International Journal of Innovative
Computing, Information and Control
Volume **8**, Number **9**, September **2012**

ICIC International ©2012 ISSN 1349-4198
pp. 6401–6413

IDENTITY-BASED SEQUENTIAL AGGREGATE SIGNATURE SCHEME BASED ON RSA

Bennian Dou[1], Chun-Hua Chen[2], Hong Zhang[3] and Chungen Xu[1]

[1]School of Science
[3]School of Computer Science and Technology
Nanjing University of Science and Technology
No. 200, Xiaolingwei, Nanjing 210094, P. R. China
doubennian@yahoo.com.cn; xuchungen@163.com; zhhong@mail.njust.edu.cn

[2]Department of Computer and Communication Engineering
Chienkuo Technology University
No. 1, Chieh Shou N. Rd., Changhua 500, Taiwan
godsons@ctu.edu.tw

Received May 2011; revised September 2011

Abstract. *Identity-based signature (IBS) schemes allow a signer to sign a message, in which the signature can be verified by his identity. Sequential aggregate signature (SAS) schemes allow multiple signers to sequentially produce a short signature of different messages and also allow signers to attest to these messages as well as the order in which they signed. At CCS 2007, Boldyreva et al. proposed the first identity-based sequential aggregate signature (IBSAS) scheme from pairings on elliptic curves, which have the merits of both SAS and IBS schemes. In 2009, Hwang et al. pointed out that the Boldyreva et al.'s scheme is not secure. How to construct a secure IBSAS scheme is still an important open problem. In this paper, we present an IBSAS scheme, which is not based on pairings but based on RSA. We define a new security model for IBSAS schemes, and we prove our scheme secure in this model. We also give the potential applications of our scheme in secure network routing, but we believe that this scheme has many other applications as well.*

Keywords: Digital signature, Identity-based signatures, Sequential aggregate signature, RSA, Network security

1. **Introduction.** Undoubtedly, reducing communication bandwidth and saving storage are crucial to modern communication. However, many communication channels are vulnerable to eavesdropping and tampering attacks by outsiders. Strong cryptography is needed to protect the communication, which may add even more overhead to the communication. It is important to limit this overhead to a minimum when one designs cryptographic primitives to protect the communication [1].

Aggregate signature (AS) *schemes*, proposed by Boneh et al. [2] in 2003, are digital signatures that allow n members (whose public and secret key pair is (PK_i, SK_i)) of a given group of potential signers to sign n different messages m_i $(1 \leq i \leq n)$ respectively, and all the signatures of those users on those messages can be aggregated into a single short signature σ. This single signature and the n original messages m_i $(1 \leq i \leq n)$ are enough to convince the verifier that the n signers did indeed sign the n original messages m_i $(1 \leq i \leq n)$ respectively. Boneh et al.'s scheme employs *parings* on elliptic curves.

Because of the aggregation of many signatures into a single short signature, AS schemes can reduce bandwidth and save storage. In the scheme of [2], the aggregate signature can be produced by anyone. Figure 1 shows how an aggregate signature scheme works.

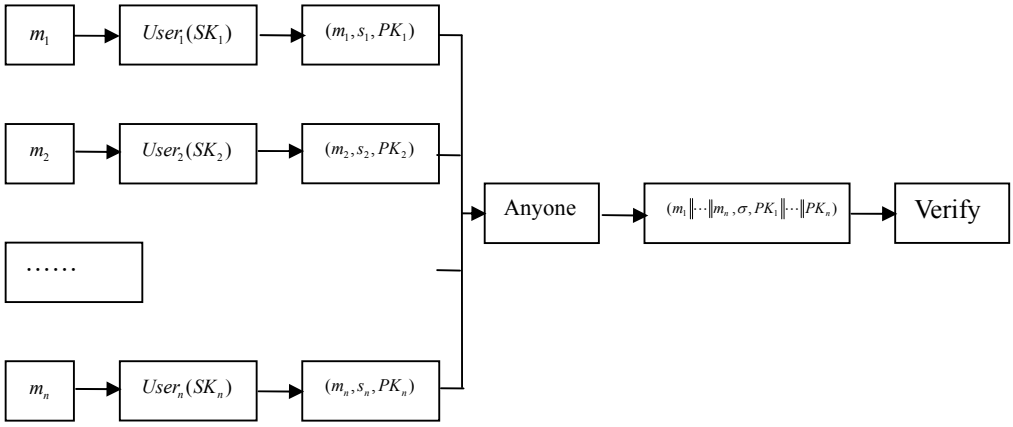

FIGURE 1. Mechanism of an AS scheme

Subsequently, in 2004, Lysyanskaya et al. proposed another aggregate signature scheme (we refer to their scheme as the LMRS scheme), namely *sequential aggregate signature* (SAS) *scheme* [3]. The LMRS scheme is based on the *RSA assumption*. In a sequential aggregate signature scheme, the aggregate signature cannot be produced by an outsider; instead, it must be constructed sequentially by each signer modifying the aggregate-so-far signature in turn. Figure 2 shows how a sequential aggregate signature scheme works differently from an aggregate signature scheme. SAS schemes can also reduce bandwidth and save storage; moreover, when a SAS is verified, not only the validity but also the order in which each signer signed can be verified.

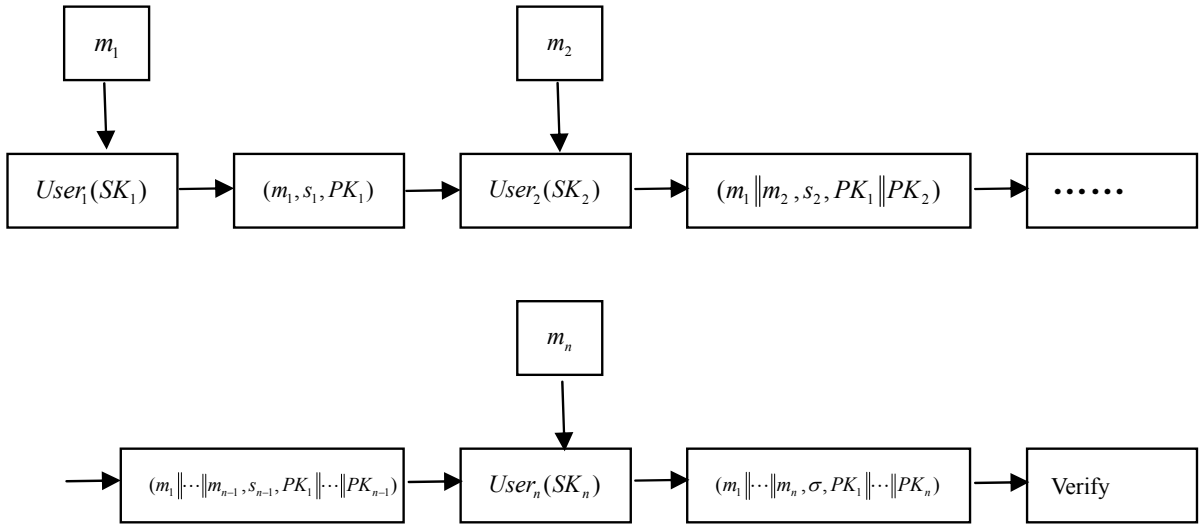

FIGURE 2. How a SAS scheme works

Applications of AS and SAS. AS and SAS schemes can be applied to traffic control, banking transaction and military applications. Particularly, AS and SAS schemes are suitable for the secure border gateway protocol (S-BGP), which is designed to improve the security of the global Internet routing system. This application has been explored in detail by [4]. In the scenario of S-BGP, each router receives a list of n signatures attesting to a certain path of length n in the network. A router signs its own segment in the path and passes the resulting list of $n + 1$ signatures to the next router. When an AS scheme or a SAS scheme is used in S-BGP, one can significantly reduce associated bandwidth overhead and memory space for signatures.

Both the AS scheme of [2] and the SAS scheme of [3] are based on the traditional *public-key-infrastructure* (PKI)-based cryptograph. However, for AS and SAS schemes in the PKI-based cryptograph, one still needs the public keys of all cosigners in order to verify the validity of such an aggregate signature. In most applications these public keys will have to be transmitted along with the aggregate signature. Each public key may come with an associated certificate containing a signature from a certification authority (CA) and the CA's public key, which on its turn may come with a chain of certificates leading to the root CA. Altogether, these sum up to many bits to be transmitted, which partially defeats the primary purpose of using an AS or SAS scheme, namely to reduce bandwidth.

In 1984, Shamir proposed a new model for public key cryptography, the *identity-based cryptography* (IBC) [5]. In paper [5], Shamir constructed an *identity-based signature* (IBS) *scheme*. The central idea of IBC or IBS is to simplify public-key and certificate managements by using a user's "identity" (e.g., its email address, telephone number and IP address) as its public key. A trusted private key generator (PKG) provides each signer with the secret signing key corresponding to his identity.

The features of an IBS scheme make it particularly appealing for use in conjunction with AS and SAS schemes. In 2005, Cheng et al. combined IBS and AS to propose an *identity-based aggregate signature* (IBAS) *scheme* (we refer to their scheme as the CLW scheme) [6]. The CLW scheme is the first identity-based aggregate signature. The scheme of [6] is interactive because the cosigners should broadcast some data to each other before signing. The length of the aggregate signature of [6] is constant. In 2005, Xu et al. proposed another non-interactive IBAS scheme (we refer to their scheme as the XZF scheme) with non-constant aggregate signature length [7]. Subsequently, in 2006, Gentry and Ramzan proposed an interactive IBAS scheme (we refer to their scheme as the GR scheme) with constant aggregate signature length [8]. In 2008, Wang et al. claimed the IBAS scheme they designed is the most efficient scheme [9]. In the same year of 2008, Wen et al. proposed an efficient IBAS scheme [10]. However, the schemes in [9,10] have been proven unsecure, as shown in [11].

All the above IBAS schemes are constructed from *pairings* on elliptic curves.

Motivation. While pairings are very useful in the design of cryptographic protocols, they were only recently brought to the attention of cryptographers [12] and therefore did not enjoy the same exposure to cryptanalytic attacks by experts as other old problems from number theory such as the discrete logarithm problem (DLP), the integer factoring problem (IFP) and RSA. This exposure is necessary to build confidence in the difficulty of the underlying problems; without it, their use in high-security applications may not be advisable. In fact, the following example shows that pairings are not thoroughly understood by the community of cryptography.

At CCS 2007, Boldyreva et al. combined IBS and SAS to construct the first *identity-based sequential aggregate signature* (IBSAS) *scheme* [13]. An IBSAS scheme allows multiple signers to sequentially produce a short signature of different messages and also allows signers to attest to these messages as well as the order in which they signed, and the signature verification of an IBSAS scheme does not require knowledge of traditional public keys.

The IBSAS scheme in [13] is also based on pairings. The authors in [13] proposed a new assumption on parings, and claimed the assumption they proposed is reasonably difficult. However, in 2009, Hwang et al. in [14] pointed out that the paring assumption used in [15] is not intractable, and they mounted a forgery attack on the IBSAS scheme in [13].

When compared with the RSA-based cryptography, pairing-based cryptography has another drawback. While efficient implementations of RSA are ubiquitous, implementation of pairings are much harder, and it is often difficult to fulfill or impossible to generate curves with the desired security parameters [1]. Companies may have invested in implementations of RSA, and may be reluctant to reinvest in new pairing implementations [1]. It is valuable and important to find alternative constructions of a pairing based cryptographic primitive from RSA.

To our best knowledge, all the existing IBAS schemes are constructed from pairings on elliptic curves and the design of a secure identity-based sequential aggregate signature scheme is still an open problem.

Our contribution. In this paper, we propose a secure IBSAS scheme which is not based on pairings, but from RSA. To our best knowledge, our scheme is the first provably secure identity-based sequential aggregate signature scheme from RSA. The basic scheme we propose is non-interactive and the aggregate signature length is not constant. We also give an interactive variant of our scheme, and in the variant scheme, the length of the aggregate signature is constant. Our schemes are based on the Guilliou-Quisquater (GQ) identity-based signature [15]. The existing secure model for IBSAS schemes is *secure against existential forgery on adaptively chosen message and ID attack* [13]. To prove the security of our scheme in the random oracle model, we define a new strong secure model for IBSAS schemes, namely *secure against existential forgery on adaptively chosen message and given ID attack*. We also give the relation between these two secure models.

Other related works. There are many works to propose alternative construction using RSA or IFP of the existing cryptography primitives. In 2007, Bellare and Neven proposed a new identity-based multi-signature (IBMS) scheme from RSA [1]. In 2008, Harn and Ren proposed an identity-based RSA multi-signature scheme [16]. The schemes in [1,16] are interactive because the signers should broadcast some data to each other before singing. There are other related papers [19,20].

Organization. The rest of the paper is organized as follows. In Section 2, we give some preliminaries. In Section 3, we give some formal definitions and the security model of identity-based sequential aggregate signatures. In Section 4, we present a new IBSAS scheme from RSA. In Section 5, the security proof of our scheme is given. In Section 6, we compare our scheme with some existing schemes. In Section 7, we propose an interactive variant of our scheme. In Section 8, we give the potential applications of our scheme. And we end with concluding remarks in Section 9.

2. Preliminaries.

In this section, we give some necessary preliminaries.

2.1. Notations.

$\{0,1\}^{l_1}$ denotes bit strings with length l_1, and $\{0,1\}^*$ denotes bit strings with arbitrary length. Z_N^* denotes the multiplicative group of the unit elements of the ring Z_N. $\phi(N)$ denotes the Euler ϕ-*function* of integer N. Both $e \in_R Z_{\phi(N)}^*$ and $y \leftarrow Z_N^*$ denote the operations of choosing an element e (or y) from $Z_{\phi(N)}^*$ (or Z_N^*) randomly.

2.2. The GQ IBS scheme.

The GQ identity-based signature scheme consists of four algorithms as follows [15]:

Setup: The trusted private-key generator (PKG) generates an RSA modulus N (which is the product of two large primes p and q), and exponents e, d such that $ed = 1 \bmod \phi(N)$. Its master public key is (N, e) and d is the corresponding master secret key. PKG also makes public two hash functions $H_1 : \{0,1\}^* \to \{0,1\}^{l_1}$, $H_2 : \{0,1\}^* \to Z_N^*$.

KeyDer: For any user's identity $ID \in \{0,1\}^*$, PKG computes $g^e = H_2(ID)$, and PKG sends g to the user ID as his private key.
Sign: For a message $m \in \{0,1\}^*$, a user ID first chooses a random number $r \in Z_N$, and then computes $t = r^e \bmod N$, $s = rg^{H_1(t,m)} \bmod N$. $\sigma = (t,s)$ is the signature on m.
Vf: The identity-based signature $\sigma = (t,s)$ of a signer with identity ID on message m is valid if and only if $s^e = tH_2(ID)^{H_1(t,m)} \bmod N$ holds.

2.3. **RSA assumption.** We now recall the well known RSAP and the RSA assumption.

RSAP. Given $N = pq$ (an RSA modulus), $e \in_R Z^*_{\phi(N)}$, $y \in_R Z^*_N$. Find x such that $x^e = y \bmod N$.

Definition 2.1. *An algorithm A is said to (t,ε)-solves RSAP if in at most time t, such that*

$$Adv(A) = \Pr\left[x^e = y \bmod N; (N,e) \leftarrow RSA(1^k); y \leftarrow Z^*_N; x \leftarrow A(N,e,y)\right] \geq \varepsilon. \quad (1)$$

RSA Assumption. There is no algorithm A which is (t,ε)-solves RSAP.

3. **Identity-Based Sequential Aggregate Signature Schemes.** In this section, we give the formal definitions and the security model of IBSAS schemes. We adopt the main notions in [13].

3.1. **The formal definition of an IBSAS scheme.**

Definition 3.1. *An IBSAS scheme IBSAS = (Setup, KeyDer, Sign, Vf) consists of four algorithms:*

Setup: Setup initially run by the trusted private-key generator (PKG) to generate its master public key mpk and corresponding master secret key msk.
KeyDer: KeyDer run by PKG on inputs msk, a user's identity $ID \in \{0,1\}^*$, to generate the private key for user ID, we identify user with his ID.
Sign: Sign run by a user ID_i on inputs its secret key sk_{ID}, a message $m_i \in \{0,1\}^*$, a list $((ID_1,m_1),\cdots,(ID_{i-1},m_{i-1}))$ of identity-message pairs, and an aggregate-so-far σ. It returns a new aggregate signature σ' on message sequences $(m_1,\cdots,m_i)$ by identity sequences $(ID_1,\cdots,ID_i)$, or $\perp$ to indicate the input was invalid.
Vf: Vf takes as inputs the master public key mpk, a list $((ID_1,m_1),\cdots,(ID_n,m_n))$ of identity-message pairs and an IBSAS σ, and outputs 1 if σ is a valid identity-based aggregate signature on message sequences $(m_1,\cdots,m_n)$ by identity sequences $(ID_1,\cdots,ID_n)$, or outputs 0 otherwise.

The existing popular security model of IBSAS schemes is the so called secure against existential forgery on adaptively chosen message and ID attack.

3.2. **Secure against existential forgery on adaptively chosen message and ID attack.** Let IBSAS = (Setup; KeyDer; Sign; Vf) be an IBSAS scheme. To give the security model of IBSAS schemes, we consider the following game associated with a challenger C and a forger A with access to three oracles. A's advantage, $\mathrm{AdvIBSAS}_A$, is defined as his probability to win in the game.

1. C first generates a master key-pair (mpk, msk) by running Setup. (mpk, msk) is given to A.
2. A can issue the following queries as he wants.
   (a) Hash function query: C computes the value of the hash function for the requested input and sends the value to A.

(b) KeyDer query: Given an identity ID, C returns the corresponding private key.
(c) Sign query: Given an identity ID_i, a message m_i, a list of $((ID_1, m_1), \cdots, (ID_{i-1}, m_{i-1}))$, and an aggregate-so-farσ, C returns a new aggregate signature σ' on message sequences $(m_1, \cdots, m_i)$ by identity sequences $(ID_1, \cdots, ID_i)$.

3. Eventually, A outputs a list of identity-messages pairs $((ID_1^*, m_1^*), \cdots, (ID_n^*, m_n^*))$ and corresponding aggregate signature σ^*.

We say A wins the game if (1) σ^* is a valid IBSAS on message sequences $(m_1^*, \cdots, m_n^*)$ by identity sequences $(ID_1^*, \cdots, ID_n^*)$; (2) there exists some $i^* \in \{1, 2, \cdots, n\}$ such that ID_{i^*} was not queried to KeyDer query; (3) $((ID_1^*, m_1^*), \cdots, (ID_{i^*}^*, m_{i^*}^*))$ was not queried to Sign query.

Definition 3.2. *An IBSAS forger A is said to $(t, q_H, q_K, q_S, n, \varepsilon)$-breaks an IBSAS scheme if: A runs in time at most t; A makes at most q_H queries to the Hash function query; q_K queries to the KeyDer query and q_S queries to the Sign query; $AdvIBSAS_A$ is at least ε; and the forged IBSAS signature is by at most n users. An IBSAS scheme is $(t, q_H, q_K, q_S, n, \varepsilon)$-secure against existential forgery on adaptively chosen message and ID attack in the random oracle if no such forger $(t, q_H, q_K, q_S, n, \varepsilon)$-breaks it.*

In order to make the security proof of our proposed scheme easier, we now give a new security model of IBSAS schemes. We will show our new security model is stronger than the existing security model for IBSAS schemes.

3.3. **Secure against existential forgery on adaptively chosen message and given ID attack.** Consider the following variant of the above game: in Step 1, C fixes an Identity ID, C then sends to A (mpk, msk) together with this ID, and in Step 3, A must output a sequential aggregate signature with the fixed ID has the property of the above ID_{i^*}. We also define $A's$ advantage, $\mathrm{AdvIBSAS}_A$, to be his probability to win in the variant game. For the variant game, we give a similar definition.

Definition 3.3. *An IBSAS forger A is said to $(t, q_H, q_K, q_S, n, \varepsilon)$-breaks an IBSAS scheme if: A runs in time at most t; A makes at most q_H queries to the Hash function query; q_K queries to the KeyDer query and q_S queries to the Sign query; $AdvIBSAS_A$ is at least ε; and the forged IBSAS signature is by at most n users. An IBSAS scheme is $(t, q_H, q_K, q_S, n, \varepsilon)$-secure against existential forgery on adaptively chosen message and given ID attack in the random oracle if no such forger $(t, q_H, q_K, q_S, n, \varepsilon)$-breaks it.*

3.4. **Relation between adaptively chosen ID attacks and given ID attacks.** Cha and Cheon have gotten the result that, for an IBS scheme, secure against existential forgery on adaptively chosen message and given ID attacks implies secure against existential forgery on adaptively chosen message and ID attacks [17]. Their result is also applicable for IBSAS schemes. In fact, we have

Lemma 3.1. *If there is an algorithm A_1 which is $(t, q_H, q_K, q_S, n, \varepsilon)$-existential forgery on adaptively chosen message and ID attack to an IBSAS scheme, then there is an algorithm A_2 which is $(t, q_H, q_K, q_S, n, \varepsilon')$-existential forgery on adaptively chosen message and given ID attack to this IBSAS scheme with $\varepsilon' \geq \frac{e}{q_H}\left(1 - \frac{1}{|H|}\right)$, here $|H|$ is the cardinality of the domain of the hash function H.*

Proof: In this paper, we only consider the security of an IBSAS scheme in the random oracle model. Without loss of generality, we suppose the hash functions for ID's and messages are the same hash function H and the size of this hash function is $|H|$.

Suppose A_1 is $(t, q_H, q_K, q_S, n, \varepsilon)$-existential forgery on adaptively chosen message and ID attack to an IBSAS scheme, we define the Hash function query, KeyDer query and Sign query for algorithm A_1 to be $Hash^1$, $Extract^1$ and $Sign^1$, respectively. We now construct an algorithm A_2 which is existential forgery on adaptively chosen message and given ID attack to this IBSAS scheme. The algorithm A_2 is given the system parameters and an fixed ID and we assume the Hash function query, KeyDer query and Sign query for algorithm A_2 to be $Hash^2$, $Extract^2$ and $Sign^2$ respectively, then A_2 can be constructed as follows:

1. Choose $r \in \{1, 2, 3, \cdots, q_H\}$ randomly. Denote by ID_i^1 the input i-th hash query to $Hash^1$ for identities. Let ID_i^1 be the fixed ID if $i = r$.
2. Run A_1 with the system parameters which are given to A_2. A_2 responds to A_1's queries $Hash^1$, $Extract^1$ and $Sign^1$ by evaluating its own $Hash^2$, $Extract^2$ and $Sign^2$.
3. At last, A_1 outputs the forgery signature $(((ID_1^*, m_1^*), \cdots, (ID_n^*, m_n^*)), \sigma^*)$ with ID_{i^*} not queried to $Extract^1$.
4. If $ID_{i^*} = ID$ and $(((ID_1^*, m_1^*), \cdots, (ID_n^*, m_n^*)), \sigma^*)$ is valid, A_2 outputs $(((ID_1^*, m_1^*), \cdots, (ID_n^*, m_n^*)), \sigma^*)$; otherwise outputs fail.

Since the distribution produced by $Hash^1$, $Extract^1$ and $Sign^1$ are indistinguishable from those produced by $Hash^2$, $Extract^2$ and $Sign^2$, A_1 learns nothing from the query results, and hence

$$\Pr\left[(((ID_1^*, m_1^*), \cdots, (ID_n^*, m_n^*)), \sigma^*) \text{ is valid}\right] \geq \varepsilon. \tag{2}$$

Since H is random oracle, the probability that $(((ID_1^*, m_1^*), \cdots, (ID_n^*, m_n^*)), \sigma^*)$ is valid without querying ID_{i^*} to $Hash^1$ is negligible, in fact

$$\Pr\left[ID_i^* = ID_j \text{ for some } j \mid (((ID_1^*, m_1^*), \cdots, (ID_n^*, m_n^*)), \sigma^*) \text{ is valid}\right] \geq 1 - \frac{1}{|H|}. \tag{3}$$

Since r is independently chosen, we have

$$\Pr[ID_i^* = ID \,|ID_i^* = ID_j \text{ for some } j] \geq \frac{1}{q_H}. \tag{4}$$

Combining these, we hence have

$$\begin{aligned}\Pr[ID_i^* = ID_r = ID \text{ and } (((ID_1^*, m_1^*), \cdots, \\ (ID_n^*, m_n^*)), \sigma^*) \text{ is valid}] \geq \frac{\varepsilon}{q_H}\left(1 - \frac{1}{|H|}\right).\end{aligned} \tag{5}$$

It is obvious that the time in which A_2 runs is not more than the time in which A_1 runs. From the above analysis, we know that A_2 is $(t, q_H, q_K, q_S, n, \varepsilon')$-existential forgery on adaptively chosen message and given ID attacks to the IBSAS scheme with $\varepsilon' \geq \frac{e}{q_H}\left(1 - \frac{1}{|H|}\right)$, here $|H|$ is the size of the hash function H. □

From Lemma 3.1, we obtain that an IBSAS scheme which is secure against existential forgery on adaptively chosen message and given ID attacks implies that it is also secure against existential forgery on adaptively chosen message and ID attacks.

4. **Our Proposed IBSAS Scheme from RSA.**

In this section, we present an IBSAS scheme based on the GQ identity-based signature scheme.

4.1. **Our IBSAS scheme.** Our scheme consists of four algorithms as follows:

Setup: PKG generates an RSA modulus $N = pq$ and exponents e, d such that $ed \equiv 1 \bmod \phi(N)$, where e has a large length. Its master public key is (N, e) and d is the corresponding master secret key. PKG also makes two hash functions $H_1 : \{0,1\}^* \to \{0,1\}^{l_1}$, $H_2 : \{0,1\}^* \to Z_N^*$ public.

KeyDer: For any user's identity $ID_i \in \{0,1\}^*$, PKG computes $g_i^e = H_2(ID_i)$, and sends g_i to him as his private key.

Sign: On inputs a list $((ID_1, m_1), \cdots, (ID_{i-1}, m_{i-1}))$ of identity-message pairs, an aggregate-so-far signature $\sigma' = ((s', (t_1, \cdots, t_{i-1}))$ (If $i = 1$, let $s' = 1 \bmod N$, no t), and a message $m_i \in \{0,1\}^*$, user ID_i firstly chooses a random number $r \in Z_N^*$, and then computes $t_i = r^e \bmod N$, $s = s' r g_i^{H_1(t_1\|t_2\|\cdots\|t_i, ID_1\|ID_2\|\cdots\|ID_i, m_1\|m_2\|\cdots\|m_i)} \bmod N$, let $\sigma = ((s, (t_1, \cdots, t_i))$, σ be the IBSAS signature on $((ID_1, m_1), \cdots, (ID_i, m_i))$.

Vf: On inputs (N, e), $((ID_1, m_1), \cdots, (ID_n, m_n))$, $\sigma = ((s, (t_1, \cdots, t_n))$, one can verify the IBSAS signature by doing the following computations:

$$v_0 = s^e \left(\prod_{i=1}^{n} t_i H_2(ID_i)^{H_1(t_1\|t_2\|\cdots\|t_i, ID_1\|ID_2\|\cdots\|ID_i, m_1\|m_2\|\cdots\|m_i)} \right)^{-1} \bmod N. \tag{6}$$

Accept $\sigma = ((s, (t_1, \cdots, t_n))$ as a valid signature if $v_0 = 1 \bmod N$, otherwise $\sigma = ((s, (t_1, \cdots, t_n))$ is invalid.

4.2. **Correctness of the proposed scheme.** Let

$$v_n = s^e \bmod N, \tag{7}$$

$$v_{n-1} = v_n \Big(t_n H_2(ID_n)^{H_1(t_1\|t_2\|\cdots\|t_n, ID_1\|ID_2\|\cdots\|ID_n, m_1\|m_2\|\cdots\|m_n)} \Big)^{-1} \bmod N, \tag{8}$$

$$v_{n-2} = v_{n-1} \Big(t_{n-1} H_2(ID_{n-1})^{H_1(t_1\|t_2\|\cdots\|t_{n-1}, ID_1\|ID_2\|\cdots\|ID_{n-1}, m_1\|m_2\|\cdots\|m_{n-1})} \Big)^{-1} \bmod N, \tag{9}$$

$$\cdots,$$

$$v_1 = v_2 \Big(t_2 H_2(ID_2)^{H_1(t_1\|t_2, ID_1\|ID_2, m_1\|m_2)} \Big)^{-1} \bmod N, \tag{10}$$

$$v_0 = v_1 \Big(t_1 H_2(ID_1)^{H_1(t_1, ID_1, m_1)} \Big)^{-1} \bmod N. \tag{11}$$

From the Sign algorithm of our IBSAS scheme, $\sigma = ((s, (t_1, \cdots, t_n))$ is a valid aggregate signature if and only if $v_0 = 1 \bmod N$ holds. On the other hand, by simple computation, we have

$$v_0 = s^e \left(\prod_{i=1}^{n} t_i H_2(ID_i)^{H_1(t_1\|t_2\|\cdots\|t_i, ID_1\|ID_2\|\cdots\|ID_i, m_1\|m_2\|\cdots\|m_i)} \right)^{-1} \bmod N. \tag{12}$$

4.3. **Efficiency of the proposed scheme.** The length of the aggregate signature in our IBSAS scheme depends on the number of users, and thus is not constant. However, in the n users setting, our scheme can save 50% storage in comparison with the GQ identity-based signature without aggregation, since in our scheme $\sigma = ((s, (t_1, \cdots, t_n))$ is stored while $\sigma_1 = (s_1, t_1)$, $\sigma_2 = (s_2, t_2)$, ..., $\sigma_n = (s_n, t_n)$ should be stored if no aggregation.

5. **Security of Our Scheme.** In this section, we prove the security of our scheme. The security of our scheme is from the following theorem.

Theorem 5.1. *Our proposed IBSAS scheme is secure against existential forgery on adaptively chosen message and ID attacks in the random oracle model under the RSA assumption.*

Proof: From Lemma 3.1, we only need to prove that our scheme is secure against existential forgery on adaptively chosen message and given ID attacks in the random oracle model. Thus Theorem 5.1 can be obtained from the following lemma. □

Lemma 5.1. *If there is a* $(t, q_H, q_K, q_S, n, \varepsilon)$ *forger* F *to our IBSAS scheme under adaptively chosen message and given ID attacks, then there exists an algorithm* A *which is* (t', ε')*-solves RSAP, with* $\varepsilon' \geq \frac{\varepsilon^2}{q_H+1} - \frac{1}{2^{l_1}}$, $t' \leq 2t + 2(q_H + q_K + 2q_S + 1)t_{\exp}$, *where* $t_{\exp}$ *is the time of an modular exponentiation in* Z_N^*.

Proof: Suppose a forger F, we can construct an algorithm A to solve RSAP. A is given $N = pq$ (the product of two large primes p and q), $e \in_R Z_{\phi(N)}^*$, $y \in_R Z_N^*$, A chooses an identity ID^A, and let $H_2(ID^A) = z^e y \bmod N$ where $z \in_R Z_N^*$. A sends (N, e) and ID^A to F. A answers F's queries as follows.

Hash function query. When F queries $(t_1\| \cdots \|t_i, ID_1\| \cdots \|ID_i, m_1\| \cdots \|m_i)$ to H_1, A returns an $u \in_R \{0,1\}^{l_1}$ as the hash value of $H_1(t_1\| \cdots \|t_i, ID_1\| \cdots \|ID_i, m_1\| \cdots \|m_i)$. When F queries ID_i to H_2, A chooses a random number $z_i \in Z_N^*$, and returns $z_i^e \bmod N$ as the hash value of $H_2(ID_i)$; if F queries ID^A to H_2, A returns $z^e y \bmod N$ as the hash value of $H_2(ID^A)$. A makes two lists H_1-list $< (t_1\| \cdots \|t_i, ID_1\| \cdots \|ID_i, m_1\| \cdots \|m_i), u >$, H_2-list $< ID_i, z_i, z_i^e >$ to record these queries.

KeyDer query. Given an identity ID_i, if ID_i has been added to H_2-list, A returns z_i. Otherwise A runs hash function query again, and then returns z_i.

Sign query. We consider two cases.

Case 1: If F queries identity ID_i (if H_2-list has no ID_i, A runs key derivation query again), a message m_i, a list of $((ID_1, m_1), \cdots, (ID_{i-1}, m_{i-1}))$, and an aggregate-so-far $\sigma' = ((s', (t_1, \cdots, t_{i-1}))$, A returns the new aggregate signature σ on message sequences $(m_1, \cdots, m_i)$ by identity sequences $(ID_1, \cdots, ID_i)$ following the real IBSAS scheme of ours using z_i as a secret key.

Case 2: If F queries identity ID^A, a message m_i, a list of $((ID_1, m_1), \cdots, (ID_{i-1}, m_{i-1}))$, and an aggregate-so-far $\sigma' = ((s', (t_1, \cdots, t_{i-1}))$, A first chooses a $k \in_R \{0,1\}^{l_1}$, then computes $t_i = (y^{-1})^k \bmod N$, and lets $H_1(t_1\| \cdots \|t_i, ID_1\| \cdots \|ID^A, m_1\| \cdots \|m_i) = k$, $s = z^k s' \bmod N$. A returns the new aggregate signature $\sigma = ((s, (t_1, \cdots, t_i))$ on message sequences $(m_1, \cdots, m_i)$ by identity sequences $(ID_1, \cdots, ID^A)$.

F's output. Because A can answer F's queries perfectly, F can give a forgery IBSAS signature $\sigma_F = ((s_F, (t_1, \cdots, t_n))$ on $((ID_1^*, m_1^*), \cdots, (ID_n^*, m_n^*))$ with probability ε in at most time t, such that $ID_{i^*} = ID^A$, $ID_{i^*} \in \{ID_1^*, \cdots, ID_n^*\}$. From the general forking lemma in [18], when A uses another random oracle to replay F, F can also give another forgery IBSAS signature $\sigma'_F = ((s'_F, (t'_1, \cdots, t'_n))$ on the same list $((ID_1^*, m_1^*), \cdots, (ID_n^*, m_n^*))$ with $\varepsilon' \geq \frac{\varepsilon^2}{q_H+1} - \frac{1}{2^{l_1}}$, such that

$$t'_i = t_i \quad (i = 1, 2, \cdots, n), \tag{13}$$

$$\begin{aligned} &H_1(t'_1\| \cdots \|t'_i, ID_1^*\| \cdots \|ID_i^*, m_1^*\| \cdots \|m_i^*) \\ &= H_1(t_1\| \cdots \|t_i, ID_1^*\| \cdots \|ID_i^*, m_1^*\| \cdots \|m_i^*) \ (i = 1, \cdots, i^* - 1, i^* + 1, \cdots, n), \end{aligned} \tag{14}$$

$$\begin{aligned} &H_1(t'_1\| \cdots \|t'_{i^*}, ID_1^*\| \cdots \|ID^A, m_1^*\| \cdots \|m_{i^*}^*) \\ &\neq H_1(t_1\| \cdots \|t_{i^*}, ID_1^*\| \cdots \|ID^A, m_1^*\| \cdots \|m_{i^*}^*). \end{aligned} \tag{15}$$

Let

$$H_1(t'_1\|\cdots\|t'_{i^*}, ID_1^*\|\cdots\|ID^A, m_1^*\|\cdots\|m_{i^*}^*) = c, \tag{16}$$

$$H_1(t_1\|\cdots\|t_{i^*}, ID_1^*\|\cdots\|ID^A, m_1^*\|\cdots\|m_{i^*}^*) = c'. \tag{17}$$

A's output. $\sigma_F = ((s_F, (t_1, \cdots, t_n))$ and $\sigma'_F = ((s'_F, (t'_1, \cdots, t'_n))$ are valid signatures, so according to the verification algorithm, the following equality holds,

$$\begin{aligned} & s_F^e \left(\prod_{i=1}^{n} t_i H_2(ID_i)^{H_1(t_1\|\cdots\|t_i, ID_1^*\|\cdots\|ID_i^*, m_1^*\|\cdots\|m_i^*)} \right)^{-1} \\ = & {s'_F}^e \left(\prod_{i=1}^{n} t'_i H_2(ID_i)^{H_1(t'_1\|\cdots\|t'_i, ID_1^*\|\cdots\|ID_i^*, m_1^*\|\cdots\|m_i^*)} \right)^{-1} = 1 \bmod N. \end{aligned} \tag{18}$$

From Equations (13)-(17), we have

$$s_F^e \left(H_2(ID^A)^c\right)^{-1} = {s'_F}^e \left(H_2\left(ID^A\right)^{c'}\right)^{-1} \bmod N. \tag{19}$$

And then

$$s_F^e ((z^e y)^c)^{-1} = {s'_F}^e \left((z^e y)^{c'}\right)^{-1} \bmod N. \tag{20}$$

And hence

$$\left(s_F z^{c'} (s'_F z^c)^{-1}\right)^e = y^{c-c'} \bmod N. \tag{21}$$

Because the length of e is greater than $c - c'$, e and $c - c'$ are coprime. Then there exist a and b such that $ae + b(c - c') = 1$, and from Equation (21) we have

$$y = y^{ae+b(c-c')} = y^{ae} y^{b(c-c')} = \left(y^a \left(s_F z^{c'} (s'_F z^c)^{-1}\right)^b\right)^e \bmod N. \tag{22}$$

For $N = pq$, $e \in_R Z_{\phi(N)^*}$, $y \in_R Z_N^*$, A now can find $x = y^a (s_F z^{c'} (s'_F z^c)^{-1})^b \bmod N$ such that $x^e = y \bmod N$ with probability $\varepsilon' \geq \frac{\varepsilon^2}{q_H+1} - \frac{1}{2^{l_1}}$.

Lastly, A returns x.

We now compute the bound for the running time of A. A's running time is that of the forger F and replay F, plus the time to answer the queries of F and replay F, plus two exponentiation to compute x. Each hash function query and key derivation query takes at most one exponentiation. A signature query takes two exponentiations. We therefore have $t' \leq 2t + 2(q_H + q_K + 2q_S + 1)t_{\exp}$, where $t_{\exp}$ is the time of an modular exponentiation in Z_N^*.

From the above analysis, we know that the algorithm A we construct is (t', ε')-solves RSAP, with $\varepsilon' \geq \frac{\varepsilon^2}{q_H+1} - \frac{1}{2^{l_1}}$, $t' \leq 2t + 2(q_H + q_K + 2q_S + 1)t_{\exp}$. □

6. **Comparisons.** In Table 1 below, we compare the proposed scheme with the existing secure identity-based aggregate signature schemes. We assume there are n cosigners involved. We compare them by using four viewpoints: (1) Interactive or non-interactive: In an interactive scheme the cosigners must broadcast some data to each other, which makes it much less efficient than a non-interactive scheme. (2) Assumption: we compare the assumptions the schemes are based on. We point out the RSA assumption is preferable to the pairing assumption, for the RSA assumption are much more to be understood than the pairing assumption. (3) Signing and verification complexity: Here E denotes the exponential computation and P denotes the pairing computation. Note that the cost of one pairing computation is roughly that of 6-20 exponential computations. (4) Saving on signature storage: We compare the signature storage with aggregation and the signature storage without aggregation. Here constant means that the length of the

aggregate signature is constant. Constant is the best one. From Table 1, we can see that the proposed scheme is not only much more efficient that the existing schemes, but also based on the more general RSA assumption.

TABLE 1. The comparisons between our scheme and other IBAS schemes

	Interactive?	Assumption	Sign Complexity	Veri Complexity	Saving
CLW [6]	Yes	Paring	$2nE$	$nE + 2P$	Constant
XZF [7]	No	Paring	$2nE$	$(2n + 1)P$	50%
GR [8]	Yes	Paring	$4nE$	$nE + 3P$	Constant
Our scheme	No	RSA	nE	$(n + 1)E$	50%

7. **Interactive Variant of Our Scheme.** In this section, we propose an interactive variant of our scheme to achieve constant aggregate signature length.

7.1. **Our interactive IBSAS scheme.** The proposed invariant IBSAS scheme consists of four algorithms as follows. Setup and KeyDer are the same as the non-interactive scheme. Sign: Before signing a message sequence, the n user $ID_1, \cdots, ID_n$ chooses a random number $r_i \in Z_N$ and computes $t_i = r_i^e \bmod N$ respectively, meanwhile broadcasts this t_i. Every user computes $t = \prod_{i=1}^{n} t_i \bmod N$. On inputs a list $((ID_1, m_1), \cdots, (ID_{i-1}, m_{i-1}))$ of identity-message pairs, an aggregate-so-far signature $\sigma' = (s', t)$ (if $i = 1$, $s' = 1 \bmod N$, set $\sigma' = (1 \bmod N)$, no t) and a message $m_i \in \{0,1\}^*$, user ID_i computes $s = s' r_i g_i^{H_1(t, ID_1 \| ID_2 \| \cdots \| ID_i, m_1 \| m_2 \| \cdots \| m_i)} \bmod N$, let $\sigma = (s, t)$, is the IBSAS signature of $((ID_1, m_1), \cdots, (ID_i, m_i))$. Vf: On inputs (N, e), $((ID_1, m_1), \cdots, (ID_n, m_n))$, $\sigma = (s, t)$, one can verify the IBSAS signature by doing the following computations:

$$v_0 = s^e \left(t \prod_{i=1}^{n} H_2(ID_i)^{H_1(t, ID_1 \| ID_2 \| \cdots \| ID_i, m_1 \| m_2 \| \cdots \| m_i)} \right)^{-1} \bmod N. \tag{23}$$

Accept $\sigma = (s, t)$ as a valid signature if $v_0 = 1 \bmod N$; otherwise $\sigma = (s, t)$ is invalid.

7.2. **Analysis of the proposed variant IBSAS scheme.** We can obtain the correctness and security of this interactive scheme by using the same methods for the non-interactive scheme. Compared with the non-interactive scheme, this interactive scheme has constant signature length, while cost more before signing. As is noted in [1], interactive schemes can be applied to the environment of a wired network of sensors that needs to report back to a remote base station through wireless communications.

8. **A Key Application of Our Scheme: S-BGP.** As we mentioned in the introduction section, sequential aggregate signatures are suitable for S-BGP. If a SAS scheme is used in the traditional PKI-based cryptography, all the cosigners are required to know the authentic public keys of all other parties involved. As a consequence, the certificates of these public keys may lead to so many bits, which defeats the purpose of using sequential aggregate signatures to minimize bandwidth in the first place.

While in an identity-based signature, any arbitrary string (e.g., router's name, router's IP address) can act as a user's public key. It is a compelling work to use IBS to design aggregate signature schemes. In the scenario of S-BGP, most of the information needed to verify an aggregate signature is then already contained in the description of "who signed what" (e.g., the announced prefix and routing path). Hence, the proposed IBSAS schemes

by combining IBS with SAS are very suitable to be used in S-BGP. On the application of IBSAS schemes, we refer to [13] for more details.

9. **Conclusions.** In this paper we propose the first IBSAS scheme from RSA. We propose two schemes. One is non-interactive scheme in which the aggregate signature length is non-constant, and the other is interactive in which the aggregate signature length is constant. How to construct a non-interactive RSA-based IBSAS scheme with constant aggregate signature length is an important open problem.

Acknowledgment. This work is partially supported by The Natural Science Foundation of Jiangsu Province Major Project Grants (No. BK2011023). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] M. Bellare and G. Neven, Identity-based multi-signatures from RSA, *Proc. of CT-RSA'2007, Lecture Notes in Computer Science*, vol.4377, pp.145-162, 2007.
[2] D. Boneh, C. Gentry, B. Lynn and H. Shacham, Aggregate and verifiably encrypted signatures from bilinear maps, *Proc. of EUROCRYPT'2003, Lecture Notes in Computer Science*, vol.2656, pp.416-432, 2003.
[3] A. Lysyanskaya, S. Micali, L. Reyzin and H. Shacham, Sequential aggregate signatures from trapdoor permutations, *Proc. of EUROCRYPT'2004, Lecture Notes in Computer Science*, vol.3027, pp.74-90, 2004.
[4] M. Zhao, S. Smith and D. Nicol, Aggregated path authentication for efficient BGP security, *Proc. of ACM CCS'2005*, pp.128-138, 2005.
[5] A. Shamir, Identity-based cryptosystem and signature scheme, *Proc. of CRYPTO'1984, Lecture Notes in Computer Science*, vol.196, pp.120-126, 1985.
[6] X. Cheng, J. Liu and X. Wang, Identity-based aggregate and verifiably encrypted signatures from bilinear pairing, *Proc. of ICCSA'2005, Lecture Notes in Computer Science*, vol.3483, pp.1046-1054, 2005.
[7] J. Xu, Z. Zhang and D. Feng, ID-based aggregate signatures from bilinear pairings, *Proc. of CANS'2005, Lecture Notes in Computer Science*, vol.3810, pp.110-119, 2005.
[8] C. Gentry and Z. Ramzan, Identity-based aggregate signatures, *Proc. of PKC'2006, Lecture Notes in Computer Science*, vol.3958, pp.257-273, 2006.
[9] Z. Wang, H. Chen, D. Ye and Q. Wu, *Practical Identity-Based Aggregate Signature Scheme from Bilinear Maps*, Shangai Jiao Tong University Press, 2008.
[10] Y. Wen and J. Ma, An aggregate signature scheme with constant pairing operations, *Proc. of CSSE'2008*, pp.830-833, 2008.
[11] S. Selvi, S. Vivek, J. Shriram, S. Kalaivani and C. P. Rangan, Security analysis of aggregate signature and batch verification signature schemes, *Cryptology ePrint Archive, Report 2009/290*, http://eprint.iacr.org/, 2009.
[12] A. Joux, A one round protocol for tripartite Diffie-Hellman, *Proc. of ANTS IV, Lecture Notes in Computer Science*, vol.1838, pp.385-394, 2000.
[13] A. Boldyreva, C. Gentry, A. O'Neill and D. Yum, Ordered multisignatures and identity-based aggregate signatures, with applications to secure routing, *Proc. of ACM CCS'2007*, pp.276-285, 2007.
[14] J. Hwang, D. Lee and M. Yung, Universal forgery of the identity-based sequential aggregate signature scheme, *Proc. of ASIACCS*, pp.157-160, 2009.
[15] L. Guillou and J. Quisquater, A "paradoxical" indentity-based signature scheme resulting from zero knowledge, *Proc. of CRYPTO'1988, Lecture Notes in Computer Science*, vol.403, pp.216-231, 1990.
[16] L. Harn and J. Ren, Efficient identity-based RSA multisignatures, *Computer and Security*, vol.27, pp.12-15, 2008.
[17] J. Cha and J. Cheon, An identity-based signature from gap Diffie-Hellman groups, *Proc. of PKC'2003, Lecture Notes in Computer Science*, vol.2567, pp.18-30, 2003.
[18] M. Bellare and G. Neven, Multi-signatures in the plain public-key model and a general forking lemma, *Proc. of ACM CCS'2006*, pp.390-399, 2005.

[19] C. H. Chen, G. Horng and C. H. Hsu, A novel private information retrieval scheme with fair privacy in the user side and the server side, *International Journal of Innovative Computing, Information and Control*, vol.5, no.3, pp.801-810, 2009.

[20] B. Dou, H. Zhang, C. H. Chen and C. Xu, Verifiably encrypted multi-signature, *ICIC Express Letters*, vol.5, no.5, pp.1697-1701, 2011.