New ID-based Threshold Signature Scheme from Bilinear Pairings *

Xiaofeng Chen[1], Fangguo Zhang[1], Divyan M. Konidala[2] and Kwangjo Kim[2]

[1] School of Information Science and Technology,
Sun Yat-sen University, Guangzhou 510275, P.R.China
{isschxf,isdzhfg}@zsu.edu.cn
[2] International Research center for Information Security (IRIS)
Information and Communications University(ICU),
103-6 Munji-dong, Yusong-ku, Taejon, 305-714 KOREA
{divyan,kkj}@icu.ac.kr

Abstract. ID-based public key systems allow the user to use his/her identity as the public key, which can simplify key management procedure compared with CA-based public key systems. However, there is an inherent disadvantage in such systems: the problem of private key escrow, *i.e.*, the "trusted" Private Key Generator (PKG) can easily impersonate any user at any time without being detected. Although the problem of escrowing the private key may be reduced by distributing the trust onto multiple centers, it will decrease the efficiency of the systems. Chen *et al.* first proposed a novel ID-based signature scheme without trusted PKG from bilinear pairings [10], *i.e.*, there is only one PKG who is not assumed to be honest in their scheme. However, the signature scheme cannot be extended to a threshold one. In this paper we propose another ID-based signature scheme without trusted PKG from bilinear pairings. Moreover, we propose an ID-based threshold signature scheme without trusted PKG, which simultaneously overcomes the problem of key escrow and adopts the approach that the private key associated with an identity rather than the master key of PKG is shared.

Key words: ID-based threshold signature, Bilinear pairings, Key escrow.

1 Introduction

The idea of threshold cryptography is to distribute the secret information (*i.e.*, a secret key) and computation (*i.e.*, decryption or signature generation) among multi parties in order to prevent a single point of failure or abuse. For example, let Alice be the president of a committee, she shared her power of signing (or decrypting) among a number of servers in such a way that only more than a certain

* This work was supported by a grant No.R12-2003-004-01004-0 from the Ministry of Science and Technology, Korea and the National Natural Science Foundation of China (No. 60403007).

number of secret shares can be used to sign a message or decrypt a ciphertext on behalf of her. There are plenty of research on threshold cryptographic schemes under CA-based public key setting [6, 13, 21, 24].

In 1984, Shamir [22] introduced the concept of ID-based systems, which simplifies key management procedure of CA-based PKI. The idea of ID-based systems is that the identity information of the user $\mathcal{I}$ acts as his/her public key $\mathcal{P}$, and a trusted third party, called Private Key Generator (PKG), calculates the private key for the user. ID-based systems can be a good alternative for CA-based systems from the viewpoint of efficiency and convenience.

The bilinear pairings, namely the Weil pairing and the Tate pairing of algebraic curves, are important tools for research on algebraic geometry. The use of them in cryptography goes back to the results of Menezes-Okamoto-Vanstone [19] and Frey-Rück [11]. However, their works were to attack elliptic curve or hyperelliptic curve cryptosystems (*i.e.*, using pairings to transform the ECDLP or HCDLP into a discrete logarithm problem in the multiplicative group of a finite field). During the last couple of years, the bilinear pairings have initiated some completely new fields in cryptography, making it possible to realize cryptographic primitives that were previously unknown or impractical [4, 5]. More precisely, they are important tools for construction of ID-based cryptographic schemes [3, 4, 9, 17, 20, 23, 25].

However, there are some drawbacks in ID-based systems [9, 14, 17]. The most criticism against ID-based systems is that PKG knows the private key of all users, so he is able to impersonate any user to sign a document or decrypt an encrypted message. It implies that the PKG must be trusted unconditionally otherwise the systems will soon be collapsed. However, it would be difficult to assume the existence of a trusted party in an *ad hoc* network, where the communication parties are changing frequently.

Boneh and Franklin [4] proposed that the threat from escrowing the private key could be reduced by using "distributed PKGs". On the other hand, they briefly mentioned that each PKG of the "distributed PKGs" can act as a decryption (similarly, a signature generation) server. However, it is a disadvantage in Boneh and Franklin's scheme for the PKG to be involved in the particular applications, which is opposed to the Shamir's original proposal that the service of the PKG is limited to issue private keys. The original purpose of "distributed PKGs" is to prevent a single dishonest PKG possessing the users' private key, rather than to distribute a user's private key. Libert and Quisquater [18] proposed a somewhat different method where one PKG plays a role as a dealer. However, the PKGs in such schemes are still involved in particular applications.

Until very recently, Baek and Zheng [1] suggested a new approach for ID-based threshold decryption in which the private key associated with an identity rather than the master key of PKG is shared. Moreover, they [2] first proposed an ID-based threshold signature scheme without distributed PKGs. However, it still suffers the problem of private key escrow as the traditional ID-based systems. Though the scheme [2] can incorporate the distributed PKGs techniques to solve the key escrow problem, we argue that using distributed PKGs will

increase the communication and computation cost of the systems. To the best of our knowledge, there seems no ID-based threshold signature scheme without distributed PKGs which simultaneously overcomes the problem of key escrow and adopts the approach that the private key associated with an identity rather than the master key of PKG is shared.

Recently, a novel ID-based signature without the trusted PKG from bilinear pairings [10] is proposed. There is only one PKG who is not assumed to be trusted in the systems, which combines the advantages of both CA-based systems (no key escrow) and ID-based systems (no certificate) while removing their disadvantages. However, it seems difficult to extend the signature scheme to a threshold one. In this paper we propose another ID-based signature scheme without the trusted PKG from bilinear pairings. Moreover, we extend it to an ID-based threshold signature scheme without distributed PKGs which overcomes the problem of key escrow. Meanwhile, we adopt the approach that the private key associated with an identity rather than the master key of PKG is shared in the proposed scheme.

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. Our new ID-based signature scheme from bilinear pairings is given in Section 3. The proposed ID-based threshold signature scheme is given in Section 4 and the analysis of our scheme is given in Section 5. Finally, concluding remarks will be made in Section 6.

2 Preliminaries

In this Section, we will briefly describe the basic definition and properties of bilinear pairings and gap Diffie-Hellman group. We also introduce ID-based public key setting and a knowledge proof for the equality of two discrete logarithm from bilinear pairings.

2.1 Bilinear Pairings

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group of the same order q. Let a and b be elements of Z_q^*. We assume that the discrete logarithm problem (DLP) in both G_1 and G_2 is hard. A bilinear pairing is a map $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:

1. Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$;
2. Non-degenerate: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$;
3. Computable: For all $P, Q \in G_1$, there is an efficient algorithm to compute $e(P, Q)$.

2.2 Gap Diffie-Hellman Group

Let G_1 be a cyclic additive group generated by P with the prime order q. Assume that the inversion and multiplication in G_1 can be computed efficiently. We introduce the following problems in G_1.

1. Discrete Logarithm Problem (DLP): Given two elements P and Q, to find an integer $n \in Z_q^*$, such that $Q = nP$ whenever such an integer exists.
2. Computation Diffie-Hellman Problem (CDHP): Given P, aP, bP for $a, b \in Z_q^*$, to compute abP.
3. Decision Diffie-Hellman Problem (DDHP): Given P, aP, bP, cP for $a, b, c \in Z_q^*$, to decide whether $c \equiv ab \bmod q$.

We call G_1 a gap Diffie-Hellman group if DDHP can be solved in polynomial time but there is no polynomial time algorithm to solve CDHP with non-negligible probability. Such group can be found in supersingular elliptic curve or hyperelliptic curve over finite field, and the bilinear pairings can be derived from the Weil or Tate pairings. For more details, see [4, 7, 12, 17].

In the following we always define G_1 be a gap Diffie-Hellman group of prime order q, G_2 be a cyclic multiplicative group of the same order q and a bilinear pairing $e : G_1 \times G_1 \to G_2$.

2.3 ID-based Setting from Bilinear Pairings

The ID-based public key systems allow some public information of the user such as name, address and email *etc.*, rather than an arbitrary string to be used his public key. The private key of the user is calculated by PKG and sent to the user via a secure channel.

ID-based public key setting from bilinear pairings can be implemented as follows:

- **Setup:** PKG chooses a random number $s \in Z_q^*$ and set $P_{pub} = sP$. Define a cryptographic hash function $H_2 : \{0,1\}^* \to G_1$. The center publishes system parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H_2\}$, and keep s as the *master-key*, which is known only himself.
- **Extract:** A user submits his/her identity information ID to PKG. PKG computes the user's public key as $Q_{ID} = H_2(ID)$, and returns $S_{ID} = sQ_{ID}$ to the user as his/her private key.

2.4 ID-based Knowledge Proof for the Equality of Two Discrete Logarithm from Bilinear Pairings

A prover with possession a secret number $\beta \in Z_q$ wants to show that $\log_g u = \log_h v$ while without exposing β, where $u = g^\beta$, $v = h^\beta$. Chaum and Pedersen [8] first proposed an interactive protocol to solve this problem. Motivated by this idea, Baek and Zheng [1, 2] construct a new ID-based knowledge proof for the equality of two discrete logarithm from bilinear pairings.

Define $g = e(P, Q_{ID})$, $u = e(P_{pub}, Q_{ID})$, $h = e(L, Q_{ID})$ and $v = e(L, S_{ID})$, where P and L are independent points of G_1. The following protocol presents a knowledge proof of that $\log_g u = \log_h v$. An interesting property of this proof is that even the prover does not know the discrete logarithm $\log_g u = \log_h v$ (just be convinced that it equals to the master-key s of the PKG), which is different

from the previous protocols. With the notation of [5], $< g, h, u, v >$ is called a Diffie-Hellman tuple.

- The prover randomly chooses an element Q in G_1 and computes $a = e(P, Q)$, $b = e(L, Q)$. The prover sends (a, b) to the verifier.
- The verifier randomly chooses an integer $c \in Z_q$ and sends c to the prover.
- The prover computes $S = Q + cS_{ID}$ and sends S to the verifier.
- The verifier checks whether $e(P, S) = au^c$ and $e(L, S) = bv^c$. If both the equations hold, returns "*accept*"; else, returns "*reject*".

As claimed in [1, 2], the above protocol can be easily converted a non-interactive knowledge proof:

- The prover randomly chooses an element Q in G_1 and computes $a = e(P, Q)$, $b = e(L, Q)$.
- Let $c = H(a, b, h, v)$, the prover computes $S = Q + cS_{ID}$ and sends (a, b, S) to the verifier.
- The verifier computes $c = H(a, b, g, h)$ and checks whether $e(P, S) = au^c$ and $e(L, S) = bv^c$. If both the equations hold, returns "*accept*"; else, returns "*reject*".[1]

3 New ID-based Signature Scheme without Trusted PKG

In this section, we first present our new ID-based key setting from bilinear pairings, and then propose a concrete signature scheme without the trusted PKG to solve the problem of key escrow, *i.e.*, we do not use the distributed PKGs in our system and the single PKG is assumed no longer to be a trusted party.

Define three cryptographic hash functions $H_1 : \{0,1\}^* \times G_1 \rightarrow G_1$, $H_2 : \{0,1\}^* \rightarrow G_1$ and $H_3 : {G_2}^4 \rightarrow Z_q$.

3.1 New ID-based Public Key Setting from Bilinear Pairings

[**Setup**]

PKG chooses a random $s \in Z_q^*$ and sets $P_{pub} = sP$. The public parameters of the system are $params = \{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3\}$. PKG keeps s secretly as the *master-key*.

[**Extract**]

A user submits his (or her) identity information ID and authenticates himself (or herself) to PKG. The user then randomly chooses an integer $r \in Z_q^*$ as his

[1] The prover also can send (c, S) to the verifier. The verifier computes $a' = e(P, S)/u^c$, $b' = e(L, S)/v^c$ and $c' = H(a', b', h, v)$. If $c = c'$, the verifier accepts the proof; else reject the proof. Therefore, the length of proof is decreased.

long-term private key and sends rP to PKG. PKG computes $S_{ID} = sQ_{ID} = sH_1(ID||t, rP)$ and sends it to the user via a secure channel, where t is the life span of r. The user's private key pair are S_{ID} and r and the public key is ID.

The user should update his key pair after period of t. For the sake of simplicity, we do not discuss this problem here.

3.2 New ID-based Signature Scheme from Bilinear Pairings

Chen *et al.* [10] have proposed an ID-based signature scheme without the trusted PKG based on Cha and Cheon's signature scheme [7]. But it is unsuitable for designing threshold signature scheme. Here we propose a new ID-based signature scheme without the trusted PKG and then extend it to a threshold scheme.

[**Signing**]

Suppose that the message to be signed is m and the signer's identity is ID.

- The signer computes $T = rH_2(m)$.
- The signer computes $v = e(H_2(m), S_{ID})$.
- Let $g = e(P, Q_{ID})$, $u = e(P_{pub}, Q_{ID})$ and $h = e(H_2(m), Q_{ID})$, the signer proves that (g, h, u, v) is a Diffie-Hellman tuple by using a non-interactive knowledge proof for the equality of two discrete logarithm. Let the proof be $(a = e(P, Q), b = e(H_2(m), Q), S = Q + cS_{ID})$, where Q is a randomly chosen element in G_1 and $c = H_3(a, b, h, v)$.

Then (T, v, rP) and the corresponding proof (a, b, S) is the signature of the message of m.

[**Verification**]

The verifier computes $Q_{ID} = H_1(ID||t, rP)$, $h = e(H_2(m), Q_{ID})$, $u = e(P_{pub}, Q_{ID})$, $c = H_1(a, b, h, v)$. He accepts the signature if the following equations hold:

$$e(T, P) = e(H_2(m), rP)$$
$$e(P, S) = au^c,\ e(H_2(m), S) = bv^c$$

3.3 Security Analysis of Our Scheme

Theorem 1. *The proposed ID-based signature scheme reaches Girault's trusted level 3.*

Proof. Suppose PKG wants to impersonate an honest user whose identity information is ID. He can do as follows:

- PKG randomly chooses $r' \in Z_q^*$ and computes $S_{ID'} = sH_1(ID||t, r'P)$.
- He then performs the above signing protocol for the message m.

– Output $(T', v', r'P, a', b', S')$.

Because $e(T', P) = e(H_2(m), r'P)$, $e(P, S') = a'u'^c$, and $e(H_2(m), S') = b'v'^c$, where $u' = e(P_{pub}, Q'_{ID})$, $c = H_3(a', b', e(H_2(m), Q'_{ID}), v')$, and $Q'_{ID} = H_1(ID||t, r'P)$, PKG successfully forged a "valid" signature of the target user for the message m.

However, the user can provide a proof to convince that the signature is forged by PKG, which is similar to CA-based systems.[2] He first sends rP to the arbiter, and then provides a "knowledge proof" that he knows $S_{ID} = sH_1(ID||t, rP)$: the arbiter randomly chooses a secret integer $a \in Z_q$ and sends aP to the user; the user then computes $e(S_{ID}, aP)$. If the equation $e(S_{ID}, aP) = e(H_1(ID||t, rP), P_{pub})^a$ holds, *i.e.*, identity ID corresponds to rP and $r'P$ for a same period t, the arbiter deduces that PKG is dishonest because the *master-key* s is only known to him.

Therefore, our scheme reaches Girault's trusted lever 3 [16], *i.e.*, the authority does not know the private key of the users, and it can be proven that the authority generates false witness if he does so. □

Theorem 2. *In the random oracle, our signature scheme is existentially unforgeable against adaptively chosen message and ID attacks under the assumption of CDHP in G_1 is intractable.*

Proof. In our scheme, the partial signature T is the "real" signature of the user for the message. The knowledge proof (a, b, S) and v can be used to convince the verifier that rP correspondences to ID for the period t. We consider the following two kinds of adversaries:

Case 1: Active Adversary

Since PKG is not a trusted party, we consider that an active adversary can collude with PKG. For a randomly chosen target user whose identity is ID. The adversary can know the target user's long-term public key rP and partial private key S_{ID} from PKG. So, it is trivial for the adversary to generate v and the proof (a, b, S) for any message. If he can compute the corresponding V for a message m, he can successfully forge a signature of the user for the message m. We consider the following game:

Suppose the adversary can query to H_2 adaptively at most k times. Suppose the i-th input of query is m_i and he gets the corresponding signature T_i, here $1 \leq i \leq k$. Finally, he outputs a new pair (m, T). We say that the adversary wins the game if m is not queried and $e(T, P) = e(H_2(m), rP)$.

If there exists an algorithm $\mathcal{A}_0$ for an adaptively chosen message attack to our scheme with a non-negligible probability, we can construct an algorithm $\mathcal{A}_1$ as follows:

[2] In the CA-based systems, CA also can forge a user's certificate and impersonate the user to communicate with others. However, the user can accuse the dishonest CA because there exist his two different "valid" certificates issued by the same CA.

– choose an integer $u \in \{1, 2, \cdots, k\}$. Define $\mathbf{Sign}(H_2(m_i)) = T_i$.
– For $i = 1, 2, \cdots, k$, $\mathcal{A}_1$ responds to $\mathcal{A}_0$'s queries to H_2 and **Sign**, while for $i = u$, $\mathcal{A}_1$ replaces m_u with m.
– $\mathcal{A}_0$ outputs (m_{out}, V_{out}).
– If $m_{out} = m$ and the signature T is valid, $\mathcal{A}_1$ outputs (m, T). Otherwise, outputs *Fail*.

Note that u is randomly chosen, $\mathcal{A}_0$ knows nothing from the queries result. Also, since H_2 is a random oracle, the probability that the output of $\mathcal{A}_0$ is valid without query of $H_2(m)$ is negligible. Let $H_2(m) = eP$, we obtain $T = reP$ from P, rP and eP, *i.e.*, we solved CDHP in G_1.

Actually, V can be regarded as the short signature of the message m and $(P, rP, H_2(m), T)$ is a valid Diffie-Hellman tuple. We know that the probability of the adversary can successfully forge a valid signature is negligible. For more details, see reference [5].

Case 2: Passive Adversary

A passive adversary cannot collude with the PKG. In this case, for a target user whose identity is ID, the adversary cannot know the information of $S_{ID} = sH_1(ID||t, rP)$(*i.e.*, a "certificate" in CBE scheme [15]) from PKG. In the following we will prove that his success probability of forgery of a valid signature is negligible, which is similar to Cha-Cheon's proof [7].

As we mentioned above, an identity ID only corresponds to one unique rP for a period of time t, so (ID, rP) can be extracted at most once. Define q_{H_1} is the maximum number of queries to H_1. If there exists an algorithm $\mathcal{A}_0$ for an adaptively chosen message and ID attack to our scheme with a non-negligible probability, we can construct an algorithm $\mathcal{A}_1$ as follows:

– choose an integer $u \in \{1, 2, \cdots, q_{H_1}\}$. Define (ID_i, r_iP) the i-th input of query H_2.
– $\mathcal{A}_1$ responds to $\mathcal{A}_0$'s queries to H_1, H_2, H_3, **Extract**, and **Signing**, while for $i = u$, $\mathcal{A}_1$ replaces ID_u, r_uP with ID, rP.
– $\mathcal{A}_0$ outputs $(ID_{out}, r_{out}P, m, T, v, a, b, S)$.
– If $ID_{out} = ID$ and the signature is valid, $\mathcal{A}_1$ outputs $(ID, rP, m, T, v, a, b, S)$. Otherwise, outputs *Fail*.

Note that u is randomly chosen, $\mathcal{A}_0$ knows nothing from the queries result. Also, since H_1, H_2 and H_3 are random oracles, the probability that the output of $\mathcal{A}_0$ is valid without query of $H_1(ID||t, rP)$ is negligible. So, $\mathcal{A}_1$ can be used for an adaptively chosen message and given ID attack to our scheme with a non-negligible probability. We then use $\mathcal{A}_1$ to construct an algorithm $\mathcal{A}_2$ to solve CDHP in G_1:

– Given P, sP, lP and let $P_{pub} = sP$. Choose integers $x_i \in Z_q$ and let (ID_i, r_iP) the i-th input of query H. Define

$$H(ID_i||t, r_iP) = \begin{cases} lP, & \text{if } \ ID_i = ID \\ x_iP, & \text{otherwise} \end{cases}$$

– $\mathcal{A}_2$ responds to $\mathcal{A}_1$'s queries to H_1, H_2, H_3, **Extract**, and **Signing**.
– If $\mathcal{A}_1$ outputs a valid message-signature pair $(ID, rP, m, T, v, a, b, S)$, $\mathcal{A}_2$ then replays with the same random tape but a different choice of H_3, for example H_3'. $\mathcal{A}_2$ outputs two valid message-signature pairs $(ID, rP, m, T, v, a, b, S)$ and $(ID, rP, m, T, v, a, b, S')$.

Note that $S = Q + cS_{ID}$ and $S' = Q + c'S_{ID}$, we have $S_{ID} = (c - c')^{-1}(S - S')$. Therefore, we can obtain $S_{ID} = slP$ from P, sP and lP, *i.e.*, we solved CDHP in G_1. □

4 ID-based Threshold Signature Scheme without Trusted PKG from Bilinear Pairings

Although the scheme [2] can incorporate the distributed PKGs, we argue that it will decrease the efficiency of the scheme to solve the key escrow problem by using distributed PKGs. In the following, based on the approach that the private key associated with an identity rather than the master key of PKG is shared, we propose an ID-based threshold signature scheme without distributed PKGs which overcomes the key escrow problem.

Private Key Distribution : *The public key setting is the same as above. Suppose the private key of the user with identity ID is r and S_{ID}. He distributes his private key to n servers as follows:*

– Chooses $a_i \in_R Z_q$ and $R_i \in_R G_1$ for $1 \leq i \leq t-1$.
– Let

$$h(x) = r + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$$

$$H(x) = S_{ID} + xR_1 + x^2 R_2 + \cdots + x^{t-1} R_{t-1}$$

Computes the distributed private key $h(i) = r_i$, $H(i) = S_i$ and the corresponding verification key $l_i = r_i P$, $u_i = e(P, S_i)$ and then sends them to server Γ_i for $1 \leq i \leq n$. Note that $h(x) = \sum_{j \in \Phi} c_{xj}^{\Phi} r_j$ and $H(x) = \sum_{j \in \Phi} c_{xj}^{\Phi} S_j$, where $c_{xj}^{\Phi} = \prod_{l \in \Phi, l \neq j} \frac{x-l}{j-l}$, $\Phi \subset \{1, 2, \cdots, n\}$ be a set and $|\Phi| \geq t$.
– The server Γ_i verifies the validity of l_i, u_i and publishes them while keeps r_i, S_i secret.

Signing : *Each of $\{\Gamma_j\}_{j \in \Phi}$ performs the following to jointly create a signature for a message m.*

– Computes and broadcasts $T_j = r_j H_2(m)$.
– Computes and broadcasts $v_j = e(H_2(m), S_j)$.
– Computes and broadcasts $a_j = e(P, Q_j), b_j = e(H_2(m), Q_j)$, where Q_j is a randomly chosen element in G_1.
– Computes $a = \prod_{j \in \Phi} a_j^{c_{0j}^{\Phi}}$, $b = \prod_{j \in \Phi} b_j^{c_{0j}^{\Phi}}$, $v = \prod_{j \in \Phi} v_j^{c_{0j}^{\Phi}}$.
– Broadcasts $W_j = Q_j + cS_j$, where $c = H(a, b, h, v)$ and $h = e(H_2(m), Q_{ID})$.

– Each server $i \in \Phi$ checks whether $e(T_j, P) = e(H_2(m), l_j)$, $e(P, W_j) = a_j u_j^c$ and $e(H_2(m), W_j) = b_j v_j^c$ for $j \in \Phi$ and $j \neq i$. If the equations fails for some j, then broadcasts **Complaint** against server j.
– If all the servers are honest, computes $T = \sum_{j \in \Phi} c_{0j}^{\Phi} T_j$, $S = \sum_{j \in \Phi} c_{0j}^{\Phi} W_j$.

Then (T, v, rP) and the corresponding proof (a, b, S) is the signature of the message of m.

Verification : *The verifier first computes* $Q = H_2(ID, rP)$, $h = e(H_2(m), Q_{ID})$, $u = e(P_{pub}, Q_{ID})$, $c = H_1(a, b, h, v)$. *He accepts the signature if the following equations hold:*

$$e(T, P) = e(H_2(m), rP)$$

$$e(P, S) = au^c, \ e(H_2(m), S) = bv^c$$

5 Analysis of Our Threshold Signature Scheme

5.1 Correctness

Note that

$$T = \sum_{j \in \Phi} c_{0j}^{\Phi} T_j = \sum_{j \in \Phi} c_{0j}^{\Phi} r_j H_2(m) = rH_2(m)$$

$$S = \sum_{j \in \Phi} c_{0j}^{\Phi} W_j = \sum_{j \in \Phi} c_{0j}^{\Phi} (Q_j + cS_j)$$

Therefore, we have

$$e(T, P) = e(H_2(m), rP)$$

$$\begin{aligned} e(P, S) = &\ e(P, \sum_{j \in \Phi} c_{0j}^{\Phi} (Q_j + cS_j)) = e(P, \sum_{j \in \Phi} c_{0j}^{\Phi} Q_j + c \sum_{j \in \Phi} c_{0j}^{\Phi} S_j) \\ = &\ e(P, \sum_{j \in \Phi} c_{0j}^{\Phi} Q_j) e(P, S_{ID})^c = au^c \end{aligned}$$

and

$$\begin{aligned} e(H_2(m), S) = &\ e(H_2(m), \sum_{j \in \Phi} c_{0j}^{\Phi} (Q_j + cS_j)) = e(H_2(m), \sum_{j \in \Phi} c_{0j}^{\Phi} Q_j + c \sum_{j \in \Phi} c_{0j}^{\Phi} S_j) \\ = &\ e(H_2(m), \sum_{j \in \Phi} c_{0j}^{\Phi} Q_j) e(H_2(m), S_{ID})^c = bv^c \end{aligned}$$

5.2 Robustness

Theorem 3. *The proposed ID-based threshold signature scheme is robust, i.e., the scheme outputs correctly even in the presence of a malicious adversary that makes the corrupted servers deviate from the normal execution.*

Proof. The robustness of "Private Key Distribution" is trivial for each servers can validate his private key share using the published verification key share.

In the "Signing" protocol, if all the following equations hold, the server Γ_j is sure not to be corrupted by a malicious adversary: $e(T_j, P) = e(H_2(m), l_j)$, $e(P, W_j) = a_j u_j^c$ and $e(H(m), W_j) = b_j v_j^c$. □

5.3 Security

Motivated by Gennaro *et al*'s idea for proving the security of the threshold DSS signature scheme, Baek and Zheng [2] defined "**Simulatability**" of the ID-based threshold signature and proved the relationship between the security of ID-based threshold signature and that of ID-based signature.

Definition 1. *An ID-based threshold signature scheme is said to be* simulatable *if the following conditions hold.*

1. "Private Key Distribution" is simulatable: Given the system parameters params and the identity ID, there exists a simulator which can simulate the view of the adversary on an execution of "Private Key Distribution".
2. "Signing" is simulatable: Given the system parameters params the identity ID, the message m, the corresponding signature σ, $t-1$ private key shares and the corresponding verification key shares, there is a simulator which can simulate the view of the adversary on an execution of " Signing".

Theorem 4. *If an ID-based threshold signature scheme is simulatable and the ID-based signature is secure in the sense of unforgeability, then the ID-based threshold signature scheme is also secure in the sense of unforgeability.*

Therefore, we only need to prove our ID-based threshold signature scheme is simulatable.

Lemma 1. *The proposed ID-based threshold signature scheme is simulatable.*

Proof. (sketch) Without loss of generality, we assume that the servers corrupted by the adversary are Γ_i, where $1 \leq i \leq t-1$. Firstly we prove "Private Key Distribution" is simulatable. Given the system parameters *params* and the identity ID, the adversary computes $u = e(P_{pub}, Q_{ID})$. Note that $u = \prod_{j=1}^{t} u_i^{c_{0j}^{\Phi}}$, so the adversary can compute $u(t)$ and the simulated value $u(t)$ is correct and identically to the Γ_t as the real execution of the "Private Key Distribution". Similarly, the simulated value $r_t P$ can be generated correctly.

Then we prove "Signing" is simulatable. Given the system parameters *params* the identity ID, the message m, the corresponding signature $\sigma = (T, v, rP, a, b, S)$,

$t-1$ private key shares (r_i, S_i) and the corresponding verification key shares $(r_iP, e(P, S_i))$. The adversary computes $T_i = r_iH_2(m)$. Let $H(x)$ be a polynomial like function of degree $t-1$ such that $H(0) = T$ and $H(i) = T_i$ for $1 \leq i \leq t-1$. The adversary can compute and broadcast $T(i) = H(i)$ for $t \leq i \leq n$. Similarly, the adversary computes and broadcasts v_i, a_i, b_i, W_i for $t \leq i \leq n$. □

With Theorem 2, Theorem 4 and Lemma 1, we can prove the following:

Theorem 5. *The proposed ID-based threshold signature scheme is secure in the sense of unforgeability.*

6 Concluding Remarks

In this paper, we propose a new ID-based signature scheme without trusted PKG. In our scheme, there is only one PKG who is not assumed to be trusted. We argue that the proposed scheme combines the advantages of both ID-based systems and CA-based systems. We then extend it to be an ID-based threshold signature scheme, which simultaneously overcomes the problem of key escrow and adopts the approach that the private key associated with an identity rather than the master key of PKG is shared. Our scheme is superior to those schemes with distributed PKGs in terms of both the communication and computation complexity.

Acknowledgement

The authors are grateful to the Joonsang Baek for his valuable suggestions and comments to this paper.

References

1. J. Baek and Y. Zheng, *Identity-based threshold decryption*, PKC 2004, LNCS 2947, pp.248-261, Springer-Verlag, 2004.
2. J. Baek and Y. Zheng, *Identity-based threshold signature scheme from the bilinear pairings*, IAS'04 track of ITCC'04, pp.124-128, IEEE Computer Society, 2004.
3. P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, *Efficient algorithms for pairings-based cryptosystems*, Advances in Cryptology-Crypto 2002, LNCS 2442, pp.354-368, Springer-Verlag, 2002.
4. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairings*, Advances in Cryptology-Crypto 2001, LNCS 2139, pp.213-229, Springer-Verlag, 2001.
5. D. Boneh, B. Lynn, and H. Shacham, *Short signatures from the Weil pairings*, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.514-532, Springer-Verlag, 2001.
6. M. Cerccedo, M. Matsumoto and H. Imai, *Efficient and secure multiparty feneration of digital signatrues based on discrete logarithms*, IEEE Trans. Fundamentals., Vol. E76-A, pp.532-545, 1993.

7. J.C. Cha and J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups*, PKC 2003, LNCS 2567, pp.18-30, Springer-Verlag, 2003.
8. D. Chaum and T.P. Pedersen, *Wallet databases with observers*, Advances in Cryptology-Crypto 1992, LNCS 740, pp.89-105, Springer-Verlag, 1993.
9. L. Chen and C. Kudla, *Identity based authenticated key agreement from pairingss*, Cryptology ePrint Archive, Report 2002/184.
10. X. Chen, F. Zhang, K. Kim, *A new ID-based group signature scheme from bilinear pairings*, Cryptology ePrint Archive, Report 2003/116.
11. G.Frey and H. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Mathematics of Computation, Vol.62, pp.865-874, 1994.
12. S.D. Galbraith, K. Harrison, and D. Soldera, *Implementing the Tate pairings*, ANTS 2002, LNCS 2369, pp.324-337, Springer-Verlag, 2002.
13. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, *Robust threshold DSS signatures*, Advances in Cryptology-Eurocrypt 1996, LNCS 1070, pp.354-371, Springer-Verlag, 1996.
14. C. Gentry and A. Siverberg, *Hierarchical ID-based cryptography*, Advances in Cryptology-Asiacrypt 2002, LNCS 2501, pp.548-566, Springer-Verlag, 2002.
15. C. Gentry, *Certificate-based encryption and the certificate revocation problem*, Advances in Cryptology-Eurocrypt 2003, LNCS 2656, pp.272-293, Springer-Verlag, 2003.
16. M. Girault, *Self-certified public keys*, Advances in Cryptology-Eurocrypt 1991, LNCS 547, pp.490-497, Springer-Verlag, 1991.
17. F. Hess, *Efficient identity based signature schemes based on pairings*, SAC 2002, LNCS 2595, Springer-Verlag, pp.310-324, 2002.
18. B. Libert and J. Quisquater, *Efficient revocation and threshold pairing based cryptosystems*, PODC 2003, ACM Press, pp.163-171, 2003.
19. A. Menezes, T. Okamoto and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transaction on Information Theory, Vol.39, pp.1639-1646, 1993.
20. K.G. Paterson, *ID-based signatures from pairingss on elliptic curves*, Electron. Lett., Vol.38, No.18, pp.1025-1026, 2002.
21. A. Shamir, *How to share a secret*, Communications of the ACM, Vol.22, pp.612-613, 1979.
22. A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in Cryptology-Crypto 1984, LNCS 196, pp.47-53, Springer-Verlag, 1984.
23. N.P. Smart, *An identity based authenticated key agreement protocol based on the Weil pairings*, Electron. Lett., Vol.38, No.13, pp.630-632, 2002.
24. D. Stinson and R. Strobl, *Provably secure distributed Schnorr signatures and a (t,n) threshold scheme for implicit certificate*, ACISP 2001, LNCS 2119, pp.417-434, Springer-Verlag, 2001.
25. F. Zhang and K. Kim, *ID-based blind signature and ring signature from pairings*, Advances in Cryptology-Asiacrypt 2002, LNCS 2501, pp.533-547, Springer-Verlag, 2002.