent. In addition, we give an application of SimFullIdent. Fig.6 is the main idea of this application.

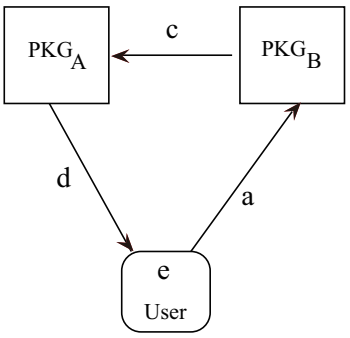

Figure 6. Our idea to solve KEP

Before giving the open problem, we first simplify Fig.6 as follows:

1.User selects a random r and sends $a = f(r)$ to PKG_B.

2. $PKG_B : c = f(a, s_2)$.

3. $PKG_A : d = f(c, s_1)$.

4. $User : e = f(r, d)$.

The function f is a kind of one way function that like pairing oprations in this paper.According to Shamir's secret sharing theory, there are at least two participators when you try to share a secret among a group. Our open problem is that if it possible for we just use only one private key generator to construct an IBC scheme without KEP. We can be inspired by Fig.6 that if we convert PKG_A into a black box. The context of the box should be set by the combinations with the PKG_A and some users. After initializating, this box can be used as PKG_A as it does in Fig.6.But as the same time, it is just a parasitic program process with the host which PKG_B located in.

So, in our open problem we suggest that some users and PKG_B cooperate to generate s_1. PKG_A can use this parameter to construct parameter c, but PKG_A can not read the concrete value of it.

Yet, we do not know if this kind of open problem can be solved on the paring based schemes. If the answer is yes, then the efficient paring computition and convenient key management can be used in many application circumstances.

References

[1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*. Springer, 1985, pp. 47–53.

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

[3] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in CryptologyCRYPTO 2001*. Springer, 2001, pp. 213–229.

[4] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Cryptography and Coding*. Springer, 2001, pp. 360–363.

[5] L. B. Oliveira, R. Dahab, J. Lopez, F. Daguano, and A. A. F. Loureiro, "Identity-based encryption for sensor networks," in *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops' 07. Fifth Annual IEEE International Conference on*. IEEE, 2007, pp. 290–294.

[6] D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," in *Advances in Cryptology-EUROCRYPT 2004*. Springer, 2004, pp. 223–238.

[7] B. Libert and J.-J. Quisquater, "New identity based signcryption schemes from pairings." *IACR Cryptology ePrint Archive*, vol. 2003, p. 23, 2003.

[8] R. Barua, R. Dutta, and P. Sarkar, "Extending jouxs protocol to multi party key agreement," in *Progress in Cryptology-INDOCRYPT 2003*. Springer, 2003, pp. 205–217.

[9] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Advances in CryptologyASIACRYPT 2001*. Springer, 2001, pp. 514–532.

[10] A. Boldyreva, "Threshold signatures, multisignatures and blind signatures based on the gap-diffie-hellman-group signature scheme," in *Public key cryptographyPKC 2003*. Springer, 2002, pp. 31–46.

[11] F. Hess, "Efficient identity based signature schemes based on pairings," in *Selected Areas in Cryptography*. Springer, 2003, pp. 310–324.

[12] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Advances in Cryptology-EUROCRYPT 2004*. Springer, 2004, pp. 56–73.

[13] L. Chen, K. Harrison, D. Soldera, and N. P. Smart, "Applications of multiple trust authorities in pairing based cryptosystems," in *Infrastructure Security*. Springer, 2002, pp. 260–275.

[14] F. Zhang and K. Kim, "Id-based blind signature and ring signature from pairings," in *Advances in cryptologyASIACRYPT 2002*. Springer, 2002, pp. 533–547.

Xie Yumin, Ph.D.Research interests include Computer security,RFID security. Email:xxyymm3721@126.com