Lightweight Anonymous Authentication for Ad Hoc Group: A Ring Signature Approach

Xu Yang[1], Wei Wu[1], Joseph K. Liu[2], and Xiaofeng Chen[3]

[1]Fujian Normal University, China
[2]Monash University, Australia
[3]Xidian University, China

ProvSec 2015

November 25, 2015

Fujian Normal University

Outline

Fujian Normal University

Outline

Fujian Normal University

Privacy Protection

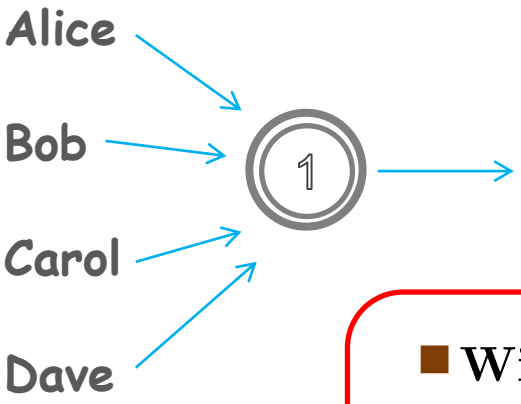
Privacy is an important factor in many areas.

For example, no one wants his own daily behaviors, like location information or web browsing history, to be known by others.

There exists various kinds of anonymization technologies that can help one become ***'anonymous'*** and protect user privacy.

Ring signature

Ring signature is a good candidate to provide anonymous authentication, especially to ad hoc group.



Romulus: "from Alice, Bob, Carol or Dave?"

- **Without revealing their identities.**
- **It is not possible to decide whether two signatures have been issued by the same group member.**

Our Contributions

There are two main contributions:

- **Lightweight.** Our scheme does not require the signer or the verifier to execute any exponentiation or pairing. Only hashing, modulus square or addition operations are needed in both signature and verify stages.
- **Improved.** Our scheme can be regard as a further improvement of on-line/offline signature scheme in two ways: (1) We do not require any offline stage in the signing part; and (2) The verification is lightweight.

Outline

Fujian Normal University

Signer Ambiguity

Definition (Signer Ambiguity) Let $L = \{pk_1, \cdots, pk_n\}$ be the list of public keys and $L_{sk} = \{sk_1, \cdots, sk_n\}$ be the corresponding secret keys. Each key is generated by Key-Gen. A ring signature scheme is said to be unconditionally signer ambiguous if, for any L, any message m, and any signature $\sigma \leftarrow \mathsf{Sign}(L, m, sk_\pi)$ where $sk_\pi \in L_{sk}$, any unbound adversary A accepts as inputs L, m and σ, outputs π with probability $1/n$.

It means that even all the private keys are known, it remains uncertain that who, out of n possible signers, actually produced the ring signature.

Existential Unforgeability I

Definition (Existential Unforgeability). For a ring signature scheme with n public keys, the existential unforgeability is defined as the following game between a challenger and an adversary A:

1. The challenger runs algorithm Key-Gen. Let $L = \{pk_1, \cdots, pk_n\}$ be the set of n public keys and $L_{sk} = \{sk_1, \cdots, sk_n\}$ be the corresponding secret keys. A is given L.

2. A can adaptively queries the signing oracle q_S times: On input any message m and L' where $L' \subseteq L$ (the corresponding secret keys are denoted by ${L'}_{sk}$), the challenger returns a ring signature $\sigma \leftarrow \mathsf{Sign}(L', m, sk_\pi)$, where $sk_\pi \in {L'}_{sk}$ and $\mathsf{Verify}(L', m, \sigma) = \mathsf{Accept}$.

3. Finally A outputs a tuple (L^*, m^*, σ^*).

Existential Unforgeability II

A wins the game if:

1. $L^* \subseteq L$,
2. (L^*, m^*) has not been submitted to the signing oracle, and
3. $\mathsf{Verify}(L^*, m^*, \sigma^*) = \mathsf{Accept}$

We define A's advantage in this game to be $Adv(A) = \Pr[A \text{ wins }]$.

Outline

Fujian Normal University

Definition

A ring signature scheme consists of three algorithms:

- $\mathsf{Key\text{-}Gen}(k) \rightarrow (sk, pk)$: $\mathsf{Key\text{-}Gen}$ is a probabilistic algorithm taking as input a security parameter k. It returns the user secret key sk and public key pk.
- $\mathsf{Sign}(L, sk, m) \rightarrow \sigma$: Sign is a probabilistic algorithm taking (L, m, sk) as input, where L is the list of n public keys to be included in the ring signature, sk is the secret key of the actual signer (such that the corresponding public key is included in L) and m is the message to be signed. It returns a signature σ.
- $\mathsf{Verify}(L, m, \sigma) \rightarrow \{\mathsf{Accept}, \mathsf{Reject}\}$. Verify is a deterministic algorithm taking (L, m, σ) as input, where L is the list of n public keys of the ring members and $m, \sigma)$ is the message/ring-signature pair. It outputs either Accept or Reject.

Proposed Scheme I

Key-Gen: Let κ be security parameters. Each user selects two safe primes p, q of length k-bit, such that $p = 2p' + 1, q = 2q' + 1$ where p', q' are also primes. The private key is (p, q) and public key is $N = pq$.

Sign: Let $L = \{N_1, \ldots, N_n\}$ be a list of n public keys to be included in the ring signature. Let $H_i : \{0,1\}^* \rightarrow Z_{N_i}$ be some hash functions for $i = 1, \ldots, n$. H_i is a random oracle. W.l.o.g., we assume user n is the actual signer. The actual signer executes the following steps:

1. Randomly generate $r_n \in_R Z_{N_n}$, compute $c_1 = H_1(L, m, r_n)$.
2. (For $n > 1$ only) For $i = 1, \ldots, n-1$, randomly generate $x_i \in_R Z_{N_i}$ and compute $c_{i+1} = H_{i+1}(L, m, c_i + x_i^2 \bmod N_i)$.

Proposed Scheme II

3. Compute $t_n = r_n - c_n \bmod N_n$. If $t_n \notin QR(N)$, repeat the following steps until $t_n \in QR(N)$.
   - (For $n > 1$) choose another random $x_{n-1} \in_R Z_{N_{n-1}}$ and compute $c_n = H_n(L, m, c_{n-1} + x_{n-1}^2 \bmod N_{n-1})$.
   - (For $n = 1$) choose another random $r_1 \in_R Z_{N_1}$ and compute $c_1 = H_1(L, m, r_1)$.
4. Compute $x_n = {t_n}^{1/2} \bmod N_n$ using the knowledge of the factorization of N_n.

Output the signature $\sigma = (x_1, \ldots, x_n, c_1)$.

Verify: To verify a signature $\sigma = (x_1, \ldots, x_n, c_1)$ for message m and public keys $L = \{N_1, \ldots, N_n\}$, computes $r_i = c_i + x_i^2 \bmod N_i$ for $i = 1, \ldots, n$ and $c_{i+1} = H_{i+1}(L, m, r_i)$ for $i \neq n$. The Verify algorithm accepts the signature if $c_1 = H_1(L, m, r_n)$. Otherwise, it rejects.

Fujian Normal University

Outline

Fujian Normal University

Complexity Assumption I

Definition (Safe Prime). p is a safe prime if it is of the form $2p' + 1$, where p' is also a prime.

Definition (Quadratic Residues). An integer $y \in Z_N^*$ is called a quadratic residue modulo N if there exists an integer $x \in Z_N^*$ such that: $x^2 = y \pmod{N}$. Let $QR(N)$ denote the set of quadratic residues modulo N.

Complexity Assumption II

Definition (Factorization Assumption with Safe Prime). Let $N = pq$ where p and q are k-bit length safe primes. Given N as the input, the goal of an algorithm of A is to output p and q. A has at least an advantage of ϵ if

$$\Pr[A(N) = p, q \mid N = pq] \geq \epsilon.$$

We say that the (ϵ, τ, k)-Factorization assumption holds if no algorithm running in time at most τ can solve the factorization problem with advantage at least ϵ, where the modulus is a product of two safe primes and each is with k-bit length.

Signer Ambiguous

Theorem. Our ring signature scheme is unconditionally signer ambiguous.

Proof. All x_i except x_n are taken randomly from Z_{N_i}. At the closing point, $x_n \in Z_{N_n}$ also distributes randomly as r_n is randomly chosen, c_n depends on previous x_{n-1} which is also a random number. The remaining c_1 is uniquely determined from L, m and r_n.

Existential Unforgeability

Theorem. This scheme is existentially unforgeable under adaptive chosen message attacks in the random oracle model, under the (ϵ', τ', k)-Factorization assumption.

Proof. Through combining all the assumption and cases, we can figure out the overall successful probability of adversary B is at least

$$\frac{\left(1-\frac{q_h q_s}{N_{min}}\right)\left(1-\frac{1}{N_{min}}\right)\epsilon}{q_h(q_h+1)n}$$

This contradicts the assumption that the (ϵ', τ', k)-Factorization assumption holds where

$$\epsilon' \leq \frac{\left(1-\frac{q_h q_s}{N_{min}}\right)\left(1-\frac{1}{N_{min}}\right)\epsilon}{q_h(q_h+1)n}, \qquad \tau' = \tau$$

Fujian Normal University

Outline

Fujian Normal University

Efficiency Analysis

Time Complexities of Existing Ring Signatures

Scheme	# of EXP (sign)	# of EXP (verify)	# of PAIR (verify)
Rivest-Shamir-Tauman [38]	n	n	0
Abe-Ohkubo-Suzuki [1]	n	n	0
Dodis-Kiayias-Nicolosi-Shoup [18]	14	14	0
Chow-Wei-Liu-Yuen [13]	n	n	0
Shacham-Waters [39]	$4n+3$	0	$2n+3$
Chandran-Groth-Sahai [11]	$5+6\sqrt{n}+\frac{n+1}{3}$	3	$6+6\sqrt{n}$
Liu-Au-Susilo-Zhou [23]	2	n	0
Our Scheme	0	0	0

Fujian Normal University

Outline

Fujian Normal University

Conclusion

We proposed a lightweight anonymous authentication protocol, the essential of which is actually a lightweight ring signature scheme.

- Lightweight in both prover and verifier sides without contain any exponentiation or pairing.
- Only requires a few hashing and modulus square operations.
- We believe it is particular suitable for lightweight devices.

In the future, we will incorporate the technique from lattices to further improve the efficiency.

Fujian Normal University

Thank you.

Fujian Normal University