A Provably Secure Ring Signature Scheme with Bounded Leakage Resilience

Huaqun Wang[1,2], Qianhong Wu[3], Bo Qin[4], Futai Zhang[5], and Josep Domingo-Ferrer[6]

[1]School of Information Engineering, Dalian Ocean University
[2]Shanghai Key Laboratory of Integrate Administration Technologies for Information Security
[3]School of Electronic and Information Engineering, Beihang University
[4]School of Information, Renmin University of China
[5]School of Computer Science and Technology, Nanjing Normal University
[6]Dept. of Computer Engineering and Maths, Universitat Rovira i Virgili
wanghuaqun@aliyun.com, qhwu@xidian.edu.cn, qinboo@xaut.edu.cn, zhangfutai@njnu.edu.cn, josep.domingo@urv.cat

Abstract. Conventionally, the unforgeability of ring signature schemes is defined in an ideal environment where the attackers cannot access any information about the secret keys of the signers. This assumption is too strong to be satisfied in the real world since the cryptographic operations involves the secret key information leakage in various ways due to power/time consumption difference in operations on the 0/1 bits of the secret key. An attacker can obtain this information both passively by collecting power consumption information or actively by injecting faults during the signing operations. Thus, provably secure ring signature in the conventional security definition may be insecure in the real world due to the key information leakage. To address this problem, we formalize the first bounded leakage resilience definition for ring signature. A leakage resilient ring signature scheme remains secure even if arbitrary, but bounded, information about the secret key is leaked to an adversary. A bound on the leaked information is necessary because a ring signature cannot be secure if some signer's secret key is fully leaked. Then we propose the first ring signature scheme with bounded leakage resilience. Following the enhanced security definition with leakage resilience, the proposed scheme is provably secure based on the difficulty of the second l-representation problem in finite field.
Keywords: Ring signature, Secret key leakage, Leakage resilience.

1 Introduction

A useful model when proving the security of a cryptographic primitive is to think of it as a black box, that is, to assume that the adversary can only use and observe the primitive in a pre-specified and limited way. This simplified model commonly assumes that no information on the secret key is accessible to the adversary. However, when cryptographic primitives are implemented in

the real world, they actually become "translucent" boxes to a clever adversary. Indeed, the adversary may succeed in recovering significant information on the secret key through side-channel cryptanalysis [1, 2], fault attacks [3, 4], timing attacks [5], *et al.* As a result, some bits of the secret key are at risk of being leaked. The conventional security definitions of cryptosystem do not capture this kind of attacks. A secure cryptographic scheme should remain secure even if some bits of the secret key have been leaked to the adversary. It can make cryptographic schemes secure after they are implemented in the real world, not just theoretically secure in an ideal security model.

We formalize an appropriate model of what information the adversary can learn during a leakage attack. We also need to bound how much information the adversary can learn since a cryptographic scheme cannot be secure if all the bits of the secret key are leaked. Therefore, in this work we assume that the attacker can repeatedly and adaptively learn arbitrary function values of the secret key sk, as long as the total number of bits leaked during the lifetime of the system is bounded by some parameter l. A cryptographic scheme is said to be secure with bounded leakage resilience if it remains secure under this attack. Specially, we study secure ring signature scheme in the model of bounded leakage resilience. We allow the leakage function to be arbitrary as long as the total leakage is bounded as some function of the secret key length $|sk|$. If the secret key is unchanging, such a restriction on the leakage is essential.

1.1 Related work

In recent years, there has been impressive progress in leakage-resilient cryptography. The early efforts were made to obtain leakage resilience encryption schemes [6, 7]. In 2009, Akavia *et al.* proposed memory attacks and proved that two lattice-based public-key encryption schemes are secure in the face of these attacks [8]. Subsequently, Naor *et al.* proposed a leakage-resilient public-key encryption scheme based on a universal hash proof system [9].

There has also been works on leakage-resilient signatures. Katz *et al.* gave a signature scheme tolerating the secret key leakage [10]. Faust *et al.* gave a tree-based, stateful leakage-resilient signature scheme from any 3-time signature scheme [11]. Boyle *et al.* constructed fully leakage-resilient signature schemes without random oracles [12]. Malkin *et al.* [13] presented the first signature scheme that is resilient to fully continual leakage: memory leakage as well as leakage from processing during signing, key generation and updates (both of the secret key and the randomness). Faust *et al.* [14] proposed the first constructions of digital signature schemes that are secure in the auxiliary input model. They designed a digital signature scheme that is secure against chosen-message attacks when given an exponentially hard-to-invert function of the secret key. Phong *et al.* [15] considered the continual key leakage scenario of strong key-insulated signature design. Guo *et al.* proposed efficient online/offline signatures with computational leakage resilience in the online phase [16]. Alwen *et al.* studied the design of cryptographic primitives resilient to key leakage attacks [17].

Most efforts have been devoted to leakage-resilient signatures in the single-signer setting. Motivated by group-oriented applications, ring signature were introduced in 2001 by Rivest *et al.* [18]. In a ring signature scheme, one user can form an on-the-fly group in an *ad hoc* way by simply adding other users' public keys to the group key list, without getting other users' agreements. Then he can sign any message on behalf of that temporal group. The resulting signature is verifiable by anyone who knows the public keys of the group members in the temporal group. For a secure ring signature, it is required that only users in the group member list can generate a valid signature and the signatures generated by different members are theoretically indistinguishable. The former property is referred to as unforgeability and the latter as unconditional anonymity. It has been shown that ring signature is a very useful cryptographic primitive in many applications [19–22]. However, to the best of our knowledge, no leakage-resilient ring signature was proposed in the public literature. This motivates us to investigate security-enhanced ring signature that can withstand bounded leakage of the secret key.

1.2 Our contribution

This paper focuses on leakage-resilient ring signature. More specifically, our contributions are twofold:

- First, we formalize the model of ring signature with bounded leakage resilience. We focus on existential unforgeability under adaptively chosen-message and bounded leakage attacks. In these attacks, an attacker is allowed not only to adaptively query for ring signature on any message of his choice, but also to access a leakage oracle through a leakage function f to gain information about the secret keys of the signers. The constraint is that the output of the leakage function after all the leakage queries should be bounded. Unforgeability states that no polynomial-time attacker can forge a valid ring signature with non-negligible probability in probabilistic polynomial time.
- Second, we propose the first ring signature scheme with bounded leakage resilience. Specifically, we follow the above model and prove that our scheme is unforgeable under the adaptively chosen message and bounded leakage attacks. The proof relies on the hardness of the second l-representation problem which is related to the well-known discrete logarithm problem. We also show that our ring signature scheme preserves unconditional anonymity even if the attacker is provided with the secret keys in the group. Thus, the anonymity of our ring signature scheme is perfectly leakage-resilient without any bound on the information leakage on the secret keys.

1.3 Plan of this paper

The rest of this paper is organized as follows. Section 2 contains some technical preliminaries. Section 3 formalizes the security model of ring signature with

bounded leakage resilience. Section 4 presents our concrete ring signature scheme with bounded leakage resilience. Section 5 evaluates the security of our scheme. Finally, Section 6 contains some conclusions and sketches future work directions.

2 Preliminaries

We review some information theory results and computational assumptions.

2.1 Information theory lemmas

The following two definitions come from the reference [23].

Definition 1 (Min-entropy). *The min-entropy of a random variable X, denoted by $H_\infty(X)$, is $H_\infty(X) \stackrel{def}{=} \min_{x\in\{0,1\}^n}\{-\log_2 Pr[X=x]\}$.*

Definition 2 (Average-conditional min-entropy). *The average-conditional min-entropy of a random variable X given Z, denoted as $\tilde{H}_\infty(X|Z)$, is*

$$\tilde{H}_\infty(X|Z) \stackrel{def}{=} -\log_2(E_{z\leftarrow Z}[\max_x Pr[X=x|Z=z]]) = -\log_2(E_{z\leftarrow Z}[2^{H_\infty[X|Z=z]}])$$

where $E_{z\leftarrow Z}(\cdot)$ means taking average of the argument over all values z of Z.

The following lemma is proven in [23].

Lemma 1. *Let X, Y, Z be random variables where Y takes values in a set of size at most 2^l. Then, $\tilde{H}_\infty(X|(Y,Z)) \geq \tilde{H}_\infty((X,Y)|Z) - l \geq \tilde{H}_\infty(X|Z) - l$, and in particular, $\tilde{H}_\infty(X|Y)) \geq \tilde{H}_\infty(X) - l$.*

The following lemma is proven in [10].

Lemma 2. *Let X be a random variable with $H \stackrel{def}{=} H_\infty(X)$, and fix $\Delta \in [0, H]$. Let f be an arbitrary function with range $\{0,1\}^\lambda$, and set*

$$Y \stackrel{def}{=} \{y \in \{0,1\}^\lambda | H_\infty(X|y = f(X)) \leq H - \Delta\}$$

Then, $Pr[f(X) \in Y] \leq 2^{\lambda-\Delta}$.

In other words, the probability that knowledge of $f(X)$ decreases the min-entropy of X by Δ or more is at most $2^{\lambda-\Delta}$. Put differently, the min-entropy of X after observing the value of $f(X)$ is greater than H' except with probability at most $2^{\lambda-H+H'}$.

2.2 Computational assumptions

We recall the computationally difficult problems underlying our constructions. In this paper, let q and p denote two secure prime numbers that satisfy $q|(p-1)$. On the other hand, $\hat{k}$ is the security parameter.

Assumption 1 (Discrete logarithm problem) *Let $\mathscr{G}$ be a probabilistic algorithm which takes a security parameter $\hat{k}$ as input and outputs (G, q, p), where G is a finite cyclic subgroup of order q which belongs to a group of order p. We say the discrete logarithm problem is hard for the group G if, for any probabilistic polynomial-time (PPT) algorithm $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible. The advantage of $\mathcal{A}$ can be defined below*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathrm{DLP}} = \Pr\left[\begin{array}{c|c} (G,q,p) \leftarrow \mathscr{G}(1^{\hat{k}}) & \\ g, h \leftarrow G & x \leftarrow \mathcal{A}(G, q, g, h,) \wedge g^x = h \end{array}\right]$$

where $x \in \mathbb{Z}_q^*, g^x = h \bmod p$, g is a generator of G.

Assumption 2 (First l-representation problem) *[10] We say that the first l-representation problem is hard for the group G if, for any PPT algorithm $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible. The advantage of $\mathcal{A}$ can be defined below*

$$\mathsf{Adv}_{\mathcal{A}}^{l\text{-FRP}} = \Pr\left[\begin{array}{c|c} (G,q,p) \leftarrow \mathscr{G}(1^{\hat{k}}) & \begin{pmatrix} x_1, x_2, \cdots, x_l \\ x_1', x_2', \cdots, x_l' \end{pmatrix} \leftarrow \mathcal{A}(G, q, g_1, g_2, \cdots, g_l) \\ g_1, g_2, \cdots, g_l \leftarrow G & \wedge \prod_i g_i^{x_i} = \prod_i g_i^{x_i'} \bigwedge \overrightarrow{x} \neq \overrightarrow{x}' \end{array}\right]$$

where q is the order of the group G, p is the size of G, $(x_1, x_2, \cdots, x_l) \in (\mathbb{Z}_q^*)^l$, $(x_1', x_2', \cdots, x_l') \in (\mathbb{Z}_q^*)^l$, $\prod_i g_i^{x_i} = \prod_i g_i^{x_i'} \bmod p$, g is a generator of G.

Notes: The discrete logarithm problem and the first l-representation problem are equivalent.

1. If the first l-representation problem is easy, then when $l = 2$, we can solve the discrete logarithm problem. Given g, h, then $\mathcal{A}$ can get two different tuples $(x, y), (x', y')$ that satisfy $g^x h^y = g^{x'} h^{y'} \bmod p$. Denote $h = g^\omega$, then we can get $\omega = \frac{x'-x}{y-y'} \bmod q$. Thus, the discrete logarithm problem is solved.
2. On the other hand, if the discrete logarithm problem is easy, then $\mathcal{A}$ can get r_i that satisfy $g_i = g^{r_i}$ for $1 \leq i \leq l$. $\mathcal{A}$ can pick a random tuple $\overrightarrow{x} = (x_1, x_2, \cdots, x_l)$ and compute $\hat{x} = \sum_{i=1}^{l} r_i x_i \bmod q$. Then, $\mathcal{A}$ solves the equation $\sum_{i=1}^{l} r_i x_i' = \hat{x} \bmod q$. It is easy to calculate another tuple $\overrightarrow{x'} = (x_1', x_2', \cdots, x_l')$ that satisfies $\sum_{i=1}^{l} r_i x_i = \sum_{i=1}^{l} r_i x_i' \bmod q$, *i.e.*, $\prod_i g_i^{x_i} = \prod_i g_i^{x_i'}$. Thus, the first l-representation problem is solved.

According to the above analysis, we know that the discrete logarithm problem and the first l-representation problem are equivalent.

Assumption 3 (Second l-representation problem) *We say that the second l-representation problem is hard for the group G if, for any PPT algorithm $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible. The advantage of $\mathcal{A}$ is defined below*

$$\mathsf{Adv}_{\mathcal{A}}^{l\text{-SRP}} = \Pr\left[\begin{array}{l|l}(G,q,p) \leftarrow \mathscr{G}(1^{\hat{k}}) & \left(x_1', x_2', \cdots, x_l'\right) \leftarrow \mathcal{A}(G,q,g_1,g_2,\cdots,g_l,(x_1, \\ g_1,g_2,\cdots,g_l \leftarrow G & x_2,\cdots,x_l)) \wedge \prod_i g_i^{x_i} = \prod_i g_i^{x_i'} \bigwedge \overrightarrow{x} \neq \overrightarrow{x}'\end{array}\right]$$

where q is the order of the group G, p is the size of G, $(x_1, x_2, \cdots, x_l) \in (\mathbb{Z}_q^*)^l$ is randomly chosen beforehand, $(x_1', x_2', \cdots, x_l') \in (\mathbb{Z}_q^*)^l$, $\prod_i g_i^{x_i} = \prod_i g_i^{x_i'} \bmod p$, g is a generator of G.

In this paper, our proposed leakage-resilient ring signature scheme is built on some subgroup of $\mathbb{Z}_p^*$ with the order q. The discrete logarithm problem, the first l-representation problem and the second l-representation problem are difficult on the subgroup of $\mathbb{Z}_p^*$.

Notes: The first l-representation problem assumption is stronger than the second l-representation problem assumption. If the assumption 3 does not hold, the adversary $\mathcal{A}$ can pick a random tuple $(x_1, x_2, \cdots, x_l)$ as the input, it can output another tuple $(x_1', x_2', \cdots, x_l')$ by taking use of *the second l-representation* oracle. Thus, the adversary $\mathcal{A}$ gets the two tuples $\overrightarrow{x} = (x_1, x_2, \cdots, x_l)$ and $\overrightarrow{x}' = (x_1', x_2', \cdots, x_l')$ that satisfy $\prod_i g_i^{x_i} = \prod_i g_i^{x_i'} \bigwedge \overrightarrow{x} \neq \overrightarrow{x}'$. Thus, the second l-representation problem assumption is weaker than the first l-representation problem assumption.

3 Modeling ring signature with bounded leakage resilience

We provide a formal definition of bounded leakage-resilient ring signature, and we state some technical lemmas that will be used in our security analysis. The security definitions are the variants of the reference [10].

Definition 3 (Ring signature). *A ring signature scheme is a tuple of PPT algorithms (* **Setup, Ring-Sign, Ring-Vrfy** *) defined as follows.*

Setup *Each potential user U_i generates his secret/public key pair (sk_i, pk_i) by using a key generation protocol that takes as input a security parameter $\hat{k}$.*

Ring-Sign *If a user U_k wants to compute a ring signature on behalf of a ring $L = \{U_1, \cdots, U_n\}$ that contains himself, i.e., $U_k \in L$, U_k executes this probabilistic polynomial time algorithm with input a message m, the public keys $pk_1, \cdots, pk_n$ of the ring and his secret key sk_k. The output of this algorithm is a ring signature σ for the message m and the ring L.*

Ring-Vrfy *This is a deterministic polynomial time algorithm that takes as input a message m and a ring signature σ, that includes the public keys of all the members of the corresponding ring L, and outputs "True" if the ring signature is valid, or "False" otherwise.*

The resulting ring signature scheme must satisfy the following properties:

1. *Correctness*: A ring signature generated in a correct way must be accepted by any verifier with overwhelming probability.
2. *Anonymity*: If a signer computes a ring signature on behalf of a ring of n members, any verifier not belonging to the ring should not have probability greater than $\frac{1}{n}$ to guess the signer's identity. If the verifier is a member of the signer's ring, but is not the signer himself, then his probability of guessing the signer's identity should not be greater than $\frac{1}{n-1}$.
3. *Unforgeability*: Any attacker has only negligible probability in forging a valid ring signature for some message m on behalf of a ring that does not contain him, even if he knows valid ring signature for messages, different from m, that he can adaptively choose.

The definition of ring signature with bounded leakage resilience is the same as the standard definition of ring signature. The security model definition of ring signature with bounded leakage resilience is similar to the standard security model definition of ring signature, except that we additionally allow the adversary to specify arbitrary leakage functions $\{f_i\}$ and obtain the value of these functions applied to the secret key. The formal security properties of ring signature with bounded leakage resilience are stated next.

Definition 4 (Unforgeability of ring signature with bounded leakage resilience). *Let* $\prod = \{Setup, Ring\text{-}Sign, Ring\text{-}Vrfy\}$ *be a ring signature scheme, and let* λ *be a function. Given an adversary* $\mathcal{A}$*, the experiment is defined as follows:*

1. *The user* U_i *can obtain the corresponding secret/public key pair* (sk_i, pk_i) *by running* $(sk_i, pk_i) \leftarrow Gen(1^{\hat{k}}, r_i)$, $1 \leq i \leq n$, *where Gen denotes an algorithm that can generate the secret/public key pair.*
2. *Run* $\mathcal{A}(1^{\hat{k}}, pk_1, \cdots, pk_n)$*. The adversary may adaptively access a ring signing oracle Ring-Sign*$(\cdot)$ *and a leakage oracle Leak*$(\cdot)$ *that have the following functionalities:*
   - *Let the i-th ring signature query be* $Ring\text{-}Sign_{sk_k}(m_i, pk_{j_1}, \cdots, pk_{j_i})$*, where* $L_i = \{pk_{j_1}, \cdots, pk_{j_i}\} \subseteq \{pk_1, \cdots, pk_n\}$ *and* $pk_k \in L_i$*. The ring signature oracle computes* $\sigma_i = Ring\text{-}Sign_{sk_k}(m_i, pk_{j_1}, \cdots, pk_{j_i})$*, and returns* σ_i *to* $\mathcal{A}$*.*
   - *In order to respond to the i-th leakage query* $Leak(f_i, sk_k)$ *(where* f_i *is specified as a circuit), the leakage oracle returns* $f_i(sk_k)$ *to* $\mathcal{A}$*, where* sk_k *is the secret key to be used for computing the ring signature.* sk_k *may be other secret key whose corresponding public key belongs to the signing set* L_i *and* $\mathcal{A}$ *queries* U_k *to sign the message. (To make the definition meaningful in the random oracle model, the* $\{f_i\}$ *are allowed to be oracle circuits that depend on the random oracle.) The* $\{f_i\}$ *can be arbitrary, subject to the restriction that the total output length of all the* $f_i(sk_k)$ *is at most* $\lambda(|sk_k|)$*.*

3. At some point, $\mathcal{A}$ outputs (m, L, σ) where $L \subseteq \{pk_1, pk_2, \cdots, pk_n\}$.

We say $\mathcal{A}$ succeeds if (1) Ring-$Vrfy_{pk_{j_1},\cdots,pk_{j_l}}(m, \sigma) = 1$, and (2) m was not previously queried to the Ring-$Sign_{sk_j}(\cdot)$ oracle. We denote the probability of this event by $Pr^{\lambda-leakage}_{\mathcal{A},\prod}(\hat{k})$. If $Pr^{\lambda-leakage}_{\mathcal{A},\prod}(\hat{k})$ is negligible for any PPT adversary $\mathcal{A}$, we say $\prod$ is λ-leakage resilient.

Definition 4 gives the unforgeability of ring signature with bounded leakage resilience. Unconditional anonymity is another important security property of ring signature that can be defined as follows.

Definition 5 (Anonymity of ring signature with bounded leakage resilience). *If a signer computes a ring signature on behalf of a ring of n members, any verifier not belonging to the ring should not have probability greater than $\frac{1}{n}$ to guess the signer's identity even some bits of the secret key are leaked . If the verifier is a member of the signer's ring, but is not the signer himself, then his probability of guessing the signer's identity should not be greater than $\frac{1}{n-1}$ even if some bits of the secret key are leaked .*

Note that unconditional anonymity means that the scheme remains anonymous even all the secret keys are exposed to the adversary. Thus, if we can prove that a ring signature scheme satisfies unconditional anonymity, then this scheme remains anonymous with bounded leakage.

The anonymity property is closely related to the witness indistinguishability notion [24]. In general, an $\mathcal{NP}$ statement may have multiple witnesses. For example, a Hamiltonian graph may have multiple Hamiltonian cycles; a 3-colorable graph may have multiple (non-isomorphic) 3-colorings; etc. In leakage-resilient public-key cryptography, we are interested in proof systems (for languages in $\mathcal{NP}$) that do not leak information about which witness the prover is using, even to a malicious verifier. In the sequel, we let $\langle \mathcal{A}(y), \mathcal{B}(z)\rangle(x)$ denote the view (*i.e.*, inputs, internal coin tosses, incoming messages) of $\mathcal{B}$ when interacting with $\mathcal{A}$ on common input x, $\mathcal{A}$ has auxiliary input y and $\mathcal{B}$ has auxiliary input z. The definition of witness indistinguishability can be used to decide whether our proposed scheme satisfies the property. It is also important to prove our scheme's unforgeability based on witness indistinguishability.

Definition 6 (Witness indistinguishability). *Let $L \in \mathcal{NP}$ and let $(\mathcal{P}, \mathcal{V})$ be an interactive proof system for L with perfect completeness. We say that $(\mathcal{P}, \mathcal{V})$ is witness-indistinguishable (WI) if for every PPT algorithm $\mathcal{V}^*$ and every two sequences $\{\omega^1_x\}_{x\in L}$ and $\{\omega^2_x\}_{x\in L}$ such that ω^1_x and ω^2_x are both witnesses for x, the following ensembles are computationally indistinguishable:*

1. $\{\langle \mathcal{P}(\omega^1_x), \mathcal{V}^*(z)\rangle(x)\}_{x\in L, z\in\{0,1\}^*}$
2. $\{\langle \mathcal{P}(\omega^2_x), \mathcal{V}^*(z)\rangle(x)\}_{x\in L, z\in\{0,1\}^*}$

(When the security parameter is not written explicitly, we simply take $|x| = \hat{k}$ without confusion.) In particular, we may have $z = (\omega^1_x, \omega^2_x)$.

4 Our ring signature scheme with bounded leakage resilience

In this section, we describe our ring signature scheme with bounded leakage resilience. Our concrete scheme is based on Schnorr signature [25] and Rivest *et al.*'s ring signature construction skeleton [18]. Here, by $a \in_R \mathbb{Z}_q^*$ we denote drawing a random number a from $\mathbb{Z}_q^*$ according to the uniform distribution. Also, by $H : \{0,1\}^* \to \mathbb{Z}_q^*$ we denote a collision-resistant hash function. Our scheme consists of three phases: **Setup, Ring-Sign, Ring-Vrfy**.

Setup Suppose that there exist n users in the system. Assume that $g_1, \cdots, g_l$ are generators of some subgroup S_G of $\mathbb{Z}_p^*$, where the order of the subgroup S_G is q. Let $(n, p, q, g_1, \cdots, g_l)$ be the publicly accessible global system parameters. For $i = 1, 2, \cdots, n$ and $j = 1, 2, \cdots, l$, select $x_{ij} \in \mathbb{Z}_q^*$. Then, the i-th user's secret/public key pair is (sk_i, pk_i), where

$$sk_i = (x_{i1}, x_{i2}, \cdots, x_{il}), \quad pk_i = \prod_{j=1}^{l} g_j^{x_{ij}} \bmod p.$$

Ring-Sign Suppose that the actual signer is U_k. He selects a signer set L containing U_k. Without loss of generality, we assume that $L = \{U_1, U_2, \cdots, U_{k-1}, U_k, U_{k+1}, \cdots, U_s\}$. The actual signer U_k performs the procedures as follows.

1. Pick $\alpha_1, \cdots, \alpha_l \in_R \mathbb{Z}_q^*$ and calculate
$$c_{k+1} = H(L, m, g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_l^{\alpha_l} \bmod p)$$
2. For $i = k+1, \cdots, s, 1, \cdots, k-1$, pick $s_{i1}, s_{i2}, \cdots, s_{il} \in_R \mathbb{Z}_q^*$ and calculate
$$c_{i+1} = H(L, m, g_1^{s_{i1}} g_2^{s_{i2}} \cdots g_l^{s_{il}} pk_i^{c_i} \bmod p)$$
where $1 = s + 1 \bmod s$, *i.e.*, they are cycle.
3. Calculate $s_{k1} = \alpha_1 - x_{k1} c_k \bmod q, \quad \cdots, \quad s_{kl} = \alpha_l - x_{kl} c_k \bmod q$. Finally, U_k outputs $\{c_1, s_{ij}, 1 \le i \le s, 1 \le j \le l\}$ as the ring signature for m, L.

Ring-Vrfy Upon receiving the ring signature $\{c_1, s_{ij}, 1 \le i \le s, 1 \le j \le l\}$ for m and L, the verifier does:

1. For $i = 1, \cdots, s$, calculate $e_i = g_1^{s_{i1}} \cdots g_l^{s_{il}} pk_i^{c_i} \bmod p, \quad c_{i+1} = H(L, m, e_i)$.
2. Check whether $c_1 \stackrel{?}{=} H(L, m, e_s)$ holds or not. If it holds, accept this signature. Otherwise, reject it.

Theorem 1 (Correctness). *If the signer and the verifier are honest, our ring signature with bounded leakage resilience can pass the verification.*

Proof. Without loss of generality, suppose the actual signer is U_k. The received ring signature is $\{c_1, s_{ij}, 1 \le i \le s, 1 \le j \le l\}$ for m and L. According to the signature process, we know that if $e_k = g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_l^{\alpha_l} \bmod p$ holds, it is straightforward that our ring signature scheme can pass the verification.

According to the signature process, we know that

$$\begin{aligned} g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_l^{\alpha_l} \bmod p &= g_1^{s_{k1}+x_{k1}c_k} g_2^{s_{k2}+x_{k2}c_k} \cdots g_l^{s_{kl}+x_{kl}c_k} \bmod p \\ &= g_1^{s_{k1}} g_2^{s_{k2}} \cdots g_l^{s_{kl}} g_1^{x_{k1}c_k} g_2^{x_{k2}c_k} \cdots g_l^{x_{kl}c_k} \bmod p \\ &= g_1^{s_{k1}} g_2^{s_{k2}} \cdots g_l^{s_{kl}} pk_k^{c_k} \bmod p \\ &= e_k \end{aligned}$$

Thus, our scheme satisfies the correctness. □

5 Security analysis

A secure ring signature scheme with bounded leakage resilience must satisfy the following requirements: unconditional anonymity and unforgeability.

Theorem 2. *Our proposed ring signature scheme with bounded leakage resilience is unconditionally anonymous.*

Proof. From the above ring signature process, we know that $(s_{i1}, s_{i2}, \cdots, s_{il}) \in_R \mathbb{Z}_q^{*l}$, where $i \in \{1, 2, \cdots, k-1, k+1, \cdots, s\}$. For the signer's subscript k, we have that $s_{k1}, s_{k2}, \cdots, s_{kl}$ are also uniformly distributed over $\mathbb{Z}_q^*$ because $(\alpha_{k1}, \cdots, \alpha_{kl}) \in_R \mathbb{Z}_q^{*l}$. Therefore, for fixed (L, m), $(s_{i1}, s_{i2}, \cdots, s_{il}), 1 \le i \le s$ has q^{sl} variations that are equally likely regardless of the signer's subscript k. The remaining element c_1 is a hash value which is determined uniquely by (L, m), $s_{sj}, 1 \le j \le l$ and pk_s. In random oracle model, c_1 is a random value which does not expose the true signer's identity. Thus, our proposed ring signature scheme is unconditionally anonymous. □

Lemma 3. *Our proposed ring signature scheme with bounded leakage resilience satisfies the property of witness indistinguishability.*

Proof. : To prove this, for two different witnesses, $(x_{k1}, x_{k2}, \cdots, x_{kl})$ and $(x'_{k1}, x'_{k2}, \cdots, x'_{kl})$ satisfying $pk_k = \prod_{j=1}^{l} g_j^{x_{kj}} = \prod_{j=1}^{l} g_j^{x'_{kj}} \bmod p$ (1), we show that even an infinitely powerful adversary $\mathcal{B}$ cannot determine which witness was used from the ring signature.

Let $\delta_{kj} = x'_{kj} - x_{kj} \bmod q$ where $1 \le j \le l$. Suppose the actual signer is U_k and the ring signature is $\{c_1, s_{ij}, 1 \le i \le s, 1 \le j \le l\}$ for m and L. Due to the ring signature procedures, we know that all the s_{ij} are random for $i \ne k, 1 \le j \le l$. When $i = k$ and $1 \le j \le l$, from the ring signature procedure, the following equation holds for the chosen random numbers α_{kj} that were picked in the phase of Ring-Sign.

$$s_{kj} = \alpha_j - x_{kj}c_k = \alpha_j + \delta_{kj}c_k - (\delta_{kj} + x_{kj})c_k = \alpha_j + \delta_{kj}c_{k-1} - x'_{kj}c_{k-1} \bmod q$$

From Equation (1), it follows that

$$\prod_{j=1}^{l} g_j^{x_{kj}} = \prod_{j=1}^{l} g_j^{x_{kj}+\delta_{kj}} \bmod p, \qquad \prod_{j=1}^{l} g_j^{\delta_{kj}} = 1 \bmod p$$

Let $\alpha'_j = \alpha_j + \delta_{kj}c_k$. We obtain

$$A_k = \prod_{j=1}^{l} g_j^{\alpha_j} = \prod_{j=1}^{l} g_j^{\alpha'_j - \delta_{kj}c_k} = \prod_{j=1}^{l} g_j^{\alpha'_j} \prod_{j=1}^{l} g_j^{-\delta_{kj}c_k}$$
$$= \prod_{j=1}^{l} g_j^{\alpha'_j} (\prod_{j=1}^{l} g_j^{\delta_{kj}})^{-c_k} = \prod_{j=1}^{l} g_j^{\alpha'_j} \bmod p$$

Thus, the distributions of $\overrightarrow{\alpha} = (\alpha_1, \cdots, \alpha_l)$ and $\overrightarrow{\alpha}' = (\alpha'_1, \cdots, \alpha'_l)$ are exactly equivalent. To the two different tuples $\overrightarrow{\alpha}$ and $\overrightarrow{\alpha}'$, the signer U_k can get the same ring signature $\{c_1, s_{ij}, 1 \le i \le s, 1 \le j \le l\}$ when it picks the same random numbers s_{ij} for $i \ne k, 1 \le j \le l$. Hence, even an infinitely powerful adversary $\mathcal{B}$ cannot determine which witness was used from the ring signature. Our proposed ring signature scheme with bounded leakage resilience satisfies the property of witness indistinguishability. □

Theorem 3. *Suppose $\mathcal{A}$ is a $(T, \epsilon, q_H, q_S, \lambda)$-forger against our ring signature scheme, i.e., $\mathcal{A}$ can forge a valid ring signature with probability ϵ within time T after q_H hash queries, q_S signature queries and leakage of at most $\lambda = (\frac{1}{2} - \frac{1}{2l} - \epsilon) \cdot l \cdot \log_2 q$ bits of the secret key, where the length of the secret key is $l \cdot \log_2 q$ bits. Then, the second l-representation problem can be solved with probability $\frac{1}{2n}(1 - \frac{q_H}{q^{2\epsilon l}})$ within time $T' \le \frac{144823 V_{q_h,n}(T + q_s T_s)}{\epsilon}$, where $V_{Q,n}$ denotes the number of n-permutations of Q elements, that is, $V_{Q,n} = Q(Q-1)\cdots(Q-n+1)$. Based on the difficulty of the second l-representation problem, our scheme is λ-leakage resilient.*

Proof. Let $\prod$ denote the scheme given above, and let $\mathcal{A}$ be a PPT adversary with success probability $\epsilon \stackrel{def}{=} Pr[Succ^{\lambda-leakage}_{\mathcal{A},\prod}(\hat{k})]$, where $\hat{k}$ is the security parameter. Input the second l-representation problem $(S_G, q, g_1, g_2, \cdots, g_l, (x_1, x_2, \cdots, x_l))$, we construct a challenger $\mathcal{B}$ solving the second l-representation problem with probability $\frac{1}{2}(1 - \frac{q_H}{q^{2\epsilon l}})$ within time $T' \le \frac{144823 V_{q_h,n}(T + q_s T_s)}{\epsilon}$.

$\mathcal{B}$ is given some secret keys $sk_i, 1 \le i \le n$, where sk_i is a secret key that corresponds to the user U_i. Algorithm $\mathcal{B}$ then answers the signing and leaking queries of $\mathcal{A}$ using the secret keys $sk_i, 1 \le i \le n$ that it knows. Since the secret keys are distributed identically to the secret key of an honest signer, the simulation for $\mathcal{A}$ is perfect.

Without loss of generality, we make a number of assumptions about $\mathcal{A}$. First, we assume that if $\mathcal{A}$ outputs $\{c_1, s_{ij}, 1 \le i \le s, 1 \le j \le l\}$ on m and L and computes the value $A_i = g_1^{s_{i1}} \cdots g_l^{s_{il}} pk_i^{c_i} \bmod p$, then (1) $\mathcal{A}$ at some point queried $H(m, L, A_k), 1 \le k \le s$ and (2) $\mathcal{A}$ never requested a signature on m. Second, for any leakage query $Leak(f_i)$ we assume $f_i(state)$ makes the same number of H-oracle calls regardless of the value of $state$ (this can always be ensured by adding dummy queries, as needed).

We construct a probabilistic polynomial-time algorithm $\mathcal{B}$ solving the second l-representation problem. Algorithm $\mathcal{B}$ proceeds as follows: Input $(S_G, q, g_1, g_2, \cdots, g_l, (x_1, x_2, \cdots, x_l))$, for $1 \le z \le n$, $\mathcal{B}$ designs $x_{z1} = x_1, x_{z2} = x_2, \cdots, x_{zl} = x_l$ and calculate $pk_z = \prod_{j=1}^{l} g_j^{x_{zj}} \bmod p$, then it chooses random $\{x_{ij}, 1 \le i \le n, 1 \le j \le l, i \ne z\}$ and computes $pk_i = \prod_{j=1}^{l} g_j^{x_{ij}} \bmod p, 1 \le i \le n$. It gives the

system parameters $(p, q, g_1, \cdots, g_l)$ and public keys $pk_i, 1 \leq i \leq n$ to $\mathcal{A}$. Thus, the challenger $\mathcal{B}$ can easily respond to the ring signature queries and leakage queries because he knows one of the secret keys.

When $\mathcal{A}$ terminates, $\mathcal{B}$ examines $\mathcal{A}$'s output $\{c_{1,1}, s_{ij,1}, 1 \leq i \leq s, 1 \leq j \leq l\}$ on the message m and the set L of ring members. If $\mathcal{A}$'s output can pass the signature verification, this forged signature is successful. According to the forking lemma of ring signature [26], the attacker $\mathcal{A}$ can also forge another ring signature $\{c'_{1,1}, s_{ij,1}, 1 \leq i \leq s, 1 \leq j \leq l\}$ on the same message m, the same set L of ring members and the same randomness. With non-negligible probability, the two forged ring signatures satisfy the following properties:

1. $c_{j,1} \neq c'_{j,1}$ for one $j \in \{1, 2, \cdots, s\}$;
2. $c_{i,1} = c'_{i,1}$ for all $i = 1, \cdots, s$ such that $i \neq j$;

Thus, due to the same randomness, we can get

$$\begin{array}{l} g_1^{s_{j1,1}} \cdots g_l^{s_{jl,1}} pk_i^{c_{j,1}} = g_1^{s'_{j1,1}} \cdots g_l^{s'_{jl,1}} pk_i^{c'_{j,1}} \bmod p \\ \prod_{i=1}^{l} g_i^{s_{ji,1}+c_{j,1}x'_{ji}} = \prod_{i=1}^{l} g_i^{s'_{ji,1}+c'_{j,1}x'_{ji}} \bmod p \\ \prod_{i=1}^{l} g_i^{(s_{ji,1}+c_{j,1}x'_{ji})-(s'_{ji,1}+c'_{j,1}x'_{ji})} = 1 \bmod p \end{array}$$

We denote $g_1 = g^{\alpha_1}, g_2 = g^{\alpha_2}, \cdots, g_l = g^{\alpha_l}$. Then, we can get

$$\sum_{i=1}^{l} \alpha_i[(s_{ji,1} + c_{j,1}x'_{ji}) - (s'_{ji,1} + c'_{j,1}x'_{ji})] = 0 \bmod q$$

After sl times to perform the above procedures, we can get sl equations

$$\sum_{i=1}^{l} \alpha_i[(s_{ji,w} + c_{j,w}x'_{ji}) - (s'_{ji,w} + c'_{j,w}x'_{ji})] = 0 \bmod q$$

where $1 \leq j \leq s, 1 \leq w \leq sl + 1$. Thus, there must exist at least one user, denoted as $j = u$, has the following l equations which correspond to l different w:

$$\sum_{i=1}^{l} \alpha_i[(s_{ui,w} + c_{u,w}x'_{ui}) - (s'_{ui,w} + c'_{u,w}x'_{ui})] = 0 \bmod q$$

We can compute all the corresponding discrete logarithms α_i if $(s_{ui,w}+c_{u,w}x'_{ui})-(s'_{ui,w} + c'_{u,w}x'_{ui}) \neq 0 \bmod q$ by calculating the above equation group. Based on the difficulty of discrete logarithm problem, we know that all the $l + 1$ equations satisfy the following $(s_{ui,w} + c_{u,w}x'_{ui}) - (s'_{ui,w} + c'_{u,w}x'_{ui}) = 0 \bmod q$. The probability of $u = z$ is $\frac{s}{n} \times \frac{1}{s} = \frac{1}{n}$. When $u = z$, it must hold that $s'_{zi,1} + c'_{z,1}x'_{zi} = s_{zi,1} + c_{z,1}x'_{zi} \bmod q$, *i.e.*, $x'_{zi} = \frac{s_{zi,1}-s'_{zi,1}}{c'_{z,1}-c_{z,1}} \bmod q$ for $1 \leq i \leq l$. At last, the challenger $\mathcal{B}$ gets another l-representation $(x_{z1}, x_{z2}, \cdots, x_{zl})$ of the value pk_z.

Next, we consider the success probability of $\mathcal{B}$ as follows.

Suppose that the adversary $\mathcal{A}$ can forge a valid ring signature with probability ϵ within time T. According to the forking lemma of ring signature [26], the adversary $\mathcal{A}$ can produce two valid ring signature such that $c_j \neq c'_j$, for some $j \in \{1, 2, \cdots, n\}$ and $c_i = c'_i$ for all $i = 1, \cdots, n$ such that $i \neq j$, in the expected time $T' \leq \frac{144823 V_{q_h,n}(T+q_s T_s)}{\epsilon}$. Then, we consider the probability that $\mathcal{B}$ can solve the second l-representation problem.

When $\mathcal{B}$ succeeds in obtaining two different forged ring signature, we need to evaluate the probability that the extracted l-representation $\overrightarrow{x}' = (x'_1, \cdots, x'_l)$ is equal to the original l-representation $\overrightarrow{x} = (x_1, \cdots, x_l)$.

Let $\lambda = (\frac{1}{2} - \frac{1}{2l} - \epsilon) \cdot l \cdot \log_2 q$, an upper bound on the number of leaked bits in each run of $\mathcal{A}$. The public key pk_j constrains $\overrightarrow{x}$ to lie in an $(l-1)$-dimensional vector space, and signature queries do not further constrain $\overrightarrow{x}$ [27]. Thus, the min-entropy of $\overrightarrow{x}$ conditioned on the public key and the observed signatures is $(l-1)\log_2 q$ bits. The views of $\mathcal{A}$ in its two runs contain only the following additional information about $\overrightarrow{x}$: at most $2 \cdot \lambda$ bits from the leakage functions (*i.e.*, λ bits in each view), and $\log_2 q_H$ bits indicating the relevant state associated with the first forgery. According to Lemmas 2 and 3, we can see that the conditional min-entropy of $\overrightarrow{x}$ is greater than 0 except with probability at most

$$2^{2\lambda + \log_2 q_H - (l-1)\log_2 q} \leq q_H q^{-2\epsilon l}.$$

From the above analysis, if the adversary $\mathcal{A}$ can forge a valid ring signature with probability ϵ within time T, then the second l-representation problem can be solved with probability $\frac{1}{2}(1 - \frac{q_H}{q^{2\epsilon l}}) \times \frac{1}{n} = \frac{1}{2n}(1 - \frac{q_H}{q^{2\epsilon l}})$ within time

$$T' \leq \frac{144823 V_{q_h,n}(T + q_s T_s)}{\epsilon}$$

under the condition that $\lambda = (\frac{1}{2} - \frac{1}{2l} - \epsilon) \cdot l \cdot \log_2 q$ bits of the secret key are leaked. Based on the difficulty of the second l-representation problem, our scheme is secure. □

Thus, based on Theorem 2 and Theorem 3, we know that our proposed ring signature scheme with bounded leakage resilience is provably secure.

6 Conclusions and future work

In this paper, we have proposed the first definition of ring signature resilient to bounded leakage and we have given a concrete instantiation of such ring signature. Based on the difficulty of the second l-representation problem, our proposed ring signature scheme with bounded leakage resilience is provably secure in the random oracle model. Our model does not cover attacks in which the attacker may obtain some information about the system's internal randomness state during the signing process. It seems interesting to explore as future work ring signature that can resist bounded leakage of the system's internal state. We plan to develop a more general leakage resiliency model for ring signature that takes internal state leaks into account.

Acknowledgement

This work was partly supported by the NSF of China through projects (No. 61272522, No. 61173154, No. 61370190, No. 61003214, No. 61170298), the Opening Project of Shanghai Key Laboratory of Integrate Administration Technologies for Information Security(No. AGK2013005), and by the Spanish Government through projects TIN2011-27076-C03-01 "CO-PRIVACY" and CONSOLIDER INGENIO 2010 CSD2007-00004 "ARES", by the Government of Catalonia under grant 2009 SGR 1135, by the European Commission under FP7 projects "DwB" and "Inter-Trust". The last author is partially supported as an ICREA-Acadèmia researcher by the Catalan Government; he leads the UNESCO Chair in Data Privacy, but this paper does not necessarily reflect the position of UNESCO nor does it commit that organization.

References

1. P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," *Crypto 1996*, LNCS 1109, pp.104-113, 1996.
2. P. C. Kocher, J. Jaffe, B. Jun, "Differential power analysis," *Crypto 1999*, LNCS 1666, pp. 388-397, 1999.
3. E. Biham, Y. Carmeli, A. Shamir, "Bug attacks", *Crypto 2008*, LNCS 5157, pp. 221-240, 2008.
4. D. Boneh, R. A. DeMillo, R. J. Lipton, "On the importance of checking cryptographic protocols for faults," *Eurocrypt 1997*, LNCS 1233, pp. 37-51, 1997.
5. D. Boneh, D. Brumley, "Remote timing attacks are practical," *Computer Networks*, 48(5):701-716, 2005.
6. S. Micali, L. Reyzin, "Physically observable cryptography," *TCC 2004*, LNCS 2951, pp. 278-296, 2004.
7. F.-X. Standaert, T. Malkin, M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," *Eurocrypt 2009*, LNCS 5479, pp. 443-461, 2009.
8. A. Akavia, S. Goldwasser, V. Vaikuntanathan, "Simultaneous hardcore bits and cryptography against memory attacks," *TCC 2009*, LNCS 5444, pp. 474-495, 2009.
9. M. Naor, G. Segev, "Public-key cryptosystems resilient to key leakage," *Crypto 2009*, LNCS 5677, pp. 18-35, 2009.
10. J. Katz, V. Vaikuntanathan, "Signature schemes with bounded leakage resilience," *Asiacrypt 2009*, LNCS 5912, pp. 703-720, 2009.
11. S. Faust, E. Kiltz, K. Pietrzak, G. N. Rothblum, "Leakage-resilient signatures," *TCC 2010*, LNCS 5978, pp. 343-360, 2010.
12. E. Boyle, G. Segev, D. Wichs, "Fully leakage-resilient signatures," *Eurocrypt 2011*, LNCS 6632, pp. 89-108, 2011.
13. T. Malkin, I. Teranishi, Y. Vahlis, M. Yung, "Signatures resilient to continual leakage on memory and computation," *TCC 2011*, LNCS 6597, pp. 89-106, 2011.
14. S. Faust, C. Hazay, J.-B. Nielsen, P.S. Nordholt, A. Zottarel, "Signature schemes secure against hard-to-invert leakage," http://eprint.iacr.org/2012/045.pdf
15. L.T. Phong, S. Matsuo, M. Yung, "Leakage resilient strong key-insulated signatures in public channel," *INTRUST 2010*, LNCS 6802, pp. 160-172, 2011
16. F. Guo, Y. Mu, W. Susilo, "Efficient online/offline signatures with computational leakage resilience in online phase," *Inscrypt 2010*, LNCS 6584, pp. 455-470, 2011.

17. J. Alwen, Y. Dodis, D. Wichs, "Leakage-resilient public-key cryptography in the bounded-retrieval model, *CRYPTO 2009*, LNCS 5677, pp. 36-54, 2009.
18. R.L. Rivest, A. Shamir, Y. Tauman, "How to leak a secret," *Asiacrypt 2001*, LNCS 2248, pp. 552-565.
19. J. Wang, B. Sun, "Ring signature schemes from lattice basis delegation," *ICICS 2011*, LNCS 7043, pp. 15-28, 2011.
20. J.K. Liu, T.H. Yuen, J. Zhou, "Forward secure ring signature without random oracles," *ICICS 2011*, LNCS 7043, pp. 1-14, 2011.
21. S. Zeng, S. Jiang, Z. Qin, "A new conditionally anonymous ring signature," *COCOON 2011*, LNCS 6842, pp. 479-491, 2011.
22. E. Fujisaki, "Sub-linear size traceable ring signature without random oracles," *CT-RSA 2011*, LNCS 6558, pp. 393-415, 2011.
23. Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing*, 38(1):97-139, 2008.
24. U. Feige, A. Shamir. "Witness indistinguishable and witness hiding protocols," *22nd ACM Symposium on Theory of Computing*, pp. 416-426, 1990.
25. C. P. Schnorr, "Efficient identification and signatures for smart cards", *CRYPTO'89*, pp.239-252
26. J. Herranz, G. Saez, "Forking lemmas for ring signature schemes," *Indocrypt 2003*, LNCS 2904, pp. 266-279, 2003.
27. T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes," *Crypto 1992*, LNCS 740, pp. 31-53, 1993.