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-Micciiancio-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: $O(N - r)$ cost for the GM at *each* revocation

- Bresson-Stern (PKC’01): signature size and signing cost in $O(r)$

- Brickell and Boneh-Shacham (CCS’04): verifier-local revocations, linear verification in $O(r)$

- Nakanishi-Fuji-Hira-Funabiki (PKC’09): $O(1)$-cost signing and verification time but $O(N)$-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
Revocable Group Signature - Eurocrypt’12

Revocation in Group Signatures

- Trivial approach: $O(N - r)$ cost for the GM at each revocation
- Bresson-Stern (PKC’01): signature size and signing cost in $O(r)$
- Brickell and Boneh-Shacham (CCS’04): verifier-local revocations, linear verification in $O(r)$
- Nakanishi-Fuji-Hira-Funabiki (PKC’09): $O(1)$-cost signing and verification time but $O(N)$-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 and 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 and 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 $O(1)$
- Revocation list of size $O(r)$ 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 $O(1)$
- Revocation list of size $O(r)$ 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 $O(1)$
- Revocation list of size $O(r)$ 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 \((i.e., \text{no random oracle})\)

Efficiency

- Signature size / Verification cost in \(O(1)\)
- Revocation list of size \(O(r)\) as in standard PKIs
- All other algorithms at most poly-log in \(N\)
Using the Naor-Naor-Lotspeich 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 $N \setminus R$
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
  - $O(r)$-size ciphertexts and $O(\log^3 N)$ 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 $U$ with identity $X (= g^x)$
  - $\text{Cert}(U) = (\sigma_0 = \text{Sign}(X, D_0), \ldots, \sigma_l = \text{Sign}(X, D_l))$

- **REVOKE**: group manager GM finds a “subset cover”
  - $RL(T = g^t) = (\text{Sign}(C_1, T), \text{Sign}(C_2, T), \text{Sign}(C_3, T))$
Construction Overview

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

- **JOIN**: new user $\mathcal{U}$ with identity $X (= g^x)$
  - $\text{Cert}(\mathcal{U}) = (\sigma_0 = \text{Sign}(X, D_0), \ldots, \sigma_l = \text{Sign}(X, D_l))$

- **REVOKE**: group manager GM finds a “subset cover”
  - $\mathcal{RL}(T = g^t) = (\text{Sign}(C_1, T), \text{Sign}(C_2, T), \text{Sign}(C_3, T))$
Construction Overview

Naor-Naor-Lots piech framework... Revocable Group Signature?

- **JOIN**: new user $\mathcal{U}$ with identity $X = g^x$
  - $\text{Cert} (\mathcal{U}) = (\sigma_0 = \text{Sign}(X, D_0), \ldots, \sigma_l = \text{Sign}(X, D_l))$

- **REVOKE**: group manager GM finds a “subset cover”
  - $\mathcal{R}\mathcal{L}(T = g^t) = (\text{Sign}(C_1, T), \text{Sign}(C_2, T), \text{Sign}(C_3, T))$
Construction Overview

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

- **JOIN**: new user \( U \) with identity \( X = g^x \)
  - \( \text{Cert}(U) = (\sigma_0 = \text{Sign}(X, D_0), \ldots, \sigma_l = \text{Sign}(X, D_l)) \)

- **REVOKE**: group manager GM finds a "subset cover"
  - \( RL(T = g^t) = (\text{Sign}(C_1, T), \text{Sign}(C_2, T), \text{Sign}(C_3, T)) \)
**Construction Overview**

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

- **JOIN**: new user $U$ with identity $X (= g^x)$
  - $\text{Cert}(U) = (\sigma_0 = \text{Sign}(X, D_0), \ldots, \sigma_l = \text{Sign}(X, D_l))$

- **REVOKE**: group manager GM finds a "subset cover"
  - $\mathcal{RL}(T = g^t) = (\text{Sign}(C_1, T), \text{Sign}(C_2, T), \text{Sign}(C_3, T))$
Construction Overview

[NNL] Subset Difference:

- **REVOKE:**
  
  \[ \sigma'_i = \text{Sign}_{AHO} \left( g^\text{time}, C^{(i)}_{\text{HIBE}}(\text{node}_i, \text{node}_j) \right) \]

  \[ \Rightarrow RL_i \text{ is a NNL encryption consisting of } O(r) \text{ HIBE ciphertexts} \]
Construction Overview

[NNL] Subset Difference:

- **Revoke**: GM computes for all subset \(1 \leq i \leq m\)
  \[
  \sigma'_i = \text{Sign}_{AHO}(g^{\text{time}}, C^{(i)}_{\text{HIBE}}(\text{node}_i, \text{node}_f))
  \]
  \(\Rightarrow RL_t\) is a NNL encryption consisting of \(O(r)\) HIBE ciphertexts.
Construction Overview

[NNL] Subset Difference:

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

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

  $\Rightarrow RCL^i$ is a NNL encryption consisting of $O(r)$ HIBE ciphertexts
Construction Overview

[NNL] Subset Difference:

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

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

  \Rightarrow RL_t is a NNL encryption consisting of $O(r)$ HIBE ciphertexts
Construction Overview

[NNL] Subset Difference:

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

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

  $\Rightarrow R_{CL_t}$ is a NNL encryption consisting of $O(r)$ HIBE ciphertexts
Construction Overview

**NNL** Subset Difference:

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

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

  \Rightarrow RL_t \text{ is a NNL encryption consisting of } O(r) \text{ HIBE ciphertexts}
[NNL] Subset Difference:

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

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

  $\Rightarrow RL_t$ is a NNL encryption consisting of $O(r)$ HIBE ciphertexts
Construction Overview

[NNL] Subset Difference:

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

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

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


**Construction Overview**

**Sign:** unrevoked $U$ combines the following techniques

Our NNL-based proofs of non-revocation

- Commit to his related HIBE ciphertext $C^{(i^*)}_{\text{HIBE}}$
  Boneh-Boyen-Goh (Eurocrypt’05): $\mathcal{O}(1)$-size HIBE ciphertexts

- Set membership $C^{(i^*)}_{\text{HIBE}} \in \mathcal{RL}_t$ + ability to decrypt $C^{(i^*)}_{\text{HIBE}}$
  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 $C_{\text{HIBE}}^{(i^*)}$
  Boneh-Boyen-Goh (Eurocrypt’05): $\mathcal{O}(1)$-size HIBE ciphertexts

- Set membership $C_{\text{HIBE}}^{(i^*)} \in \mathcal{RL}_t$ + ability to decrypt $C_{\text{HIBE}}^{(i^*)}$
  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 $U$ combines the following techniques

Our NNL-based proofs of non-revocation

- Commit to his related HIBE ciphertext $C_{HIBE}^{(i^*)}$
  Boneh-Boyen-Goh (Eurocrypt’05): $O(1)$-size HIBE ciphertexts

- Set membership $C_{HIBE}^{(i^*)} \in RL_t +$ ability to decrypt $C_{HIBE}^{(i^*)}$
  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

- **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.
  
  \[
  e(a, \tilde{a}) = e(g_z, z_j) \cdot e(g_r, r_j) \cdot e(s_j, t_j) \\
  e(b, \tilde{b}) = e(h_z, z_j) \cdot e(h_r, u_j) \cdot e(v_j, w_j)
  \]

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

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

- **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

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

Concretely at the 128-bit security level

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