Ring Signature Lecture Notes

Chi Yin Lee
The Hong Kong Polytechnic University
Department of Computing

June 20, 2019

Abstract

A ring signature scheme is a group signature scheme with no group manager to setup a group or revoke a signer. A linkable ring signature, introduced by Liu, et al. [20], additionally allows anyone to determine if two ring signatures are signed by the same group member (a.k.a. they are linked). Ring signature is a type of digital signature that can be performed by any member of a group of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people. One of the security properties of a ring signature is that it should be computationally infeasible to determine which of the group members' keys was used to produce the signature. Ring signatures are similar to group signatures but differ in two key ways: first, there is no way to revoke the anonymity of an individual signature, and second, any group of users can be used as a group without additional setup.

1 Proving the Knowledge of Several Discrete Logarithms

In this section, we describe some three-move interactive HVZK PoK protocols that we will use as basic building blocks for our event-oriented linkable threshold ring signature scheme. These protocols all work in finite cyclic groups of quadratic residues modulo safe prime products. For each $i = 1, ..., n$, let Ni be a safe-prime product and define the group $Gi \doteq QR(Ni)$ such that its order is of length $\ell_i - 2$ for some $\ell_i \in \mathbb{N}$. Also let g_i, h_i be generators of G_i such that their relative discrete logarithms are not known.

Let $1 < \epsilon \in \mathbb{R}$ be a parameter and let $\mathcal{H} : 0, 1^* \to \mathbb{Z}_q$ be a strong collision resistant hash function, where q is a k-bit prime for some security parameter $k \in \mathbb{N}$. Define $\mathcal{N} \doteq \{1, ..., n\}$ and $\Gamma_i \doteq \{-2^{\ell_i}q, ..., (2^{\ell_i}q)^{\epsilon}\}$.

This protocol is a straightforward generalization of the protocol for proving the knowledge of a discrete logarithm over groups of unknown order in [7]. This allows a prover to prove to a verifier the knowledge of n discrete logarithms $x_1, ..., x_n \in \mathcal{Z}$ of elements $y_1, ..., y_n$ respectively and to the base $g_1, ..., g_n$ respectively. Using the notation in [9], the protocol is denoted by:

$$PK\{(\alpha_1, ..., \alpha_n) : \bigwedge_{i=1}^{n} y_i = g_i^{\alpha_i}\}. \tag{1}$$

2 Classical Ring Signature

We review the existing constructions of (linkable) ring signatures. The generic construction introduced by Rivest, Shamir and Tauman [49] in 2001 (RST). This generic construction is

based on one-way trapdoor permutations along with a block cipher. It can be instantiated from the RSA assumption. In 2004, Abe, Ohkubo and Suzuku [1] (AOS) proposed a new generic construction which allows discrete-log type of keys. This generic construction can make use of hash-and-sign signature or any three-move sigma-protocol-based signature. It can be instantiated from RSA or discrete-log assumptions. Both of the RST and AOS constructions are secure in the random oracle model and the signature sizes are linear to the ring size. To achieve the security in standard model, Bender, Katz and Morselli [12] (BKM) presented a ring signature scheme which adopts a public-key encryption scheme, a signature scheme and a ZAP protocol for any language in N P [25]. Even though BKM construction is secure in standard model, the signature size is still linear in the number of group members and the generic ZAPs are actually quite impractical. Shacham and Waters [?] then proposed a more efficient linear-size ring signature scheme without random oracle from bilinear pairing.

To reduce the signature size, Dodis et al. proposed the first ring signature scheme with constant signature size in 2004 [20]. It relies on accumulator with one-way domain and is secure in the random oracle model. The first ring signature with sub-linear without random oracle model is due to Chandran, Groth and Sahai [17]. This scheme has signature size $O(\sqrt{\ell})$ where ℓ is the number of users in the ring. All of the above sub-linear size constructions are secure in the common reference string model that requires a trusted setup. The first sub-linear ring signatures without relying on a trusted setup is due to Groth and Kohlweiss [30]. It features logarithmic size signature and is secure in the random oracle model.

As noted before, the protocol can be turned into a signature scheme by replacing the challenge by the hash of the commitment together with the message M to be signed: $c \leftarrow \mathcal{H}((g_1, y_1)||...||(g_n, y_n)||t_1||...||t_n||M)$ where $t_n = g^{s_{n-1}} * y_{n-1}^{(}c_{n-1})$. In this case, the signature is $(c, s_1, ..., s_n)$ and the verification becomes:

$$c \stackrel{?}{=} \mathcal{H}((g_1, y_1)||...||(g_n, y_n)||t_1||...||t_n||M) \tag{2}$$

Following [9], we denote this signature scheme by:

$$SPK\{(\alpha_1, ..., \alpha_n) : \bigwedge_{i=1}^{n} y_i = g_i^{\alpha_i}\}(M). \tag{3}$$

With above description, a classic ring signature scheme formed.
With below setup:

- Finite Field: $\mathbb{N}$
- KeyPair : $\{x_i, y_i\}, y_i = g^{x_i}$
- Group : $L = \{y_0, ..., y_n\}$
- Position: the signer position in Group L, $p \in L$
- Message: m
- Ring Size: n
- Hash Function: $\mathcal{H}(...)$

Algorithm 1: Classic Ring Signature - Sign

Input: $\{L, p, m, x_p, g, \mathbb{N}\}$
Output: $\{C, s_0, ..., s_n\}$

$u \leftarrow \{0,1\}^{\mathbb{N}}$
$T_p \leftarrow g^u$
$c_p \leftarrow \mathcal{H}(L||m||T_p)$
for $i \leftarrow p+2$ ***to*** $p \bmod n$ **do**
  $s_{i-1} = \{0,1\}^{\mathbb{N}}$
  $T_i = g^{s_{i-1}}.y_{i-1}^{c_{i-1}}$
  $c_i = \mathcal{H}(L||m||T_i)$
$s_p \leftarrow u - c_p x_p$
$C \leftarrow c_0$
return $\{C, s_0, ..., s_n\}$

Algorithm 2: Classic Ring Signature - Verify

Input: $\{L, m, C, s0, ..., sn, g, \mathbb{N}\}$
Output: $true$ or $false$

for $i \leftarrow 0$ ***to*** n **do**
  $T_i = g^{s_i}.y_i^{c_i}$
  $c_i = \mathcal{H}(L||m||T_i)$
return $c_n \stackrel{?}{=} C$

2.1 Explanation

$$\because y_i = g^{x_i}$$
$$\therefore T_p = g^{u-c_p x_p}.y_p^{c_p} = g^{u-c_p x_p}.g^{x_p.c_p} = g^u$$
$$\therefore c_p = \mathcal{H}(L||m||g^u)$$

Thus, the verifier will recover the origin random number : g^u.

3 Linkable Ring Signature

Since the first proposal of linkable ring signature [39], we have seen a sequence of work [55, 7, 38, 52] that provides different features. In 2005, Tsang and Wei [55] extends the genric ring siganture introduced by Dodis et al. [20] to a linkable version, which also feature constant signature size and is secure in the random oracle model. Au et al. [7] presented a new security model for linkable ring signatures and a new short linkable ring signature scheme that is secure in this strengthened model. In 2014, Liu et al. [38] presented the first linkable ring signature scheme achieving unconditional anonymity. Sun et al. [52] proposed a new generic linkable ring signature to construct RingCT 2.0 for Monero. There are also schemes with special properties such as identity-based linkable ring signatures [54, 9] and certificate-based linkable ring signatures [8].

$$SPK\{(\alpha_1, ..., \alpha_n) : \bigwedge_{i=1}^{n} y_i = g_i^{\alpha_i} \wedge v_i = h_i^{\alpha_i}\}(M). \tag{4}$$

Given the same setup from Classic Ring Signature , h is a pre-defined variable by the Group.

Algorithm 3: Linkable Ring Signature - Sign

Input: $\{L, p, m, x_p, g, h, \mathbb{N}\}$
Output: $\{C, Y, s_0, ..., s_n\}$

$Y \leftarrow h^{x_p}$
$u \leftarrow \{0,1\}^{\mathbb{N}}$
$T_p \leftarrow g^u$
$t_p \leftarrow h^u$
$c_p \leftarrow \mathcal{H}(L||m||T_p||t_p)$
for $i \leftarrow p+2$ ***to*** $p \bmod n$ **do**
  $s_{i-1} = \{0,1\}^{\mathbb{N}}$
  $T_i = g^{s_{i-1}}.y_{i-1}^{c_{i-1}}$
  $t_i = h^{s_{i-1}}.Y^{c_{i-1}}$
  $c_i = \mathcal{H}(L||m||T_i||t_i)$
$s_p \leftarrow u - c_p x_p$
$C \leftarrow c_0$
return $\{C, Y, s_0, ..., s_n\}$

Algorithm 4: Linkable Ring Signature - Verify

Input: $\{L, m, C, Y, s0, ..., sn, g, h, \mathbb{N}\}$
Output: $true$ or $false$

for $i \leftarrow 0$ ***to*** n **do**
  $T_i = g^{s_i}.y_i^{c_i}$
  $t_i = h^{s_i}.Y^{c_i}$
  $c_i = \mathcal{H}(L||m||T_i||t_i)$
return $c_n \stackrel{?}{=} C$

3.1 Ring Explanation

$$\because y_i = g^{x_i}$$
$$\therefore T_p = g^{u-c_p x_p}.y_p^{c_p} = g^{u-c_p x_p}.g^{x_p.c_p} = g^u$$
$$\therefore c_p = \mathcal{H}(L||m||g^u)$$

Thus, the verifier will recover the origin random number : g^u.

3.2 Linkable Signer Explanation

$$\because Y = h_p^x$$
$$\therefore t_p = h^{s_p}.Y_p^c = h^{u-c_p x_p}.h^{x_p c_p} = h^u$$
$$\therefore c_p = \mathcal{H}(L||m||g^u||h^u)$$

Thus, the verifier will recover the origin random number : h^u ; For every signature with the same h, Y will be the same as $Y = h_p^x$. Signatures can be linked by checking $\Delta Y \stackrel{?}{=} Y$.

4 Threshold Linkable Ring Signature

Threshold cryptography allows n parties to share the ability to perform a cryptographic operation (e.g., creating a digital signature(. Any d parties can perform the operation jointly, whereas it is infeasible for at most $d-1$ to do so. In a (d, n)-threshold ring signature scheme, the generation of a ring signature for a group of n members requires the involvement of at least d members / signers, and yet the signature reveals nothing about the identities of the signers.

Please notice signers will know each others identity when signing the threshold linkable ring signature. To sign for an event without any acknowledge for any other signers. In this case, we should reduce the problem to use the same pre-defined generate h and create multiple Linkable Ring Signature to the verifier, the verifier can later check any linkability between signatures to count unique signature.

We can denote this signature scheme by:

$$SPK\left\{(\alpha_1, ..., \alpha_n) : \bigvee_{I \subseteq \mathbb{N}, |I|=d} \left(\bigwedge_{i \in I} y_i = g_i^{\alpha_i} \wedge v_i = h_i^{\alpha_i}\right)\right\}(M). \tag{5}$$