ID-Based Sequential Aggregate Signatures

Xiangguo Cheng
School of Information Engineering, Qingdao University, Qingdao 266071, China
Email: chengxg@qdu.edu.cn

Lifeng Guo, Chen Yang and Jia Yu
School of Computer and Information Technology, Shanxi University, Taiyuan 030006, China
China Electronics Standardization Institute, Beijing 100007,China.
School of Information Engineering, Qingdao University, Qingdao 266071, China
Email: lfguo@sxu.edu.cn yangchenyf@163.com yujia@qdu.edu.cn

***Abstract*—An aggregate signature provides a method for combining *n* signatures of *n* different messages from *n* different signers into one signature of unit length. The main benefit of such schemes is that they allow bandwidth and computational savings. There exist several trials for the construction of ID-based aggregate signature schemes so far. Unfortunately, the computational complexity and (or) signature length of these schemes grow linearly with the number of signers. This paper focuses on the solution of these problems and proposes a new ID-based sequential aggregate signature scheme based on IB-mRSA. It is compatible with RSA and has the fixed signature length. The security analysis shows that it is secure in the random oracle model with the assumption of classical RSA.**

***Index Terms*—ID-based cryptography, digital signature, aggregate signature, RSA**

I. INTRODUCTION

An aggregate signature, primitively proposed by Boneh *et al.*[2], is a signature that support aggregation: Given *n* signatures on *n* distinct messages from *n* distinct users, it is possible to aggregate all these signatures into one signature. Such a signature (and all the original messages) will convince any verifier that the *n* users did signed the *n* original messages. Thus an aggregate signature provides non-repudiation at once on many different messages by many users. Aggregate signatures are useful for reducing the size of certificate chains (by aggregating all signatures in the chain) and for reducing message size in secure routing protocols such as SBGP[1], *etc*. However, such aggregation technique is only used by the verifier after all the individual signatures having been finished, while the individual signatures have to be sent along with the signed messages. This is restricted in the environment of low bandwidth and storage. Lysyanskaya *et al*. proposed a sequential aggregate signature scheme from trapdoor permutations [3]. A sequential aggregate signature is in fact an aggregate signature that signature aggregation can be done during the signing process. Each signer in turn sequentially adds his signature to the current aggregation. Aggregation of the individual signatures is performed incrementally and sequentially. In a sequential aggregate signature scheme, signing and aggregation are finished at the same time and only the aggregated signature is to be sent to the next signer.

The concept of identity (ID)-based cryptography was first introduced by Shamir [5] in 1984. Its aim is to eliminate the need for public key certificates by allowing a public key to be uniquely derived from a user's identity information. ID-based public key setting can be a good alternative for certificate-based public key setting, especially when efficient key management and moderate security are required. Many ID-based encryption and signature schemes [6-13] have been proposed since 1984. But none of them provides efficient solutions to revoke a user's identity. Boneh *et al*. [14] proposed an ID-based mediated RSA (IB-mRSA) scheme. IB-mRSA is a practical and RSA [4] compatible method of splitting the private key corresponding to a user's ID between the user and the security mediator (SEM). Neither the user nor the SEM knows the factorization of the RSA modulus and neither can sign/decrypt message without the other's help. IB-mRSA not only presents a practical ID-based cryptography, but also provides an efficient solution to the fast revocation of a user's ID.

There exist several trials for constructing ID-based aggregate signature schemes [15-20] so far. However, the schemes are not quite ID-based aggregate signature schemes in the original sense of [2] since they require an additional communication round to aggregate random parts of ID-based signatures provided by multiple signers into a single element [15], or a certain synchronization for sharing the same random string [20], or their signature length grows linearly with the number of signers [16-19]. In fact, the most difficult issue in the construction of such a scheme is how to reduce the aggregate signature length from $O(n)$ to $O(1)$ for n signers. This paper focuses on the solution of this issue. To see the difficulty, we note that almost all the previous ID-based aggregate signature schemes are constructed from some ID-based signature schemes based on bilinear pairing, and these schemes, unlike BLS signature scheme [21], are not deterministic. If each successive signer contributed a randomness to the

Manuscript received Jan 20, 2011; revised Mar 30, 2011; accepted Apr 5, 2011.
Corresponding author: Xiangguo Cheng

doi:10.4304/jsw.6.12.2495-2499

aggregate signature in a trivial way, this randomness would cause the size of the signature to grow linearly with n. IB-mRSA is a deterministic ID-based signature scheme. It allows multiple users of the system to share the same modulus, and each private-public key pair corresponding to an ID is generated by a trusted Private Key Generator (PKG), not by the signer himself, which guarantees each trapdoor permutation is a certified one. These properties of IB-mRSA provide us a good way to realize the construction of an ID-based sequential aggregate signature scheme using the method given in [3].

II. IB-mRSA Signature Scheme

The main idea behind IB-mRSA is to introduce a security mediator (SEM) in classical RSA. The private key corresponding to a user's ID is divided into two parts by PKG. One part is given to the user and the other is given to SEM. Neither the user nor SEM can sign/decrypt a message without the other's help. As a result, a user's ID (*i.e.* sign/decrypt capability) can be immediately revoked by asking SEM not to help him any more. To prepare for our scheme, we first give a review of IB-mRSA as follows.

Setup: Given a security parameter κ, PKG randomly chooses a κ-bit RSA modulus $n = pq$, where p and q are two $\kappa/2$-bit primes. Define two hash functions:

$$H_1 : \{0,1\}^* \to \{0,1\}^l,\ H_2 : \{0,1\}^* \to \mathbb{Z}_n$$

where l is a parameter depending on κ. PKG broadcasts n, H_1, H_2.

Extract: Given a user's identity ID, PKG computes $e = 0^s \| H_1(ID) \| 1$ and $d = e^{-1} \bmod \varphi(n)$, where $s = k - l - 1$. Then it chooses a number $d_u \in_R \mathbb{Z}_n^*$ and computes $d_s = (d - d_u) \bmod \varphi(n)$. d_u and (d_s, *ID*) are secretly sent to the user and SEM, respectively.

Sign: To sign a message *m*, the signer sends *m* along with his ID to SEM. They perform the following tasks in parallel.

—SEM first checks that the signer's ID has not been revoked. It then computes $Sig_s = H_2(m)^{d_s} \bmod n$ and sends it back to the signer.

—The signer computes $Sig_u = H_2(m)^{d_u} \bmod n$ and $\sigma = (Sig_s \cdot Sig_u) \bmod n$. It checks whether $H_2(m) = \sigma^e \bmod n$. If so, the signature on *m* under ID is set to be σ.

Verify: Given a signature σ of message *m* under ID, the verifier computes $e = 0^s \| H_1(ID) \| 1$. He accepts the signature if $H_2(m) = \sigma^e \bmod n$.

Theorem 1. The IB-mRSA signature scheme is unforgeable in the random oracle model under the assumption of classical RSA.

Proof: Note that the IB-mRSA signature is in fact a (2,2) threshold signature. A threshold signature scheme is unforgeable if the underlying signature scheme is secure and the threshold signature is simulatable [17]. The underlying signature is a classical RSA signature. In the following, we need only to show that the IB-mRSA signature is simulatable.

To prove the simulatability of the IB-mRSA signature scheme, we construct a simulator *SIM* to simulate the IB-mRSA signature generation protocol *Sign*. Suppose that an adversary *A* has corrupted a signer whose identity is ID. His goal is to forge a signature of this signer without the help of SEM. The view of an adversary *A* consists of the message *m*, the modulus *n*, the signer's public-private key pair (e, d_u), and the signature σ of *m* under ID. Let $VIEW_A(Sign(n, e, d_u, m), \sigma)$ denote all the information that *A* is able to get. *SIM*'s inputs are the message *m*, the modulus *n*, the signer's public-private key pair (e, d_u), and the signature σ. Let $SIM(n, e, d_u, m, \sigma)$ denote all the information produced by the simulator. The following description shows that $VIEW_A(Sign(n, e, d_u, m), \sigma)$ is computationally indistinguishable from $SIM(n, e, d_u, m, \sigma)$.

On the one hand, the partial signatures given by the signer and SEM are

$$Sig_u = H_2(m)^{d_u} \bmod n,\ Sig_s = H_2(m)^{d_s} \bmod n.$$

Both are random numbers in $\mathbb{Z}_n$ since d_u is randomly chosen from $\mathbb{Z}_n$ and $d_s = (d - d_u) \bmod \varphi(n)$; On the other hand, the partial signature of the corrupted user in *SIM* can be computed as $Sig'_u = H_2(m)^{d_u} \bmod n$, and the partial signature of the SEM in *SIM* is Sig'_s such that $\sigma = (Sig'_s \cdot Sig'_u) \bmod n$. They are also random numbers in $\mathbb{Z}_n$. Therefore, Sig_u, Sig_s, Sig'_u and Sig'_s have the same distribution in $\mathbb{Z}_n$.

We recall that it is completely insecure to have a common modulus for several users in classical RSA since the knowledge of a single private-public key pair allows a user to factor the modulus. However, IB-mRSA allows multiple users to share the same modulus since neither the users nor SEM is able to completely know the private key corresponding to an ID. Note that collusion between a user and SEM would result in a total break of the whole scheme. Therefore, SEM here must be assumed to be a totally trusted and secure entity and no user is able to compromise it.

III. ID-Based Sequential Aggregate Signature

We introduce the definition of an ID-based sequential aggregate signature and present its security model in this section.

A. Definition of ID-Based Sequential Aggregate Signature

An ID-based sequential aggregate signature can be viewed as a combination of a sequential aggregate signature and an ID-based signature. Namely, it is a sequential aggregate signature, but, all the public keys are the users' IDs. It generally consists of four algorithms: *Setup*, *Extract*, *Aggregate Signing* and *Aggregate Verify*.

Setup: Given a security parameter κ, PKG generates and publishes the system parameters.

Extract: Given an identity ID_i of a user U_i, PKG generates a private key sk_i corresponding to ID_i and secretly sends it to U_i.

Aggregate Signing: Signing and aggregation is a combined operation. The operation takes as inputs a private key sk_i, a message m_i to sign, and a sequential aggregate signature σ' on messages $m_1, m_2, \cdots, m_{i-1}$ under $ID_1, ID_2, \cdots, ID_{i-1}$, where m_1 is the inmost message. It adds a signature on m_i under ID_i and outputs a sequential aggregate signature σ on all messages $m_1, m_2, \cdots, m_i$.

Aggregate Verify: Verifies that σ is a valid sequential aggregate signature on messages $m_1, m_2, \cdots, m_i$ under $ID_1, ID_2, \cdots, ID_i$.

B. Security of ID-Based Sequential Aggregate Signature

The security of an ID-based sequential aggregate signature scheme is defined as the non-existence of an adversary capable of existentially forging an ID-based sequential aggregate signature. Existential forgery here means that the adversary attempts to forge a sequential aggregate signature, on some messages of his choice, under some set of IDs.

Similar to [3], we formalize the security model of an ID-based sequential aggregate signature scheme as sequential aggregate chosen ID security. In this model, the adversary *A* is first given an ID. His goal is the existential forgery of an ID-based sequential aggregate signature. We give *A* the power of choosing all IDs expect the challenge ID. The adversary is also given access to a sequential aggregate signing oracle on the challenge ID. We say the adversary succeeded if he won the following game.

Setup. The adversary *A* is provided with an ID, generated at random.

Queries. Proceeding adaptively, *A* can request the public-private key pairs corresponding to some IDs except the provided ID. *A* can also request the sequential aggregate signatures under these IDs on messages of his adaptive choice. For each query, we allow *A* to supply a sequential aggregate signature σ' on some messages $m_1, m_2, \cdots, m_{i-1}$ under some distinct identities $ID_1, ID_2, \cdots, ID_{i-1}$ and an additional message m_i to be signed under ID.

Responses. Finally, *A* outputs *j* distinct identities $ID_1, ID_2, \cdots, ID_j$, *j* messages $m_1, m_2, \cdots, m_j$ and a sequential aggregate signature σ.

A wins the game if σ is a valid sequential aggregate signature on messages $m_1, m_2, \cdots, m_j$ under some distinct identities $ID_1, ID_2, \cdots, ID_j$, and one of these identities is ID.

IV. ID-Based Sequential Aggregate Signature Scheme

Using the IB-mRSA signature scheme as an underlying scheme, we first manage to construct an ID-based sequential aggregate signature scheme, then we show the security analysis of this scheme. For the convenience of description, we first introduce some notations used in our scheme. Suppose that (*e*, *d*) is a public-private key pair of RSA, then $\pi(x) = x^e \bmod n$ is a permutation on $\mathbb{Z}_n^*$ and $\pi^{-1}(x) = x^d \bmod n$ is its inverse, which are derived uniquely from *e* and *d*. In the following, we use (π, π^{-1}) to denote (*e*, *d*) and use $a +_n b$ to denote the operation of $(a+b) \bmod n$.

A. Proposed Scheme

Our ID-based sequential aggregate signature scheme is described as follows:

Setup: It is the same as that in the underlying IB-mRSA signature scheme.

Extract: Given an identity ID_i of user U_i, PKG computes $e_i = 0^s \| H_1(ID_i) \| 1$ and $d_i = e_i^{-1} \bmod \varphi(n)$, where $s = k - l - 1$. Then it chooses a number $d_i^u \in_R \mathbb{Z}_n^*$ and computes $d_i^s = (d_i - d_i^u) \bmod \varphi(n)$. d_i^u is sent to U_i and (d_i^s, ID_i) is sent to SEM.

Aggregate Signing: Without lose of generality, suppose that *j* signers $U_1, U_2, \cdots, U_j$ orderly generate an ID-based sequential aggregate signature on *j* messages $m_1, m_2, \cdots, m_j$. Signer U_1 first signs message m_1. He interacts with SEM to do the following work:

— U_1 computes $h_1 = H_2(ID_1, m_1)$ and sends it to SEM.

— SEM first checks that U_1's identity ID_1 has not been revoked. If so, it computes a partial signature $Sig_1^s = h_1^{d_1^s} \bmod n$ and sends it back to U_1.

— U_1 computes $Sig_1^u = h_1^{d_1^u} \bmod n$. After doing this, he then checks whether $h_1 = (Sig_1^s \cdot Sig_1^u)^{e_1} \bmod n$ holds. If so, the signature on message m_1 under ID_1 is set to be $\sigma_1 = (Sig_1^s \cdot Sig_1^u) \bmod n$ and is sent to the second user U_2.

Using the above π notation, σ_1 can be written as $\sigma_1 = \pi_1^{-1}(h_1)$.

Having received σ_1, U_2 first verifies that σ_1 is a valid signature on m_1 under ID_1 using the verification algorithm *Verify* of IB-RSA. Suppose that σ_1 is valid, he then computes $h_2 = H_2(ID_1 \| ID_2, m_1 \| m_2)$ and $h_2' = h_2 +_n \sigma_1$. After a procedure of interacting with SEM, U_2 can obtain a signature $\sigma_2 = \pi_2^{-1}(h_2') = \pi_2^{-1}(h_2 +_n \pi_1^{-1}(h_1))$, ……. For the *j*-th signer U_j, having received σ_{j-1}, he first verifies its validity using the algorithm *Aggregate Verify*. If so, U_j computes $h_j = H_2(ID_1 \| ID_2 \| \cdots \| ID_j, m_1 \| m_2 \| \cdots \| m_j)$ and $h_j' = h_j +_n \sigma_{j-1}$. With the help of SEM, U_j can obtain his signature

$$\sigma_j = \pi_j^{-1}(h_j') = \pi_j^{-1}(h_j +_n \pi_{j-1}^{-1}(h_{j-1} +_n \pi_{j-2}^{-1}(\cdots \pi_2^{-1}(h_2 +_n \pi_1^{-1}(h_1)))))$$

where $h_i = H_2(ID_1 \| ID_2 \| \cdots \| ID_i, m_1 \| m_2 \| \cdots \| m_i)$ for $i = 1, 2, \cdots, j$. The ID-based sequential aggregate signature on messages $m_1, m_2, \cdots, m_j$ under $ID_1, ID_2, \cdots, ID_j$ is set to be $\sigma = \sigma_j$.

Aggregate Verify: Given the ID-based sequential aggregate signature σ on messages $m_1, m_2, \cdots, m_j$ under

$ID_1, ID_2, \cdots, ID_j$, the verifier sets $\sigma_{i-1} = \pi_i(\sigma_i) +_n (-h_i)$ for $i = j, j-1, \cdots, 2, 1$, he accepts the sequential aggregate signature if $\sigma_0 = 0$, where 0 is the zero element of $\mathbb{Z}_n$.

B. Security Analysis

Using the security model of ID-based sequential aggregate signature scheme given in Section III, we analyze the security of our scheme.

Theorem 2. The proposed scheme is secure against existential forgery under an adaptive sequential aggregate chosen ID attack in the random oracle.

Proof. Suppose that there is a forger F that breaks the security of our ID-based sequential aggregate signature scheme, we will construct an algorithm F' to forge the based IB-mRSA signature scheme by using F.

F' simulates the challenger and interacts with F as the following.

Setup: F' randomly chooses an identity ID as a chosen ID and sends it to F.

ID Queries: F requests the private-public key pairs corresponding to some identities IDs except the chosen ID. F' makes queries on these IDs to its own oracle and gives the corresponding keys to F.

Hash Queries: F requests a hash on some identities $ID_1, ID_2, \cdots, ID_j$ and some messages $m_1, m_2, \cdots, m_j$. F' makes the same query to its own hash oracle and gives the value back to F.

Aggregate Signature Queries: Proceeding adaptively, F requests an ID-based sequential aggregate signature under the chosen ID on some messages of his choice. For each query, F supplies a sequential aggregate signature σ' on messages $m_1, m_2, \cdots, m_{j-1}$ under distinct identities $ID_1, ID_2, \cdots, ID_{j-1}$ and an additional message m_j to be signed under ID. F' first makes a hash query on $h_i = H_2(ID_1 \| ID_2 \| \cdots \| ID_{j-1} \| ID, m_1 \| m_2 \| \cdots \| m_{j-1} \| m_j)$ and obtains the response h, then F' makes a signature query on $h +_n \sigma'$ and gives the response back to F.

Outputs: Eventually F halts, outputting some messages $m_1, m_2, \cdots, m_j$, some identities $ID_1, ID_2, \cdots, ID_j$, and the corresponding sequential aggregate signature forgery σ. The forgery must be nontrivial: The challenge ID must be in $ID_1, ID_2, \cdots, ID_j$, at some location $i (1 \le i \le j)$, and F must not have asked for a sequential aggregate signature on $m_1, m_2, \cdots, m_i$ under $ID_1, ID_2, \cdots, ID_i$. If F fails to output a valid and nontrivial forgery, F' reports failure and terminates. Otherwise, F' does the following work:

Case 1. The chosen ID is at the end of some identities $ID_1, ID_2, \cdots, ID_j$. That is, $ID = ID_j$. F' requests the hash values of $H_2(ID_1 \| ID_2 \| \cdots \| ID_i, m_1 \| m_2 \| \cdots \| m_i)$ and gets the response h_i for $i = 1, 2, \cdots, j$. Then F' manages to get some signatures from his signing oracle. After having obtained the signature σ_1 of m_1 under ID_1. F' computes $h'_2 = h_2 +_n \sigma_1$ and gets a signature σ_2 on h'_2 under ID_2 from the signature query. The rest may be deduced by an analogy. After having obtain the signature σ_{j-2} on h'_{j-2} under ID_{j-2}, F' computes $h'_{j-1} = h_{j-1} +_n \sigma_{j-2}$. The signature σ_{j-1} on h'_{j-1} under ID_{j-1} can also be obtained from the signature query. We note that the sequential aggregate forgery σ is in fact an IB-mRSA signature of $h'_j = h_j +_n \sigma_{j-1}$ under ID_j, then F' get a forgery by using F.

Case 2. The chosen ID is in the middle of some identities $ID_1, ID_2, \cdots, ID_j$. That is to say, there exists an ID_l, where $1 \le l < j$, such that $ID = ID_l$. F' requests the hash values of $H_2(ID_1 \| ID_2 \| \cdots \| ID_i, m_1 \| m_2 \| \cdots \| m_i)$ and gets the response h_i for $i = l+1, l+2, \cdots, j$. Then F' sets $\sigma = \sigma_j$ and $\sigma_{i-1} = \pi_i(\sigma_i) +_n (-h_i)$ for $i = j, j-1, \cdots, l+1$. At last, F' obtains

$$\sigma_1 = \pi_{l+1}((-h_{l+1}) +_n \pi_{l+2}((-h_{l+2}) +_n \cdots \pi_{j-1}((-h_{j-1}) +_n \pi_j(s_j))))$$

We note that σ_1 is in fact a sequential aggregate signature on messages $m_1, m_2, \cdots, m_l$ under $ID_1, ID_2, \cdots, ID_{l-1}, ID$.

Therefore, Case 2 can be easily derived into Case 1.

If there exists an efficient algorithm F to forger our ID-based sequential aggregate signature scheme, then we can construct an algorithm F', with the same advantage, to forge the underlying IB-mRSA signature scheme. However, Theorem 1 has shown that the IB-mRSA signature scheme is existentially unforgeable. Therefore, Our ID-based sequential aggregate signature scheme is secure against existential forgery.

V. COMPARISON

Compared with previous ID-based aggregate signature schemes, our scheme has some advantages described as follows.

(1) Our scheme is based on IB-mRSA. It is compatible with classical RSA. However, all the previous ID-based aggregate signature schemes are constructed from bilinear pairings. We note that the pairing computation is the most time-consuming in pairing-based cryptosystems. Although there have been many works discussing the complexity of pairings and how to speed up the pairing computation, the computation of the pairing still remains time-consuming.

(2) A "good" aggregate signature scheme should satisfy the following properties:

—Flexibility: This property requires that, any user can add his individual signature into the aggregate signature at any time and without the cooperation of the signers.

—Compactness: Compactness requires that, a series of individual signatures by distinct signers on distinct messages should be compressed into a single, compact aggregate signature.

— Deletion: Deletion requires that, any individual signature can be easily removed from the aggregate signature by the signer.

Schemes [15] and [20] don not satisfy the property of flexibility since they need cooperation of the signers while aggregation. Schemes [16-19] don not satisfy compactness property since the aggregate signature length grows linearly with the number of signers. Our

scheme satisfies the above two properties. All the pairing-based aggregate signature schemes satisfy the deletion property. Unfortunately, our scheme do not satisfies this property since it is sequential, The signers can only inversely remove their individual signatures from the aggregate signature.

An efficiency comparison of our scheme with the existing ones is given in Table I, where √ denotes "satisfy" and × denotes "do not satisfy" and "FP", "CP", "DP" and "SL" are abbreviations of "Flexibility Property", "Compactness Property" , "Deletion Property" and "Signature Length".

TABLE I. FUNCTIONALITY COMPARISON OF THE SCHEMES

Scheme	FP	CP	DP	SL
Scheme[15]	×	√	√	$O(1)$
Scheme[17]	√	×	√	$O(n)$
Scheme[18]	√	×	√	$O(n)$
Scheme[19]	√	×	√	$O(n)$
Scheme[20]	×	√	√	$O(1)$
Our Scheme	√	√	×	$O(1)$

VI. CONCLUSIONS

Based on IB-mRSA signature scheme, we proposed an ID-based sequential aggregate signature scheme and give its security analysis in the random oracle. The advantage of this scheme is that the signature length is the same as the single signature, regardless of the number of signers. Furthermore, it is compatible with classical RSA.

ACKNOWLEDGMENT

This work was supported by a grant from the National Natural Science Foundation of China (No.60703089), the Shandong Province Natural Science Foundation of China (No. ZR2010FQ019) and the Plan Foundation of Science and Technology of Shandong Provincial Education Department of China (No. J08LJ02).

REFERENCES

[1] S. Kent, C. Lynn and K. Seo, "Secure border gateway protocol (Secure-BGP)," *IEEE J. Seclected Areas in Comm.*, Vol. 18(4), 2000, pp. 582-592.

[2] D. Boneh, C. Gentry, B. Lynn and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," *Advances in Eurocrypt'03*, LNCS, Vol. 2656, Springer-Verlag, 2003, pp. 416-432.

[3] A. Lysyanskaya, S. Micali, L. Reyzin and H. Shacham, "Sequential aggregate signatures from trapdoor permutations," *Advances in Eurocrypt'04*, LNCS, Vol. 3027, Springer-Verlag, 2004, pp.74-90.

[4] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Commun. ACM*, vol. 21(2), 1978, pp.120-126.

[5] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Crypto'84*, LNCS 196, Springer-Verlag, 1984, pp.47-53.

[6] H. Tanaka, "A realization scheme for the identity-based cryptosystem," *Advances in Crypto'87*, LNCS 293, Springer-Verlag, 1987, pp.341-349.

[7] S. Tsuji and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem," *IEEE Journal of Selected Areas in Communications*, Vol. 7(4), pp.467-473, 1989.

[8] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," *Advances in Crypto'86*, LNCS, Vol. 263, Springer-Verlag, 1987, pp.186-194.

[9] U. Feige, A. Fiat and A. Shamir, "Zero-knowledge proofs of identity," *J. Cryptology*, Vol.1, pp.77-94, 1988.

[10] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," *Advances in Crypto'01*, LNCS Vol. 2139, Springer-Verlag, 2001, pp.213-229.

[11] X. Yi, "An identity-based signature scheme from the Weil pairing," *IEEE Communications Letters*, Vol. 7(2), 2003, pp.76-78.

[12] J. C. Cha and J. H. Cheon, "An identity-based signature from gap Diffie-Hellman groups," *Advances in Public Key Cryptography-PKC 2003*, LNCS, Vol. 2567, Springer-Verlag, 2003, pp.18-30.

[13] F. Hess, "Efficient identity based signature schemes based on pairings," *Proceedings of Select Areas in Cryptography, SAC 2002*, LNCS, Vol. 2595, Springer-Verlag, 2002, pp.310-324.

[14] X. Ding and G. Tsudik, "Simple identity-based cryptography with mediated RSA," *Proceedings of CT-RSA 2003*, LNCS, Vol. 2612, Springer-Verlag, 2003, pp.193-210.

[15] X. Cheng, J. Liu and X. Wang, "Identity-based aggregate and verifiably encrypted signatures from bilinear pairing," *Proceedings of ICCSA 2005*, LNCS, Vol. 3483, Springer-Verlag, 2005, pp.1046-1054.

[16] J. H. Cheon, Y. Kim and H. J. Yoon, "A new ID-based signature with batch verification," *Cryptology ePrint Archive*, Report 2004/13, available at http://eprint.iacr.org.

[17] H. J. Yoon, J. H. Cheon and Y. Kim, "Batch verification with ID-based signatures," *ICISC'04*, LNCS, Vol. 3506, Springer-Verlag, 2005, pp. 233-248.

[18] J. Xu, Z. Zhang and D. Feng, "ID-based aggregate signatures from bilinear pairings," *CANS'05*, LNCS, Vol. 3810, Springer-Verlag, 2005, pp. 110-119.

[19] J. Herranz, "Deterministic identity-based signatures for partial aggregation," *The Computer Journal*, Vol. 49(3), 2006, pp.322-330.

[20] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," *Advances in Public Key Cryptography-PKC 2006*, LNCS, Vol. 3958, Springer-Verlag, 2006, pp.257-273.

[21] D. Boneh, B. Lynn, H. Shacham, "Short signatures from the Weil pairing," *Advances in Asiacrypt'01*, LNCS, Vol. 2248, Springer-Verlag, 2002, pp. 514-532.