A More Efficient Instantiation of Witness-Indistinguishable Signature

Joseph K. Liu[1] and Duncan S. Wong[2]
(Corresponding author: Duncan S. Wong)

Department of Computer Science, University of Bristol[1]
Bristol, UK (Email: liu@cs.bris.ac.uk)
Department of Computer Science, City University of Hong Kong[2]
Hong Kong, China (Email: duncan@cityu.edu.hk)

(Received Dec. 8, 2005; revised and accepted Jan. 27 & Feb. 20, 2006)

Abstract

A ring signature or a witness-indistinguishable signature is a setup-free group signature with no group manager. Defined by a set of public keys, a group is created spontaneously without any group member's collaboration or awareness. It allows members of the group to sign messages on behalf of the group without revealing their identities (signer anonymity). Since there is no group manager, no one can revoke the identities of the signers. In this paper, we point out that a ring signature scheme proposed by Abe, Ohkubo and Suzuki in ASIACRYPT'2002, is not signer anonymous. We also note that the authors' full paper version in IEICE Transaction Fundamentals contains a different version that defends against our attack. However, the full-paper version is more difficult to implement and is less efficient. We propose a different approach to fix the problem and show that our modification does not degrade the performance of the original scheme and is easier to implement than their full-paper version.

Keywords: Anonymity, ring signature, signature schemes

1 Introduction

A ring signature scheme [1, 5, 9, 13] allows members of a group to sign messages on behalf of the group without revealing their identities (signer anonymity). It is also not possible to decide whether two signatures have been issued by the same group member. Different from a group signature scheme [3, 6, 7], the formation of a group is spontaneous and there is no group manager to revoke the identity of the signer. That is, under the assumption that each user is already associated with the public key of some standard signature scheme, a user can form a group by simply collecting the public keys of all the group members including his own. These diversion group members can be totally unaware of being conscripted into the group.

On signer anonymity, most current ring signature schemes are even providing unconditional anonymity, that is, given a ring signature, a resource-unrestrained entity cannot tell who the signer is among the members of the group defined by the signature.

Ring signatures could be used for whistle blowing [13], anonymous membership authentication for ad hoc groups [5] and many other applications which do not want complicated group formation stage but require signer anonymity. For example, in the whistle blowing scenario, a whistleblower gives out a secret as well as a ring signature of the secret to the public. From the signature, the public can be sure that the secret is indeed given out by a group member while cannot figure out who the whistleblower is.

In [13], Rivest et al. formalized the notion of ring signatures. They also pointed out that the witness-indistinguishable interactive proof due to Cramer et al. [8] can be viewed as a ring signature scheme after combining with the Fiat-Shamir technique [10]. A ring signature scheme constructed using this approach is known as *a Witness-Indistinguishable Signature Scheme*. Cramer et al.'s technique is based on secret sharing and special honest verifier zero-knowledge (Special HVZK) proofs.

In [1, Section 3.1], Abe et al. described a concrete instantiation of witness-indistinguishable signature schemes with a discrete logarithm setting. Here we call it the Abe-Ohkubo-Suzuki Instantiation. The instantiation allows each group member to have different discrete logarithm (DL) domain parameters. This property is generally referred to as separability. The scheme was claimed to be secure under the random oracle model [4] in terms of both existential unforgeability and signer anonymity. However, no proof was given.

In this paper, we point out that the Abe-Ohkubo-Suzuki Instantiation in [1] is not signer anonymous due to some collision property of the committed values in their algorithm. We describe an attacking technique which allow the public, who only has the public keys of the group

members, to identify with overwhelming probability the actual signer of any given signature.

To fix the flaw of [1], we first explain why the collision property on the committed values in their algorithm must be eliminated. We then propose a modification to solve the problem.

We also notice that the authors' full paper version in [2] contains a different version that defends against our attack. However, there is no withdrawal of the security claim of the scheme in [1], nor any explanation on why they changed the algorithm to a more complicated one in their full-paper version. The full-paper version requires additional hash functions for members holding keys in DL groups with orders of different length in binary representation. That is, the number of additional hash functions needed is linear to the number of DL groups with orders in different length. This makes the system less scalable, more difficult to implement and less efficient.

In our modification, we do not need any additional hash operations. Instead, we only introduce a constraint on the domain of committed values that is easy to realize. Our scheme does not degrade the level of anonymity either, that is, it also achieves unconditional anonymity.

In Section 2, we review the Abe-Ohkubo-Suzuki witness-indistinguishable signature scheme and show that it is easy for an adversary to find out the signer of a signature. In Section 3, we propose several approaches for defending against the attack described in Section 2. In Section 4, we compare our solution with the one proposed in [2] in terms of performance. Finally, we conclude the paper in Section 5.

2 Analysis of the Abe-Ohkubo-Suzuki Instantiation in [1]

Let p_i, q_i be large primes. Let $\langle g_i \rangle$ denote a prime subgroup of $\mathbb{Z}_{p_i}^*$ generated by g_i whose order is q_i. For $i = 1, \cdots, n$, user i randomly picks a private key x_i from $\mathbb{Z}_{q_i}$, which is denoted by $x_i \in_R \mathbb{Z}_{q_i}$, computes $y_i = g_i^{x_i} \bmod p_i$, and sets the public key to (p_i, q_i, g_i, y_i). Let $L = \{(p_i, q_i, g_i, y_i)\}_{1 \le i \le n}$.

Let $H : \{0,1\}^* \to \{0,1\}^\ell$ be a hash function viewed as a random oracle, where ℓ is larger than the largest $|q_i|$, $1 \le i \le n$. Sometimes, we pass in the set L for hashing and we implicitly assume that certain appropriate encoding method is applied.

(Signature Generation) For message $m \in \{0,1\}^*$ and the group defined by L, a signer k, $1 \le k \le n$, who owns the private key x_k, generates a signature $\sigma = (c_1, s_1, \cdots, c_n, s_n)$ as follows.

1) For $i = 1, \cdots, n$, $i \ne k$, randomly select $s_i, c_i \in_R \mathbb{Z}_{q_i}$ and compute $z_i = g_i^{s_i} y_i^{c_i} \bmod p_i$.

2) Randomly select $r_k \in_R \mathbb{Z}_{q_k}$ and compute $z_k = g_k^{r_k} \bmod p_k$.

3) Find c_k such that $c_1 \oplus \cdots \oplus c_k \oplus \cdots \oplus c_n = H(L, m, z_1, \cdots, z_n)$.

4) Compute $s_k = r_k - c_k x_k \bmod q_k$.

(Signature Verification) For a triple of group, message and signature, (L, m, σ), it is valid if

$$c_1 \oplus \cdots \oplus c_n = H(L, m, g_1^{s_1} y_1^{c_1} \bmod p_1, \cdots, g_n^{s_n} y_n^{c_n} \bmod p_n).$$

2.1 Anonymity Attack

The attack is straightforward. The idea of the attack is to study the possible information leak from the variation of the length of c_i corresponding to the size of the corresponding group order, for each i from 1 to n.

Notice that if c_k computed in Step 3 of signature generation above is greater than q_k, then it can be sure that the user who owns x_k must be the actual signer because all other c_i's are in their corresponding domains $[0, q_i - 1]$, for $1 \le i \le n$, $i \ne k$.

Suppose $\ell = |q_{max}| + l$ where q_{max} is the largest q_i, $1 \le i \le n$, and $l > 0$. As H is viewed as a random oracle mapping to numbers over the range $[0, 2^\ell - 1]$, the distribution of c_k will be uniform over $[0, 2^\ell - 1]$. Therefore, the chance of having $c_k \ge q_k$ is $1 - q_k/2^\ell$ which is greater than $1 - 2^{-l}$. This is because $1 - q_k/2^\ell \ge 1 - q_{max}/2^\ell \ge 1 - 2^{|q_{max}|}/2^\ell = 1 - 2^{-l}$. Hence even in the special case when $q_k = q_{max}$ and $l = 1$, the chance of leaking the actual signer's identity will still be greater than half. In the general case, since the value of ℓ can be arbitrarily large (so is l), we can see that no matter which member of the group is the actual signer, this scheme will leak the identity of the actual signer with probability arbitrarily close to one.

As a concrete example, consider $l = 1$, some group members are using 1024-bit keys while the others are using 512-bit keys. If the actual signer is the one using a 512-bit key, then the chance of identifying his identity from the signature will be greater than $1 - 2^{-513}$. Hence it is almost certain that the signature is always giving out the actual signer's identity.

3 An Improving Approach

There are several ways to fix the problem. One of the approaches we are focusing on is to minimize the effect on the complexity of the algorithm. We retain the basic operations and procedure of the scheme and have all the c_i's in Step 1 of signature generation be chosen randomly from the *same* space, instead of from the corresponding $\mathbb{Z}_{q_i}$'s.

Let Ψ be the common space. One proposal is to set Ψ to $\{0,1\}^\ell$. Hence in Step 1 of signature generation, $c_i \in_R \{0,1\}^\ell$ for $i = 1, \cdots, n$, $i \ne k$. The rest of the scheme will remain unchanged. By assuming that H is a random oracle, the value of c_k obtained in Step 3 of signature

generation will also be uniformly distributed over $\{0,1\}^\ell$. Signer anonymity can therefore be ensured.

However, there could be more than one possible value of c_i over the range $[0, 2^\ell - 1]$ 'committed' in Step 1 of signature generation by each z_i. That is, for each i, $1 \le i \le n$ and $i \ne k$, $z_i = g_i^{s_i} y_i^{r_i} \bmod p_i$ for all possible values r_i over $[0, 2^\ell - 1]$ such that $r_i \equiv c_i \pmod{q_i}$. Since $\ell > |q_{max}|$, there are at least two values for r_i satisfying the condition above. In the following, we show that this leads us to an attack which allows anyone who knows only the public keys to forge a signature with high probability when the number of group members n exceeds the number of bits ℓ.

(Forgery Algorithm) A signature $\sigma' = (r_1, s_1, \cdots, r_n, s_n)$ of (L, m) can be forged as follows.

1) For $i = 1, \cdots, n$, randomly select $s_i \in_R \mathbb{Z}_{q_i}$ and $c_i \in_R \{0,1\}^\ell$.

2) Compute

$$c = H(L, m, g_1^{s_1} y_1^{c_1} \bmod p_1, \cdots, g_n^{s_n} y_n^{c_n} \bmod p_n)$$

3) Find $r_1, \cdots, r_n$ over $[0, 2^\ell - 1]$ such that $r_1 \oplus \cdots \oplus r_n = c$ and $r_i \equiv c_i \pmod{q_i}$, $1 \le i \le n$.

If the number of values n exceeds the number of bits ℓ, it can be shown that, with high probability, there exists at least one subset of $\{r_i\}_{1 \le i \le n}$ whose XOR is any desired ℓ-bit target c. We can use linear algebra to find the subset. Let $c = a_1 r_1 \oplus \cdots \oplus a_n r_n$ where $a_i = 1/0$, for $1 \le i \le n$. Let $\mathbf{a} = (a_1, \cdots, a_n)$ be the binary vector we want to find. We call it a *selection vector*. Let the binary representation of c be $(c_1, \cdots, c_\ell)$. For each $i = 1, \cdots, n$, let the binary representation of r_i be $(r_{i,1}, \cdots, r_{i,\ell})$. We solve the following set of linear equations to find $\mathbf{a}$ if a solution exists.

$$c_i = a_1 r_{1,i} \oplus \cdots \oplus a_n r_{n,i} \ , \quad \text{for } i = 1, \cdots, \ell.$$

However, our goal is to represent c as the XOR of all the values $r_1, \cdots, r_n$, rather than as an XOR of a proper subset of these values. To overcome this problem, we use the fact above, that is, there are at least two r_i over $[0, 2^\ell - 1]$ satisfying $r_i \equiv c_i \pmod{q_i}$, and give details of Step 3 of the forgery algorithm above in the following.

3a) Set $c' = c \oplus c_1 \oplus \cdots \oplus c_n$.

3b) For $i = 1, \cdots, n$, set $r_i' = c_i \oplus (c_i \bmod q_i)$.

3c) Use the algorithm above to find the subset of $\{r_i'\}_{1 \le i \le n}$ whose XOR is c'. Suppose the corresponding selection vector is $\mathbf{a} = (a_1, \cdots, a_n)$.

3d) For $i = 1, \cdots, n$, if $a_i = 0$, set $r_i = c_i$; otherwise, set $r_i = c_i \bmod q_i$.

Hence if the number of group members n exceeds the number of bits ℓ, anyone can forge a signature with high probability without knowing any of the private keys.

One solution to counteract this attack is to let ℓ grow with n. However, performance is the tradeoff.

Another solution is to make sure that there is only one value in Ψ committed to each z_i in Step 1 of the signature generation algorithm. We propose to set the common space Ψ to $\{0,1\}^\ell$ but change the value of ℓ such that $2^\ell \le q_{min}$, where q_{min} is the smallest q_i, $1 \le i \le n$. For security, the value of ℓ should still be sufficiently large to thwart the birthday attack against H. For example, we can set $\ell = |q_{min}| - 1$ and therefore $\Psi = \{0, 1, \cdots, 2^\ell - 1\}$ when Ψ is considered as a set of integers. Hence the hash function H is now mapping from $\{0,1\}^*$ to $\{0,1\}^{|q_{min}|-1}$. In Step 1 of signature generation, we randomly select $c_i \in_R \Psi$, for $1 \le i \le n$, $i \ne k$. In Step 3, c_k must be in Ψ and will be uniformly distributed (assume H is a random oracle). In practice, we recommend the value of ℓ to be at least 160. In the special case of $|q_{min}| = 160$, we can set $\ell = 160$ and Ψ to $\mathbb{Z}_{q_{min}}$. But we also need to make sure that c_k obtained in Step 3 is also in $\mathbb{Z}_{q_{min}}$. This may require multiple iterations from Step 1 to 3. The number of iterations is expected to be at most 2. In the following, we give a formal security analysis to our modification.

3.1 Security Analysis

The security of a ring signature has two aspects: unforgeability and signer anonymity.

For unforgeability, we follow the definition proposed by Abe et al. [1, 2] that captures the security of existential unforgeability against adaptive chosen message and public-key attacks. Below is a brief description of the definition of [1, 2].

Definition 1 (Existential Unforgeability against Adaptive Chosen Message and Public-key Attacks (Informal)). *Let $\ell \in \mathbb{N}$ be a security parameter. Let $\mathcal{U}$ be a set of N public keys, each is generated honestly according to the underlying scheme with security parameter being set of ℓ. A ring signature scheme is unforgeable if, for any probabilistic polynomial-time algorithm (PPT) $\mathcal{A}$ with signing oracle $\mathcal{SO}$ such that $(L, m, \sigma) \leftarrow \mathcal{A}^{\mathcal{SO}}(1^\ell, \mathcal{U})$, its output σ is a valid signature of message m under the group defined by L only with negligible probability in ℓ, where $L \subseteq \mathcal{U}$ and $|L| = n$. Restriction is that (L, m, σ) should not be in the set of oracle queries and replies between $\mathcal{A}$ and $\mathcal{SO}$.*

In the definition above, the signing oracle $\mathcal{SO}$ takes as inputs any $L' \subseteq \mathcal{U}$, $|L'| = n'$, and any message m', produces a valid signature σ'. As shown by Liu and Wong [11], this model is stronger than the original one due to Rivest et al. [13]. This stronger model essentially captures the following two kinds of attacks that are not considered in the original model of Rivest et al.: (1) Given several signatures of some message m with respect to a public-key list L, an adversary forges a new signature σ

with respect to the *same* message m and the same public-key list L; (2) Given several signatures of m and L, an adversary forges a new signature with respect to the same message m but a different public-key list L'.

For signer anonymity, we require that given a signature with respect to a group of n members and suppose that the actual signer is chosen at random over these n group members, an adversary should not have any advantage of identifying the identity of the actual signer over random guessing even all private keys are known to the adversary.

Definition 2 (Signer Anonymity (Informal)). *Let L be a set of n public keys, each is generated honestly according to the underlying scheme. A ring signature scheme is signer anonymous if, for any L, any message m, and any valid signature σ on (m, L) generated using a private key x_π corresponding to the public key in L indexed by π, any unbound adversary $\mathcal{A}$ outputs π with probability $1/n$. (Please refer to [1, 2] for the formal definition.)*

In the following, we show that our modification is existentially unforgeable against adaptive chosen message and public-key attacks, and also signer anonymous.

Theorem 1 (Existential Unforgeability). *Given a set $\mathcal{U}$ of N public keys, suppose $\mathcal{A}$ is a PPT algorithm which outputs a valid signature with non-negligible probability in security parameter $\ell \in \mathbb{N}$ as defined in Def. 1, then there exists a PPT algorithm $\mathcal{B}$ which solves the DLP (Discrete Logarithm Problem) with non-negligible probability in ℓ.*

Proof. Let $\ell \in \mathbb{N}$ be a security parameter. Given a forger $\mathcal{A}$ that takes N public keys and generates a valid message-signature pair (m, σ) where $m \in \{0,1\}^*$ and $\sigma = (c_1, s_1, \cdots, c_n, s_n)$, $n \leq N$, we construct an algorithm $\mathcal{B}$ that solves at least one of N discrete-log problem (DLP) instances: Q_1, $\cdots$, Q_N where $Q_i \in \mathbb{Z}^*_{p_i}$ of order q_i, $1 \leq i \leq N$. For $i = 1, \cdots, N$, $\mathcal{B}$ sets $y_i \leftarrow Q_i$. Let $\mathcal{U} = \{(p_1, q_1, g_1, y_1), \cdots, (p_N, q_N, g_N, y_N)\}$. Suppose the corresponding discrete logarithms (i.e. secrets) are x_i, $1 \leq i \leq N$. $\mathcal{B}$ simulates $\mathcal{A}$'s view by answering queries of random oracle H and the signing oracle. Note that in our modification, we require that $2^\ell \leq q_{min}$ where q_{min} is the smallest q_i, $1 \leq i \leq N$.

For a H-query, $\mathcal{B}$ randomly picks $c \in_R \{0,1\}^\ell$ and returns provided that the value has not been assigned. Otherwise, $\mathcal{B}$ repeats the process until a 'fresh' one is picked. Without loss of generality, we assume that $\mathcal{A}$ only submits distinct queries as previous replies can be cached. For a sign query of some n-element subset L of $\mathcal{U}$ and message $m \in \{0,1\}^*$, the answer is simulated as follows.

> For simplicity, let $L = \{(p_1, q_1, g_1, y_1), \cdots, (p_n, q_n, g_n, y_n)\}$. For $i = 1, \cdots, n$, randomly pick $s_i \in_R \mathbb{Z}_{q_i}$ and $c_i \in_R \{0,1\}^\ell$. Set the evaluation of
>
> $$H(L, m, g_1^{s_1} y_1^{c_1} \bmod p_1, \cdots, g_n^{s_n} y_n^{c_n} \bmod p_n)$$
>
> to $c_1 \oplus \cdots \oplus c_n$. If collision occurs, repeat this procedure. Otherwise, output $(c_1, s_1, \cdots, c_n, s_n)$.

First note that $\mathcal{A}$ cannot distinguish between $\mathcal{B}$'s simulation and a real simulation, under the assumption that H is a random oracle. In one successful simulation, suppose the forgery of $\mathcal{A}$ is $(c_1^1, s_1^1, \cdots, c_n^1, s_n^1)$ on some n-element subset L of $\mathcal{U}$. By the assumption of random oracle model, $\mathcal{A}$ has a query $H(L, m, z_1, \cdots, z_n)$ where $z_i = g_i^{s_i} y_i^{c_i} \bmod p_i$, $1 \leq i \leq n$. Suppose this is done at the ρ-th query of H and $\mathcal{B}$ returns c^1. Since $c^1 = c_1^1 \oplus \cdots \oplus c_n^1$ and by the assumption of random oracle model, there is at least one c_i^1, $1 \leq i \leq n$, that is determined *after* c^1 is returned by $\mathcal{B}$. Otherwise, c^1 is pre-determined by $\{c_i\}_{1 \leq i \leq n}$ before c^1 is returned by $\mathcal{B}$ on answering the ρ-th query of H, and this contradicts the assumption of the random oracle model.

Hence by applying the technique of rewind simulation [12], that is, $\mathcal{B}$ runs the simulation again with identical inputs and coin flips until reaching the step of ρ-th query of H. Then from this step on, a different set of query answers will be made by $\mathcal{B}$ in this new simulation. According to the forking lemma [12], it is non-negligible that this rewind simulation will succeed, that is, $\mathcal{A}$ successfully makes another forgery. Suppose $\mathcal{A}$'s forgery in this simulation is $(c_1^2, s_1^2, \cdots, c_n^2, s_n^2)$ and the answer for the ρ-th query of H is c^2. Since $c^2 \neq c^1$, then $c_i^2 \neq c_i^1$ for at least one value of i, $1 \leq i \leq n$. Then $\mathcal{B}$ can obtain the secret x_i by computing $\frac{s_i^1 - s_i^2}{c_i^2 - c_i^1} \bmod q_i$. □

On the signer anonymity of our modification, we show that all components in any valid signature $\sigma = (c_1, s_1, \cdots, c_n, s_n)$ are uniformly distributed over their corresponding domains.

Theorem 2 (Signer Anonymity). *The modification of Abe-Ohkubo-Suzuki witness indistinguishable signature scheme described above is signer anonymous under the random oracle model.*

Proof. For any valid signature $\sigma = (c_1, s_1, \cdots, c_n, s_n)$ on some arbitrary message m and any set L of n public keys (p_i, q_i, g_i, y_i), such that $2^\ell \leq |q_i|$, for all $1 \leq i \leq n$, we first show that all components in the signature are uniformly distributed over their corresponding domains. Suppose the actual signer is indexed by π where $1 \leq \pi \leq n$. For any $i \neq \pi$, c_i is uniformly distributed over $\{0,1\}^\ell$ and s_i is uniformly distributed over $\mathbb{Z}_{q_i}$. Due to the random oracle assumption, given $\{c_i\}_{1 \leq i \leq n, i \neq \pi}$, the evaluation c of $H(L, m, z_1, \cdots, z_n)$ is uniformly distributed over $\{0,1\}^\ell$, for some appropriate values of z_i, $1 \leq i \leq n$. Therefore, c_π is also uniformly distributed over $\{0,1\}^\ell$. We remain to show that s_π is also uniformly distributed over $\mathbb{Z}_{q_i}$.

Since $s_\pi = r - c_\pi x_\pi \bmod q_i$ where r is randomly chosen from $\mathbb{Z}_{q_i}$, x_π is the private key corresponding to y_π. We can see that given x_π and c_π, s_π must be uniformly distributed over $\mathbb{Z}_{q_i}$ as r is.

Therefore, if π is also randomly chosen from $\{1, \cdots, n\}$, then the probability of finding the value of π is exactly $1/n$. □

4 Performance

We note that the authors' full-paper version in [2] contains a different version that defends against the attack given in Section 2. However, there is no withdrawal of the security claim of the scheme in [1], nor any explanation on why they change the algorithm to a more complicated one in their full-paper version.

In the signature generation of the full-paper version, c_i is randomly picked from $\{0,1\}^\ell$ for $i = 1, \cdots, n$, $i \neq k$, where $\ell \geq |q_{max}|$. Also z_i is computed as $g_i^{s_i} y_i^{CRH_i(c_i)} \bmod p_i$ where $CRH_i : \{0,1\}^* \rightarrow \mathbb{Z}_{q_i}$ is a collision resistant hash function. s_k is computed as $r_k - CRH_k(c_k) \cdot x_k \bmod q_k$ where $CRH_k : \{0,1\}^* \rightarrow \mathbb{Z}_{q_k}$ is a collision resistant hash function. In the worst case, it requires n additional hash functions for generating a ring signature with group size n. For implementation, these additional hash functions are to be considered as special system-wide functions. This makes their scheme less conventional and has the risk of losing spontaneity property of ring signature schemes. In addition, they make the implementation more complicated and the system less scalable. Although single hash operation can be carried out quite efficiently by common computing devices, the additional complexity introduced by these hash operations can still be significant when n becomes large. In addition, the signature size depends mainly on the value of $|q_{max}|$ as all the c_i's are of size at least $|q_{max}|$ bits long.

Our solution proposed at the end of Section 3 above, on the other hand, is more scalable, much easier to implement, and more efficient with smaller signatures when comparing to the enhanced version above. Our solution does not require any additional hash functions. The complexity is essentially the same as the original Abe-Ohkubo-Suzuki instantiation. In addition, the signature size depends mainly on the value of $|q_{min}|$ as all the c_i's are of size at most $|q_{min}|$ bits long. Therefore, our solution yields shorter signatures in the general case.

5 Conclusion

We point out that the Abe-Ohkubo-Suzuki Instantiation of witness-indistinguishable signature schemes in [1] is not signer anonymous. The signature leaks information about the identity of the actual signer with overwhelming probability in the general case and with probability greater than half in a special case. We also note that the authors' full-paper version in [2] contains a different version that defends against our attack. The enhanced version is more complicated to implement and is less efficient. To fix the flaw of the original scheme, we propose a method by enforcing a common space for the random numbers to choose from. We further explain the security subtleties of setting the common space by describing a forgery algorithm which succeeds with high probability if the space is chosen inappropriately. We finally suggest several secure confinements for the space in different cases and explain that our solution is more efficient and easier to implement than their full-paper version.

Acknowledgements

The work was supported by a grant from CityU (Project No. 7001844). We would like to thank the anonymous reviewers for their helpful comments and suggestions.

References

[1] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," in *Proceedings of ASIACRYPT 2002*, LNCS 2501, pp. 415-432, Springer-Verlag, 2002.

[2] M. Abe, M. Ohkubo, and K. Suzuki, "1-out-of-n signatures from a variety of keys," *IEICE Transactions on Fundamentals*, E87-A, no. 1, pp. 131-140, Jan. 2004.

[3] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions," in *Proceedings of EUROCRYPT 2003*, LNCS 2656, pp. 614-629, Springer-Verlag, 2003.

[4] M. Bellare, and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols, in *Proceedings of* 1*st ACM Conference on Computer and Communications Security*, pp. 62-73. ACM Press, 1993.

[5] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in *Proceedings of CRYPTO 2002*, LNCS 2442, pp. 465-480, Springer-Verlag, 2002.

[6] J. Camenisch, and M. Stadler, "Efficient group signature schemes for large groups," in *Proceedings of CRYPTO 97*, LNCS 1294, pp. 410–424. Springer-Verlag, 1997.

[7] D. Chaum, and E. Van Heyst, "Group signatures," in *Proceedings of EUROCRYPT 91*, LNCS 547, pp. 257-265, Springer-Verlag, 1991.

[8] R. Cramer, I. Damgård, and B. Schoenmakers, "Proofs of partial knowledge and simplified design of witness hiding protocols," in *Proceedings of CRYPTO 94*, LNCS 839, pp. 174-187, Springer-Verlag, 1994.

[9] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, "Anonymous identification in ad-hoc groups," in *Proceedings of EUROCRYPT 2004*, LNCS 3027, pp. 609-626, Springer-Verlag, 2004.

[10] A. Fiat, and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," in *Proceedings of CRYPTO 86*, pp. 186-199, LNCS 263, Springer-Verlag, 1987.

[11] J. Liu, and D. Wong, "On the security models of (threshold) ring signature schemes," in *The 7th Annual International Conference on Information Secu-*

rity and Cryptology (ICISC 2004), LNCS 3506, pp. 204-217, Springer-Verlag, 2005.

[12] D. Pointcheval, and J. Stern. "Security proofs for signature schemes, in *Proceedings of EUROCRYPT 96*, LNCS 1070, pp. 387-398, Springer-Verlag, 1996.

[13] R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Proceedings of ASIACRYPT 2001*, LNCS 2248, pp. 552-565, Springer-Verlag, 2001.

Joseph Liu is now a Croucher research fellow in the Department of Computer Science, University of Bristol at UK. He got his B. Engin, M.Phil and PhD degree from the Department of Information Engineering, The Chinese University of Hong Kong in 1999, 2001 and 2004 respectively. He was an Assistant Professor at the same department from 2004 to 2005. His research interest includes public key cryptography, provable security and secure e-commerce protocols.

Duncan S. Wong received the BEng degree from the University of Hong Kong in 1994, the MPhil degree from the Chinese University of Hong Kong in 1998, and the PhD degree from Northeastern University, Boston, MA, U.S.A. in 2002. He is an assistant professor in the Department of Computer Science at the City University of Hong Kong. Contact him at: duncan@cityu.edu.hk.