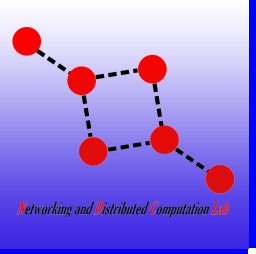


1-out-of-2 Signature

Mirosław Kutyłowski[1] and Jun Shao[2]

[1]Institute of Mathematics and Computer Science
Wrocław University of Technology
[2]College of Computer and Information Engineering
Zhejiang Gongshang University

2011-3-22

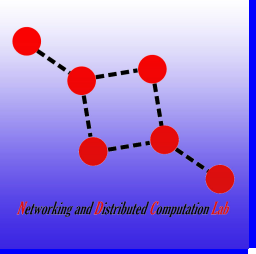
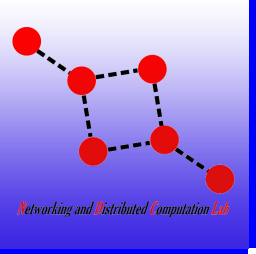


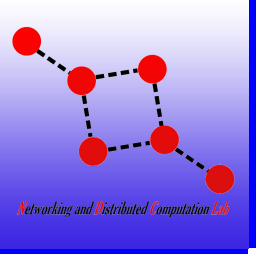
Table of Content



Signature with delegation capability

Mirosław Kutyłowski[1] and Jun Shao[2]

In digital signature, when the signer is absent, he/she will delegate his/her signing rights to a proxy.

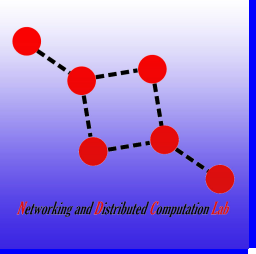


Signature with delegation capability

Mirosław Kutyłowski[1] and Jun Shao[2]

In digital signature, when the signer is absent, he/she will delegate his/her signing rights to a proxy.

- Proxy signature

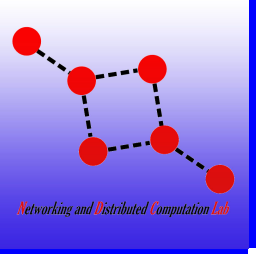


Signature with delegation capability

Mirosław Kutyłowski[1] and Jun Shao[2]

In digital signature, when the signer is absent, he/she will delegate his/her signing rights to a proxy.

- Proxy signature
- Proxy re-signature

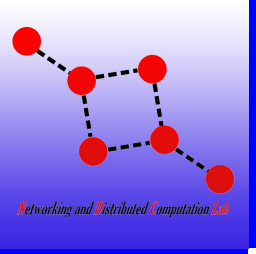


Signature with delegation capability

Mirosław Kutyłowski[1] and Jun Shao[2]

In digital signature, when the signer is absent, he/she will delegate his/her signing rights to a proxy.

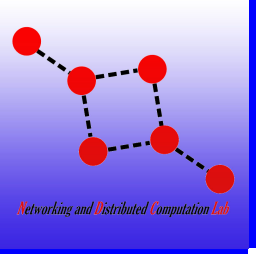
- Proxy signature
- Proxy re-signature
- Mediated signature



Signature with delegation capability

In digital signature, when the signer is absent, he/she will delegate his/her signing rights to a proxy.

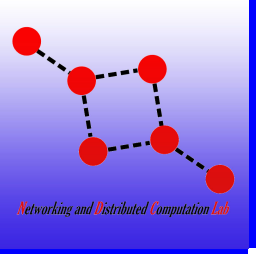
- Proxy signature
  - In a proxy signature scheme, the original signer delegates his/her signing rights to a proxy, who can sign messages on behalf of the original signer afterwards.



Signature with delegation capability

In digital signature, when the signer is absent, he/she will delegate his/her signing rights to a proxy.

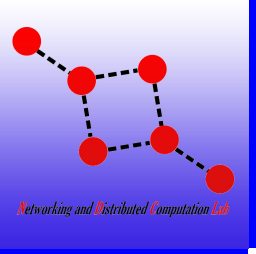
- Proxy signature
- Proxy re-signature
  - In a proxy re-signature scheme, a proxy can transform a signature of the delegatee to another signature of the delegator on the same message.



Signature with delegation capability

In digital signature, when the signer is absent, he/she will delegate his/her signing rights to a proxy.

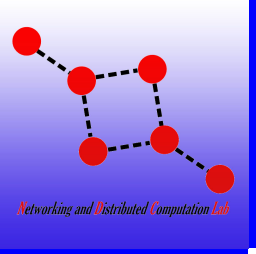
- Proxy signature
- Proxy re-signature
- Mediated signature
  - In a mediated signature scheme, an on-line semi-trusted mediator (SEM) should involve in every signing process to help the original signer to generate the signature.



Scenario

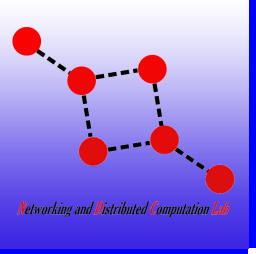
In some cases, the signer just wanna give the proxy the limited delegation, which satisfies that

- The proxy can generate the signature on only one message from two given messages.
- The signature generated by the proxy is indistinguishable from the one by the signer.



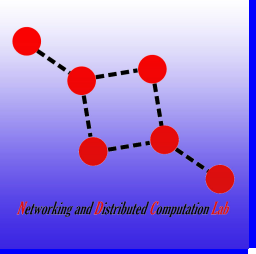
Scenario

- Proxy signature ✖
  - Distinguishable



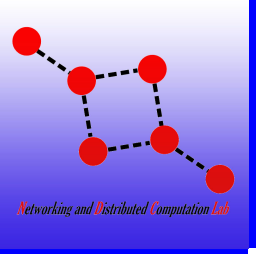
Scenario

- Proxy signature ✖
  - Distinguishable
- Proxy re-signature ✖
  - Public key is changed



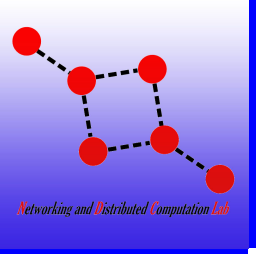
Scenario

- Proxy signature ✖
  - Distinguishable
- Proxy re-signature ✖
  - Public key is changed
- Mediated signature ✖
  - The proxy is always involved



Functionality of 1-out-of-2 signature

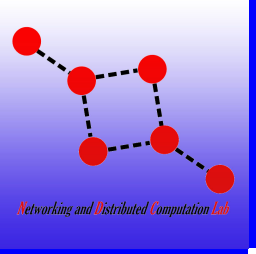
1-out-of-2 signature is a kind of signature with delegation capability.



Functionality of 1-out-of-2 signature

1-out-of-2 signature is a kind of signature with delegation capability. In particular,

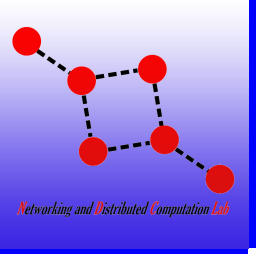
- The proxy can transform one of two given partial signatures of the signer into one full signature.



Functionality of 1-out-of-2 signature

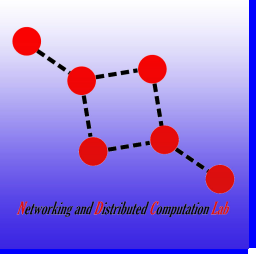
1-out-of-2 signature is a kind of signature with delegation capability. In particular,

- The proxy can transform one of two given partial signatures of the signer into one full signature.
- The proxy can transform only one of the two given partial signatures; otherwise, the secret key of the proxy will be revealed.



Definition

- $\texttt{SKeyGen}(1^k) \rightarrow (pk_S, sk_S)$.
- $\texttt{PKeyGen}(1^k) \rightarrow (pk_P, sk_P)$.
- $\texttt{PreSign}(sk_S, pk_P, (m_0, m_1)) \rightarrow ((\sigma_0, m_0), (\sigma_1, m_1))$.
- $\texttt{Trans}(\sigma_0, \sigma_1, sk_P) \rightarrow \sigma'_b$, $(b \in \{0, 1\})$.
- $\texttt{Verify}((\sigma', m), pk_S) \rightarrow 1$ or 0.
- $\texttt{Reveal}((\sigma_0, \sigma_1), (\sigma'_0, \sigma'_1), pk_P) \rightarrow sk_P$.



Security Model—Existential Unforgeability

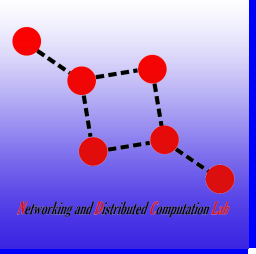
Setup (pk_S, sk_S), (pk_P, sk_P).

Queries

- Secret key oracle $\mathcal{O}_{Psk}$.
- Partial signature generation oracle $\mathcal{O}_{ps}$.
- Full signature generation oracle $\mathcal{O}_t$.

Forgery The adversary outputs a full signature (σ^*, m^*).

- $\texttt{Verify}((\sigma^*, m^*), pk_S) \rightarrow 1$.
- $(*, m^*)$ has not been queried to $\mathcal{O}_t$.
- m^* has not been queried to $\mathcal{O}_{ps}$ or $\mathcal{O}_{Psk}$ has not been queried.



Security Model—Confidentiality

Setup Identical to that in the game for Existential Unforgeability.

Queries
- Secret key oracle $\mathcal{O}_{Ssk}$.
- Partial signature generation oracle $\mathcal{O}_{ps}$.
- Full signature generation oracle $\mathcal{O}_t$.

Output The adversary wins if he/she outputs the proxy's secret key sk_P.

Our proposal—one-time signature method

It works in a finite cyclic group $G =< g >$ with prime order p.

- `SKeyGen`: $X = g^x \in G$, $x \in Z_p^*$.
- `PKeyGen`: $Y = g^y \in G$, $y \in Z_p^*$.
- `PreSign`: (x, Y, m_0, m_1)
  - The proxy sends $A = g^a$ to the signer, where a is a random number from Z_p^*.
  - On receiving A, the signer computes two partial signatures on m_0, m_1 as follows. For $(b' = 0, 1)$

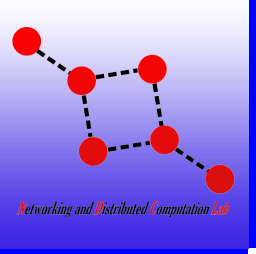
$$\begin{aligned} R_{b'} &= (Y^{H_1(Y||A||b')} \cdot A) \cdot g^{r_{b'}}, \\ S_{b'} &= r_{b'} + H_2(m_{b'}||R_{b'}) \cdot x \bmod p, \end{aligned}$$

    where $r_{b'}$, $(b' = 0, 1)$ are random numbers from Z_p^*.
  - The signer sends $(R_{b'}, S_{b'}, b')$, $(b' = 0, 1)$ to the proxy.

Our proposal

- `Trans`: On input $(R_{b'}, S_{b'}, m_{b'})$, $(b' = 0, 1)$, a, y, it outputs (R'_b, S'_b, b), $(b \in \{0, 1\})$:
  $R'_b = R_b, \quad S'_b = S_b + (y \cdot H_1(Y||g^a||b) + a) \bmod p.$
- `Verify`: On input (R', S', m), X, it outputs 1 if $g^{S'} = R' \cdot X^{H_2(m||R')}$ holds; otherwise, it outputs 0.
- `Reveal`: On input $(R_{b'}, S_{b'}, b')$, $(b' = 0, 1)$, $(R'_{b'}, S'_{b'}, b')$, $(b' = 0, 1)$, A, Y, it outputs y.

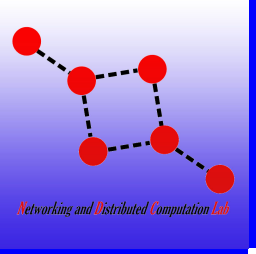
$$\begin{cases} S'_0 - S_0 = y \cdot H_1(Y||A||0) + a \bmod p, \\ S'_1 - S_1 = y \cdot H_1(Y||A||1) + a \bmod p. \end{cases}$$



Security analysis

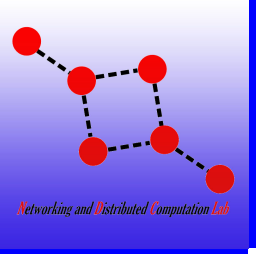
Theorem

The above proposal is existentially unforgeable and confidential in the random oracle model based on the DL assumption.



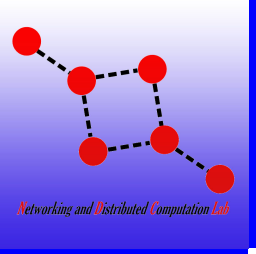
1-out-of-k signature

- In algorithm `PreSign`, the signer returns k partial signatures to the proxy, other algorithms remain the same.



Strong 1-out-of-2 signature

The adversary has the unlimited computational power while the signer or the proxy only has the polynomially bounded power.



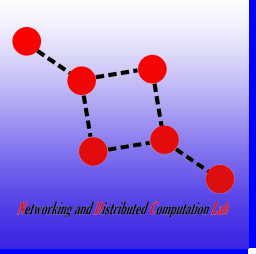
Strong 1-out-of-2 signature scheme—fail-stop signature method

- `SKeyGen`: The signer chooses $4\ell + 2$ random numbers $x_1^{(0)}, x_2^{(0)}, \{x_1^{(i)}, x_2^{(i)}, x_3^{(i)}, x_4^{(i)}\}_{i=1}^{\ell}$ from Z_p^*, and computes $X^{(0)} = g^{x_1^{(0)}} h^{x_2^{(0)}}$ and $X_0^{(i)} = g^{x_1^{(i)}} h^{x_3^{(i)}}$, $X_1^{(i)} = g^{x_2^{(i)}} h^{x_4^{(i)}}$ for $(i = 1, \cdots, \ell)$. The public key is

$$\mathcal{X} = (X^{(0)}, \{X_0^{(i)}, X_1^{(i)}\}_{i=1}^{\ell}),$$

and the secret key is

$$\mathbb{x} = (x_1^{(0)}, x_2^{(0)}, \{x_1^{(i)}, x_2^{(i)}, x_3^{(i)}, x_4^{(i)}\}_{i=1}^{\ell}).$$



Strong 1-out-of-2 signature scheme

- `PKeyGen`: The proxy chooses $2\ell + 2$ random numbers $\{y_1^{(i)}, y_2^{(i)}\}_{i=0}^{\ell}$ from Z_p^*, and computes $Y_i^{(0)} = g^{y_1^{(i)}} h^{y_2^{(i)}}$ for $(i = 0, \cdots, \ell)$. The public key is

$$\mathcal{Y} = \{Y^{(i)}\}_{i=0}^{\ell},$$

and the secret key is

$$\mathbb{y} = \{y_1^{(i)}, y_2^{(i)}\}_{i=0}^{\ell}.$$

Strong 1-out-of-2 signature scheme

- `PreSign`: On input the signer's secret key $\mathbb{x} = (x_1^{(0)}, x_2^{(0)}, \{x_1^{(i)}, x_2^{(i)}, x_3^{(i)}, x_4^{(i)}\}_{i=1}^{\ell})$, the proxy's public key $\mathcal{Y} = \{Y^{(i)}\}_{i=0}^{\ell}$, and two messages m_0, m_1 from the message space, the partial signature generation algorithm is performed as follows.
  - Assume that it is the κ-th time, then the signer computes two partial signatures on m_0, m_1 as follows. For $(b' = 0, 1)$

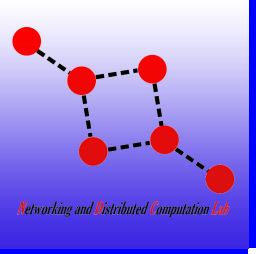
$$\begin{aligned} \sigma_{b'}^{(1)} &= x_1^{(0)} + H_2(m_{b'}||\kappa) \cdot x_{1+b'}^{(\kappa)} \bmod p, \\ \sigma_{b'}^{(2)} &= x_2^{(0)} + H_2(m_{b'}||\kappa) \cdot x_{3+b'}^{(\kappa)} \bmod p. \end{aligned}$$

  - The signer sends $(\kappa, b', \sigma_{b'}^{(1)}, \sigma_{b'}^{(2)})$, $(b' = 0, 1)$ to the proxy.

Strong 1-out-of-2 signature scheme

- `Trans`: On input two partial signatures $(\kappa, b', \sigma_{b'}^{(1)}, \sigma_{b'}^{(2)})$, $(b' = 0, 1)$, the 1-out-of-2 full signature generation algorithm outputs a full signature $(\kappa, b, \sigma_b^{(1)'}, \sigma_b^{(2)'})$, $(b \in \{0, 1\})$.

$$\begin{aligned} \sigma_b^{(1)'} &= \sigma_b^{(1)} + (y_1^{(0)} + y_1^{(\kappa)} \cdot H_1(\kappa||b)) \bmod p, \\ \sigma_b^{(2)'} &= \sigma_b^{(2)} + (y_2^{(0)} + y_2^{(\kappa)} \cdot H_1(\kappa||b)) \bmod p. \end{aligned}$$



Strong 1-out-of-2 signature scheme

- `Verify`: On input a full signature $(\kappa, b, \sigma^{(1)'}, \sigma^{(2)'}, m)$, the signer's public key $\mathcal{X}$, it outputs 1 if

$$g^{\sigma'^{(1)}} \cdot h^{\sigma'^{(2)}} = (X^{(0)} \cdot Y^{(0)} \cdot (Y^{(\kappa)})^{H_1(\kappa||b)}) \cdot (X_b^{(\kappa)})^{H_2(m||\kappa)}$$

holds; otherwise, it outputs 0.

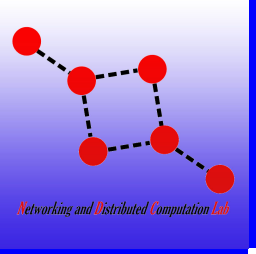
Strong 1-out-of-2 signature scheme

- `Reveal`: On input two partial signatures $(\kappa, b', \sigma_{b'}^{(1)}, \sigma_{b'}^{(2)})$, $(b' = 0, 1)$, two full signatures $(\kappa, b', \sigma_{b'}^{(1)'}, \sigma_{b'}^{(2)'})$, $(b' = 0, 1)$, and the proxy's public key $\mathcal{Y}$, it outputs the proxy's secret key $(y_1^{(0)}, y_2^{(0)})$ by the following equations.

$$\begin{cases} \sigma_0^{(1)'} - \sigma_0^{(1)} = y_1^{(0)} + y_1^{(\kappa)} \cdot H_1(\kappa||0) \bmod p, \\ \sigma_0^{(2)'} - \sigma_0^{(2)} = y_2^{(0)} + y_2^{(\kappa)} \cdot H_1(\kappa||0) \bmod p, \\ \sigma_1^{(1)'} - \sigma_1^{(1)} = y_1^{(0)} + y_1^{(\kappa)} \cdot H_1(\kappa||1) \bmod p, \\ \sigma_1^{(2)'} - \sigma_1^{(2)} = y_2^{(0)} + y_2^{(\kappa)} \cdot H_1(\kappa||1) \bmod p, \end{cases}$$

Strong 1-out-of-2 signature scheme

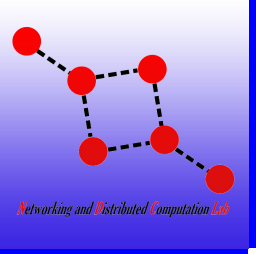
- `Stop-fail`: With a forgery $(\kappa^*, b^*, (\sigma^{(1)'})^*, (\sigma^{(2)'})^*, m^*)$, the proxy and the signer do the following steps: The signer generates a partial signature $(\kappa^*, b^*, \sigma^{(1)}, \sigma^{(2)}, m^*)$, and sends it to the proxy with $(\kappa^*, b^*, (\sigma^{(1)'})^*, (\sigma^{(2)'})^*, m^*)$. Upon receiving the data from the signer, the proxy first checks the validity of the received data. If it is valid, then the proxy computes and outputs the full signature $(\kappa^*, b^*, \sigma^{(1)'}, \sigma^{(2)'}, m^*)$; otherwise, the proxy aborts the algorithm.



Security analysis

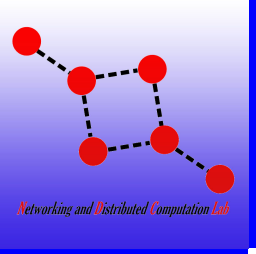
Theorem

The strong 1-out-of-2 signature scheme is existentially unforgeable and confidential in the standard model based on the DL assumption.



Future work

- Non-interactive
- t-out-of-n
- . . .



Mirosław Kutyłowski[1] and Jun Shao[2]

Thank you for your attention!