Hierarchical Ring Signatures

Łukasz Krzywiecki, Mirosław Kutyłowski, Anna Lauks-Dutka

Institute of Mathematics and Computer Science
Wrocław University of Technology

WEWoRC 2009
July 7-9, Graz University of Technology
Outline

1. Ring Signatures
   - Concept
   - Problem

2. Hierarchical Ring Signatures
   - Idea
   - Building Blocks
   - Scheme Description
   - Signatures Graph
Outline

1. Ring Signatures
   - Concept
   - Problem

2. Hierarchical Ring Signatures
   - Idea
   - Building Blocks
   - Scheme Description
   - Signatures Graph
The Concept of Ring Signatures - [1]

**Ring signature** = digital signature used to sign a document in anonymous way

### Basic Properties

1. Signer uses his private key and public keys of some arbitrary group of people
2. Identity of the signer is hidden within this group (called a ring)
3. One cannot prevent being involved into a ring

The Concept of Ring Signatures - [1]

**Ring signature** = digital signature used to sign a document in anonymous way

**Basic Properties**

1. Signer uses his private key and public keys of some arbitrary group of people

2. Identity of the signer is hidden within this group (called a ring)

3. One cannot prevent being involved into a ring

The Concept of Ring Signatures - [1]

**Ring signature** = digital signature used to sign a document in anonymous way

### Basic Properties

1. Signer uses his private key and public keys of some arbitrary group of people
2. Identity of the signer is hidden within this group (called a **ring**)
3. One cannot prevent being involved into a ring

The Concept of Ring Signatures - [1]

**Ring signature** = digital signature used to sign a document in anonymous way

**Basic Properties**

1. Signer uses his private key and public keys of some arbitrary group of people
2. Identity of the signer is hidden within this group (called a ring)
3. One cannot prevent being involved into a ring

The public keys of all ring members are necessary for verification

Consequences

- the signature size is proportional to the ring size
- higher anonymity level = longer signatures
The public keys of all ring members are necessary for verification

Consequences

- the signature size is proportional to the ring size
- higher anonymity level = longer signatures
Observations from [2]

- In practical situations, the ring does not change for a long period of time.
- Rings can have implicit short descriptions, e.g.:
  
  "the ring of public keys of all members of the President’s Cabinet"

The signature size does not have to be linear in the size of the ring.

Hierarchical Ring Signatures

Anna Lauks-Dutka

Ring Signatures

Concept Problem

Hierarchical Ring Signatures

Idea
Building Blocks
Scheme Description
Signatures Graph

Previous Solution

Signature Scheme from [2]

- based on one-way accumulators
- uses group secret and public keys
- produces constant-size ring rignature

Outline

1. Ring Signatures
   - Concept
   - Problem

2. Hierarchical Ring Signatures
   - Idea
   - Building Blocks
   - Scheme Description
   - Signatures Graph
The Core Idea of Proposed Solution

1. Reuse the information about the previously created rings to get shorter signatures

2. Form a hierarchical structure – signatures created on a particular level utilizes anonymity sets from lower levels

Anonymity set grows exponentially with the level number
The Core Idea of Proposed Solution

Hierarchical Ring Signatures

1. Reuse the information about the previously created rings to get shorter signatures

2. Form a hierarchical structure – signatures created on a particular level utilizes anonymity sets from lower levels

Anonymity set grows exponentially with the level number
### Building Blocks of The Construction

#### Non-Interactive Zero Knowledge Proof of knowledge and equality 1 out of $n$ discrete logarithms

Given $(y_1, g_1), \ldots, (y_n, g_n)$ and $(y, g)$ prove that

$$\log_g y = \log_{g_i} y_i$$
for some unrevealed $i$.

Notation: $\text{NIZKP}(g, y, \{(g_1, y_1), \ldots, (g_n, y_n)\})$

---

#### Standard Digital Signature Scheme

$\text{SIG}(g^x, M)$ - signature of the message $M$.

Assumption: scheme with secret and public keys in the form of $(x, g^x)$

---

#### Hash function

$H : \{0, 1\}^* \rightarrow \langle g \rangle$
Building Blocks of The Construction

Non-Interactive Zero Knowledge Proof of knowledge and equality 1 out of \( n \) discrete logarithms

Given \((y_1, g_1), \ldots, (y_n, g_n)\) and \((y, g)\) prove that

\[
\log_g y = \log_{g_i} y_i
\]

for some unrevealed \( i \)

Notation: \( \text{NIZKP}(g, y, \{(g_1, y_1), \ldots, (g_n, y_n)\}) \)

Standard Digital Signature Scheme

\[ \text{SIG}(g^x, M) \] - signature of the message \( M \).

Assumption: scheme with secret and public keys in the form of \((x, g^x)\)

Hash function

\[ H : \{0, 1\}^* \rightarrow \langle g \rangle \]
Building Blocks of The Construction

Non-Interactive Zero Knowledge Proof of knowledge and equality 1 out of \( n \) discrete logarithms

Given \((y_1, g_1), \ldots, (y_n, g_n)\) and \((y, g)\) prove that

\[ \log_g y = \log_{g_i} y_i \] for some unrevealed \( i \)

Notation: \( \text{NIZKP}(g, y, \{(g_1, y_1), \ldots, (g_n, y_n)\}) \)

Standard Digital Signature Scheme

\( \text{SIG}(g^x, M) \) - signature of the message \( M \).

Assumption: scheme with secret and public keys in the form of \( (x, g^x) \)

Hash function

\( \mathcal{H} : \{0, 1\}^* \rightarrow \langle g \rangle \)
## Assumptions

- there is a PKI for registering public keys of the users
- \((x_u, y_u = g^{x_u})\) - the private and public key of user \(u\)
- there is a bulletin board (BB) where all hierarchical signatures can be published
Signature Creation at The Base Level

- $A = (y_1, y_2, \ldots, y_j, \ldots, y_n)$ - ring
- $j$ - the signer
- $g_A$ - generator obtained from $\mathcal{H}$

$$\text{SHRS}_A := \text{NIZKP}(g_A, g_A^{x_j}, \{(g, y_1), \ldots, (g, y_n)\}) \ || \ || \ \text{SIG}(g_A^{x_j}, M_A)$$

Signature size at the base level is proportional to the cardinality of the ring
Scheme Description

Signature Creation at The Base Level

- \( A = (y_1, y_2, \ldots, y_j, \ldots, y_n) \) - ring
- \( j \) - the signer
- \( g_A \) - generator obtained from \( \mathcal{H} \)

\[
\text{SHRS}_A := \text{NIZKP}(g_A, g_A^{x_j}, \{(g, y_1), \ldots, (g, y_n)\}) \ || \ \text{SIG}(g_A^{x_j}, M_A)
\]

Signature size at the base level is proportional to the cardinality of the ring
**Scheme Description**

**Signature Creation at The Next Levels**

- \( g_C \) - generator obtained from \( \mathcal{H} \)
- \( \text{SHRS}_A \) - hierarchical ring signature created by \( j \)
- \( \text{SHRS}_B \) - hierarchical ring signature created by \( i \neq j \)

\[
\text{SHRS}_C := \text{NIZKP}(g_C, g_C^{x_j}, \{(g_A, g_A^{x_j}), (g_B, g_B^{x_i})\}) \parallel \text{SIG}(g_C^{x_j}, M_C)
\]

Signature size at the next levels is **much lower** than the cardinality of the ring!
Scheme Description

Signature Creation at The Next Levels

- $g_C$ - generator obtained from $\mathcal{H}$
- $\text{SHRS}_A$ - hierarchical ring signature created by $j$
- $\text{SHRS}_B$ - hierarchical ring signature created by $i \neq j$

\[
\text{SHRS}_C := \text{NIZKP}(g_C, g_C^{x_j}, \{(g_A, g_A^{x_j}), (g_B, g_B^{x_j})\}) \parallel \parallel \text{SIG}(g_C^{x_j}, M_C)
\]

Signature size at the next levels is much lower than the cardinality of the ring!
Creating New Signatures

Anonymity Sets at The Base Level

Hierarchical Ring Signatures

Anna Lauks-Dutka

Ring Signatures

Concept Problem

Hierarchical Ring Signatures

Idea

Building Blocks

Scheme Description

Signatures Graph

A  B  C  D  E  F
Creating New Signatures
Anonymity Sets at The Second Level

G = A ∪ B

H = C ∪ D

I = E ∪ F
Creating New Signatures
Anonymity Sets at The Third Level

\[ J = G \cup H \]
\[ G = A \cup B \]
\[ H = C \cup D \]
\[ I = E \cup F \]
\[ A \]
\[ B \]
\[ C \]
\[ D \]
\[ E \]
\[ F \]
Creating New Signatures
Anonymity Sets at The Next Levels

\[ K = J \cup I \]

\[ J = G \cup H \]

\[ G = A \cup B \]

\[ H = C \cup D \]

\[ I = E \cup F \]

\[ A \]

\[ B \]

\[ C \]

\[ D \]

\[ E \]

\[ F \]
Signature Verification

Phases

1. check if \( \text{SIG}(g^x_j, M_C) \) verifies correctly with the verification key \( g^x_j \)

2. check \( \text{NIZKP}(g_C, g^x_j, \{(g_A, g^x_A), (g_B, g^x_B)\}) \)

if OK

- \( M_C \) was signed by a user whose private key is hidden in the exponent of \( g^x_j \)
- the exponent hidden in \( g^x_j \) is equal to one of the exponents hidden in the elements of the ring \( A \) or \( B \)
Signature Verification

Phases

1. check if $\text{SIG}(g_C^{x_j}, M_C)$ verifies correctly with the verification key $g_C^{x_j}$

2. check $\text{NIZKP}(g_C, g_C^{x_j}, \{(g_A, g_A^{x_j}), (g_B, g_B^{x_i})\})$

if OK

- $M_C$ was signed by a user whose private key is hidden in the exponent of $g_C^{x_j}$
- the exponent hidden in $g_C^{x_j}$ is equal to one of the exponents hidden in the elements of the ring $A$ or $B$
Thank you for your attention!