Step-out Ring Signatures

Marek Klonowski, Łukasz Krzywiecki, Mirosław Kutyłowski and Anna Lauks

Institute of Mathematics and Computer Science
Wrocław University of Technology

MFCS 2008
25-29 August 2008, Toruń, Poland

Wrocław University of Technology

1. Introduction
   - Digital signatures
   - Step-out Signatures

2. Construction
   - Preliminaries
   - Signature Creation
   - Confession Procedure
   - Step-out

Wrocław University of Technology

Digital Signatures

Procedures :

- key setup:
  - private key - for creating a signature
  - public key - for verifying a signature
- creating a signature
- signature verification

Wrocław University of Technology

Digital Signatures

Procedures :

- key setup:
  - private key - for creating a signature
  - public key - for verifying a signature
- creating a signature
- signature verification

Signing M :

Alice takes her private key k_{Alice} and computes

$$s := \mathrm{sign}(M, k_{Alice})$$

Wrocław University of Technology

Digital Signatures

Procedures :

- key setup:
  - private key - for creating a signature
  - public key - for verifying a signature
- creating a signature
- signature verification

Signing M :

Alice takes her private key k_{Alice} and computes

$$s := \mathrm{sign}(M, k_{Alice})$$

Verifying signature s of M :

Bob takes the public key p_{Alice} and checks if

$$\mathrm{test}(s, M, p_{Alice}) = \mathrm{true}$$

Wrocław University of Technology

Digital Signatures

Properties:

1. verification outcome is positive, if k_{Alice} used for signature creation and p_{Alice} for verification,

Wrocław University of Technology

Digital Signatures

Properties:

1. verification outcome is positive, if k_{Alice} used for signature creation and p_{Alice} for verification,
2. $\mathrm{test}(s, M, p_{Alice}) = \mathrm{false}$, if M has been changed after creating signature s,

Wrocław University of Technology

Digital Signatures

Properties:

1. verification outcome is positive, if k_{Alice} used for signature creation and p_{Alice} for verification,
2. $\mathrm{test}(s, M, p_{Alice}) = \mathrm{false}$, if M has been changed after creating signature s,
3. without the private key k_{Alice}, it is infeasible to produce a signature of Alice that is verified positively.

Wrocław University of Technology

Digital Signatures

Properties:

1. verification outcome is positive, if k_{Alice} used for signature creation and p_{Alice} for verification,
2. $\mathrm{test}(s, M, p_{Alice}) = \mathrm{false}$, if M has been changed after creating signature s,
3. without the private key k_{Alice}, it is infeasible to produce a signature of Alice that is verified positively.

So

if $\mathbf{test}(s, M, p_{Alice}) = \mathbf{true}$,
then only the holder of k_{Alice} (i.e. Alice) could produce s for message M.

Ring Signatures

Properties:

1. the signer is within the group of potential signers called a ring,

Ring Signatures

Properties:

1. the signer is within the group of potential signers called a ring,
2. the signer uses his own private key and the public keys of the other ring members to create a signature,

Ring Signatures

Properties:

1. the signer is within the group of potential signers called a ring,
2. the signer uses his own private key and the public keys of the other ring members to create a signature,
3. for verification the public keys of the ring members are used,

Ring Signatures

Properties:

1. the signer is within the group of potential signers called a ring,
2. the signer uses his own private key and the public keys of the other ring members to create a signature,
3. for verification the public keys of the ring members are used,
4. it is infeasible to detect which ring member created a signature.

Ring Signatures

Properties:

1. the signer is within the group of potential signers called a ring,
2. the signer uses his own private key and the public keys of the other ring members to create a signature,
3. for verification the public keys of the ring members are used,
4. it is infeasible to detect which ring member created a signature.
5. the signer is perfectly hidden in the ring.
6. one cannot prevent being a member of a ring.

Malicious Application of Ring Signatures

Leaking information

A member of a group (i.e. a parliament commission) can leak a secret information to the press.
The message is authenticated with a ring signature - with the commission members as the ring.

Malicious Application of Ring Signatures

Leaking information

A member of a group (i.e. a parliament commission) can leak a secret information to the press.
The message is authenticated with a ring signature - with the commission members as the ring.

Properties

1. one can easily check that some commission member has signed it, and so the information is authentic,
2. no investigation can reveal the information source.

Wrocław University of Technology

Malicious Application of Ring Signatures

Leaking information

A member of a group (i.e. a parliament commission) can leak a secret information to the press.
The message is authenticated with a ring signature - with the commission members as the ring.

Properties

1. one can easily check that some commission member has signed it, and so the information is authentic,
2. no investigation can reveal the information source.

As soon as public keys (e.g. RSA keys) of the commission members are published, nothing can prevent this scenario!

Wrocław University of Technology

Step-out Signatures – Target Applications

Electronic auction

Requirements:

1. strong authentication and anonymity of the bids (also against the auction manager),
2. possibility of immediate withdrawal of the deposit immediately after leaving the auction.

Wrocław University of Technology

Step-out Signatures – Target Applications

Electronic auction

Requirements:

1. strong authentication and anonymity of the bids (also against the auction manager),
2. possibility of immediate withdrawal of the deposit immediately after leaving the auction.

Ring signatures?

1. a ring signature authentication and anonymity,
2. however, there is no way to force the winner to reveal himself!

a useless solution ...

Step-out Signatures

Properties

Anonymity: ring type signature: identity of the signer(s) is hidden among identities of non-signers in a ring.

Confession procedure: the real signer can prove that he has participated in signature creation.

Step-out procedure: a non-signer can prove that he has not participated in signature creation.

Wrocław University of Technology

Step-out Signatures

Properties for auction protocol

Strong anonymity: necessary for fairness of e-auctions.

Confession procedure: the real signer of the winning bid can reveal himself against the auction.

Step-out procedure: a non-signer of the highest bid can step out during the auction and withdraw the deposit.

Wrocław University of Technology

Discrete Logarithm

DL hardness

we use a cyclic group G such that

- computing g^x is easy for each g, x
- given a random y, it is infeasible to find x such that $y = g^x$.

Secret keys

Each user U has its private key x_U selected at random
the corresponding public key is $y_U = g^{x_U}$, where g is a fixed generator of G.

Wroclaw University of Technology

Non-interactive Zero Knowledge Proofs

Proof of knowledge of discrete logarithm

A signer with a private key x and a public key y can prove that

he knows discrete logarithm of y (i.e. x)

in a non-interactive protocol that reveals no information on x.

Wrocław University of Technology

Non-interactive Zero Knowledge Proofs

Proof of equality of discrete logarithms

A signer with a private key x and a public key y can prove for $y_1 = g_1^x$ that

$$\log_g y = \log_{g_1} y_1$$

in a non-interactive protocol that reveals no information on x.

Proof of equality of discrete logarithms, 1 out of n

- Given $(y_1, g_1), \ldots, (y_n, g_n)$ prove that

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

- the proof can be uniquely bound to a message m

Signature Creation

Setup

- generators g and $\hat{g}$,
- ring members with public keys $y_1, \ldots, y_k$
- the signer holds y_j and the private key x_j

Signature

proof of equality of discrete logarithms depending on m and created with x_j

Wrocław University of Technology

Signature Creation

Details

1. $r_1, \ldots, r_n$ chosen at random,
2. $w_i \leftarrow g^{r_i}$, for $i = 1, \ldots, n$ [a]
3. $\hat{w} \leftarrow \hat{g}^{r_j}$, $\hat{y} \leftarrow \hat{g}^{x_j}$,
4. the signature is a non-interactive zero knowledge proof (depending on m) that

$$\log_{\hat{g}} \hat{y}\hat{w}$$

equals one of the logarithms

$$\log_g(y_1 w_1), \ldots, \log_g(y_n w_n)$$

Signature Verification

Idea

Simply checking the non-interactive zero knowledge proof provided by the signature

Revealing the Signer

Idea

1. the signer (say with y_1) creates the second signature with a ring such that the signer is the only member of both rings,

Revealing the Signer

Idea

1. the signer (say with y_1) creates the second signature with a ring such that the signer is the only member of both rings,
2. the same parameters $\hat{w}\hat{y}$ and $w_1, \ldots, w_n$ are used in both proofs– this enforces that $\log_{\hat{g}}(\hat{w}\hat{y})$ occurs on both lists:

$$\log_g(y_1 w_1), \log_g(y_2 w_2) \ldots, \log_g(y_n w_n)$$
$$\log_g(y_1 w_1), \log_g(y_2' w_2') \ldots, \log_g(y_n' w_n')$$

so it must be $\log_g(y_1 w_1)$ as it is the only common element.

Revealing the Signer

Idea

1. the signer (say with y_1) creates the second signature with a ring such that the signer is the only member of both rings,
2. the same parameters $\hat{w}\hat{y}$ and $w_1, \dots, w_n$ are used in both proofs– this enforces that $\log_{\hat{g}}(\hat{w}\hat{y})$ occurs on both lists:

$$\log_g(y_1 w_1), \log_g(y_2 w_2) \dots, \log_g(y_n w_n)$$
$$\log_g(y_1 w_1), \log_g(y_2' w_2') \dots, \log_g(y_n' w_n')$$

   so it must be $\log_g(y_1 w_1)$ as it is the only common element.
3. recall that the element of the same discrete logarithm has been created by the signer!

Step out

Idea of stepping out of the ring

1. a signature s contains $\hat{y}\hat{w}$ and $w_1, \ldots, w_n$,
2. a non-signer A provides two step-out signatures for the message *"I have not signed m"*,
3. these two signatures are obtained in the same way as in the confession procedure - so they point to A!

Step out

Idea of stepping out of the ring

1. a signature s contains $\hat{y}\hat{w}$ and $w_1, \ldots, w_n$,
2. a non-signer A provides two step-out signatures for the message *"I have not signed m"*,
3. these two signatures are obtained in the same way as in the confession procedure - so they point to A!
4. the same strings w_i are used, ...
5. but with $\hat{y}'\hat{w}'$ instead of $\hat{y}\hat{w}$.

Step out

Idea of stepping out of the ring

1. a signature s contains $\hat{y}\hat{w}$ and $w_1, \ldots, w_n$,
2. a non-signer A provides two step-out signatures for the message *"I have not signed m"*,
3. these two signatures are obtained in the same way as in the confession procedure - so they point to A!
4. the same strings w_i are used, ...
5. but with $\hat{y}'\hat{w}'$ instead of $\hat{y}\hat{w}$.
6. however, $\hat{y}\hat{w}$ is uniquely determined by w_i, if y_i corresponds to the signer!
   So the signer cannot create these additional signatures.

Thank you for your attention

Wrocław University of Technology