Liu DYW, Liu JK, Mu Y *et al.* Revocable ring signature. JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY 22(6): 785~794 Nov. 2007

Revocable Ring Signature

Dennis Y. W. Liu[1](廖忻宏), Joseph K. Liu[2](廖啟瑞), Yi Mu[3] (穆　怡), Willy Susilo[3] and Duncan S. Wong[1](王　石)

[1] *Department of Computer Science, City University of Hong Kong, Hong Kong, China*

[2] *Institute for Infocomm Research (I^2R), 21 Heng Mui Keng Terrace, Singapore 119613*

[3] *Centre for Computer and Information Security Research, School of Computer Science and Software Engineering University of Wollongong, Wollongong, NSW 2522, Australia*

E-mail: {dliu,duncan}@cs.cityu.edu.hk; ksliu@i2r.a-star.edu.sg; {ymu,wsusilo}@uow.edu.au

Received November 26, 2006; revised September 21, 2007.

Abstract Group signature allows the anonymity of a real signer in a group to be revoked by a trusted party called group manager. It also gives the group manager the absolute power of controlling the formation of the group. Ring signature, on the other hand, does not allow anyone to revoke the signer anonymity, while allowing the real signer to form a group (also known as a ring) *arbitrarily* without being controlled by any other party. In this paper, we propose a new variant for ring signature, called *Revocable Ring Signature*. The signature allows a real signer to form a ring arbitrarily while allowing a set of authorities to revoke the anonymity of the real signer. This new variant inherits the desirable properties from both group signature and ring signature in such a way that the real signer will be responsible for what it has signed as the anonymity is revocable by authorities while the real signer still has the freedom on ring formation. We provide a formal security model for revocable ring signature and propose an efficient construction which is proven secure under our security model.

Keywords anonymity, group signature, revocability, ring signature

1 Introduction

Ring signature[1~8] allows a member of a group (we will call it a ring in the rest of the paper) to sign a message on behalf of the ring without revealing its identity. The notion of ring signature was first formalized by Rivest, Shamir and Tauman[1] in 2001. The idea was actually proposed earlier by Cramer, Damgård and Schoenmakers[9] in 1994, in the context of partial proof of knowledge. They proposed a three-move honest-verifier proof system which allows a prover to show that it knows the solutions to t out of n questions without telling which t questions are. By using the Fiat-Shamir transform[10], the protocol can be turned into a signature scheme, which is a (t, n)-threshold ring signature.

The two main properties of ring signature are *spontaneity* and *anonymity*. Spontaneity allows the actual signer to form a ring of members arbitrarily without collaboration of any of those ring members, provided that the actual signer is also in the ring. Anonymity of a ring signature protects the actual signer in such a way that no one can identify who the actual signer is among the ring members. There is no *revocation* to the anonymity of a ring signature. In addition, many proposed ring signature schemes[1~3,5,6] achieve unconditional anonymity, that is, it is impossible for an adversary to find out who, among the ring members, is the actual signer, even the computational power of the adversary is unlimited. Due to these two properties of ring signature, it could be used for whistle blowing[1], anonymous membership authentication for ad hoc groups[2] and many other applications which require signer anonymity but do not want or cannot afford to have a complicated group formation stage.

Unlike ring signature, a group signature[11~13] does not have the two properties of ring signature mentioned above. First, the formation of a group is not spontaneous. There is a group manager who is responsible for this task and all the group members need to collaborate. Second, the anonymity of the group signature is *revocable*, namely, the group manager is always able to identify the actual signer of a group signature.

When comparing the properties between ring signature and group signature, a natural question one may ask is that whether it is possible to construct a signature scheme such that the ring/group formation is spontaneous as a conventional ring signature while the

Regular Paper

Dennis Y. W. Liu and Duncan S. Wong were supported by CityU grants (Project Nos. 7001844, 7001959, 7002001).

anonymity is revocable as a conventional group signature. More precisely, such a signature scheme should allow the actual signer to form a ring arbitrarily without collaboration with other ring members (i.e., spontaneity) and at the same time have anyone in a set of parties (or authorities) to revoke the anonymity of a ring signature (i.e., revocable anonymity). The revocation is *mandatory*, namely if a revocable ring signature is valid, then the anonymity of the signature must be revocable by anyone in the set of revocation authorities. However, the set of authorities does not control or get involved in the ring formation at all. Since this new type of signature scheme inherits the unique feature of spontaneity in ring formation, and at the same time relax the anonymity level of a ring signature from non-revocable anonymity to a revocable one, we call this new scheme a *Revocable Ring Signature*.

1.1 Related Work and Applications

As we have already explained, a revocable ring signature is not the same as a group signature, because the former one retains the spontaneity property of the ring formation. There is no group manager as in a group signature and the ring formation does not require the actual signer to collaborate with other ring members.

Revocable ring signature is also different from democratic group signature, which has recently been proposed by Manulis[14]. Although democratic group signature does not contain a group manager, the group formation requires collaboration of the group members. Therefore, democratic group signature does not have a spontaneous group formation as a ring signature has. In addition, any group member of a democratic group signature can revoke the anonymity of the actual signer. This is also different from a revocable ring signature of which only a set of authorities can revoke the anonymity.

When comparing with some variants of ring signature, such as linkable ring signature[15,16] and deniable ring signature[17], we can see that a linkable ring signature only allows the public to determine if two signatures with respect to the same ring are generated by the same actual signer. However, it is infeasible to determine who the actual signer is and does not facilitate anonymity revocation. For the revocable ring signature, the signatures are not linkable. In addition, it is required that once a revocable ring signature is publicly verified to be valid, then we require that any of the revocation authorities can revoke the anonymity. In other words, anonymity revocation of a revocable ring signature is mandatory. A deniable ring signature scheme allows a verifier to communicate with the signer (or a member of a group) in an interactive way for finding out who the actual signer is. This is different from a revocable ring signature in two aspects. First, the revocation process of a revocable ring signature is not interactive and can be carried out solely by any of the authorities. Second, the revocation of a revocable ring signature can only be carried out by the set of revocation authorities. The set of authorities can be entirely disjoint from the ring members. For a deniable ring signature, we can consider the set of revocation authorities to be restricted and fixed to the set of all ring members.

Revocable ring signature is suitable for applications where some trusted parties are desirable to have for making the actual signers' ambiguous signatures accountable; while the actual signer should have absolute freedom on ring formation. For example, in a delegation system, a party can delegate its signing right to a group of delegatees. A delegatee can generate a signature without revealing its identity while still allowing the party who delegates to find out who the actual signer is. Similar scenario such as electronic alliance among an ad hoc group of entities on the Internet, for example, some online book stores, those entities can generate ambiguous signature on behalf of the alliance without letting any "outsider" find out the actual signer while allowing members of the alliance to know who the actual signer is. In this application, the set of revocation authorities is the set of ring members.

1.2 Our Results

We formalize the notion of Revocable Ring Signature by providing a definition and a security model to capture the following three properties.

1) Spontaneous Ring Formation — the actual ring signer specifies a ring without any interaction with any other party in the system.

2) Mandatory Anonymity Revocation — there exists a set of authorities such that any authority in the set can identify the actual signer of a signature provided that the signature is valid; and

3) Non-Interactive Anonymity Revocation — the revocation process carried out by the authorities does not require any interaction with the ring members or any other party. The actual signer does not prove interactively to anybody about the authorship. Instead, the revocable ring signature itself will provide the authorship information to the revocation authorities.

We propose a construction based on bilinear pairings and non-interactive proof of knowledge.

Paper Organization. In Section 2, the definition and security model of revocable ring signature are given. In Section 3, an efficient revocable ring signature is proposed. Its security is analyzed and its

performance is evaluated in Section 4. In Section 5, we conclude the paper by making some remarks.

2 Definition and Security Model

Definition 2.1. *A revocable ring signature scheme is a quadruple of algorithms denoted by (Gen, Sig, Ver, Revoke). The first two algorithms are randomized but the last two may not be.*

- $(x, y) \leftarrow Gen(1^k)$ *takes a security parameter* $k \in \mathbb{N}$ *and outputs a private/public key pair* (x, y).
- $\sigma \leftarrow Sig(S, x, T, m)$ *takes a set* S *of public keys, a private key* x*, another set* T *of public keys and a message* m*, produces a signature* σ.
- $1/0 \leftarrow Ver(S, m, T, \sigma)$ *takes a set* S *of public keys, a message* m*, another set* T *of public keys and a signature* σ*, returns* 1 *or* 0 *for* accept *or* reject*, respectively.*
- $y' \leftarrow Revoke(S, x, T, \sigma)$ *takes a public key set* S*, a private key* x*, another public key set* T*, and a valid signature* σ *(i.e.,* $Ver(S, m, T, \sigma) = 1$*), returns a public key* y'.

Signature Correctness. We require that for any $k \in \mathbb{N}$, message $m \in \{0,1\}^*$, $(x, y) \leftarrow Gen(1^k)$, public key sets S and T such that all keys in S and T are generated by $Gen(1^k)$ and $y \in S$,

$$Ver(S, m, T, Sig(S, x, T, m)) = 1.$$

In other words, if everything is generated and computed accordingly, the signature verification will always accept the signature.

Besides this conventional correctness requirement on ring signature, we also require correctness on revocation. If everything is generated and computed exactly according to the specification of the scheme, any member in T should be able to find out the actual signer of any (valid) signature with T specified as the set of revocation authorities. Below is the formalization.

Revocation Correctness. We require that for any $k \in \mathbb{N}$, message $m \in \{0,1\}^*$, public key sets $S = \{y_1, \ldots, y_n\}$ and $T = \{\hat{y}_1, \ldots, \hat{y}_\ell\}$, where all keys in them are generated by $Gen(1^k)$, π, $1 \leqslant \pi \leqslant n$, ξ, $1 \leqslant \xi \leqslant \ell$, and any valid signature $\sigma \leftarrow Sig(S, x_\pi, T, m)$,

$$y_\pi \leftarrow Revoke(S, \hat{x}_\xi, T, \sigma)$$

where $\hat{x}_\xi$ is the private key of $\hat{y}_\xi$ in T.

In the following, we discuss the security requirements of a revocable ring signature scheme. There are three aspects: unforgeability, signer anonymity and signer revocability.

2.1 Unforgeability

We adopt the unforgeability definition for ring signature schemes due to Abe, Ohkubo and Suzuki[3] and extend it to capture insider corruption described by Bender, Katz and Morselli[8]. The difference between the unforgeability model of [3] and that of [8] is that the model of [3] captures a notion similar to the strong existential unforgeability of conventional digital signature[18] while the model of [8] only considers the existential unforgeability in the general sense[19]. Another difference is that the signing oracle of [8] allows the adversary to specify the actual signer in each query while the signing oracle of [3] does not allow the adversary to do so.

Let $k \in \mathbb{N}$ be a security parameter. Let $\mathcal{U} = \{y_1, \ldots, y_N\}$ be a set of public keys where N is some polynomial in k and each public key (with the associated private key) is generated by $Gen(1^k)$. To support adaptive chosen message attack, we provide the adversary a signing oracle $\mathcal{SO}$. It takes a public-key subset $S' \subseteq \mathcal{U}$, another public-key subset $T' \subseteq \mathcal{U}$ and a message m', returns a signature σ' such that $Ver(S', m', T', \sigma') = 1$. Another oracle called corruption oracle denoted by $\mathcal{CO}$ allows the adversary to query for the corresponding private key of a public key in $\mathcal{U}$. This is added onto the original model of [3] due the technical requirement of the signer anonymity model that will be defined in the next subsection. Adding $\mathcal{CO}$ onto the model also allows us to capture insider corruption[8]. Let CorruptSet be the set of public keys which have been queried with $\mathcal{CO}$ by the adversary. Below is the formal definition of *Existential Unforgeability Against Chosen Message and Public-Key Attacks and Insider Corruption.*

Definition 2.2. *A revocable ring signature scheme is unforgeable if for any probabilistic polynomial-time algorithm (PPT)* $\mathcal{A}$ *with signing oracle* $\mathcal{SO}$ *and corruption oracle* $\mathcal{CO}$*, it is negligible in* k *that* $(S, T, m, \sigma) \leftarrow \mathcal{A}^{\mathcal{SO},\mathcal{CO}}(\mathcal{U})$ *such that* $Ver(S, m, T, \sigma) = 1$ *and* $S, T \subseteq \mathcal{U}$*. Restrictions are that* (S, T, m, σ) *should not be in the set of oracle queries and replies between* $\mathcal{A}$ *and* $\mathcal{SO}$*, and* $\mathsf{CorruptSet} \cap S = \emptyset$.

A real-valued function ϵ is negligible if for every $c > 0$ there exists a constant $k_c > 0$ such that $\epsilon(k) < k^{-c}$ for all $k > k_c$.

2.2 Signer Anonymity

Given a revocable ring signature of n ring members. Suppose the actual signer is chosen uniformly at random over the n members. By signer anonymity, an adversary should not be able to identify who the actual signer is with probability non-negligibly greater than $1/n$ when *none* of the private keys of the ring

members is known.

This is different from and weaker than the anonymity notion for conventional ring signature scheme defined by Bender, Katz and Morselli[8]. In their definition, anonymity of a conventional ring signature scheme should hold even if all ring members have given the adversary their secret information. However, we cannot adopt this notion due to the requirement of signer revocability. The best we can do currently is to make sure that an adversary cannot do any better to find out the actual signer than guessing randomly among all the uncorrupted ring members if none of the revocation authorities is compromised. We consider the construction of a revocable ring signature which can maintain the signer anonymity against full key exposure to be an open problem.

Also notice that some conventional ring signature schemes support computational signer anonymity while others support unconditional signer anonymity (we refer readers to [1, 2 ,8] for more details). Again, due to the requirement of signer revocability, anyone who knows the secret information of a revocation authority should be able to identify the actual signer. Therefore, we only consider computational signer anonymity for a revocable ring signature.

Consider an experiment of two stages: choose and guess. In the choose stage, adversary $\mathcal{A}$ with oracles $\mathcal{SO}$ and $\mathcal{CO}$ chooses $S, T \subseteq \mathcal{U}$, public keys $y_{\pi_0}, y_{\pi_1} \in S$ and a message $m \in \{0,1\}^*$. This stage is denoted by $(S, T, y_{\pi_0}, y_{\pi_1}, m, State) \leftarrow \mathcal{A}^{\mathcal{SO},\mathcal{CO}}(\mathcal{U}, \mathsf{choose})$ where $State$ is some state information. In other words, $\mathcal{A}$ specifies a ring, a set of revocation authorities, a message to be signed and also chooses two signers.

In the guess stage, $\mathcal{A}$ is to determine which of y_{π_0} and y_{π_1} corresponds to the actual signer of a given signature σ. Let W be the set of private keys corresponding to the public keys in $\mathcal{U} \setminus (T \cup \{y_{\pi_0}, y_{\pi_1}\})$. The guess stage of $\mathcal{A}$ is denoted by $y_\zeta \leftarrow \mathcal{A}^{\mathcal{SO},\mathcal{CO}}(\sigma, W, State, \mathsf{guess})$, where $y_\zeta \in \{y_{\pi_0}, y_{\pi_1}\}$. Below is the complete description of the experiment.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{\mathrm{anon}}(k)$

For $i = 1, \ldots, N$, $(x_i, y_i) \leftarrow Gen(1^k)$, where N is some polynomial in k

Set $\mathcal{U} = \{y_1, \ldots, y_N\}$

$(S, T, y_{\pi_0}, y_{\pi_1}, m, State) \leftarrow \mathcal{A}^{\mathcal{SO},\mathcal{CO}}(\mathcal{U}, \mathsf{choose})$

$b \overset{R}{\leftarrow} 0/1$, $\sigma \leftarrow Sig(S, x_{\pi_b}, T, m)$.

$y_\zeta \leftarrow \mathcal{A}^{\mathcal{SO},\mathcal{CO}}(\sigma, W, State, \mathsf{guess})$

The experiment halts with failure **if**

- $\mathcal{A}$ fails, or
- $\mathsf{CorruptSet} \cap (T \cup \{y_{\pi_0}, y_{\pi_1}\}) \neq \emptyset$

Return 1 if $y_\zeta = y_{\pi_b}$, otherwise return 0

An experiment succeeds if it halts with no failure. We denote by $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{anon}}(k) = \Pr[\mathbf{Exp}_{\mathcal{A}}^{\mathrm{anon}}(k) = 1 \mid \text{Exp. succeeds}] - 1/2$ the advantage of $\mathcal{A}$ in breaking the signer anonymity of a revocable ring signature scheme.

The experiment above simulates a scenario where $\mathcal{A}$ has compromised all the keys in $\mathcal{U}$ except those in $T \cup \{y_{\pi_0}, y_{\pi_1}\}$, then signature σ is generated using the private key corresponding to one of y_{π_0} and y_{π_1}, and finally, the adversary is to guess which of the two keys is used.

Below is the definition of *Signer Anonymity Against Chosen Message and Public-Key Attacks.*

Definition 2.3. *A revocable ring signature is signer anonymous if for all sufficiently large k and PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{anon}}(\cdot)$ is negligible.*

2.3 Signer Revocability

Intuitively, as long as a revocable ring signature is valid, the revocation algorithm *Revoke* should be able to identify the actual signer when the secret information of any revocation authority is given. In the experiment below, the adversary is modeling a malicious signer who tries to hide its identity from being extracted from its signature by any of the revocation authorities. We continue using the notations above.

Experiment $\mathbf{Exp}_{\mathcal{A}}^{\mathrm{revo}}(k)$

For $i = 1, \ldots, N$, $(x_i, y_i) \leftarrow Gen(1^k)$ with fresh coin flips

Set $\mathcal{U} = \{y_1, \ldots, y_N\}$

$(S, T, m, \sigma) \leftarrow \mathcal{A}^{\mathcal{SO},\mathcal{CO}}(\mathcal{U})$ where $S \subseteq \mathcal{U}$ and $|S| = n$

The experiment halts with failure **if**

- $\mathcal{A}$ fails, or
- $Ver(S, m, T, \sigma) \neq 1$, or
- $|\mathsf{CorruptSet} \cap S| \neq 1$

Let $\{y_\pi\} = \mathsf{CorruptSet} \cap S$

For each public key $\hat{y}_i \in T$, suppose the corresponding private key is $\hat{x}_i$.

$y_{\theta,i} \leftarrow Revoke(S, \hat{x}_i, T, \sigma)$

return 1 **if** $y_{\theta,i} \neq y_\pi$;

Return 0.

Define

$$\mathbf{Adv}_{\mathcal{A}}^{\mathrm{revo}}(k) = \Pr[\mathbf{Exp}_{\mathcal{A}}^{\mathrm{revo}}(k) = 1 \mid \text{Exp. succeeds}]$$

the advantage of $\mathcal{A}$ in breaking the signer revocability.

In the experiment above, we allow the adversary to adaptively corrupt private keys under the restriction that the adversary can corrupt one private key in S and all other keys do not belong to S. The adversary possibly uses the corrupted private key (corresponding to the public key y_ζ in the experiment above) to generate signature σ.

Below is the definition of *Signer Revocability Against Chosen Message and Public-Key Attacks.*

Definition 2.4. *A revocable ring signature is signer revocable if for all sufficiently large k and PPT adversary $\mathcal{A}$, $\mathbf{Adv}_{\mathcal{A}}^{\mathrm{revo}}(\cdot)$ is negligible.*

3 Construction

We start with a generic construction of ring signature scheme based on the partial proof of knowledge due to Cramer, Damgård and Schoenmakers[9]: a (1-out-of-n) ring signature for message m is a non-interactive proof system of the following disjunction.

$$SPK\{\alpha : \vee_{i\in[1,n]}(\alpha, y_i) \in \mathcal{R}_i\}(m)$$

where $[1,n]$ denotes the set $\{1,\ldots,n\}$ and $\mathcal{R}_i = \{(x_i, y_i)\}$ is the private-public key relation of the i-th member (of the ring). The prover shows the knowledge of 1-out-of-n relations and the verifier does not know which particular relation that the prover is showing. We refer readers to [12] for details of the *SPK* notation above. There are many types of constructions of ring signature proposed, such as ring type[1~4], polynomial interpolation type[9,20,21], and accumulator type[6,22,23].

Our construction of revocable ring signature is based on bilinear pairings[24]. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of the same order q. Let P be a generator of $\mathbb{G}_1$. Assume that the discrete logarithm problem in both $\mathbb{G}_1$ and $\mathbb{G}_2$ are hard. Suppose there exists a computable bilinear map $\hat{e}$ such that $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ and it satisfies the following properties: 1) bilinear: for any $P_1, P_2 \in \mathbb{G}_1$, and $a, b \in \mathbb{Z}$, $\hat{e}(aP_1, bP_2) = \hat{e}(P_1, P_2)^{ab}$; 2) non-degenerate: $\hat{e}(P, P) \neq 1$. Below is the description of our construction.

Key Generation. Let $k \in \mathbb{N}$ be a security parameter. Suppose the order q of $\mathbb{G}_1$ and $\mathbb{G}_2$ is of length polynomial in k. On input 1^k, *Gen* outputs (x, y) where the private key x is randomly chosen from $\mathbb{Z}_q$ and $y = xP$.

Signature Generation and Verification. Suppose $m \in \{0,1\}^*$ is the message to be signed, $S = \{y_1, \ldots, y_n\}$ is the set of public keys that defines the ring and π, $1 \leqslant \pi \leqslant n$, is the index of the actual signer. Let $T = \{\hat{y}_1, \ldots, \hat{y}_\ell\}$ be the set of revocation authorities. It is assumed that all public keys y_i, $1 \leqslant i \leqslant n$, $\hat{y}_j$, $1 \leqslant j \leqslant \ell$ and their corresponding private keys x_i's and $\hat{x}_j$'s are generated by *Gen*. The signature generation algorithm $Sig(S, x_\pi, T, m)$ is carried out as follows.

1) Randomly select $r \in_R \mathbb{Z}_q$ and compute $R = rP$.
2) For $j = 1, \ldots, \ell$, compute $E_j = \hat{e}(y_\pi, \hat{y}_j)^r$.
3) Generate a non-interactive proof as follows:

$$SPK\Big\{ \alpha : \Big\{ \bigwedge_{j\in[1,\ell]} E_j = \hat{e}(R, \hat{y}_j)^\alpha \Big\} \bigwedge \Big\{ \bigvee_{i\in[1,n]} y_i = \alpha P \Big\}\Big\}(m). \quad (1)$$

The signature σ of m with respect to S and T is $(R, E_1, \ldots, E_\ell)$ and the transcript of $SPK(1)$. Verification of σ is the verification of $SPK(1)$. In Appendix A, we describe an instantiation of $SPK(1)$.

Revocation. If an authority indexed by ξ, $1 \leqslant \xi \leqslant \ell$, in T wants to revoke the identity of the actual signer, the authority uses its private key $\hat{x}_\xi$ and determines if

$$E_\xi \stackrel{?}{=} \hat{e}(y_i, R)^{\hat{x}_\xi} \quad \text{for some} \quad i, \quad 1 \leqslant i \leqslant n. \quad (2)$$

If the equation holds at, say when $i = \pi$, then the user sets the output of $Revoke(S, \hat{x}_\xi, T, \sigma)$ to y_π meaning that ring member indexed by π in S is the actual signer.

4 Security Analysis and Performance

To see the correctness of the scheme, first it is obvious that the ring signature part in (1), that is

$$SPK\{\alpha : \bigvee_{i\in[1,n]} y_i = \alpha P\}(m) \quad (3)$$

satisfies the definition of signature correctness. We remain to show that the revocation part, that is

$$SPK\Big\{\alpha : \bigwedge_{j\in[1,\ell]} E_j = \hat{e}(R, \hat{y}_j)^\alpha\Big\}(m) \quad (4)$$

also satisfies the signature correctness definition. In the formation of E_j, $1 \leqslant j \leqslant \ell$ during the signature generation, the actual signer computes

$$\begin{aligned} E_j &= \hat{e}(y_\pi, \hat{y}_j)^r = \hat{e}(P, \hat{y}_j)^{rx_\pi} \\ &= \hat{e}(rP, \hat{y}_j)^{x_\pi} = \hat{e}(R, \hat{y}_j)^{x_\pi} \end{aligned}$$

which is the same as in (1). Therefore, the signature correctness holds.

For revocation correctness, an authority, say holding private key $\hat{x}_\xi$, computes for some i where $1 \leqslant i \leqslant n$, that

$$\begin{aligned} \hat{e}(y_i, R)^{\hat{x}_\xi} &= \hat{e}(y_i, P)^{\hat{x}_\xi r} \\ &= \hat{e}(y_i, \hat{y}_\xi)^r \\ &= E_\xi \text{ iff } i = \pi. \end{aligned}$$

Therefore, if the signature is generated according to the specification, there will be one and only one signer extracted from the revocation algorithm.

4.1 Unforgeability

On existential unforgeability against chosen message and public-key attacks and insider corruption (with respect to Definition 2.2), the security of our construction can easily be seen from the ring signature part of $SPK(1)$, namely $SPK(3)$. Note that

$S = \{y_1, \ldots, y_n\}$ and one of the restrictions in Definition 2.2 is that $\mathsf{CorruptSet} \cap S = \emptyset$. That is, the adversary does not know any of the discrete logarithms x_i of the public keys y_i in S. Therefore, we can readily reduce the forgery of our construction with respect to Definition 2.2 to the strong existential forgery against chosen message and public-key attacks (in the sense of [3]) of $SPK(3)$. This yields the following theorem.

Theorem 4.1. *The construction described in Section 3 is unforgeable (in the sense of Definition 2.2) if the ring signature $SPK(3)$ is existentially unforgeable against chosen message and public-key attacks (in the sense of [3]) and N, the size of $\mathcal{U}$ in Definition 2.2, is constant.*

One technical detail in the reduction is the requirement of simulating corruption oracle $\mathcal{CO}$ which is not supported in the model of [3]. Our approach is to set N to a constant and have the challenger guess S so that for all public keys in $\mathcal{U} \setminus S$, they are generated by the challenger. Therefore, the challenger is able to simulate $\mathcal{CO}$ on any key in $\mathcal{U} \setminus S$ successfully. If the challenger guesses S incorrectly, the simulation fails. The probability that the challenger does not fail in simulation is $1/\binom{N}{n}$. Since N is a constant, the success probability of the challenger is non-negligible.

4.2 Signer Anonymity

On signer anonymity against chosen message and public-key attacks (with respect to Definition 2.3), we consider the two parts of $SPK(1)$, namely the ring signature part $SPK(3)$ and the revocation part $SPK(4)$. $SPK(3)$ is a conventional ring signature which ensures signer anonymity against chosen message and public-key attacks with respect to Definition 2.3 if $SPK(3)$ is instantiated using a scheme which has been proven to be signer anonymous under a model which is at least as strong as that of experiment $\mathbf{Exp}_{\mathcal{A}}^{\text{anon}}$, for example, the unconditional anonymity model of [1] or the full key exposure model of [8]. We now consider the revocation part, $SPK(4)$. Note that if adversary $\mathcal{A}$ in $\mathbf{Exp}_{\mathcal{A}}^{\text{anon}}$ corrupts a key in S, say y_w, that is, $\mathcal{A}$ knows x_w, $\mathcal{A}$ can tell if the actual signer is w. This can be done by checking whether

$$E_1 \stackrel{?}{=} \hat{e}(R, \hat{y}_1)^{x_w}.$$

Hence according to experiment $\mathbf{Exp}_{\mathcal{A}}^{\text{anon}}$, if $\mathcal{A}$ has obtained $n-2$ keys in S, provided that these keys are not in T, then $\mathcal{A}$ has at least $1/2$ chance of guessing the identity of the actual signer correctly, which is corresponding either to y_{π_0} or y_{π_1}.

To show that the construction in Section 3 is signer anonymous, we start with an Indistinguishability Based Bilinear Decisional Diffie-Hellman (IND-BDDH) problem. In this problem, given four elements $P_1, P_2, P_3^0 = a_3^0 P$, $P_3^1 = a_3^1 P \in \mathbb{G}_1$ and one element $P_4 \in \mathbb{G}_2$ such that half chance that $\hat{e}(P_1, P_2)^{a_3^0} = P_4$ and the other half of the chance that $\hat{e}(P_1, P_2)^{a_3^1} = P_4$. The problem is to find out which case it is. This problem is related to the conventional Bilinear Decisional Diffie-Hellman (BDDH) problem, namely, given $P_1^*, P_2^*, P_3^* = a_3 P \in \mathbb{G}_1$ and $P_4^* \in \mathbb{G}_2$, decide whether $P_4^* = \hat{e}(P_1^*, P_2^*)^{a_3}$. If $P_4^* = \hat{e}(P_1^*, P_2^*)^{a_3}$, then we say that $(P_1^*, P_2^*, P_3^*, P_4^*)$ is a BDH (Bilinear Diffie-Hellman) tuple.

Lemma 4.1. *If there exists an algorithm $\mathcal{A}$ which solves the IND-BDDH problem with probability at least ϵ greater than wild guess, that is, $1/2$, then there exists an algorithm $\mathcal{B}$ which solves BDDH problem with probability at least $\epsilon/2$ greater than $1/2$, and the running time of $\mathcal{B}$ is in polynomial of that of $\mathcal{A}$.*

Proof. Given a BDDH problem instance $(P_1^*, P_2^*, P_3^*, P_4^*) \in \mathbb{G}_1^3 \times \mathbb{G}_2$, we construct $\mathcal{B}$ as follows. Set $P_1 := P_1^*$, $P_2 := P_2^*$ and $P_4 := P_4^*$. Toss a coin $b \leftarrow 0/1$. Set $P_3^b := P_3^*$. Let $\bar{b} = 1 - b$. Set $P_3^{\bar{b}}$ as a random element in $\mathbb{G}_1$. Execute $\mathcal{A}$ with input $(P_1, P_2, P_3^0, P_3^1, P_4)$. If $\mathcal{A}$ outputs b, $\mathcal{B}$ outputs 1; otherwise, outputs 0.

Let $E_{\mathcal{A}}$ be the event that $\mathcal{A}$ solves the IND-BDDH problem successfully. $\Pr[E_{\mathcal{A}}] \geqslant 1/2 + \epsilon$. This is conditioned by the case that (P_1, P_2, P_3^b, P_4) is indeed a BDH tuple. Let E_{BDH} be the event that (P_1, P_2, P_3^b, P_4) is a BDH tuple. Let $E_{\mathcal{B}}$ be the event that $\mathcal{B}$ solves the BDDH problem. We have $\Pr[E_{\mathcal{B}}] = \Pr[\mathcal{A} \text{ ouputs } b \mid E_{BDH}]/2 + \Pr[\mathcal{A} \text{ outputs } \bar{b} \mid \overline{E}_{BDH}]/2 = \Pr[E_{\mathcal{A}}]/2 + \Pr[\mathcal{A} \text{ outputs } \bar{b} \mid \overline{E}_{BDH}]/2$. In the vent that $\overline{E}_{BDH}$ (that is, (P_1, P_2, P_3^b, P_4) is not a BDH tuple), it is negligible that $(P_1, P_2, P_3^{\bar{b}}, P_4)$ is a BDH tuple since $P_3^{\bar{b}}$ is randomly chosen in $\mathbb{G}_1$. Also because b is randomly picked, we must have, with negligible exceptional case (when $(P_1, P_2, P_3^{\bar{b}}, P_4)$ is indeed a BDH tuple), $\Pr[\mathcal{A} \text{ outputs } \bar{b} \mid \overline{E}_{BDH}] = 1/2$. Therefore

$$\Pr[E_{\mathcal{B}}] = \frac{1}{2}\Pr[E_{\mathcal{A}}] + \frac{1}{4} \geqslant \frac{1}{2} + \frac{\epsilon}{2}.$$

It is also obvious that the running time of $\mathcal{B}$ is in polynomial of that of $\mathcal{A}$. □

On the revocation part, that is, $SPK(4)$, the corresponding parameters in the signature σ are $(R, E_1, \ldots, E_\ell)$. Since r is uniformly chosen from $\mathbb{Z}_q$, R is uniformly distributed over $\mathbb{G}_1$. For each E_j, $1 \leqslant j \leqslant \ell$, an adversary has to determine whether $E_j = \hat{e}(R, \hat{y}_j)^{x_{\pi_0}}$ or $\hat{e}(R, \hat{y}_j)^{x_{\pi_1}}$ under the model formalized by experiment $\mathbf{Exp}_{\mathcal{A}}^{\text{anon}}$. We will show that $SPK(4)$ does not leak any information about the actual signer if IND-BDDH problem is hard. There is one additional technical requirement for proving the

lemma below, that is, $SPK(1)$ should be *simulatable by game challenger*. $SPK(1)$ is said to be simulatable by the game challenger of $\mathbf{Exp}_{\mathcal{A}}^{\text{anon}}$ if the game challenger can answer queries to signing oracle $\mathcal{SO}$ without knowing any of the required knowledge of $SPK(1)$ (which is some private key of the ring defined by S). More precisely, the simulated transcripts of $SPK(1)$ generated by the game challenger should be computationally indistinguishable from genuine transcripts of $SPK(1)$ generated as if a private key is known. For example, if $SPK(1)$ is instantiated as in Appendix A, then under the random oracle model[25], the instantiation is simulatable by game challenger.

Lemma 4.2. *If there exists an algorithm $\mathcal{C}$ which breaks the signer anonymity of the construction in Section 3 (in the sense of Definition 2.3) with advantage at least ϵ, then there exists an algorithm $\mathcal{A}$ which solves IND-BDDH with probability at least $2\epsilon/[N(N-1)]$ greater than $1/2$ for some N which is polynomial in the security parameter k. The condition is that $SPK(1)$ is simulatable by game challenger.*

Proof. Given an IND-BDDH problem instance $(P_1, P_2, P_3^0 = a_3^0 P, P_3^1 = a_3^1 P, P_4) \in \mathbb{G}_1^4 \times \mathbb{G}_2$, we construct $\mathcal{A}$ as follows. For $i = 1, \ldots, N$, in experiment $\mathbf{Exp}_{\mathcal{A}}^{\text{anon}}$, randomly pick $\alpha_i \in_R \mathbb{Z}_q$ and set $y_i = \alpha_i P_2$. Set $\mathcal{U} = \{y_1, \ldots, y_N\}$. Randomly pick two public keys in $\mathcal{U}$ and set them to P_3^0 and P_3^1. Since $SPK(1)$ is simulatable by game challenger, all queries to signing oracle can be simulated by $\mathcal{A}$ which acts as the game challenger. When running $\mathcal{C}$, $\mathcal{C}$ will return an n-element ring definition S, a set T of ℓ revocation authorities and two public keys y_{π_0} and y_{π_1} at the choose stage. If the experiment does not fail and y_{π_0} and y_{π_1} chosen by $\mathcal{C}$ are exactly the two public keys that $\mathcal{A}$ has set them to P_3^0 and P_3^1, $\mathcal{A}$ generates the challenge signature σ. Thanks to that $SPK(1)$ is simulatable by game challenger, in σ, R is set to P_1, E_j is set to $\alpha_j P_4$ for $j = 1, \ldots, \ell$, and a transcript of $SPK(1)$ is generated. Without loss of generality, assume that $y_{\pi_0} = P_3^0$ and $y_{\pi_1} = P_3^1$.

Note that for all j, $1 \leqslant j \leqslant \ell$, $E_j = \alpha_j P_4 = \hat{e}(P_1, P_2)^{\alpha_j a_3^b}$, for $b = 1/0$. This is because for the IND-BDDH problem instance, either (P_1, P_2, P_3^0, P_4) or (P_1, P_2, P_3^1, P_4) is a BDH tuple, now P_1 is R in σ, P_2 is transposed to $\alpha_j P_2$, which is the public key of a revocation authority, for $j = 1, \ldots, \ell$, E_j is set to $\alpha_j P_4$, hence if (P_1, P_2, P_3^0, P_4) is a BDH tuple, then the signer corresponding to y_{π_0} should be identified as the actual signer; otherwise, the signer corresponding to y_{π_1} should be identified as the actual signer.

Therefore, if $\mathcal{C}$ outputs y_{π_0}, $\mathcal{A}$ outputs 0 indicating that $\mathcal{A}$ guesses that (P_1, P_2, P_3^0, P_4) is a BDH tuple; otherwise, if $\mathcal{C}$ outputs y_{π_1}, $\mathcal{A}$ outputs 1. Hence if the advantage of $\mathcal{C}$ is at least ϵ, then the advantage of $\mathcal{A}$ is solving IND-BDDH problem instance is also at least ϵ over wild guess (i.e., $1/2$).

On the success rate of $\mathcal{A}$ on simulating experiment $\mathbf{Exp}_{\mathcal{A}}^{\text{anon}}$, since P_3^0 and P_3^1 are uniformly distributed over $\mathcal{U}$, the probability that $\mathcal{C}$ chooses these two public keys as y_{π_0} and y_{π_1} (the order does not matter) is only $\lambda = 2/N(N-1)$. Hence only a fraction of time (i.e., $2/N(N-1)$) that $\mathcal{A}$ simulates $\mathbf{Exp}_{\mathcal{A}}^{\text{anon}}$ successfully, but the fraction is non-negligible. If the simulation is not successful, $\mathcal{A}$ then randomly chooses a bit as the output. Hence if the simulation is not successful, the probability that $\mathcal{A}$ solves IND-BDDH problem is $1/2$. In summary, the probability that $\mathcal{A}$ solves IND-BDDH problem is

$$\begin{aligned}&\Pr[\mathcal{A} \text{ solves IND-BDDH problem}]\\ &= \Big(\frac{1}{2} + \epsilon\Big)\lambda + \frac{1}{2}(1-\lambda)\\ &= \frac{1}{2} + \frac{2\epsilon}{N(N-1)}.\end{aligned}$$

□

Theorem 4.2. *The construction in Section 3 is signer anonymous against chosen message and public-key attacks (in the sense of Definition 2.3) if $SPK(3)$ is anonymous in the unconditional anonymity model of [1] or the full key exposure model of [8], BDDH problem is hard and $SPK(1)$ is simulatable by game challenger (e.g., under the random oracle model[25]).*

This theorem follows directly from the discussion at the beginning of this subsection as well as Lemmas 4.1 and 4.2.

4.3 Signer Revocability

Theorem 4.3 (Revocability). *The construction in Section 3 is signer revocable against chosen message and public-key attacks (in the sense of Definition 2.4) if the construction is unforgeable (in the sense of Definition 2.2) and given the private key of any ring member, it is infeasible to obtain the private key of another ring member.*

Proof. First note that even if the construction in Section 3 is unforgeable, it does not imply that given the private key of any ring member, it is infeasible to obtain the private key of another ring member. Hence we additionally assume that even the adversary in experiment $\mathbf{Exp}_{\mathcal{A}}^{\text{revo}}$ can obtain the private key of a ring member, the adversary is infeasible to obtain the private key of any other ring member. This assumption is justified as all the public key pairs in $\mathcal{U}$ are generated independently using $Gen(1^k)$ with fresh coin flips.

For contradiction, suppose there exists a PPT adversary $\mathcal{A}$ who succeeds in running experiment $\mathbf{Exp}_{\mathcal{A}}^{\text{revo}}$ non-negligibly with experiment output equal

to 1. Note that $\mathcal{A}$ is allowed to know exactly one private key of the ring members in S. Without loss of generality, suppose x_π is the private key known to $\mathcal{A}$. In a successful run of the experiment with output 1, suppose the signature is σ, which must be generated by applying x_π during the signature generation since the construction is unforgeable in the sense of Definition 2.2. For σ to be valid, according to $SPK(1)$, the discrete logarithm for E_j $(1 \leqslant j \leqslant \ell$ to the base $\hat{e}(R, \hat{y}_j))$ must be the private key of a public key in S.

Suppose $y_\gamma \leftarrow Revoke(S, \hat{x}_\theta, T, \sigma)$ for some corresponding public key $\hat{y}_\theta \in T$, but $y_\gamma \neq y_\pi$. We have

$$E_\theta \neq \hat{e}(y_\pi, R)^{\hat{x}_\theta} = \hat{e}(R, \hat{y}_\theta)^{x_\pi}. \tag{5}$$

Since the signature verification is passed, according to $SPK(1)$, $\mathcal{A}$ shows its knowledge of α where

$$E_\theta = \hat{e}(R, \hat{y}_\theta)^\alpha \tag{6}$$

and α is one of the private key of the n group members. Combining (5) and (6), we have

$$\hat{e}(R, \hat{y}_\theta)^{x_\pi} \neq \hat{e}(R, \hat{y}_\theta)^\alpha.$$

That is, $x_\pi \neq \alpha$ since $\hat{e}$ is a deterministic mapping. In other words, $\mathcal{A}$ knows the knowledge of two distinct private keys, x_π and α, which contradicts our assumption. □

4.4 Performance

The performance of our construction relies on the efficiency of bilinear pairing and the instantiation of $SPK(1)$. If the set of authorities T has been determined, all the computations of $\hat{e}(R, \hat{y}_j)$, for $j = 1, \ldots, \ell$, can all be pre-computed. This significantly improves the online performance of our scheme.

On the signature size, it also depends on the instantiation of $SPK(1)$. For example, if the instantiation given in Appendix A is adopted, the signature size will be $20 + 128\ell + 40n$ bytes long if q is 20 bytes long and elements in $\mathbb{G}_2$ are 128 bytes long. Note that if constant-size signature schemes are used for the ring signature part, $SPK(3)$, the size can further be reduced and the term linear to n can be eliminated.

5 Conclusion

In this paper, we proposed a variant of ring signature called *Revocable Ring Signature*. This variant relaxes the level of anonymity in such a way that it allows a set of authorities to revoke the anonymity of the actual signer, while maintaining signer anonymity to other parties in the system. In addition, it still retains the spontaneity property for ring formation. The actual signer still has the absolute freedom in forming a ring and no collaboration with the revocation authorities or other ring members is required whatsoever.

Our proposed scheme can be viewed as a generic construction based on non-interactive proof of knowledge. If pre-computation is allowed, the most time-consuming part in our scheme, that is, the bilinear pairing operations, can be carried out offline, and leave the online part of the signature generation much more efficient. Further improvement of the efficiency in space or time complexity is an interesting open problem. It is also interesting to construct a constant-size revocable ring signature scheme with the size of the signature independent of the number of revocation authorities.

Our current solution can only achieve anonymity under a relaxed anonymity model specified in Subsection 2.2, which does not capture full key exposure as defined in [8]. We consider the construction of a revocable ring signature which can maintain the signer anonymity against full key exposure, provided that no secret information of the revocation authorities is known, to be an open problem.

References

[1] Rivest R, Shamir A, Tauman Y. How to leak a secret. In *Proc. ASIACRYPT 2001*, Australia, *Lecture Notes in Computer Science*, 2248, Springer-Verlag, 2001, pp.552∼565.

[2] Bresson E, Stern J, Szydlo M. Threshold ring signatures and applications to ad-hoc groups. In *Proc. CRYPTO 2002*, USA, *Lecture Notes in Computer Science*, 2442, Springer-Verlag, 2002, pp.465∼480.

[3] Abe M, Ohkubo M, Suzuki K. 1-out-of-n signatures from a variety of keys. In *Proc. ASIACRYPT 2002*, New Zealand, *Lecture Notes in Computer Science*, 2501, Springer-Verlag, 2002, pp.415∼432.

[4] Wong D S, Fung K, Liu J, Wei V. On the RS-code construction of ring signature schemes and a threshold setting of RST. In *Proc. 5th Int. Conference on Information and Communication Security* (*ICICS 2003*), China, *Lecture Notes in Computer Science*, 2836, Springer-Verlag, 2003, pp.34∼46.

[5] Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps. In *Proc. EUROCRYPT 2003*, Poland, *Lecture Notes in Computer Science*, 2656, Springer-Verlag, 2003, pp.416∼432.

[6] Dodis Y, Kiayias A, Nicolosi A, Shoup V. Anonymous identification in ad doc groups. In *Proc. EUROCRYPT 2004*, Switzerland, *LNCS* 3027, Springer-Verlag, 2004, pp.609∼626, Full version: http://www.cs.nyu.edu/ nicolosi/papers/

[7] Liu J K, Wong D S. On the security models of (threshold) ring signature schemes. In *Proc. 7th Annual International Conference on Information Security and Cryptology* (*ICISC 2004*), Korea, *Lecture Notes in Computer Science*, 3506, Springer-Verlag 2005, pp.204∼217.

[8] Bender A, Katz J, Morselli R. Ring signatures: Stronger definitions, and constructions without random oracles. In

Proc. Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, USA, *Lecture Notes in Computer Science*, 3876, Springer, 2006, pp.60~79, Full version: http://eprint.iacr.org/2005/304/.

[9] Cramer R, Damgård I, Schoenmakers B. Proofs of partial knowledge and simplified design of witness hiding protocols. In *Proc. CRYPTO 94*, USA, *Lecture Notes in Computer Science*, 839, Springer-Verlag, 1994, pp.174~187.

[10] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems. In *Proc. CRYPTO 86*, USA, *LNCS* 263, Springer-Verlag, 1987, pp.186~199.

[11] Chaum D, Eugène van Heyst. Group signatures. In *Proc. EUROCRYPT '91*, UK, *LNCS* 547, Springer, 1991, pp.257~265.

[12] Camenisch J, Stadler M. Efficient group signature schemes for large groups. In *Proc. CRYPTO 97*, USA, *LNCS* 1294, Springer-Verlag, 1997, pp.410~424.

[13] Bellare M, Micciancio D, Warinschi B. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *Proc. EUROCRYPT 2003*, Poland, *LNCS* 2656, Springer, 2003, pp.614~629.

[14] Manulis M. Democratic group signatures — On an example of joint ventures. In *Proc. ACM Symposium on Information, Computer and Communications Security* (*ASIACCS 2006*), Taiwan, China, 2006, p.365.

[15] Liu J K, Wei V K, Wong D S. Linkable spontaneous anonymous group signature for ad hoc groups. In *Proc. ACISP 04*, Australia, *LNCS* 3108, Springer-Verlag, 2004, pp.325~335.

[16] Liu J K, Wong D S. Enhanced security models and a generic construction approach for linkable ring signature. *International Journal of Foundations of Computer Science*, Dec. 2006, 17(6): 1403~1422.

[17] Komano Y, Ohta K, Shimbo A, Kawamura S. Toward the fair anonymous signatures: Deniable ring signatures. In *Proc. CT-RSA 2006*, USA, *LNCS* 3860, Springer-Verlag, 2006, pp.174~191.

[18] An J H, Dodis Y, Rabin T. On the security of joint signature and encryption. In *Proc. EUROCRYPT 02*, The Netherlands, *LNCS* 2332, Springer-Verlag, 2002, pp.83~107.

[19] Goldwasser S, Micali S, Rivest R L. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.*, 1998, 17(2): 281~308.

[20] Liu J K, Wei V K, Wong D S. A separable threshold ring signature scheme. In *Proc. ICISC 2003*, Korea, *LNCS* 2971, Springer-Verlag, 2004, pp.12~26.

[21] Patrick P Tsang, Victor K Wei, Tony K Chan, Man Ho Au, Joseph K Liu, Duncan S Wong. Separable linkable threshold ring signatures. In *Proc. INDOCRYPT 2004*, India, *LNCS* 3348, Springer-Verlag, 2004, pp.384~398.

[22] Patrick P Tsang, Victor K Wei. Short linkable ring signatures for e-voting, e-cash and attestation. In *Proc. ISPEC 2005*, Singapore, *LNCS* 3439, Springer-Verlag, 2005, pp.48~60.

[23] Wu Q, Susilo W, Mu Y, Zhang F. Ad hoc group signatures. In *Proc. First International Workshop on Security* (*IWSEC 2006*), Japan, *LNCS* 4266, Springer-Verlag, 2006, pp.120~135.

[24] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. In *Proc. CRYPTO 2001*, USA, *LNCS* 2139, 2001, pp.213~229.

[25] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. 1st ACM Conference on Computer and Communications Security*, USA, ACM Press 1993, pp.62~73.

[26] Chaum D, Pedersen T. Wallet databases with observers. In *Proc. CRYPTO 92*, USA, *LNCS* 740, Springer-Verlag, 1993, pp.89~105.

Dennis Y. W. Liu received his B.S. degree in computer science from City University of Hong Kong. He is currently an M.Phil. student of the City University of Hong Kong. His research interest is information security, applied cryptography, and particularly, digital signature.

Joseph K. Liu obtained his Ph.D. degree in 2004 from the Department of Information Engineering, The Chinese University of Hong Kong. His research interest includes cryptography protocol and provable security. He has obtained Croucher Foundation Fellowship Award that supported him as a research fellow in the University of Bristol, UK from 2005~2007. Since September 2007, he works as a research fellow in the Institute of Infocomm Research, Singapore.

Yi Mu received his Ph.D. degree from the Australian National University in 1994. He currently is an associate professor in School of Computer Science and Software Engineering and the director of Centre for Computer and Information Security Research, University of Wollongong. Prior to joining University of Wollongong, he worked as a lecturer in the School of Computing and IT, University of Western Sydney, and later as a senior lecturer in the Department of Computing, Macquarie University. His current research interests include network security, computer security, and cryptography. He is the editor-in-chief of International Journal of Applied Cryptography and serves as an editor for six other international journals. He has served in program committees for a number of international conferences. He is a senior member of the IEEE and a member of the IACR.

Willy Susilo received a Ph.D. degree in computer science from University of Wollongong, Australia. Currently, he is an associate professor at the School of Computer Science and Software Engineering at the University of Wollongong. He is the Director of Centre for Computer and Information Security Research at the University of Wollongong. His research interests include cryptography, informa-

tion security, computer security and network security. His major research is in the area of digital signature schemes. His major inventions include the design and invention of short signature schemes and identity-based short signature schemes. He has published over 100 publications in the area of cryptography and information security.

Duncan S. Wong received the B.Eng. degree from the University of Hong Kong in 1994, the M.Phil. degree from the Chinese University of Hong Kong in 1998, and the Ph.D. degree from Northeastern University, Boston, MA, U.S.A. in 2002. He is currently an assistant professor in the Department of Computer Science at the City University of Hong Kong. His primary research interest is applied cryptography; in particular, cryptographic protocols and security for wireless communications. In addition, he has many years of experience in developing practical cryptographic systems.

Appendix A. Instantiation of $SPK(1)$

Based on [9, 26], we describe an instantiation of $SPK(1)$ which is reviewed as follows.

$$SPK\Big\{\alpha : \Big\{ \bigwedge_{j\in[1,\ell]} E_j = \hat{e}(R,\hat{y}_j)^{\alpha}\Big\} \bigwedge \Big\{ \bigvee_{i\in[1,n]} y_i = \alpha P\Big\}\Big\}(m).$$

For clear presentation, we first divide $SPK(1)$ into two components:

$$SPK\big\{\alpha : \bigwedge_{j\in[1,\ell]} E_j = \hat{e}(R,\hat{y}_j)^{\alpha}\big\}(m), \quad \text{(A1)}$$

$$SPK\big\{\alpha : \bigvee_{i\in[1,n]} y_i = \alpha P\big\}(m). \quad \text{(A2)}$$

Let $\mathcal{H} : \{0,1\}^* \to \mathbb{Z}_q$ be a hash function which is used as in the Fiat-Shamir transformation[10] to convert a three-move honest-verifier zero-knowledge proof to a signature scheme. By $\mathcal{H}(a\|b)$, we mean the string concatenation of a and b. From now on, S is considered to be a sequence of public keys denoted by $(y_1,\ldots,y_n)$.

To generate a transcript of $SPK(7)$, given T, R, $E_1,\ldots,E_\ell \in \mathbb{G}_2$, the actual signer indexed by π, for some $1 \leqslant \pi \leqslant n$, proves the knowledge of x_π such that $E_j = \hat{e}(R,\hat{y}_j)^{x_\pi}$, for $1 \leqslant j \leqslant \ell$, by releasing (s,c) as the transcript such that

$$c = \mathcal{H}(T\|R\|E_1\|\cdots\|E_\ell\|\hat{e}(R,\hat{y}_1)^s {E_1}^c\| \cdots\|\hat{e}(R,\hat{y}_\ell)^s {E_\ell}^c\|m).$$

This can be done by randomly pick $r \in_R \mathbb{Z}_q$ and compute

$$c \leftarrow \mathcal{H}(T\|R\|E_1\|\cdots\|E_\ell\|\hat{e}(R,\hat{y}_1)^r\|\cdots\|\hat{e}(R,\hat{y}_\ell)^r\|m)$$

and then setting $s = r - cx_\pi \bmod q$.

To generate the transcript of $SPK(8)$, given S, the actual signer indexed by π, for some $1 \leqslant \pi \leqslant n$, proves the knowledge of x_π out of n discrete logarithms x_i, where $y_i = x_i P$, for $1 \leqslant i \leqslant n$, without revealing the value of π. This can be done by releasing $(s_1,\ldots,s_n,c_1,\ldots,c_n)$ as the transcript such that $c_0 = \sum_{i=1}^n c_i \bmod q$ and

$$c_0 = \mathcal{H}(S \parallel s_1 P + c_1 y_1 \parallel \cdots \parallel s_n P + c_n y_n\|m).$$

To generate this transcript, the actual signer first picks randomly $r \in_R \mathbb{Z}_q$ and $s_i, c_i \in_R \mathbb{Z}_q$ for $1 \leqslant i \leqslant n$, $i \neq \pi$, then computes

$$c_0 \leftarrow \mathcal{H}(S\|s_1 P + c_1 y_1\|\cdots\| s_{\pi-1}P + c_{\pi-1}y_{\pi-1}\|rP\| s_{\pi+1}P + c_{\pi+1}y_{\pi+1}\|\cdots\|s_n P + c_n y_n\|m)$$

and finds c_π such that $c_0 = c_1 + \cdots + c_n \bmod q$. Finally the signer sets $s_\pi = r - c_\pi x_\pi \bmod q$.

Now we combine the constructions of $SPK(7)$ and $SPK(8)$ together. First, the actual signer randomly picks $r_1, r_2 \in_R \mathbb{Z}_q$ and $s_i, c_i \in_R \mathbb{Z}_q$, for $1 \leqslant i \leqslant n$, $i \neq \pi$, then computes

$$c \leftarrow \mathcal{H}(S\|T\|R\|E_1\|\cdots\|E_\ell\|\hat{e}(R,\hat{y}_1)^{r_1}\|\cdots\|\hat{e}(R,\hat{y}_\ell)^{r_1}\| s_1 P + c_1 y_1\|\cdots\|s_{\pi-1}P + c_{\pi-1}y_{\pi-1}\|r_2 P\| s_{\pi+1}P + c_{\pi+1}y_{\pi+1}\|\cdots\|s_n P + c_n y_n\|m).$$

After that, the actual signer sets $s = r_1 - cx_\pi \bmod q$, finds c_π such that $c = c_1 + \cdots + c_n \bmod q$, and set $s_\pi = r_2 - c_\pi x_\pi \bmod q$. The transcript of $SPK(1)$ is therefore $(s, s_1,\ldots,s_n,c_1,\ldots,c_n)$.

To verify the transcript, the public checks

$$\sum_{i=1}^n c_i \stackrel{?}{=} \mathcal{H}(S \parallel T \parallel R \parallel E_1 \parallel \cdots \parallel E_\ell \parallel \hat{e}(R,\hat{y}_1)^s E_1^{\sum_{i=1}^n c_i} \parallel \cdots \parallel \hat{e}(R,\hat{y}_\ell)^s E_n^{\sum_{i=1}^n c_i} \parallel s_1 P + c_1 y_1 \parallel \cdots \parallel s_n P + c_n y_n\|m).$$