Confessible Threshold Ring Signatures

Yu-Shian Chen

DCNSLab@NTUEE
Outline

- Introduction
- Generic threshold ring signatures
- Proposed schemes
- Recent results
- Conclusions
Introduction

- Two threshold ring signature schemes with new properties.
  - I: Confessibility
  - II: Threshold Confessibility
- Built on generic threshold ring signature schemes and can be easily adapted to most existing ring signature schemes
Generic Threshold Ring Signatures (1/2)

- Ring Signature
  - Anonymity of the *actual* signer.

- To produce a *(t,n)* threshold ring signature on a message $M$, the *actual signers* declares an arbitrary set of *innocent signers* to form a group of *possible signers* including themselves while the innocent signers may be completely unaware.
Any recipient can only verify that at least the threshold number \((t)\) of members in the group had generated the signature but not ascertain who they are.

Without loss of generality, assume \(\{U_1 .. U_t\}\) are the actual signers, \(\{U_{t+1} .. U_n\}\) are the innocent signers.
Generic Threshold Ring Signatures

\[ G_i \text{ is the 1-way trapdoor function of } U_i; \quad G_i^{t+1} \text{ can be only computed by } U_i; \quad H_j \text{ are publicly known hash functions.} \]
The ring signature $G_{t+1}$ satisfies a $(n-t)$-degree polynomial $f()$?
Consider such a situation….

- Alice, Bob, and Charles plan to leak a juicy fact to Philip about an embezzlement.

- To hide their identities, they pick up 5 other innocent employees, generate a (3, 8) threshold ring signature.
Then...

- After verifying the fact of the embezzlement, Philip would like to offer a premium to the informers.
  - Can Alice confess and claim the premium while the other two tended to be kept hidden?
  - Can Alice, Bob, or Charles also confess jointly in a threshold fashion?
    - Ex: only these combination (A,B), (B,C), (C,A), or (A,B,C) are able to confess.
New Security Notions

- Confessibility
  - The actual signers can confess their involvement in the signature.

- Threshold Confessibility
  - The actual signers can confess in a “threshold” structure inside the signing threshold structure.
Confess What?

- Basically, due to the anonymity of ring signatures, the actual signers have to hold some secret information, which we call “voucher”, to prove that they are not innocent signers.
Voucher

- While confessing, the actual signer is aiming to uncover its secret "voucher".
- Each voucher is coupled with a predefined and publicly known value $r_k$.
  - Ex: $r_1=111$, $r_2=222$, $r_3=333$.
  - Ex: $r_k = H(k,\{U_1..U_n\})$.
  - Not collide with the signer identities.
Scenario I: (Individual) Confessibility

- Satisfy “Confessibility”
  - The actual signers can confess their involvement in the signature individually.
- Each actual signer generates individual voucher and extends the polynomial with one more degree.
Scenario I: (Individual) Confessibility

Confessibility

\( r_k \) is a pre-defined (publicly known) value.

\[
\begin{align*}
U_1 & \quad \cdots \quad U_t \quad U_{t+1} \quad \cdots \quad U_n \\
\end{align*}
\]

Construct a \( n \)-degree polynomial \( f() \)

Secret vouchers

The ring signature
To Confess

- To confess, signer $A$ opens its secret voucher $\alpha_A$ to the verifier $V$, then $V$ can derive \("V_{(A)}"\).
- Check if $V_{(A)}$ matches one of the $V_{(i)}$.
- Since the chain of hash is irreversible, $V$ can verify that $A$ actually involved in generating the signature.
Scenario II: Threshold Confessibility

- Satisfy Threshold-Confessibility
  - The actual signers can confess in a “threshold” structure inside the signing threshold structure.

- Adapt *Distributed Key Generation (DKG)* to manipulate vouchers.
Distributed Key Generation (DKG)

- A set of $t$ members jointly generate a pair of public and private keys.
- The public key is open and the private key is shared in $(t', t)$ threshold scheme
  - Shamir’s secret sharing scheme
  - $t' \leq t$.
- Ex: Discrete logarithm cryptosystem.
  - Each $U_i$ randomly generates secret $\beta_i$.
  - Afterwards, $\{U_1.. U_t\}$ has the public key $v_s = g^d$ while the secret key $d$ is shared in $f'$.
Scenario II: Threshold Confessibility

Threshold-confessibility

$r_s$ is a pre-defined (publicly known) value.

Construct a \((n-t+1)\)-degree polynomial \(f()\)

Secret vouchers

The ring signature

DKG protocol
To Confess (threshold)

- A number $\geq t'$ of the actual signers open their vouchers $\alpha_i$ to the verifier $V$, then $V$ can follow DKG and derive the secret $d$.
- $V$ checks if $v_s = g^d$ holds.
Publication

Go Further...

- Distributed ring signature for general access structure.
- Ex: \{U_1, U_2, U_3, U_4, U_5\} is the set of possible signers
  - \{U_1, U_2\}, \{U_1, U_3\}, \{U_1, U_4\}, \{U_2, U_4, U_5\} are the set of possible subsets of actual signers
Recent Results

Confessibility of different levels

- Individual confessibility
- Threshold confessibility
- General confessibility
Conclusions

- Provide an optional function for regular ring signature.
- Applications with confessibility
  - E-voting
  - E-lottery
  - E-gambling
- Other properties?
  - Linkability
  - Accountability
  - ...
References