Identity-Based Signature and Key-Insulated Threshold Signature

Jin Li[1] and Fangguo Zhang[2]

[1] School of Mathematics and Computational Science, Sun Yat-sen University
Guangzhou, 510275, P.R.China
[2] Department of Electronics and Communication Engineering
Sun Yat-Sen University, Guangzhou, 510275, P.R.China

Abstract. Identity-based (simply ID-based) cryptosystem was proposed in order to simplify key management procedures of certificate-based public key infrastructures. In 2003 Sakai and Kasahara proposed a new ID-based encryption scheme (SK-IBE). In our paper, it is intended to build a new ID-based signature (IBS) scheme which shares the same system parameters with SK-IBE. SK-IBE and our signature scheme yield a new complete ID-based public key cryptosystem. The proposed signature scheme is provably secure against existential forgery for adaptive chosen message and identity attack in the random oracle model based on a reasonably well-explored hardness assumption. Another contribution of this paper is that we first propose the notion of key-insulated threshold signature and present a generic method for constructing key-insulated threshold signature scheme.

Keywords: ID-based Signature, Bilinear Pairings, Key-Insulated Threshold Signature

1 Introduction

In a certificate-based public key system, before using the public key of a user, the participants must verify the certificate of the user at first. As a consequence, this system requires a large storage and computing time to store and verify each user's public key and the corresponding certificate. In order to simplify key management procedures of certificate-based public key infrastructures (PKIs), Shamir [20] introduced the concept of ID-based cryptosystem in 1984. In such cryptosystem, the public key of a user is derived from his identity information and his private key is generated by a trusted third party called Private Key Generator (PKG). Since then, several ID-based encryption schemes and signature schemes [21-23] have been proposed based on the integer factorization and discrete logarithm problem. Recently, Boneh and Franklin [4] proposed the first practical ID-based encryption scheme based on bilinear maps on elliptic curves. Subsequently, many cryptographic schemes have been proposed motivated by [4], such as ID-based signature schemes [6,8,13,16,18], Boyen's ID-based signcryption signature scheme [5]. These protocols have a very similar private key extraction

algorithm, in which an identity string is mapped to a point (maptopoint) on an elliptic curve and then the corresponding private key is computed by multiplying the mapped point with the master private key. In 2003 Sakai and Kasahara proposed a new ID-based encryption scheme (SK-IBE) [18]. Security proof of SK-IBE has been given by Chen and Cheng [7] recently at CRYPTOGRAPHY AND CODING 2005. The new IBE scheme using another identity-based key extraction algorithm, which requires much simpler hashing and therefore improves performance. More specially, it maps an identity to an element $\mathbb{Z}_q^*$ instead of a point on an elliptic curve.

Our Contributions. This work is intended to build a new ID-based signature scheme (IBS) which shares the same system parameters with SK-IBE. Combining our signature scheme with the SK-IBE yields a new complete ID-based public key cryptosystem. We show the new scheme is provably secure in the secure ID-based signature model given by [2,6], in which they gave a definition of security for ID-based signature schemes called security against existential forgery on adaptively chosen message and ID attacks. The new ID-based signature scheme has several attractive advantages such as it is very efficient and it only requires the conventional hash function, instead of the maptopoint hash function.

Another contribution of this paper is that the notion of key-insulated threshold signature is first proposed, which provides benefits over key-insulated signature and threshold signature in terms of security. Furthermore, we give a generic method for constructing key-insulated threshold signature scheme. Key-insulated public key cryptosystem [10] was proposed to mitigate the damage of secret key exposure. The secret key associated with a public key is here shared between the user and a physically-secure device: The master key is stored on a physically-secure device and a temporary secret key used to perform cryptographic operations is stored in an insecure device and updated regularly with the help of a physically-secure device that stores a master key. An adversary compromises the insecure device for some periods cannot break the remaining time periods.

Organization. The next section briefly explains the bilinear pairing and some problems related to pairings. Section 3 gives the new ID-based signature scheme. section 4 is the exact security proof and efficiency analysis of the new scheme. Definition and generic constructing method of key-insulted threshold signature is given in section 5. The paper ends with some concluding remarks.

2 Preliminary

Let $\mathbb{G}_1$ be a cyclic additive group generated by P, whose order is a prime q, and $\mathbb{G}_2$ be a cyclic multiplicative group with the same order q. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a map with the following properties:

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$; $a, b \in_R \mathbb{Z}_q^*$;
2. Non-degeneracy: There exists $P, Q \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$, in other words, the map does not send all pairs in $\mathbb{G}_1 \times \mathbb{G}_1$ to the identity in $\mathbb{G}_2$;

3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

Now we describe some underlying mathematical problems in $\mathbb{G}_1$.

- Discrete Logarithm Problem (DLP): Given two group elements P and Q, find an integer n, such that $Q = nP$ whenever such an integer exists.
- Decision Diffie-Hellman Problem (DDHP): For $a, b, c \in_R \mathbb{Z}_q^*$, given P, aP, bP, cP, decide whether $c \equiv ab \ mod \ q$;
- Computational Diffie-Hellman Problem (CDHP): For $a, b \in_R \mathbb{Z}_q^*$, given P, aP, bP, compute abP.

A Gap Diffie-Hellman (GDH) group is a group in which the DDHP is easy, but the CDHP is hard. Such groups can be found on supersingular elliptic curves or hyperelliptic curves over finite field. We can refer to [4, 6] for more details.

Definition 1. (k-CAA Assumption) *For an integer k, and $x \in_R \mathbb{Z}_q$, $P \in \mathbb{G}_1$, given P, xP, $h_1, \cdots, h_k \in \mathbb{Z}_q$, $\frac{1}{h_1+x}P, \cdots, \frac{1}{h_k+x}P$, it is hard to output a pair $(h, \frac{1}{h+x}P)$ for some $h \notin \{h_1, \cdots, h_k\}$.*

As stated in [3], k-CAA is actually a weaker version of Strong Diffie-Hellman (SDH) problem, i.e., if there exists a polynomial time algorithm to solve k-CAA problem, then there exists a polynomial time algorithm to solve $k+1$-SDH problem. For more detail analysis we can refer reader to [3, 24].

3 The New ID-based Signature Scheme

3.1 Definition of ID-based Signature

We recall here the definition introduced in [6] for identity based signature:

1. Setup: is a probabilistic algorithm run by a private key generator (PKG) that takes as input a security parameter 1^k and outputs a key pair (P_{pub}, sk). P_{pub} is its public key and sk is its master key that is kept secret.
2. Extract: is a key generation algorithm run by the PKG on input of a master key sk and a user's identity ID to return the user's private key S_{ID}.
3. Sign: is a probabilistic algorithm takes as input a message m, the user's private key S_{ID} and some random numbers to output a signature σ.
4. Vrfy: is a deterministic algorithm that takes as input a signature σ, message m and an ID. Output 1 if it is a valid signature. Otherwise, output 0.

3.2 Security Model

Cha-Cheon [6] first gave the security model of an ID-based signature against existential forgery on adaptively chosen message and ID attack, which is defined through the following game between a challenger $\mathcal{B}$ and an adversary $\mathcal{A}$:

1. $\mathcal{B}$ runs Setup of the scheme. The resulting parameters are sent to $\mathcal{A}$.
2. $\mathcal{A}$ issues the following queries:

- Extract query. Given an identity ID for extraction query, $\mathcal{B}$ returns the private key corresponding to ID which is obtained by running algorithm Extract.
- Sign query. Given an identity ID and a message m for ID-based signature query, $\mathcal{B}$ returns a signature which is obtained by running algorithm Sign.

3. Finally, $\mathcal{A}$ outputs (ID, m, σ), where ID is an identity, m is a message, and σ is a signature, such that ID and (ID, m) are not equal to the inputs of any query to Extract and Sign, respectively. A wins the game if σ is a valid signature of m for ID.

Definition 2. (Exact security of ID-based signatures) *A forger $\mathcal{F}$ is said to $(t, q_H, q_E, q_S, \epsilon)$-break the ID-based signature scheme $S =< Setup, Extract, Sign, Vrfy >$ via an adaptive chosen message attack and ID attack if after at most q_H queries to the hash oracle, q_E private key extraction queries, q_S signatures queries and t processing time, it outputs a valid forgery with probability at least ϵ. An ID-based signature scheme S is $(t, q_H, q_E, q_S, \epsilon)$-secure if there is no forger who $(t, q_H, q_E, q_S, \epsilon)$-breaks the scheme.*

3.3 The Scheme

Let $\mathbb{G}_1$ be a cyclic additive group generated by P, whose order is a prime q, $\mathbb{G}_2$ be a cyclic multiplicative group of the same order q. A bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Define two hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q$ and $H_2 : \{0,1\}^* \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q$. The proposed ID-based signature scheme includes the following four procedures.

Setup: PKG chooses a random number $s \in \mathbb{Z}_q^*$ and sets $P_{pub} = sP$. The public parameters of the systems are $params = \{\mathbb{G}_1, \mathbb{G}_2, e, q, P, P_{pub}, H_1, H_2\}$. PKG keeps s secret as the master key.

Extract: Given an identity ID for private key extraction, the PKG computes $S_{ID} = \frac{1}{s+H_1(ID)}P$ as the corresponding private key for ID.

Sign: Given a secret key S_{ID} and a message m, select $r \in_R \mathbb{Z}_q^*$ and output a signature (U, V), where $U = rP$ and $V = (r + H_2(m, U))S_{ID}$.

Vrfy: To verify a signature (U, V) of a message m for an identity ID, check whether $e(V, P_{pub} + H_1(ID)P) = e(U + H_2(m, U)P, P)$. If the equality holds, the result is valid; otherwise, the result is invalid.

The signature consists of two elements in $\mathbb{G}_1$. In practice, the size of the element in $\mathbb{G}_1$ (elliptic curve group or hyperelliptic curve Jacobians) can be reduced by a factor of 2 with compression techniques.

4 Proposed Scheme Analysis

4.1 Correctness

Correctness is easily proved as follows: If (U, V) is a valid signature of a message m for an identity ID, then $U = rP$ and $V = (r+H_2(m,U))S_{ID}$ for $r \in_R \mathbb{Z}_q^*$. Thus the verification of the ID-based signature is justified by the following equations:

$$\begin{aligned} & e(V, P_{pub} + H_1(ID)P) \\ &= e((r + H_2(m,U))S_{ID}, P_{pub} + H_1(ID)P) \\ &= e(\frac{r + H_2(m,U)}{s + H_1(ID)}P, sP + H_1(ID)P) \\ &= e(U + H_2(m,U)P, P) \end{aligned} \tag{1}$$

4.2 Efficiency Analysis

The new scheme requires two point scalar multiplication computations in $\mathbb{G}_1$ and one addition in $\mathbb{Z}_q$ in signature generation. In verification phase, it needs two pairing computations and two point scalar multiplication computations in $\mathbb{G}_1$. The new IBS is more efficient than [8,13,16], and is as efficient as the Cha-Cheon's IBS [6]. Moreover, in operation of mapping an identity to an element in $\mathbb{G}_1$, the maptopoint algorithm used by Cha-Cheon's IBS is not required. Instead of that, our scheme makes use of an ordinary hash-function. Although there has been much discussion on the construction of the maptopoint algorithm [4,6], these algorithms are still probabilistic, which was also remarked in [7,24].

4.3 Security Analysis

We can have the following result to the security of new ID-based signature scheme.

Theorem 1. *If there is an algorithm $\mathcal{A}$ for an adaptively chosen message and ID attack to our scheme which queries H_1, H_2, Sign and Extract at most q_{H_1}, q_{H_2}, q_S and q_E times, respectively, and has running time t and advantage $\epsilon \geq 10(q_S+1)(q_S+q_{H_2})q_{H_1}/(q-1)$, then $(q_{H_1}-1)$-CAA problem can be solved with probability $\epsilon' \geq 1/9$ within running time $t' \leq \frac{23q_{H_1} \cdot q_{H_2} t}{\epsilon \times (1-\frac{1}{q})}$.*

Proof. Suppose for contradiction that there exists an adversary $\mathcal{A}$ breaks the scheme in the random oracle, then we show there exists an algorithm $\mathcal{B}$ that, by interacting with $\mathcal{A}$, solves the k-CAA problem. Assume $\mathcal{A}$ asks q_{H_i} times queries to random oracles H_i (i=1,2), our algorithm $\mathcal{B}$ described below solves $(q_{H_1}-1)$-CAA problem for a randomly given instance $\{P, Q = xP, h_1, \cdots, h_{(q_{H_1}-1)} \in \mathbb{Z}_q, \frac{1}{h_1+x}P, \cdots, \frac{1}{h_{(q_{H_1}-1)}+x}P\}$ and asked to compute $\frac{1}{h+x}P$ for some $h \notin \{h_1, \cdots, h_{(q_{H_1}-1)}\}$. The details are as follows.

First, $\mathcal{B}$ puts $P_{pub} = Q$ as the PKG's public key and sends it to $\mathcal{A}$. Meanwhile, $\mathcal{B}$ randomly chooses a $h \in \mathbb{Z}_q$ and gets the set $\{h_1, \cdots, h_{(q_{H_1}-1)}, h\}$. Then $\mathcal{B}$ permutates these q_{H_1} values randomly and gets a new set $\{h'_1, \cdots, h'_{q_{H_1}}\}$, where $h = h'_k$ for an integer $k \in [1, q_{H_1}]$. $\mathcal{B}$ also prepares q_{H_2} responses $b_s \in_R \mathbb{Z}_q^*$ of the H_2 queries for $1 \leq s \leq q_{H_2}$.

Denote by ID_i, (m_s, U_s), ID_{i_k}, and (ID_{i_j}, m_j) the inputs of the i-th H_1 query, the s-th H_2 query, the k-th Extract query, and the j-th Sign query asked by $\mathcal{A}$, respectively. $\mathcal{B}$ will answer hash oracle queries and signing queries itself. We assume that $\mathcal{A}$ never repeats a hash query or a signature query. Define

- Hash function query: There are two types of hash function query H_1 and H_2. After received ID_i for H_1 query, $\mathcal{B}$ answers $H_1(ID_i)$=h'_i for $1 \leq i \leq q_{H_1}$. If (m_s, U_s) is sent for H_2 query, $\mathcal{B}$ answers $H_2(m_s, U_s) = b_s$ for $1 \leq s \leq q_{H_2}$.
- Extract query: When adversary requests private key extraction corresponding to ID_{i_k}, $\mathcal{B}$ responds with $S_{ID_{i_k}} = \frac{1}{x+h'_{i_k}} P$ if $i_k \neq k$. Otherwise, $\mathcal{B}$ aborts.
- Sign query: When adversary requests signature (ID_{i_j}, m_j), $\mathcal{B}$ chooses $r_j \in_R \mathbb{Z}_q^*$ and computes $U_j = r_j \times (P_{pub} + H_1(ID_{i_j})P) - b_j P$ and $V_j = r_j P$, where b_j=$H_2(m_j, U_j)$. Output (U_j, V_j) as the corresponding signature of message m_j for ID_{i_j}. It can be easily verified that (U_j, V_j) computed as above is a valid signature from the viewpoint of $\mathcal{A}$ for $e(V_j, P_{pub} + H_1(ID_{i_j})P) = e(U_j + H_2(m_j, U_j)P, P)$.

This completes the description of Algorithm $\mathcal{B}$. From the viewpoint of $\mathcal{A}$, the simulation provided by $\mathcal{B}$ is indistinguishable from a real attack scenario. After the simulation, if the adversary outputs a forged ID-based signature as (ID, m, U, b, V) and $ID = ID_k$, where $b = H_2(m, U)$. By replaying of $\mathcal{A}$ with the same random tape but different choices of H_2, as done in the forking lemma [17], we also obtain signatures (ID, m, U, b', V'), which are expected to be valid ones with respect to hash functions H_2 and H'_2, which have different values b and b' on (m, U), respectively. If both outputs are expected signatures, then compute $(b - b')^{-1}(V - V')$ and output it. Since $V = \frac{r+b}{x+h} P$ and $V' = \frac{r+b'}{x+h} P$, then $\frac{1}{x+h} P$ $= (b - b')^{-1}(V - V')$. So the $(q_{H_1} - 1)$-CAA problem solved. The reduction probability of the new scheme can be easily get from [6] for the simulation is very similar to each other, and both of them used the same forking lemma [17]. So the reduction probability is the same with [6].

5 Key-Insulated Threshold Signature Scheme

The notion of key-insulated public key cryptosystem was first introduced by Dodis et. al [10]. In the key-insulated public key cryptosystem, a user first generates a public key which remains for the lifetime of the scheme. The secret key associated with a public key is here shared between the user and a physically-secure device: The master key is stored on a physically-secure device and a temporary secret key used to perform cryptographic operations is stored in an insecure device, for which key exposures may occur, and updated regularly with

the help of a physically-secure device that stores a master key. A scheme is called (t, N)-key-insulated if an adversary who compromises the insecure device up to $t < N$ periods cannot break the remaining $N - t$ periods, where the lifetime of the scheme is divided into distinct periods $1, 2 \cdots, N$. Additionally, a scheme is called a strong (t, N)-key-insulated scheme if an adversary who compromises either the physically-secure device or the insecure device, but not both of them, cannot break the scheme in the remaining $N - t$ periods. By identifying time periods with identities, we see that any ID-based signature scheme yields a $(N-1, N)$ key-insulated (but not necessarily strong) signature scheme. A strong $(N-1, N)$ key-insulated signature can also derived from the new IBS by using the method showed in [23]. So, a strong $(N-1, N)$ key-insulated signature can be derived from the new IBS in section 3.

Apart from the key-insulated cryptography, threshold cryptography [9,12] was also suggested to reduce the damage of secret key exposure. In threshold cryptography models, the secret key is shared in a distributed manner and the attacker should compromise more than a predetermined number of share holders. What is interesting here is that by combining key-insulated and threshold cryptography, the resulted key-insulated threshold signature ($\mathcal{KITHS}$) provides benefits over previous ones in terms of security. In (t, N) key-insulated (k, n)-threshold cryptostystem, the user's master key is stored on a physically-secure device, however, a temporary secret key during one time period used to perform cryptographic operations is now distributed and stored in n insecure devices, instead of storing in only one insecure device. So, the adversary have to break a predetermined number of servers in order to get a temporary secret key for only one time period, which obviously strengthens the security of key-insulated cryptosystem. And the system remains secure even if the adversary has t temporary secret keys.

Definition 3. **[Key-Insulated (k, n)-Threshold Signature]** *A $\mathcal{KITHS}$ consists 6-tuple of poly-time algorithms (Gen, Upd*, DK, Upd, Sign, Vrfy) defined as follows:*

- *Gen: The key generation algorithm, is a probabilistic algorithm taking as input a security parameter 1^k. It returns a public key pk, a master key sk^*, and an initial key sk_0.*
- *Upd*: The device key-update algorithm, is a probabilistic algorithm that takes as input indices i, j, and the master private key sk^*. It returns a partial secret key $sk'_{i,j}$.*
- *DK: The distribution algorithm that takes as input the partial secret key $sk'_{i,j}$ and n. It returns $sk'^{(\kappa)}_{i,j}$ as the shares of $sk'_{i,j}$ for $\kappa = 1, \cdots, n$.*
- *Upd: The user key-update algorithm, is a deterministic algorithm that takes as input indices i, j, $sk_i^{(\kappa)}$, $sk'^{(\kappa)}_{i,j}$. It returns $sk_j^{(\kappa)}$ as the share of secret key sk_j for $\kappa = 1, \cdots, n$.*
- *Sign: The signing algorithm, is a probabilistic algorithm that takes as input an index i of a time period, a message m, and $sk_i^{(\kappa)}$ for $\kappa = 1, \cdots, n$. Sign returns a signature value σ for m.*

– *Vrfy: The verification algorithm, is a deterministic algorithm that takes as input pk, time period i, message m and signature σ. Vrfy returns a bit b. If b = 1, the signature is valid; otherwise, it is invalid.*

In a $\mathcal{KITHS}$ scheme, a user begins by generating (pk, sk^*, sk_0) through $Gen(1^k, N)$, registering pk, storing sk^* on a physically-secure device, and distributing sk_0 using algorithm DK to n insecure devices as $sk_0^{(\kappa)}$ for $\kappa = 1, \cdots, n$. When it is time to update keys from period i to j, after get $sk_{i,j}^{\prime(\kappa)}$ from the secure device, it runs $Upd^*(i, j, sk_i^{(\kappa)}, sk_{i,j}^{\prime(\kappa)})$ and gets $sk_j^{(\kappa)}$ as the κ_{th} share of sk_j. With $sk_j^{(\kappa)}$ for $\kappa = 1, \cdots, n$, they can jointly sign messages at time period j by running $Sign$.

5.1 Generic Construction of Key-Insulated Threshold Signature Scheme

ID-based threshold signature ($\mathcal{IDTHS}$) was introduced by Baek and Zheng [1]. In their $\mathcal{IDTHS}$, the private key associated with an identity is shared among many signature generation servers. We shows the definition briefly follows [1]: A (k, n) $\mathcal{IDTHS}$ consists of algorithms (GC, EX, DK, S, V), where GC is parameter generation algorithm run by PKG to generate its public key pk and secret key sk on inputting security parameter 1^k; EX is the private key extraction algorithm that returns s_{ID} on inputting an identity ID and sk; DK is the distribution algorithm that on inputting s_{ID} and n, by $s_{ID}^{(\kappa)}$ denote each of the private key share of s_{ID}, it generates and sends secret share $s_{ID}^{(\kappa)}$ to the κ_{th} holder for $\kappa = 1, \cdots n$; S is the signing algorithm run by n signature generation servers on inputting shares $s_{ID}^{(\kappa)}$ associated with an identity ID, a message m, it returns σ as the signature; V is the verification algorithm that checks the validity of the signature on inputs pk, m, σ and ID, V returns 1 if it is valid, otherwise, it is invalid. For more details, we can refer reader to [1].

The most general known notion of security of a key-insulated signature scheme is security against existential forgery for an adversary with two oracles: a key exposure oracle and a signing oracle. The first oracle takes input time period i, and returns a secret key sk_i. The second oracle takes input a tuple (i, m), and returns the signature for m. The goal of the adversary is to produce a valid signature of m at an un-exposure time period j and (j, m) was not submitted to the signing oracle. We refer the reader to [11] for the notion of security for key-insulated signatures. The security notion can be extended to $\mathcal{KITHS}$. We say that a (t, N) key-insulated (k, n)-threshold signature scheme is unforgeable, if no malicious adversary who corrupts at most k players can produce, with non-negligible probability, the signature on any new message m at an un-exposure time period j and (j, m) was not submitted to the signing oracle, given the key exposure oracle, signing oracle.

The conversion from any such $\mathcal{IDTHS}$ scheme to a secure $\mathcal{KITHS}$ scheme proceeds as follows:

- *Gen*: Run $GC(1^k)$ to get user's public key pk and secret key sk. It then returns pk, a master key $sk^* = sk$, and an initial key $sk_0 = \phi$.
- Upd*: Takes as input i, j and master key sk^*, it run $EX(j, sk^*)$ and returns $sk'_{i,j}$ where $sk'_{i,j} = EX(j, sk^*)$.
- DK: To distribute the partial secret key $sk'_{i,j}$ to n signature generation servers, run DK on inputting $sk'_{i,j}, n$, and returns the result $sk'^{(\kappa)}_{i,j}$ to the κ_{th} server for $\kappa = 1, \cdots, n$.
- Upd: On inputting $sk'^{(\kappa)}_{i,j}$, each signature generation server stores $sk'^{(\kappa)}_{i,j}$ as the share of sk_j for time period j, i.e, $sk^{(\kappa)}_j = sk'^{(\kappa)}_{i,j}$, and deletes $sk^{(\kappa)}_i$ for $\kappa = 1, \cdots, n$.
- Sign: On inputting a message m, i and $sk^{(\kappa)}_i$ for $\kappa = 1, \cdots, n$, run S to get σ as the signature.
- Vrfy: Run algorithm $V(pk, m, \sigma, i)$ and returns b. If $b = 1$, the signature is valid; otherwise, it is invalid.

From the conversion method, it can be easily proved that if the underlying $\mathcal{IDTHS}$ is secure, then the $\mathcal{KITHS}$ is secure.

6 Conclusion

In this paper, we propose a provably secure ID-based signature scheme. The new IBS shares the same system parameters with SK-IBE, which only uses the conventional hash function, instead the special hash function used in [7]. Combining our signature scheme with the SK-IBE yields a complete new solution of an ID-based public key cryptosystem. Also, we prove that the new IBS is secure against existential forgery for adaptive chosen-message-and-identity attack in the random oracle based on the k-CAA assumption. Another contribution of this paper is that the notion of key-insulated threshold signature is first proposed. Furthermore, we give a generic method for constructing key-insulated threshold signature scheme from ID-based threshold signature scheme.

References

1. J. Baek, Y. Zheng. *Identity-based Threshold Signature Scheme From the Bilinear Pairings*. Proceedings of the international conference on information Technology: Coding and Computing 2004.
2. M. Bellare, C.Namprempre, and G.Neven. *Security Proofs for Identity-based Identification and Signature Schemes*. EuroCrypt'04, LNCS 3027, pp. 268-286.
3. D. Boneh and X.Boyen, *Short signatures without random oracles*, Proc. of Eurocypt'04, LNCS 3027, pp. 56-73, Springer-Verlag, 2004.
4. D. Boneh and M. Franklin, *Identity based encryption from the weil pairing*, Proc. of Crypto'01, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.
5. X. Boyen, *Multipurpose identity-based signcryption-A Swiss army knife for identity-based cryptography*, CRYPTO'03, LNCS 2729, pp. 382-398, Springer-Verlag, 2003.

6. J.C. Cha and J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups*, PKC'03, LNCS 2567, pp. 18-30, Springer-Verlag, 2003.
7. L. Chen and Z. Cheng, *Security Proof of Sakai-Kasahara's Identity-Based Encryption Scheme*. Cryptology ePrint Archive, Report 2005/131, 2005. Accepted by 10th IMA International Conference on Cryptography and Coding.
8. J.H. Cheon, Y. Kim, H.J. Yoon, *A new ID-based Signature with Batch Verification*. Cryptology ePrint Archive, Report 2004/131, 2004.
9. Y. Desmedt and Y. Frankel. Threshold cryptosystems. Crypto'89.
10. Y. Dodis, J. Katz, S. Xu and M. Yung. Key-Insulated Public-Key Cryptosystems. Eurocrypt 2002. pp. 65-82,Springer-Verlag, 2002.
11. Y. Dodis, J. Katz, S. Xu and M. Yung. Strong Key-Insulated Signature Schemes. PKC 2003. LNCS 2567, pp. 130-144, Springer-Verlag, 2003.
12. R.Gennaro, S.jarecki, H. Krawczyk and T.Rabin, *Secure Distributed Key Generation for Discrete-Log Based Cryptosystem*, Proc. of EUROCRYPT'99, LNCS 1592, pp 295-310, Springer-verlag, 1999.
13. F. Hess, *Efficient identity based signature scheme based on pairings*, SAC'02, LNCS 2595, pp. 310-324, Springer-Verlag, 2003.
14. S. Mitsunari, R. Sakai, and M. Kasahara, *A new traitor tracing*, IEICE Trans. Vol. E85-A, No.2, pp. 481-484, 2002.
15. T. Okamoto and D. Pointcheval, *The gap-problems: a new class of problems for the security of cryptographic Schemes*, Proc. of PKC'01, LNCS 1992, pp. 104-118, Springer-Verlag, 2001.
16. K. Paterson, *ID-based signatures from pairings on elliptic curves*, Available from http://eprint.iacr.org, 2002.
17. D. Pointcheval and J. Stern, *Security arguments for digital signatures and blind signatures*, Journal of Cryptology, Vol.13, No.3, pp.361-396, 2000.
18. R. Sakai and M. Kasahara. *ID based cryptosystems with pairing on elliptic curve*. Cryptology ePrint Archive, Report 2003/054.
19. R. Sakai, K. Ohgishi, and M. Kasahara, *Cryptosystems based on pairing*, SCIS 2000, Okinawa, Japan, 2000.
20. A. Shamir, *Identity-based cryptosystems and signature schemes*, Advances in Cryptology-Crypto 84, LNCS 196, pp.47-53, Springer-Verlag, 1984.
21. H. Tanaka, *A realization scheme for the identity-based cryptosystem*, Proc. of Crypto'87, LNCS 293, pp. 341-349, Springer-Verlag, 1987.
22. S. Tsuji and T. Itoh, *An ID-based cryptosystem based on the discrete logarithm problem*, IEEE Journal of Selected Areas in Communications, Vol. 7, No. 4, pp. 467-473, 1989.
23. D.H. Yum and P.J. Lee, *Efficient Key Updating Signature Schemes Based on IBS*, Proc. of Cryptography and Coding 2003, LNCS 2898, pp. 167-182, Springer-Verlag, 2003.
24. F. Zhang, R. Safavi-Naini, and W. Susilo, *An efficient signature scheme from bilinear pairings and its applications*, In Proceedings of PKC 2004, LNCS 2947, pp. 277-290, Springer-Verlag, 2004.