

Group Signature and Identity Escrow Schemes

Jan Camenisch

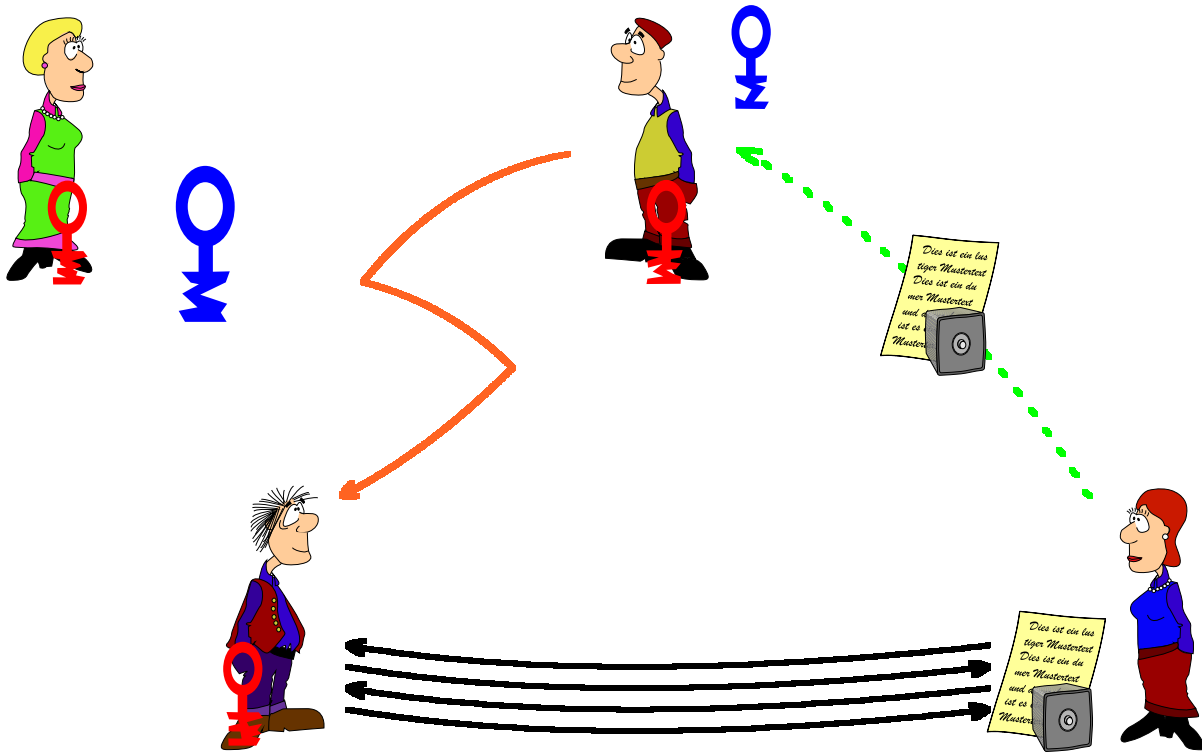
IBM Research
Zurich Research Laboratory

Overview

- Id escrow & group signature
- Overview of different solutions
- History
- Details of the most recent scheme

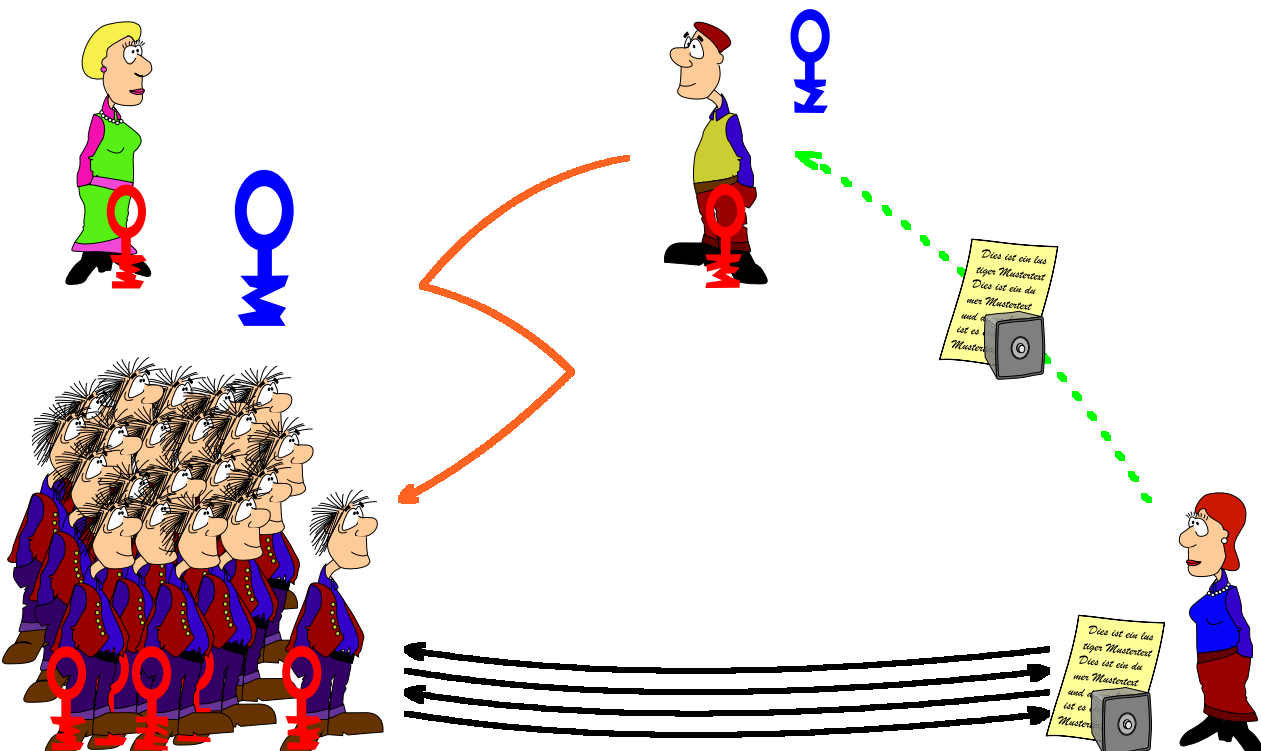
Identity Escrow

[Kilian/Petrank '98]



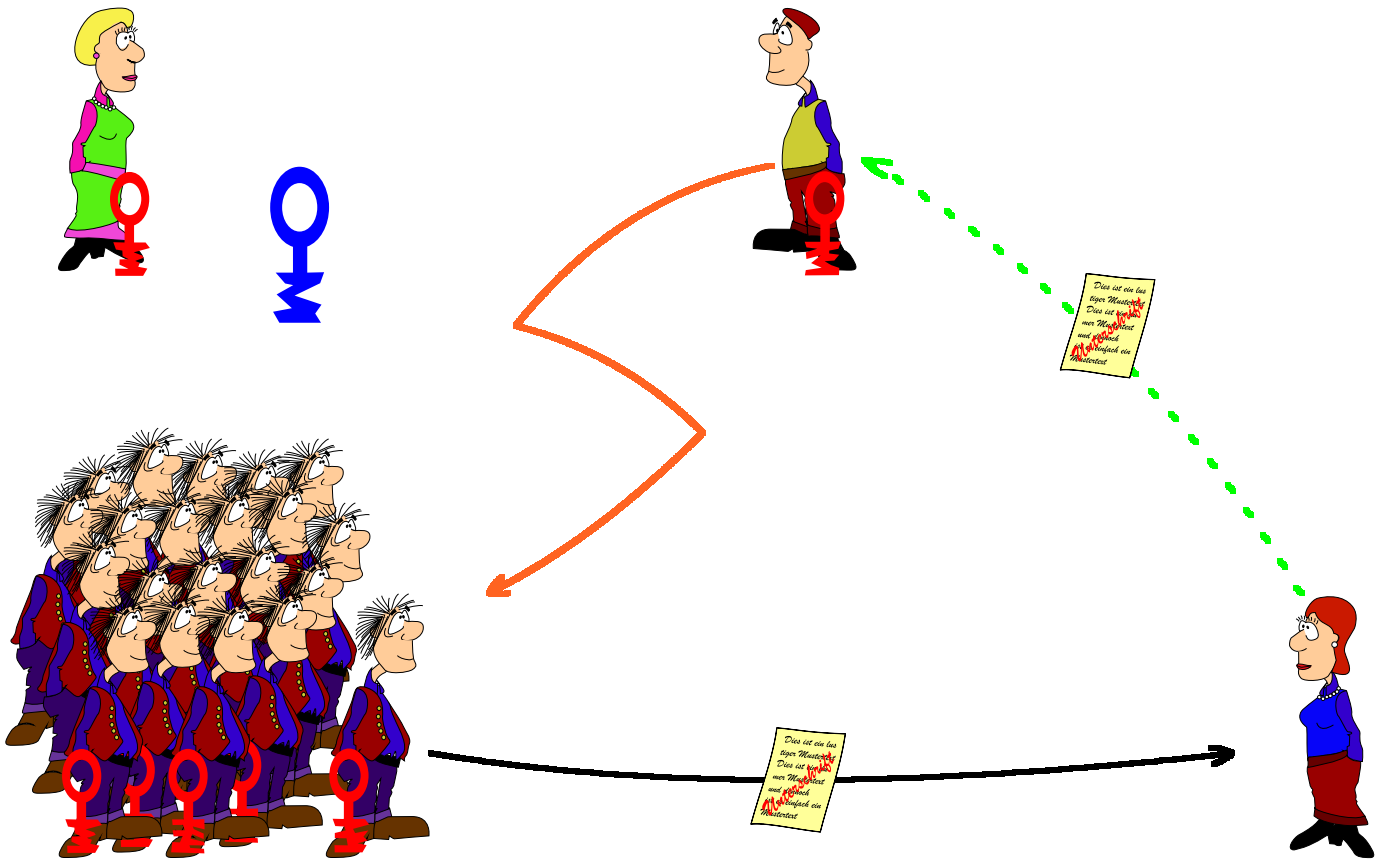
Identity Escrow

[Kilian/Petrank '98]

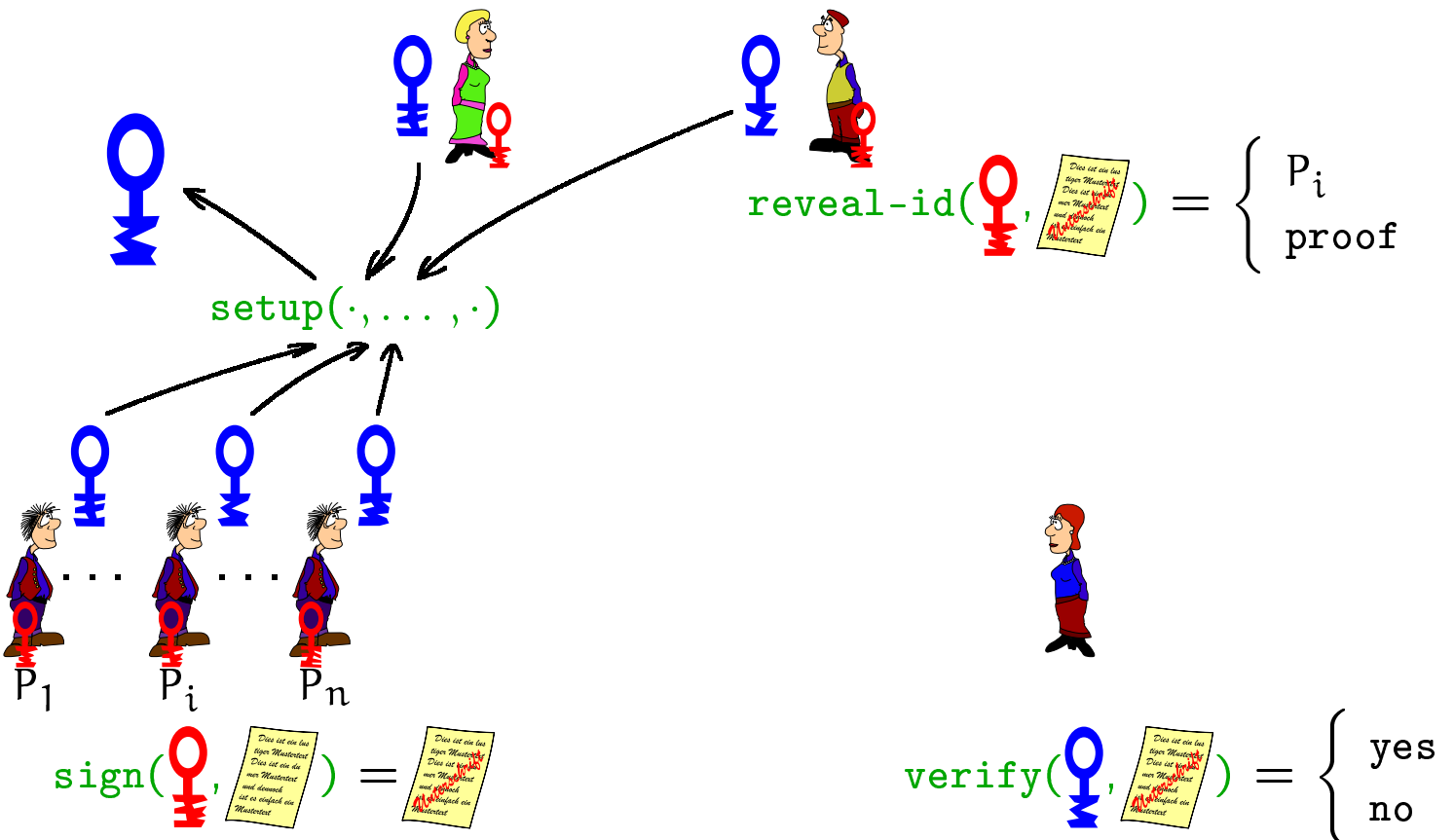


Group Signature Scheme

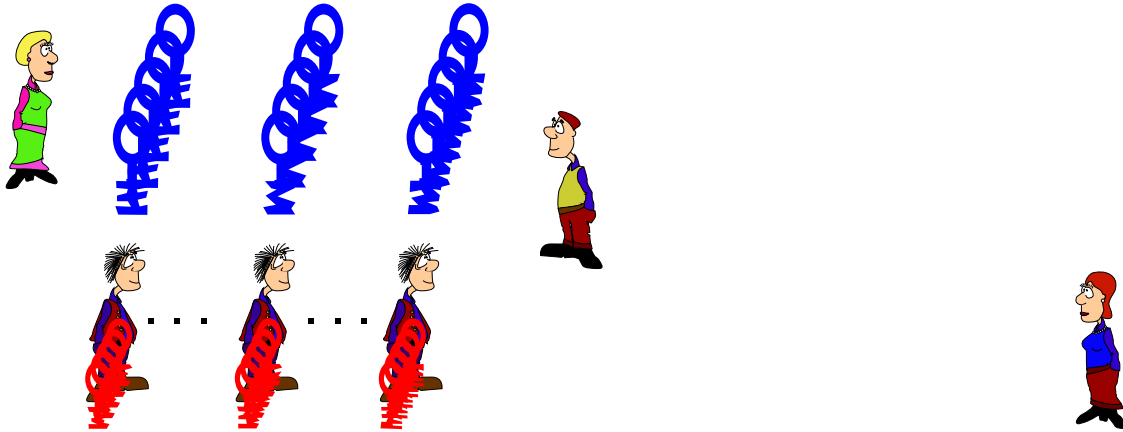
[Chaum/van Heyst '91]



Model



A Simple Solution



Properties:

- + Signatures are short
- Group's PK is large
- Members' SK is large
- Number of signatures is limited

Security Requirements

- Correctness
- Unforgeability
- Anonymity & Unlinkability
- Exculpability (no framing)
- Traceability

Other Requirements

- Size of group's public key
- Size of secret keys
- Length of signatures
- Separability (w.r.t. revocation manager)
- Efficiency
- Ease of management of the group

Solutions for Small Groups

[Chaum & van Heyst]

- Group's Public Key :
 - List of member's public keys PK_1, \dots, PK_N where $PK_i = f(SK_i)$
 - revocation manager's PK E_R of any encryption scheme
- to sign a message m , a group member computes $z = E_R(PK_i)$ and provides
 - $P_1 = PK\{(\alpha) : z = E_R(\alpha) \wedge \alpha \in \{PK_1, \dots, PK_N\}\}$
 - $P_2 = PK\{(\alpha, \gamma) : z = E_R(\alpha) \wedge \alpha = f(\gamma)\}$

Realizations:

- Size of proof P_1 is linear in number of group members
- Separable

Solutions for Large Groups

[Camenisch & Stadler '97]

- Group's Public Key:
 - membership manager's PK S_M of any signature scheme
 - revocation manager's PK E_R of any encryption scheme
- Group members: choose PK $PK_i = f(SK_i)$
- Group manager issues certificates on group members' PKs
- to sign a message m , a group member computes $z = E_R(PK_i)$ and provides
 - $P_1 = PK\{(\alpha, \beta) : z = E_R(\alpha) \wedge Cert(S_M, \alpha) = \beta\}$
 - $P_2 = PK\{(\alpha, \gamma) : z = E_R(\alpha) \wedge \alpha = f(\gamma)\}$

Realizations:

- separable solutions exists
- efficient solutions with separability for revocation manager

History

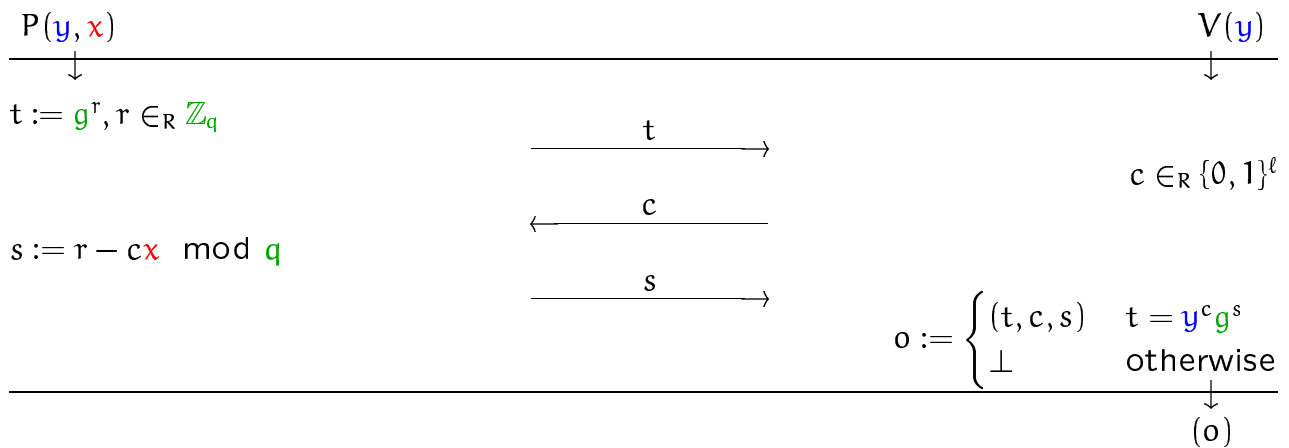
	Non-Separable	Separable
small groups	Chaum & van Heyst '91 Chen & Pedersen '94 Camenisch '97 Petersen '97	Camenisch & Damgård '98
large groups	Camenisch & Stadler '97 Camenisch & Michels '98 Traoré '99 ACJT 2000	Kilian & Petrank '98 Camenisch & Michels '99

green: purely discrete log based schemes.

Building Blocks: 3-Move HVZKPK

[CEvdG88,Schnor89]

Group $G = \langle g \rangle$ of order q . Secret key: $x \in \mathbb{Z}_q$, Public key: $y = g^x$.



Notation: $PK\{(\alpha) : y = g^\alpha\}$

Non-interactive/signature scheme: $(s, c) : c = \mathcal{H}(t||m) = \mathcal{H}(y^s g^c || m)$.

Notation: $SPK\{(\alpha) : y = g^\alpha\}(m)$

Building Blocks: 3-Move HVZKPK's cont.

- $PK\{(\alpha, \beta, \gamma) : y_1 = g^\alpha h^\beta \wedge y_2 = g^\alpha h^\gamma\}$
- Let $G = \langle g \rangle = \langle h \rangle$ be \mathcal{Q}_n for some RSA modulus n .

$$PK\{(\alpha, \beta) : y = g^\alpha h^\beta \wedge \ell_1 < \alpha < \ell_2\}$$

This requires S-RSA and some extra care:

- i.e., check that $y, g, h \in \mathcal{Q}_n \subset \mathbb{Z}_n^*$
- RSA modulus n product of two Sophie Germain primes
- if square roots \hat{g} and \hat{h} of g and h are known, e.g.:

If $y = g^x h^r$ then set $\hat{y} = \hat{g}^x \hat{h}^r$ and send \hat{y} to the verifier.

Strong RSA Assumption

The flexible RSA problem: Given an RSA modulus n and a number $z \in \mathbb{Z}_n$ find an $e \geq 2$ and a $u \in \mathbb{Z}_n$ such

$$u^e \equiv z \pmod{n}$$

Strong RSA assumption: solving the flexible RSA problem is hard for big n .

Remember : FACTORING \geq RSA \geq S-RSA

A variation: Given $n, z, w, (x_1, e_1, u_1), \dots, (x_\ell, e_\ell, u_\ell)$, with

$$u_i^{e_i} \pmod{n} \equiv z^{x_i} w \quad \text{and} \quad x_i \in \Gamma, e_i \in \Delta, u_i \in \mathbb{Z}_n,$$

find an $x \in \Gamma, e \in \Delta$ and a $u \in \mathbb{Z}_n$ such that

$$u^e \equiv z^x w \pmod{n} \quad \text{and} \quad (x, e) \neq (x_i, e_i) \quad \forall i = 1, \dots, \ell.$$

Solving this variation is as hard as solving the flexible RSA problem.

Concrete Solution based on S-RSA

Underlying idea:

- Group manager's PK: n, z, w
- Group member's secret key: $x \in \Gamma$
Group member's membership key: $y = z^x \pmod{n}$
- Group member's certificate: u, e s.t. $yw \equiv z^x w \equiv u^e \pmod{n}$
- Generation new membership certificate is as hard as S-RSA if the x 's and e 's are random.

Group's Key Setup

Group/Revocation Manager:

Choose 2 primes p', q' such that $p = 2p' + 1$ and $q = 2q' + 1$ are prime and set $n = pq$. (Thus $|\mathcal{Q}_n| = p'q'$.)

Choose random $\hat{g}, \hat{h}, \hat{z}, \hat{w} \in \mathbb{Z}_n^*$

Choose random $s \in \mathbb{Z}_{p'q'}$ and compute $\hat{y} = \hat{g}^s$.

Choose intervals Γ and Δ .

Publish: $n, \hat{g}, \hat{h}, \hat{z}, \hat{w}, \Gamma$, and Δ and prove that

- n is the product of two Sophie Germain primes
- \hat{h} was chosen at random.

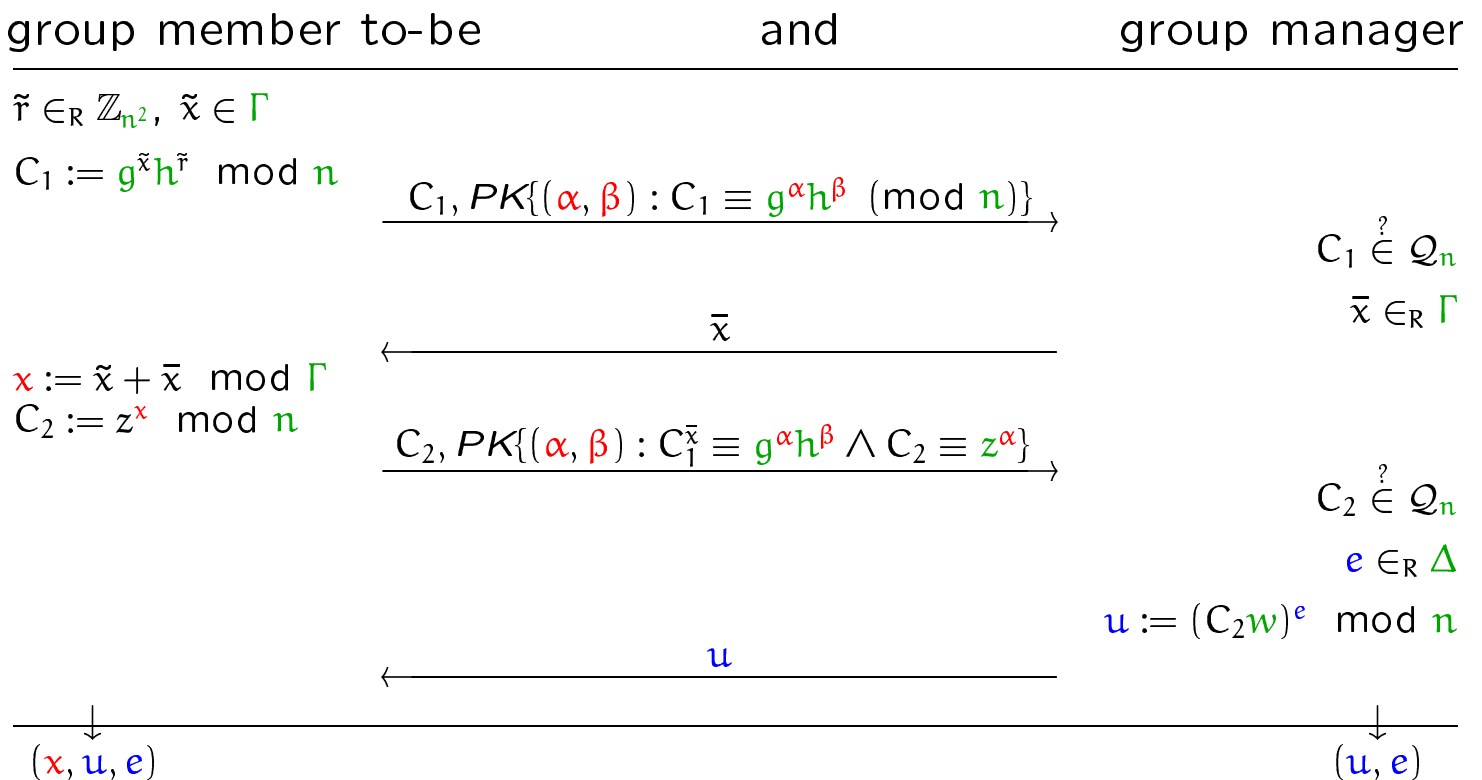
Everybody:

Check $\gcd(\hat{g} \pm 1, n) = \gcd(\hat{h} \pm 1, n) = \gcd(\hat{z} \pm 1, n) = \gcd(\hat{w} \pm 1, n) = 1$.

Set $g := \hat{g}^2, h := \hat{h}^2, z := \hat{z}^2, w := \hat{w}^2, y := \hat{y}^2 \pmod n$

(Thus $\mathcal{Q}_n = \langle g \rangle = \langle h \rangle = \langle z \rangle = \langle w \rangle$)

Becoming a Group Member



Thus: $z^x w \equiv (u)^e \pmod n$.

Signing on Behalf the Group

Given: (e, x, u) such that $z^x w \equiv u^e \pmod{n}$ and message m

Choose $r \in_R \mathbb{Z}_{n-2}$, compute $T_1 = u y^r \pmod{n}$, $T_2 = g^r \pmod{n}$, and the following non-interactive proof

$$\begin{aligned} \sigma = SPK\{(\alpha, \beta, \gamma, \delta) : & w \equiv T_1^\alpha \left(\frac{1}{z}\right)^\beta \left(\frac{1}{y}\right)^\gamma \pmod{n} \wedge \\ & 1 \equiv T_2^\alpha \left(\frac{1}{g}\right)^\gamma \pmod{n} \wedge \\ & T_2 \equiv g^\delta \pmod{n} \wedge \\ & \alpha \in \Gamma \wedge \beta \in \Delta\} (T_1 \| T_2 \| m) . \end{aligned}$$

Signature on m consists of (σ, T_1, T_2) .

What σ Proves

$$T_2 \equiv g^\delta \pmod{n} \quad \Rightarrow \quad \delta \text{ s.t. } T_2 \equiv g^\delta \pmod{n}$$

$$1 \equiv T_2^\alpha \left(\frac{1}{g}\right)^\gamma \pmod{n} \quad \Rightarrow \quad g^\gamma \equiv T_2^\alpha \equiv (g^\delta)^\alpha \pmod{n}$$

$$\Rightarrow \quad \gamma \equiv \delta \alpha \pmod{\varphi(n)}$$

$$w \equiv T_1^\alpha \left(\frac{1}{z}\right)^\beta \left(\frac{1}{y}\right)^\gamma \pmod{n} \quad \Rightarrow \quad z^\beta w \equiv T_1^\alpha \left(\frac{1}{y}\right)^{\delta \alpha} \equiv \left(\frac{T_1}{y^\delta}\right)^\alpha \pmod{n}$$

$$\alpha \in \Gamma \wedge \beta \in \Delta \quad \Rightarrow \quad \left(\beta, \alpha, \frac{T_1}{y^\delta}\right) \text{ is a certificate.}$$

Identifying a Signature's Originator

Revocation manager: $y = g^s$

Given a signature (σ, T_1, T_2) on m , the revocation manager

- checks validity of signature,
- computes $u := \frac{T_1}{T_2^s} \pmod n$,
- computes $PK\{\alpha : y \equiv g^\alpha \pmod n \wedge \frac{T_1}{u} \equiv T_2^\alpha \pmod n\}$.

(Recall $T_1 = u y^r \pmod n$ and $T_2 = g^r \pmod n$)

Security Requirements

- Correctness
- Unforgeability
- Anonymity & Unlinkability
- Exculpability (no framing)
- Traceability

Conclusion

- efficient and secure schemes
- tools for controllable anonymity
- anonymity: now or never
- open problem: efficient scheme based on DL only