Identity Based Ring Signature

Why, How, and What Next

Sherman S.M. Chow   Richard W.C. Lui
Lucas C.K. Hui   S.M. Yiu

The University of Hong Kong

Outline

- Introduction
- PKI vs ID-based Ring Signatures
- Technical Preliminaries
- Classifying the Schemes
- Summary and Some Possible Directions

Motivations

One of the government officials wants to leak a secret to the public, however he wants to remain anonymous. On the other hand, he wants the public to be convinced that the secret is actually leaked from one of the many officers and is thus reliable.

So, we want a signature scheme to have the properties of correctness, unforgeabilitiy, and anonymous.

A Similar Notation: Group Signature

A group signature

- One or more group member(s) sign(s) on behalf of the whole group such that the verifier knows someone inside the group signed the signature, but cannot identify who is (are) the real signer(s).
- A predefined group and a group manager (thus requires a set up procedure etc.).
- An mechanism to reveal the actual signer (by the group manager).

=> Ring Signature

Ring Signature

- Spontaneity: The signer can use any ad-hoc group of n users (the members of the group may even not be aware that they have been used) to produce such a signature (thus is setup free).
- Signer-ambiguous: The verifier is unable to determine the identity of the real signer (usually unconditional anonymity, can't even link additional signatures to the same signer).
- Correntness & Unforgeability

- In 2001, Rivest, Shamir and Tauman formalized this notion, with solutions based on the trapdoor one-way permutations.
- In their paper, they provided two constructions of ring signatures (one based on RSA, the other based on Rabin's Signature Scheme).
- Afterwards, there are many PKI-based ring signature schemes being proposed:
  - Cramer, Damgård and Schoenmakers [CDS94]
  - Abe, Ohkubo and Suzeki [AST02]
  - Gao, Yao and Li [GYL03]
  - ……

Identity-based Ring Signature

- Arguments favour ID-based schemes
- Classification of existing ID-based ring signature schemes based on how they generate the ring signature.
- Possible future directions

Certificate and Public Key Infrastructure

In public key cryptosystems that are based on public key infrastructure (PKI),

- The public key of a user is a “random” string that is unrelated to the identity of the user.
- To get the public key of another user, a user must obtain an authorized certificate that binds the public key with that user.

Identity Based Cryptography

- A user's public key can be any binary string (e.g. email address) that can identify the user.
- A Private Key Generator (PKG) generates private key for the user on request, thus PKG knows all private keys (key escrow problem).
- This notion was introduced in 1984, with a concrete signature scheme.
- In 2001, The first practical ID-based encryption scheme using pairings appeared [Boneh and Franklin].

Some Questions

- Are ID-based ring signature schemes really ring signatures (no group manager, no *group* setup procedure, no coordination)?
  - Some people think that it is not. PKG has to be completely trustworthy due to the inherent key escrow, so
    - PKG is the group manager?!
    - Will PKG know who is the signer?
- Any advantages of using ID-based?

c.f. CA in PKI

- A certificate authority (CA) is assumed.
  - The involvement of the CA and the PKG is only for setting up the parameters for the whole system but not for the setting up of the signer's group.
  - In PKI, a signer needs to get all public keys (maybe from CA) before it can sign a ring signature while it is not necessary for ID-based schemes.

- Certificate Verification
  - Any verifier of the signature must obtain a copy of each involved user's certificate and check the validity of the certificate before checking the validity of the signature.
  - The signer has to do the same verification before producing the signature.
  - On the other hand, ID-based schemes do not need this verification.

- Spontaneity
  - PKI-based
    - The certificate is the "identity card", but not everyone has such a certificate.
  - ID-based
    - One just needs to know the identity of another party.
    - It is *common* for everyone to have their digital identity (e.g. email address).
- PKG is not able to tell who is the signer

Bilinear Pairings

- Let G_1 and G_2 be a cyclic additive and multiplicative group of prime order q respectively, P be a generator of G_1.
- e: $G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing if
  - Bilinearity: For all P, Q, R in G_1

    $e(P + Q, R) = e(P, R)\, e(Q, R)$

    $e(P, Q + R) = e(P, Q)\, e(P, R)$

    $e(aP, bR) = e(P, bR)a = e(P, R)ab = e(bP, aR)$

Framework of ID-based Ring Signature

- Setup
  - Output public parameter (*params*) and master secret (s)
- KeyGen(ID, s, *params*)
  - Output the private key S_{ID} of the user
- Setup and KeyGen are executed by PKG for any ID-based schemes.
- Sign(ID_1, ID_2, … ID_n, S_{ID^*}, m , *params*)
  - Executed by one who wants to produce a ring signature (to be explained more)
  - Output the signature σ
- Verify(ID_1, ID_2, … ID_n, σ, m, *params*)
  - Executed by the verifier

Notations

- H_1: $\{0, 1\}^* \rightarrow G_1$
  - For hashing the identity string
- H_2: $\{0, 1\}^* \rightarrow Z_q$
  - For the message to be signed (and other auxiliary information)
- n: number of users in the “ring”
- $L = \{ID_1, ID_2, \ldots, ID_n\}$: the identities of n users
- k: the index of the actual signer in L
- m: message to be signed

Identity-based Key Generation

- Setup
  - Select s from Zq^* and a generator P from G_1. The system's public key is $P_{Pub} = sP$ and the master key is s.
- KeyGen(ID)
  - Public key Q_{ID} is $H_1(ID)$.
  - Private key S_{ID} is sQ_{ID}.
- Common for all ID-based schemes.

Ring Signature Generation - A High Level Overview

- Initialization
- Generating the (ring) sequence for other members
  - introducing randomness (source of anonymity)
- Closing the ring
  - can only be done by the private key of the signer
  - provides the property for verification
- Output the signature (the sequence and the starting point)

Existing ID-based Ring Signature Schemes

w.r.t. how to generate the ring sequences

- Ring Structure
  - Zhang and Kim's [AsiaCrypt 02]
  - Lin and Wu's [ePrint 03 / AINA 04]
  - Awasthi and Lai [ePrint 05]
- Parallel Structure
  - Herranz and Sáez [ICICS 04]
  - Chow *et al.* [ACNS 05]

Abe *et al.*'s Ring Signature

- We consider the discrete logarithm based scheme for easy understanding.
- Public-Private key pair: ($y = g^x \bmod p$, x)
  - p is a prime
  - Z_p^* is a group of prime order q
  - g is the generator of Z_p^*
- H: $\{0, 1\}^* \rightarrow Z_q$

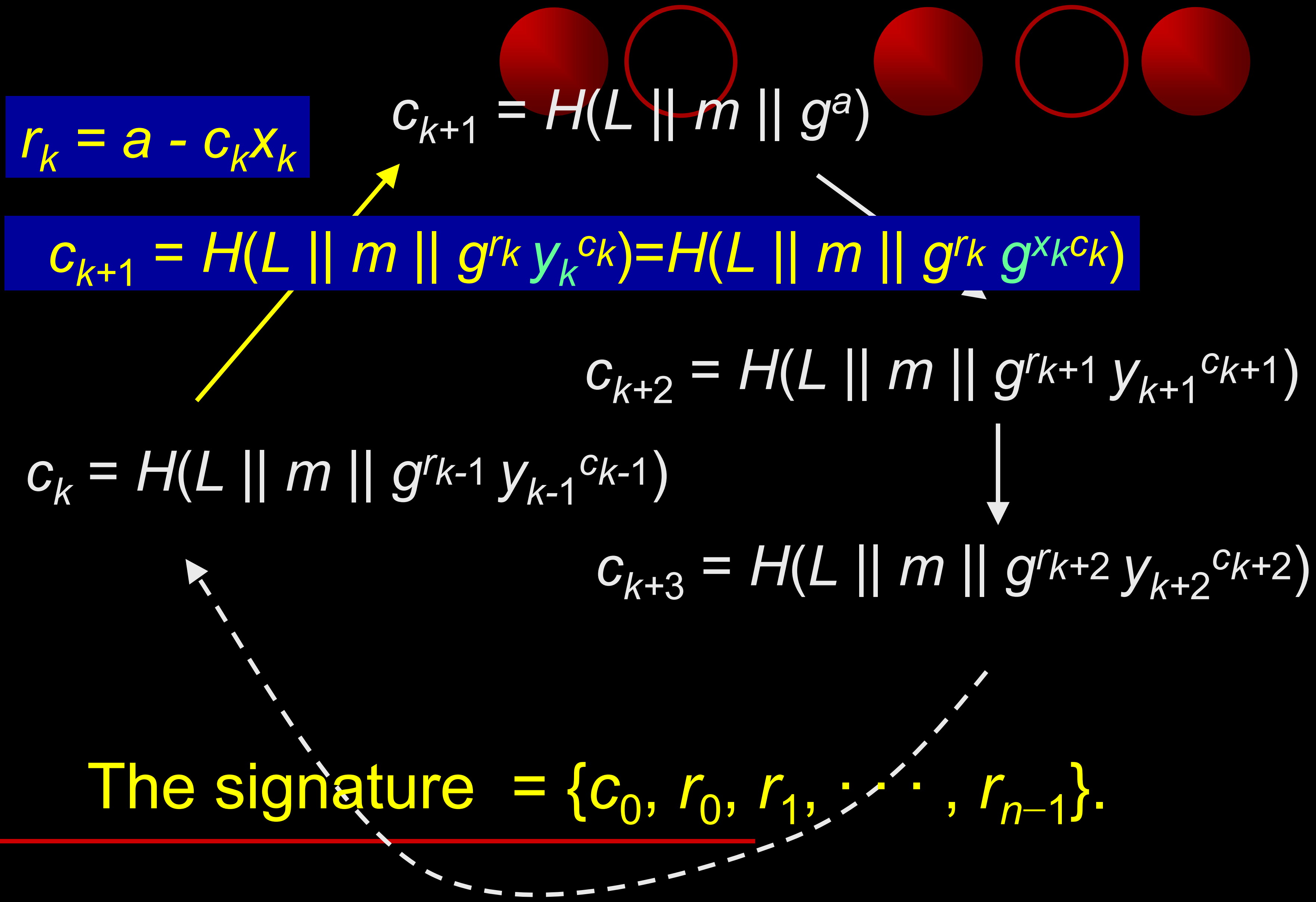
Abe *et al.*'s Signing

- Choose a random element a from Zq
- Compute $c_{k+1} = H(L \,||\, m \,||\, g^a)$
- For $i = k + 1, \cdots, n - 1, 0, \cdots, k - 1$
  - Choose a random r_i from Zq.
  - Compute $c_{i+1} = H(L \,||\, m \,||\, g^{r_i} y_i^{c_j} \bmod p)$
- Compute $r_k = a - c_k x_k \bmod q$
  - Equivalent to solving $g^a = g^{r_k} y_k^{c_k} \bmod p$ for r_k.
  - $c_{k+1} = H(L \,||\, m \,||\, g^{r_k} y_k^{c_k} \bmod p) = H(L \,||\, m \,||\, g^a)$.

Initialization

Ring Sequence Generation

Closing the Ring



$r_k = a - c_k x_k$

$c_{k+1} = H(L \,||\, m \,||\, g^{a})$

$c_{k+1} = H(L \,||\, m \,||\, g^{r_k}\, y_k^{c_k}) = H(L \,||\, m \,||\, g^{r_k}\, g^{x_k c_k})$

$c_{k+2} = H(L \,||\, m \,||\, g^{r_{k+1}}\, y_{k+1}^{c_{k+1}})$

$c_k = H(L \,||\, m \,||\, g^{r_{k-1}}\, y_{k-1}^{c_{k-1}})$

$c_{k+3} = H(L \,||\, m \,||\, g^{r_{k+2}}\, y_{k+2}^{c_{k+2}})$

The signature $= \{c_0, r_0, r_1, \cdots, r_{n-1}\}$.

Abe *et al.*'s Verification

- For $i = 0, 1, \cdots, n - 1$,
  - compute $c_{i+1} = H(L \,||\, m \,||\, g^{r_i} y_i^{c_j} \bmod p)$.
- Accept if $c_n = c_0$, reject otherwise.

Zhang and Kim ’s Ring Signature

- Randomly choose an element A from G_1
- $c_{k+1} = H_2(L \,||\, m \,||\, e(A, P))$
- For $i = k + 1, \cdot\cdot\cdot, n - 1, 0, \cdot\cdot\cdot, k - 1$
  - Randomly choose R_i from G_1
  - $c_{i+1} = H_2(L \,||\, m \,||\, e(R_i, P)e(c_i H_1(ID_i), P_{pub}))$
- Compute $R_k = A - c_k S_{ID_k} \bmod q$
  - i.e. $e(A, P) = e(R_k, P)e(c_k H_1(ID_k), P_{pub})$
- The signature $= \{c_0, R_0, R_1, \cdot\cdot\cdot, R_{n-1}\}$.

Initialization

Ring Sequence Generation

Closing the Ring

Output the Signature

- To verify, for $i = 0, 1, \cdots, n - 1$,
  - compute $R_i = H_2(L \,||\, m \,||\, e(R_i, P)e(c_i H_1(ID_i), P_{pub}))$.
- Accept if $R_n = R_0$, reject otherwise.

- In “Ring Structure” based schemes, the challenge term c_i is used as input to generate the next challenge term c_{i+1}.
- On the other hand, in “Parallel Structure” based schemes, these challenge terms are generated independently.

Chow et al.'s Ring Signature

- For all i in $\{1, 2, \ldots, k - 1, k + 1, \ldots, n\}$
  - $c_i = H_2(m \,||\, L \,||\, U_i)$, $U_i \in_R G_1$
- Randomly choose r'_k from Z_q
- $U_k = r'_k Q_{IDk} - \sum_{(i \neq k)} \{U_i + c_i Q_{IDi}\}$.
- $c_k = H_2(m \,||\, L \,||\, U_k)$.
- $\sigma = \{U_1, U_2, \cdots, U_n, V = (c_k + r'_k) S_{IDk}\}$.
- Note: U_k is calculated to cancel all the othe terms.

Sign

- Accept if $e(P, V) = e(P_{pub}, \sum(U_i + c_i Q_{IDi}))$

Verify

Possible Directions for ID-based Ring Signatures

- Other properties and extensions
  - Linkability
    - Two ring signatures signed by the same private key can be linked publicly and efficiently.
    - Application: journalists may only believe the secret if more than one source leaks it.
    - It seems not trivial how the techniques of adding linkability to PKI-based schemes can be applied to ID-based schemes.
  - Separability
    - To allow a ring signature to involve parties using different favors of private keys.

- Threshold ring signature
  - Any group of t entities spontaneously conscript arbitrarily n – t entities to produce a publicly verifiable t-out-of-n signature, yet the actual signers remain anonymous.
- Blind ring signature
  - Do not know which message is being signed
  - Cannot link the signing process with the signature.
- Ring Authenticated Encryption
  - Only the designated recipient can recover the message and verify the signature..

- Identify real and interesting applications for ID-based or PKI-based ring signatures.

‹ Thank you ›