Anonymous Proxy Signatures

G. Fuchsbauer D. Pointcheval

École normale supérieure

SCN ’08
09/11/2008

Anonymous Consecutive Delegation of Signing Rights

Delegation A delegator delegates his signing rights to a proxy signer (or delegatee) who can then sign on the delegator’s behalf

Consecutiveness A delegatee may re-delegate the received signing rights ⇒ intermediate delegators

Anonymity All intermediate delegators and the proxy signer remain anonymous

After verifying a proxy signature one knows that someone entitled signed but nothing more

Application: GRID computing

User authenticates herself and starts process which needs to authenticate to resources / start subprocesses

⇒ Delegation and re-delegation of signing rights

No need to know that it was not the user herself to be authenticated

Our Results

- Algorithm specifications
- Security definitions
- Proof of concept: existence assuming trapdoor permutations

Relation to Other Primitives

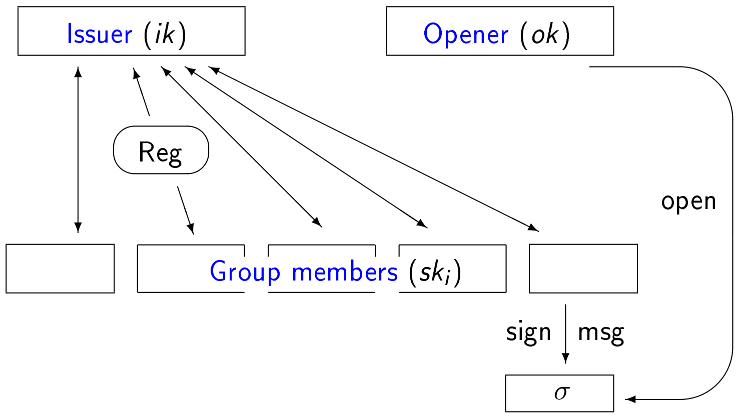
Anonymous proxy signatures are a generalization of

- Proxy signatures (consecutive delegation)
  formalized by [BPW03]
- Group signatures (anonymity)
  formalized by [BMW03, BSZ05]
  - dynamic (users can join after setup of group)
  - hierarchical (tree structure by consecutive delegations) [TW05]

and satisfy the respective security notions

Group Signatures

Group public key: *pk*



Algorithms for (Dynamic) Group Signatures

Algorithms

Setup produces group public key, issuing key, opening key

Reg registers new members joining the group using the issuing key

Sig enables a group member to sign on behalf of the group

Ver checks validity of a group signature using the group public key

Open reveals the signer's identity using the opening key

Security Definitions for (Dynamic) Group Signatures

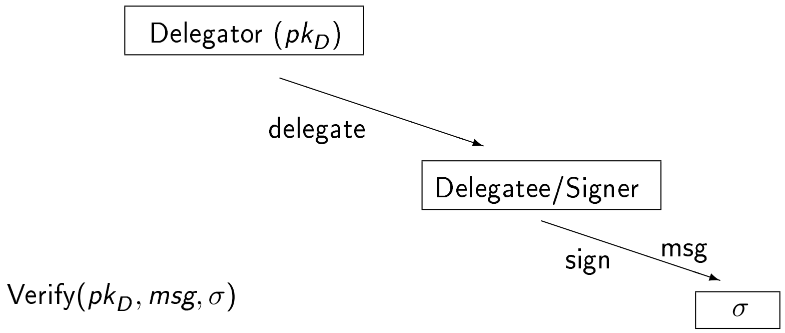
Security [BSZ05]

Anonymity no one except the opener can tell who produced a signature

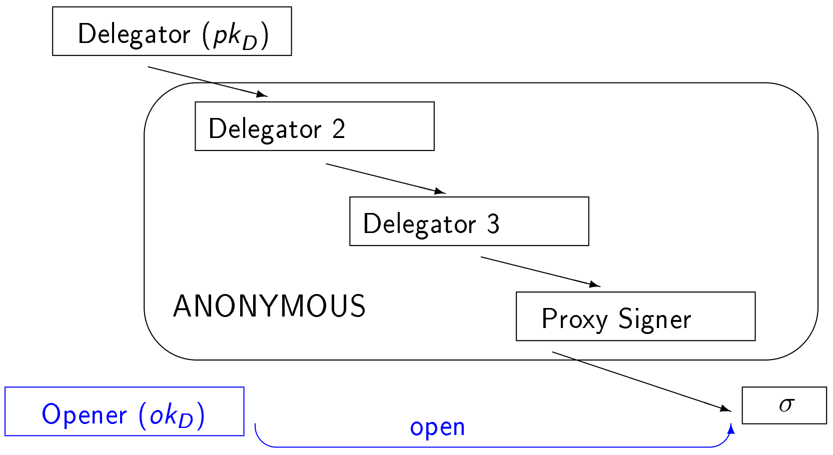
Traceability every valid signature can be traced to its signer by the opener

Non-Frameability no one can produce a signature that opens to a member who did not sign

Proxy Signatures



Proxy Signatures, Consecutive Delegations



Tasks

Delegation by Certificate

Delegator signs a warrant containing the proxy's public key pk_P
Proxy signs message with her own signing key

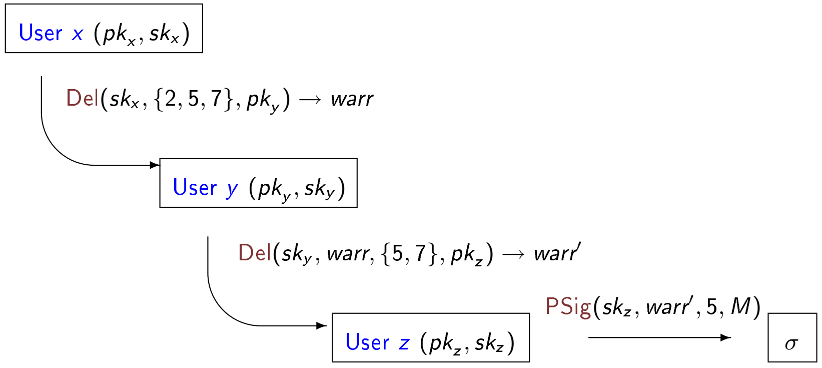
$\Rightarrow$ Verify signature on warrant (w.r.t. pk_D) and message (w.r.t. pk_P).

Delegation of Tasks

- possibility to delegate rights only for certain set of tasks
- re-delegate rights for restricted set of tasks

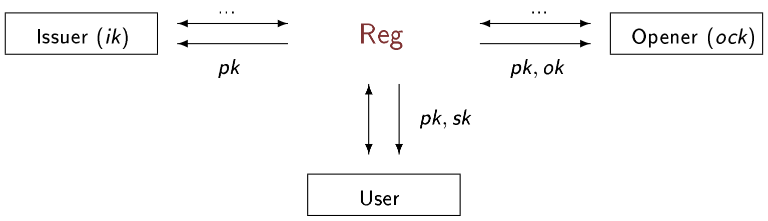
Delegation of *TList*, a set of natural numbers representing tasks

Example: Redelegation of Reduced Task Set


User x (pk_x, sk_x)
Del(sk_x, $\{2, 5, 7\}$, pk_y) $\rightarrow$ $warr$
User y (pk_y, sk_y)
Del(sk_y, $warr$, $\{5, 7\}$, pk_z) $\rightarrow$ $warr'$
User z (pk_z, sk_z)
PSig(sk_z, $warr'$, 5, M)
σ

PVer(pk_x, 5, M, σ) $\rightarrow$ 1
Open(ok_x, 5, M, σ) $\rightarrow$ $\{pk_y, pk_z\}$

Algorithms of Anonymous Proxy Signature Scheme $\mathcal{PS}$



$$\begin{array}{rcccl}
\lambda & \rightarrow & \text{Setup} & \rightarrow & pp, ik, ock \\
sk_x, [warr_{\rightarrow x},]\ TList, pk_y & \rightarrow & \text{Del} & \rightarrow & warr_{[\rightarrow]x \rightarrow y} \\
sk_y, warr_{x \rightarrow \ldots \rightarrow y}, task, M & \rightarrow & \text{PSig} & \rightarrow & \sigma \\
pk_x, task, M, \sigma & \rightarrow & \text{PVer} & \rightarrow & b \in \{0,1\} \\
ok_x, task, M, \sigma & \rightarrow & \text{Open} & \rightarrow & \text{a list of users or } \perp \text{ (failure)}
\end{array}$$

Security for Anonymous Proxy Signatures

Anonymity intermediate delegators and proxy signer remain anonymous

– **BUT:** the number of delegations may not remain hidden (if no restriction on number of delegations)

Traceability every valid signature can be traced to its intermediate delegators and proxy signer

Non-Frameability no one can produce a signature that, when opened, wrongfully reveals a delegator or signer

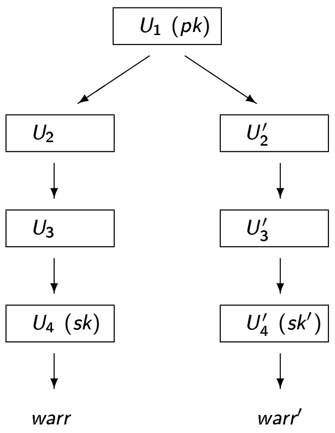
Anonymity I

Idea:

- Adversary controls users and issuer
- produces 2 warrants
- one of them used to sign
- Adversary must decide which one

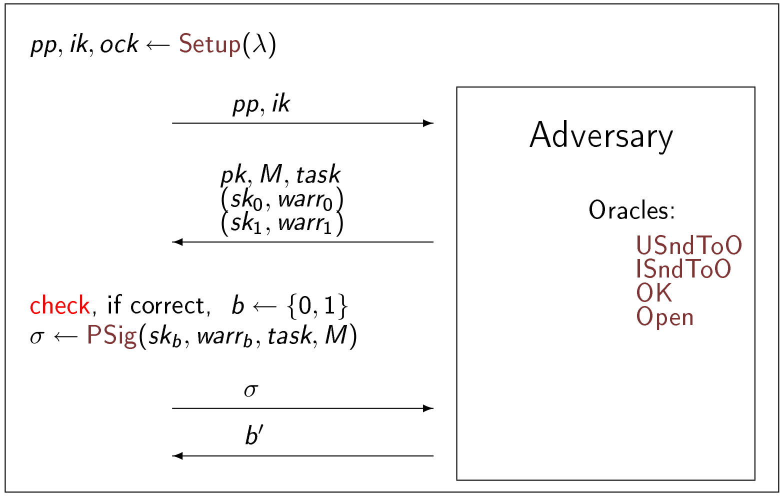
Restrictions:

- U_1 must be registered with the opener
- both warrants correctly formed
- both delegation chains of same length



Anonymity II

$\mathbf{Exp}^{\text{anon}}_{\mathcal{PS},A}(\lambda)$



$pp, ik, ock \leftarrow \mathsf{Setup}(\lambda)$

pp, ik

$pk, M, task$
$(sk_0, warr_0)$
$(sk_1, warr_1)$

check, if correct, $b \leftarrow \{0,1\}$
$\sigma \leftarrow \mathsf{PSig}(sk_b, warr_b, task, M)$

σ

b'

Adversary

Oracles:
USndToO
ISndToO
OK
Open

Anonymity III

The experiment $\mathbf{Exp}^{\text{anon}}_{\mathcal{PS},A}(\lambda)$ returns 1 if

- $b = b'$
- no queries $\mathsf{OK}(pk)$ and $\mathsf{Open}(pk, task, M, \sigma)$ made

Definition

A proxy signature scheme is anonymous if for all p.p.t. adversaries A

$$\Pr\left[\mathbf{Exp}^{\text{anon}}_{\mathcal{PS},A}(\lambda) = 1\right] - \frac{1}{2} \;=\; \mathrm{negl}(\lambda)$$

Traceability I

Idea:

- Adversary can corrupt users and opener (which follows the protocol)
- gets SndToI and SndToO oracles for Reg that return a transcript between them and opening key
- must produce signature that is valid but not openable

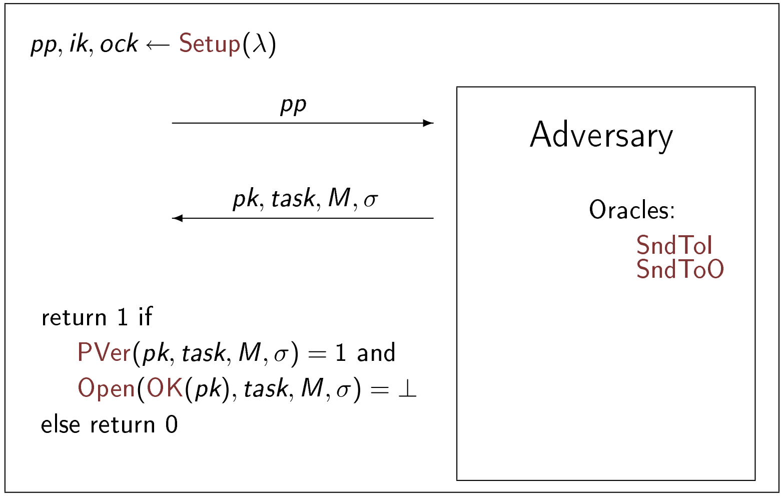
Definition

A proxy signature scheme is traceable if for all p.p.t. adversaries A

$$\Pr[\mathbf{Exp}^{\mathrm{trace}}_{\mathcal{PS},A}(\lambda) = 1] \;=\; \mathsf{negl}(\lambda)$$

Traceability II

$\mathbf{Exp}^{\mathrm{trace}}_{\mathcal{PS},A}(\lambda)$

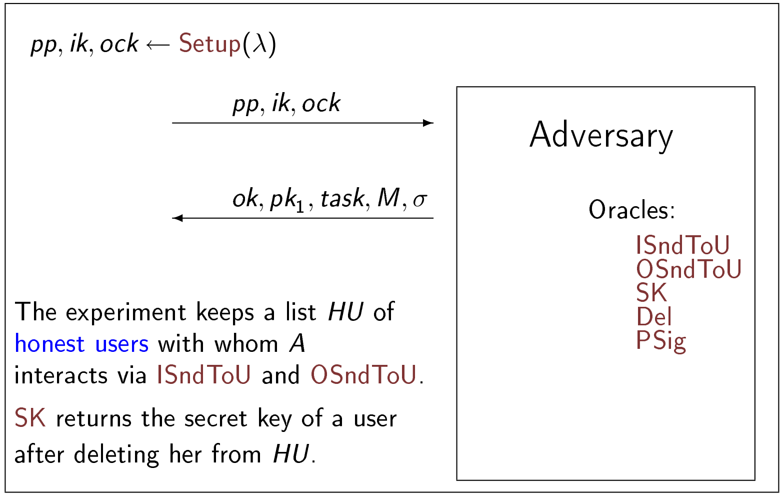


$pp, ik, ock \leftarrow \mathsf{Setup}(\lambda)$

return 1 if
  $\mathsf{PVer}(pk, task, M, \sigma) = 1$ and
  $\mathsf{Open}(\mathsf{OK}(pk), task, M, \sigma) = \perp$
else return 0

Non-Frameability I

$\mathbf{Exp}^{\mathrm{n\text{-}frame}}_{\mathcal{PS},A}(\lambda)$



$pp, ik, ock \leftarrow \mathsf{Setup}(\lambda)$

The experiment keeps a list HU of honest users with whom A interacts via ISndToU and OSndToU.

SK returns the secret key of a user after deleting her from HU.

Non-Frameability II

The experiment $\mathbf{Exp}^{\mathrm{n\text{-}frame}}_{\mathcal{PS},A}(\lambda)$ returns 1 if σ is valid and its opening reveals

- either a delegation by an honest user which was not queried via Del
- or an honest proxy signer who was not queried via PSig

Definition

A proxy signature scheme is non-frameable if for all p.p.t. adversaries A

$$\Pr[\mathbf{Exp}^{\mathrm{n\text{-}frame}}_{\mathcal{PS},A}(\lambda) = 1] \;=\; \mathsf{negl}(\lambda)$$

Generic Construction

using

- Digital signatures (EUF-CMA)
- Public-key encryption (IND-CCA)
- NIZK (simulation sound)

(follow from trapdoor permutations)

Conclusion

- Defined new primitive encompassing group and proxy signatures (satisfies rigorous security notions of both)
- Non-frameable dynamic hierarchical group signatures

Open Problem

- Efficient implementation