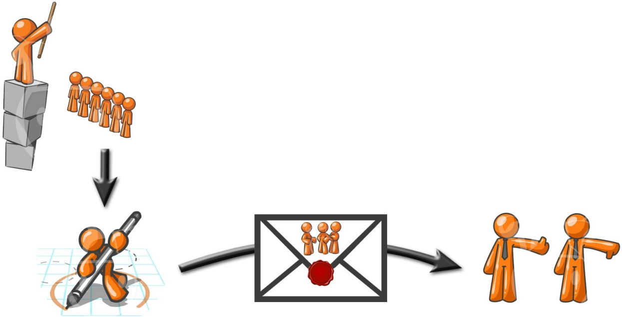
Scalable Group Signature with Revocation

Benoit Libert[1], Thomas Peters[1], Moti Yung[2]

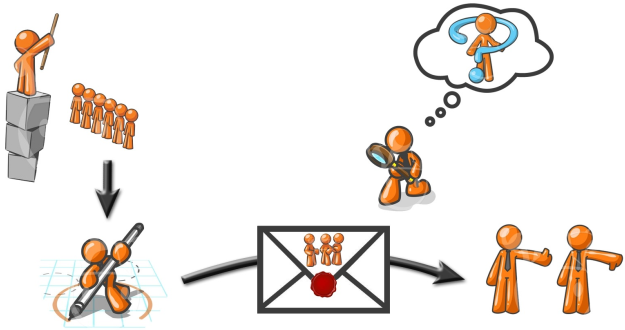
1 - Université catholique de Louvain, Crypto Group (Belgium)
2 - Columbia University and Google Inc. (USA)

Eurocrypt - 18th April 2012

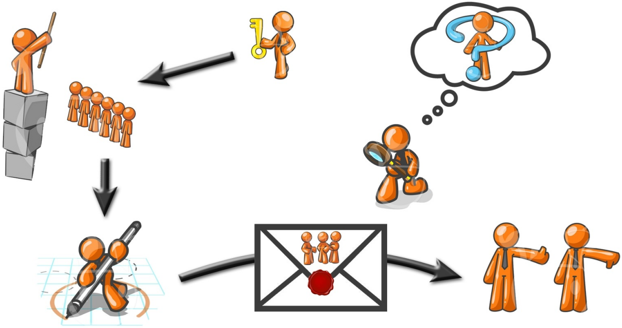
Group Signatures



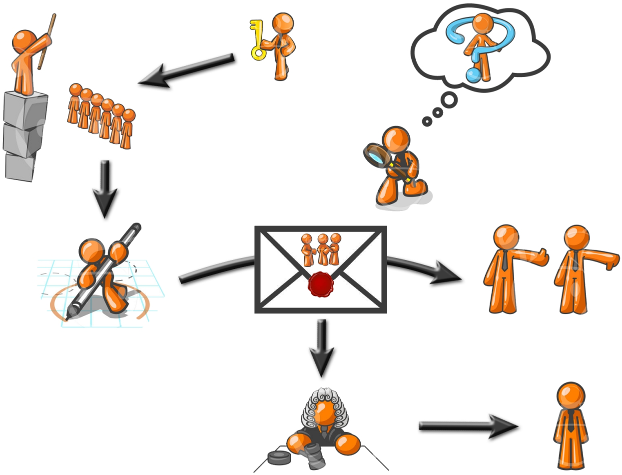
Group Signatures



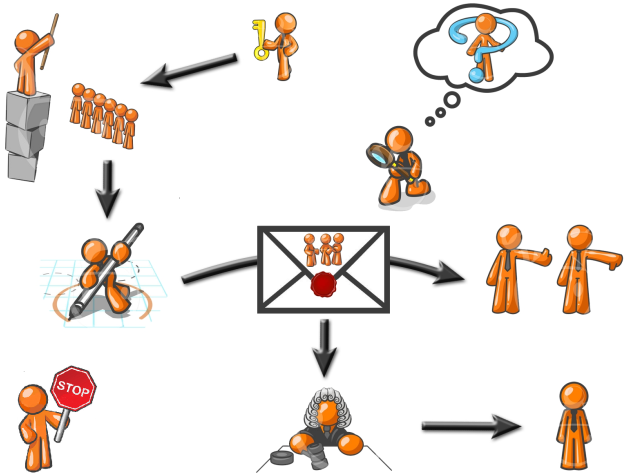
Group Signatures



Group Signatures



Group Signatures



Security Model

Fully anonymous signature on behalf of a group

- Users' signatures are anonymous and unlinkable

Non-misidentification of a group signature

- Infeasibility of producing a signature which traces outside the set of unrevoked corrupted users

Non-frameability of a group signature

- Infeasibility of claiming falsely that a member produced a given signature

Group Signatures

- Chaum-van Heyst (Eurocrypt'91): allow registered group members to sign messages while remaining anonymous
- Ateniese-Camenisch-Joye-Tsudik (Crypto'00): a scalable coalition-resistant construction... but analyzed *w.r.t.* a list of security requirements
- Bellare-Micciancio-Warinschi (Eurocrypt'03): security model; construction based on general assumptions
- Bellare-Shi-Zhang (CT-RSA'05), Kiayias-Yung (J. of Security and Networks 2006): extensions to dynamic groups
- Boyen-Waters (Eurocrypt'06 - PKC'07), Groth (Asiacrypt'06 -'07): in the standard model

Group Signatures

- Chaum-van Heyst (Eurocrypt'91): allow registered group members to sign messages while remaining anonymous
- Ateniese-Camenisch-Joye-Tsudik (Crypto'00): a scalable coalition-resistant construction. . . but analyzed *w.r.t.* a list of security requirements
- Bellare-Micciancio-Warinschi (Eurocrypt'03): security model; construction based on general assumptions
- Bellare-Shi-Zhang (CT-RSA'05), Kiayias-Yung (J. of Security and Networks 2006): extensions to dynamic groups
- Boyen-Waters (Eurocrypt'06 - PKC'07), Groth (Asiacrypt'06 -'07): in the standard model

Group Signatures

- Chaum-van Heyst (Eurocrypt'91): allow registered group members to sign messages while remaining anonymous
- Ateniese-Camenisch-Joye-Tsudik (Crypto'00): a scalable coalition-resistant construction... but analyzed *w.r.t.* a list of security requirements
- Bellare-Micciancio-Warinschi (Eurocrypt'03): security model; construction based on general assumptions
- Bellare-Shi-Zhang (CT-RSA'05), Kiayias-Yung (J. of Security and Networks 2006): extensions to dynamic groups
- Boyen-Waters (Eurocrypt'06 - PKC'07), Groth (Asiacrypt'06 -'07): in the standard model

Revocation in Group Signatures

- Trivial approach: $\mathcal{O}(N-r)$ cost for the GM at *each* revocation
- Bresson-Stern (PKC'01): signature size and signing cost in $\mathcal{O}(r)$
- Brickell and Boneh-Shacham (CCS'04): verifier-local revocations, linear verification in $\mathcal{O}(r)$
- Nakanishi-Fuji-Hira-Funabiki (PKC'09): $\mathcal{O}(1)$-cost signing and verification time but $\mathcal{O}(N)$-size group public keys
- Camenisch-Lysyanskaya (Crypto'02): based on accumulators, optimal asymptotic efficiency but requires users
  - To update their credentials at *every* revocation
  - To know of all changes in the population of the group

Revocation in Group Signatures

- Trivial approach: $\mathcal{O}(N - r)$ cost for the GM at *each* revocation
- Bresson-Stern (PKC'01): signature size and signing cost in $\mathcal{O}(r)$
- Brickell and Boneh-Shacham (CCS'04): verifier-local revocations, linear verification in $\mathcal{O}(r)$
- Nakanishi-Fuji-Hira-Funabiki (PKC'09): $\mathcal{O}(1)$-cost signing and verification time but $\mathcal{O}(N)$-size group public keys
- Camenisch-Lysyanskaya (Crypto'02): based on accumulators, optimal asymptotic efficiency but requires users
  - To update their credentials at *every* revocation
  - To know of all changes in the population of the group

Current Situation

Despite 20 years of research

- No system has a mechanism where the revocation is truly scalable (contrast with CRLs in regular signatures)
- Situation is only worse in schemes in the standard model (e.g., pairing-based accumulators do not always scale well)

We take a different approach

- Develop a revocation technique inspired by broadcast encryption!
- Start from an existing revocation structure an adapt it (algebraically) in the group signature scenario

Current Situation

Despite 20 years of research

- No system has a mechanism where the revocation is truly scalable (contrast with CRLs in regular signatures)
- Situation is only worse in schemes in the standard model (e.g., pairing-based accumulators do not always scale well)

We take a different approach

- Develop a revocation technique inspired by broadcast encryption!
- Start from an existing revocation structure an adapt it (algebraically) in the group signature scenario

Contributions

Scalable Group Signature with Revocation

Features

- History-independent revocation/verification
- Provable in the standard model (*i.e.*, *no random oracle*)

Efficiency

- Signature size / Verification cost in $\mathcal{O}(1)$
- Revocation list of size $\mathcal{O}(r)$ as in standard PKIs
- All other algorithms at most poly-log in N

Contributions

Scalable Group Signature with Revocation

Features

- History-independent revocation/verification
- Provable in the standard model (*i.e.*, *no random oracle*)

Efficiency

- Signature size / Verification cost in $\mathcal{O}(1)$
- Revocation list of size $\mathcal{O}(r)$ as in standard PKIs
- All other algorithms at most poly-log in N

Contributions

Scalable Group Signature with Revocation

Features

- History-independent revocation/verification
- Provable in the standard model (*i.e.*, *no random oracle*)

Efficiency

- Signature size / Verification cost in $\mathcal{O}(1)$
- Revocation list of size $\mathcal{O}(r)$ as in standard PKIs
- All other algorithms at most poly-log in N

Contributions

Scalable Group Signature with Revocation

Features

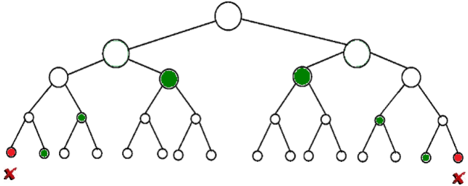
- History-independent revocation/verification
- Provable in the standard model (*i.e.*, *no random oracle*)

Efficiency

- Signature size / Verification cost in $\mathcal{O}(1)$
- Revocation list of size $\mathcal{O}(r)$ as in standard PKIs
- All other algorithms at most poly-log in N

New Approach

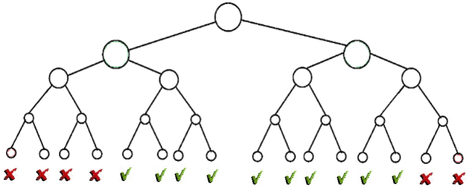
Using the Naor-Naor-Lotspiech framework (Crypto'01):



- Broadcast (symmetric) encryption/revocation
  - Public-key variant due to Dodis-Fazio (DRM'02)
- Members are assigned to a leaf and belong to several subsets
- *Subset Cover:* find a cover $S_1, \ldots, S_m$ of the unrevoked set $N \backslash R$

New Approach

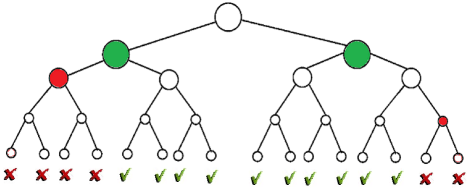
Using NNL in the public-key setting (Dodis-Fazio, DRM'02):



- *Subset Difference* (SD) method
  - Each S_i is the difference between two subtrees
  - Uses Hierarchical Identity-Based Encryption (HIBE): each node obtains a decryption key from its father
  - $\mathcal{O}(r)$-size ciphertexts and $\mathcal{O}(\log^3 N)$ private keys

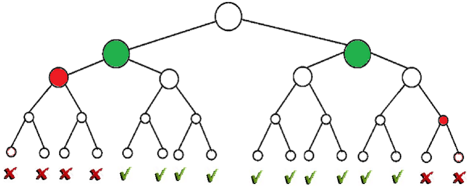
New Approach

Using NNL in the public-key setting (Dodis-Fazio, DRM'02):



- *Subset Difference* (SD) method
  - Each S_i is the difference between two subtrees
  - Uses Hierarchical Identity-Based Encryption (HIBE): each node obtains a decryption key from its father
  - $\mathcal{O}(r)$-size ciphertexts and $\mathcal{O}(\log^3 N)$ private keys

NNL-Based Revocation in Group Signatures



- Broadcast encryption ciphertext is turned into a revocation list RL

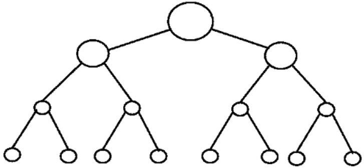
  $\Rightarrow$ RL is a set of HIBE ciphertexts $C_1, \ldots, C_m$

- Signers prove their non-revocation in 3 steps

  1. Commit to the HIBE ciphertext C_i they can decrypt
  2. Prove that $C_i \in RL$ (set membership proof)
  3. Prove their ability to decrypt the committed C_i

Construction Overview

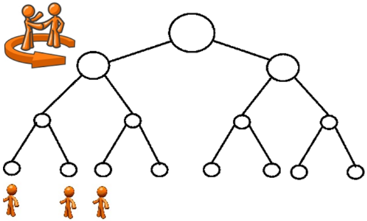
Naor-Naor-Lotspiech framework... Revocable Group Signature?



- JOIN: new user $\mathcal{U}$ with identity $X\,(= g^x)$
  - $\mathsf{Cert}(\mathcal{U}) = (\sigma_0 = \mathsf{Sign}(X, D_0), \ldots, \sigma_l = \mathsf{Sign}(X, D_l))$
- REVOKE: group manager GM finds a *"subset cover"*
  - $\mathcal{RL}(T = g^t) = (\mathsf{Sign}(C_1, T), \mathsf{Sign}(C_2, T), \mathsf{Sign}(C_3, T))$

Construction Overview

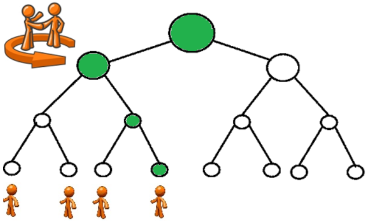
Naor-Naor-Lotspiech framework... Revocable Group Signature?



- JOIN: new user $\mathcal{U}$ with identity $X\,(=g^x)$
  - $\mathsf{Cert}(\mathcal{U}) = (\sigma_0 = \mathsf{Sign}(X, D_0), \ldots, \sigma_l = \mathsf{Sign}(X, D_l))$
- REVOKE: group manager GM finds a *"subset cover"*
  - $\mathcal{RL}(T = g^t) = (\mathsf{Sign}(C_1, T), \mathsf{Sign}(C_2, T), \mathsf{Sign}(C_3, T))$

Construction Overview

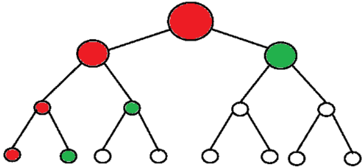
Naor-Naor-Lotspiech framework... Revocable Group Signature?



- JOIN: new user $\mathcal{U}$ with identity $X\,(= g^x)$
  - $\mathsf{Cert}(\mathcal{U}) = \big(\sigma_0 = \mathsf{Sign}(X, D_0), \ldots, \sigma_l = \mathsf{Sign}(X, D_l)\big)$
- REVOKE: group manager GM finds a *"subset cover"*
  - $\mathcal{RL}(T = g^t) = \big(\mathsf{Sign}(C_1, T), \mathsf{Sign}(C_2, T), \mathsf{Sign}(C_3, T)\big)$

Construction Overview

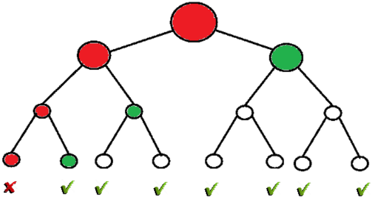
Naor-Naor-Lotspiech framework... Revocable Group Signature?



- JOIN: new user $\mathcal{U}$ with identity $X\,(= g^x)$
  - $\text{Cert}(\mathcal{U}) = \big(\sigma_0 = \text{Sign}(X, D_0), \ldots, \sigma_l = \text{Sign}(X, D_l)\big)$
- REVOKE: group manager GM finds a *"subset cover"*
  - $\mathcal{RL}(T = g^t) = \big(\text{Sign}(C_1, T), \text{Sign}(C_2, T), \text{Sign}(C_3, T)\big)$

Construction Overview

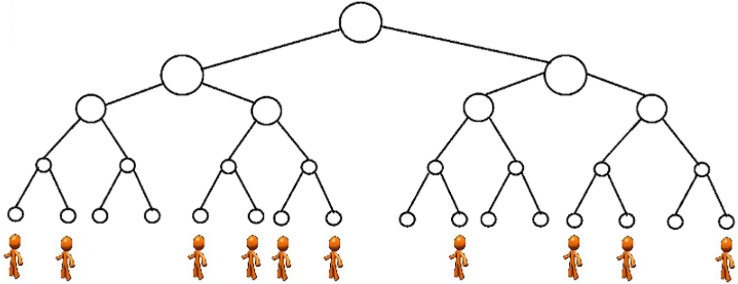
Naor-Naor-Lotspiech framework... Revocable Group Signature?



- JOIN: new user $\mathcal{U}$ with identity $X\,(= g^x)$
  - $\mathsf{Cert}(\mathcal{U}) = \big(\sigma_0 = \mathsf{Sign}(X, D_0), \ldots, \sigma_l = \mathsf{Sign}(X, D_l)\big)$
- REVOKE: group manager GM finds a *"subset cover"*
  - $\mathcal{RL}(T = g^t) = \big(\mathsf{Sign}(C_1, T), \mathsf{Sign}(C_2, T), \mathsf{Sign}(C_3, T)\big)$

Construction Overview

[NNL] *Subset Difference:*



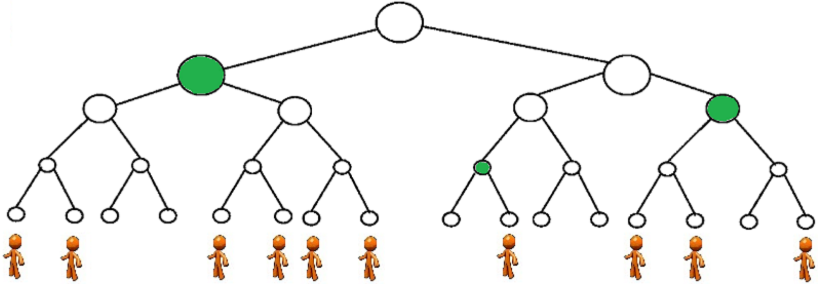
- REVOKE: GM computes for all subset $1 \leq i \leq m$

$$\sigma_i' = \mathrm{Sign}_{\mathsf{AHO}}\left(g^{\mathsf{time}}, C^{(i)}_{\mathsf{HIBE}}(\mathsf{node}_i, \mathsf{node}_i)\right)$$

$\Rightarrow \mathcal{RL}_t$ is a NNL encryption consisting of $\mathcal{O}(r)$ HIBE ciphertexts

Construction Overview

[NNL] *Subset Difference:*



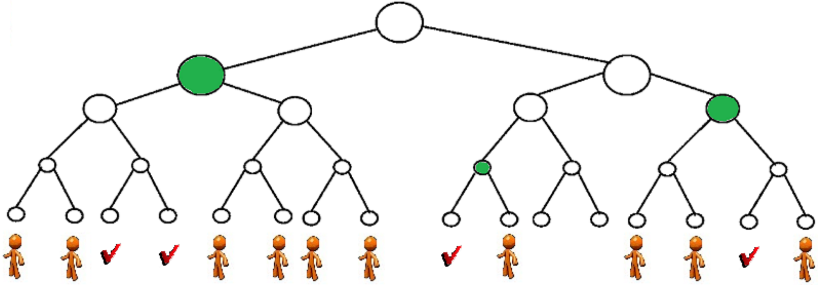
- REVOKE: GM computes for all subset $1 \leq i \leq m$

$$\sigma_i' = \mathrm{Sign}_{\mathrm{AHO}}\left(g^{\mathrm{time}}, C_{\mathrm{HIBE}}^{(i)}(\mathrm{node}_i, \mathrm{node}_l)\right)$$

$\Rightarrow \mathcal{RL}_t$ is a NNL encryption consisting of $\mathcal{O}(r)$ HIBE ciphertexts

Construction Overview

[NNL] *Subset Difference:*



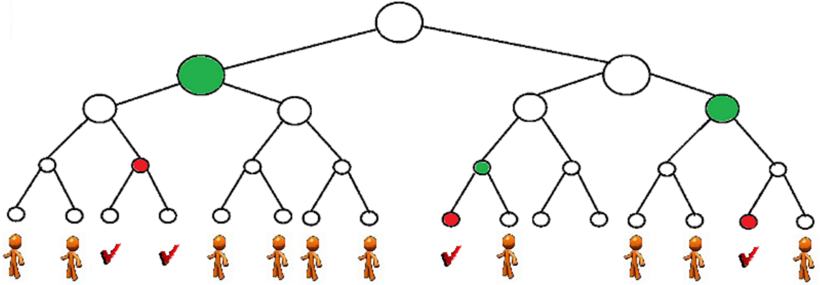
- REVOKE: GM computes for all subset $1 \leq i \leq m$

$$\sigma'_i = \mathsf{Sign}_{\mathsf{AHO}}\left(g^{\mathsf{time}}, C^{(i)}_{\mathsf{HIBE}}(\mathsf{node}_i, \mathsf{node}_i)\right)$$

$\Rightarrow \mathcal{RL}_t$ is a NNL encryption consisting of $\mathcal{O}(r)$ HIBE ciphertexts

Construction Overview

[NNL] *Subset Difference:*



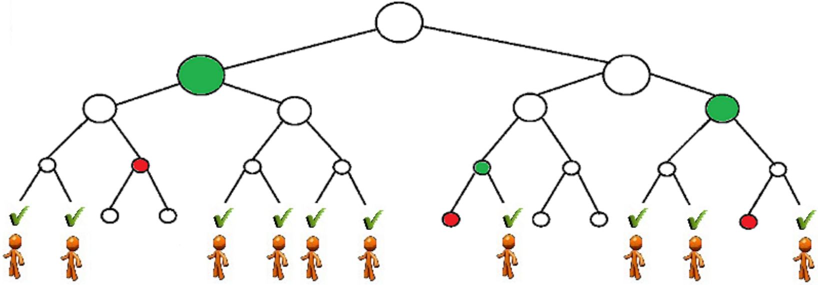
- REVOKE: GM computes for all subset $1 \leq i \leq m$

$$\sigma'_i = \text{Sign}_{\text{AHO}}\left(g^{\text{time}}, C^{(i)}_{\text{HIBE}}(\text{node}_i, \text{node}_i)\right)$$

$\Rightarrow \mathcal{RL}_t$ is a NNL encryption consisting of $\mathcal{O}(r)$ HIBE ciphertexts

Construction Overview

[NNL] *Subset Difference:*



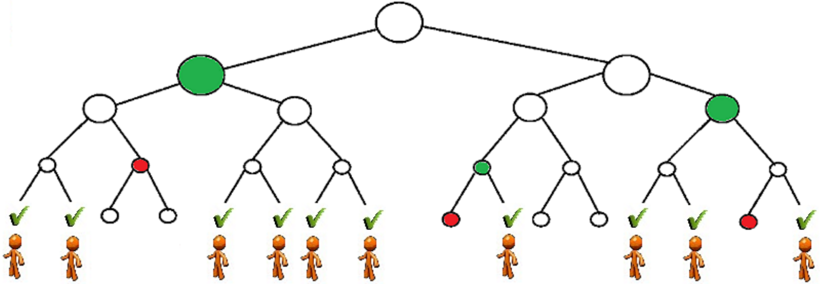
- REVOKE: GM computes for all subset $1 \leq i \leq m$

$$\sigma_i' = \mathrm{Sign}_{\mathrm{AHO}}\left(g^{\mathrm{time}}, C_{\mathrm{HIBE}}^{(i)}(\mathrm{node}_i, \mathrm{node}_i)\right)$$

$\Rightarrow \mathcal{RL}_t$ is a NNL encryption consisting of $\mathcal{O}(r)$ HIBE ciphertexts

Construction Overview

[NNL] *Subset Difference:*



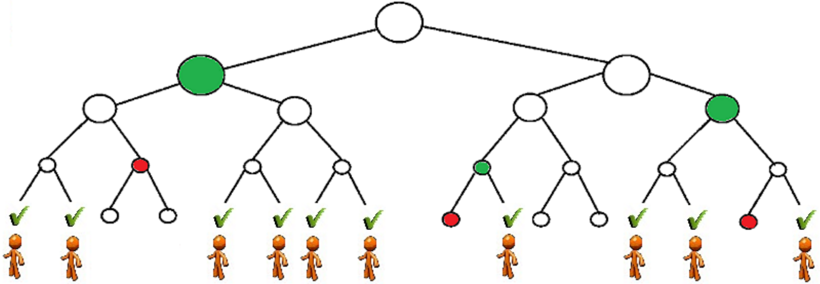
- REVOKE: GM computes for all subset $1 \leq i \leq m$

$$\sigma_i' = \mathsf{Sign}_{\mathsf{AHO}}\left(g^{\mathsf{time}}, C_{\mathsf{HIBE}}^{(i)}(\mathsf{node}_i, \mathsf{node}_i)\right)$$

$\Rightarrow \mathcal{RL}_t$ is a NNL encryption consisting of $\mathcal{O}(r)$ HIBE ciphertexts

Construction Overview

[NNL] *Subset Difference:*



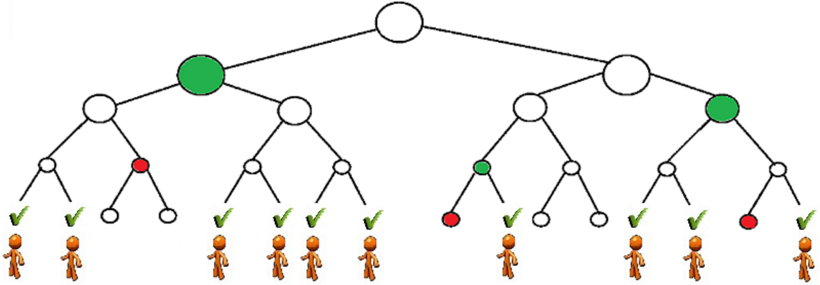
- REVOKE: GM computes for all subset $1 \leq i \leq m$

$$\sigma'_i = \mathsf{Sign}_{\mathsf{AHO}}\left(g^{\mathsf{time}}, C^{(i)}_{\mathsf{HIBE}}(\mathsf{node}_i, \mathsf{node}_i)\right)$$

$\Rightarrow \mathcal{RL}_t$ is a NNL encryption consisting of $\mathcal{O}(r)$ HIBE ciphertexts

Construction Overview

[NNL] *Subset Difference:*



- REVOKE: GM computes for all subset $1 \leq i \leq m$

$$\sigma'_i = \mathsf{Sign}_{\mathsf{AHO}}\Big(g^{\mathsf{time}}, C^{(i)}_{\mathsf{HIBE}}(\mathsf{node}_i, \mathsf{node}_i)\Big)$$

$\Rightarrow \mathcal{RL}_t$ is a NNL encryption consisting of $\mathcal{O}(r)$ HIBE ciphertexts

Construction Overview

SIGN: unrevoked $\mathcal{U}$ combines the following techniques

Our NNL-based proofs of non-revocation

- Commit to his related HIBE ciphertext $C_{\mathsf{HIBE}}^{(i^*)}$
  Boneh-Boyen-Goh (Eurocrypt'05): $\mathcal{O}(1)$-size HIBE ciphertexts
- Set membership $C_{\mathsf{HIBE}}^{(i^*)} \in \mathcal{RL}_{\mathsf{t}}$ + ability to decrypt $C_{\mathsf{HIBE}}^{(i^*)}$
  Abe-Haralambiev-Ohkubo (Crypto'10): structure-preserving sign

Groth's signing technique (Asiacrypt'07)

- One-time signatures, weak Boneh-Boyen signatures
  CCA-secure tag-based encryption and Groth-Sahai proofs.

Construction Overview

SIGN: unrevoked $\mathcal{U}$ combines the following techniques

Our NNL-based proofs of non-revocation

- Commit to his related HIBE ciphertext $C_{\mathsf{HIBE}}^{(i^*)}$
  Boneh-Boyen-Goh (Eurocrypt'05): $\mathcal{O}(1)$-size HIBE ciphertexts
- Set membership $C_{\mathsf{HIBE}}^{(i^*)} \in \mathcal{RL}_{\mathsf{t}}$ + ability to decrypt $C_{\mathsf{HIBE}}^{(i^*)}$
  Abe-Haralambiev-Ohkubo (Crypto'10): structure-preserving sign

Groth's signing technique (Asiacrypt'07)

- One-time signatures, weak Boneh-Boyen signatures
  CCA-secure tag-based encryption and Groth-Sahai proofs.

Construction Overview

SIGN: unrevoked $\mathcal{U}$ combines the following techniques

Our NNL-based proofs of non-revocation

- Commit to his related HIBE ciphertext $C_{\mathsf{HIBE}}^{(i^*)}$
  Boneh-Boyen-Goh (Eurocrypt'05): $\mathcal{O}(1)$-size HIBE ciphertexts
- Set membership $C_{\mathsf{HIBE}}^{(i^*)} \in \mathcal{RL}_{\mathsf{t}}$ + ability to decrypt $C_{\mathsf{HIBE}}^{(i^*)}$
  Abe-Haralambiev-Ohkubo (Crypto'10): structure-preserving sign

Groth's signing technique (Asiacrypt'07)

- One-time signatures, weak Boneh-Boyen signatures
  CCA-secure tag-based encryption and Groth-Sahai proofs.

Security

Theorem

The scheme provides security if all these problems are hard

1. *The q-***SFP Problem***: given* $(g_z, h_z, g_r, h_r, a, \tilde{a}, b, \tilde{b}) \in \mathbb{G}^8$ *and tuples* $\{(z_j, r_j, s_j, t_j, u_j, v_j, w_j)\}_{j=1}^{q}$ *s.t.*

$$\begin{aligned} e(a, \tilde{a}) &= e(g_z, z_j) \cdot e(g_r, r_j) \cdot e(s_j, t_j) \\ e(b, \tilde{b}) &= e(h_z, z_j) \cdot e(h_r, u_j) \cdot e(v_j, w_j) \end{aligned}$$

   find a new such tuple $(z^\star, r^\star, s^\star, t^\star, u^\star, v^\star, w^\star)$ *with* $z^\star \neq 1_{\mathbb{G}}$

2. *The q-***Strong Diffie-Hellman Problem***: given* $(g, g^a, \ldots, g^{(a^q)})$ *with* $a \stackrel{R}{\leftarrow} \mathbb{Z}_p$*, find a pair* $(g^{1/(a+s)}, s) \in \mathbb{G} \times \mathbb{Z}_p$

3. *The* **Decision Linear Problem***: given* $(g^a, g^b, g^{ac}, g^{bd}, \eta)$*, decide whether* $\eta = g^{c+d}$ *or* $\eta \in_R \mathbb{G}$

Efficiency of the SD-Based Scheme

Asymptotic Complexity

- $\mathcal{O}(1)$-size signatures and $\mathcal{O}(1)$ verification time
- $\mathcal{O}(r)$-size revocation lists at each period as in standard PKIs
- $\mathcal{O}(\log N)$-size group public keys
- $\mathcal{O}(\log^3 N)$-size membership certificates

Concretely at the 128-bit security level

- Each signature takes 6 kB (for 512-bit element representation)

Thank you!