Group Signatures with Almost-for-free Revocation

Benoît Libert[1] Thomas Peters[1] Moti Yung[2]

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

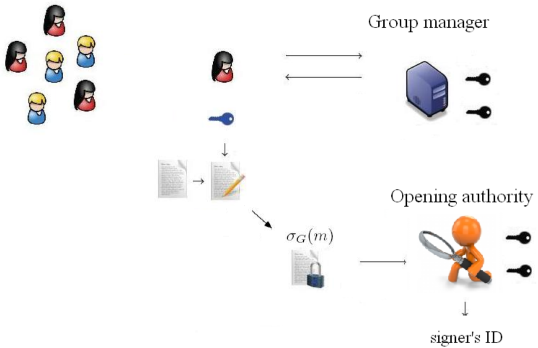
Santa Barbara,
August 22, 2012

Outline

1. Introduction
   - Background and Prior Work
   - The Revocation Problem
2. NNL-Based Revocation in Group Signatures
   - Description and Efficiency Analysis
3. Our Contribution: Construction with Short Private Keys
   - Overview of the Scheme
   - Efficiency and Security Analysis

Group Signatures

- Group members anonymously and accountably sign messages on behalf of a group (Chaum-Van Heyst, 1991)



- Applications in trusted computing platforms, auction protocols, ...

Security Properties

Full anonymity of signatures

- Users' signatures are anonymous and unlinkable

Security against misidentification attacks

- 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): introduction of the primitive
- 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

Current Situation

So far, 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., accumulator-based approaches do not always scale well)

Recent approach (Libert-Peters-Yung; Eurocrypt 2012):

- Revocation mechanism based on broadcast encryption
- Starts from a revocation structure and adapt it (algebraically) in the group signature scenario

NNL-Based Revocation in Group Signatures

Features of our approach (Eurocrypt'12)

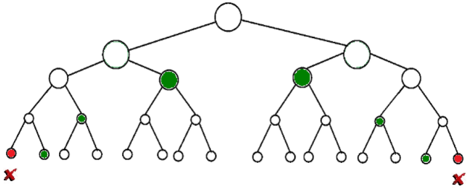
- History-independent revocation / verification
- Provable in the standard model (*i.e.*, *no random oracle*)

Efficiency:

- Signature size / Verification cost in $\mathcal{O}(1)$
- Revocation list of size $\mathcal{O}(r)$ as in standard PKIs
- At most $\mathcal{O}(\mathrm{polylog}\ N)$ complexity elsewhere
- **Disadvantage**: membership certificates of size $\mathcal{O}(\log^3 N)$

NNL-Based Revocation in Group Signatures

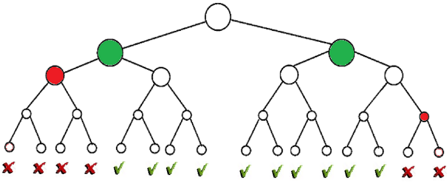
Using the Naor-Naor-Lotspiech framework (Crypto'01):



- Broadcast (symmetric) encryption / revocation
- Users are assigned to a leaf
- *Subset Cover:* find a cover $S_1, \ldots, S_m$ of the unrevoked set $\mathcal{N} \backslash \mathcal{R}$ and compute an encryption for each S_i

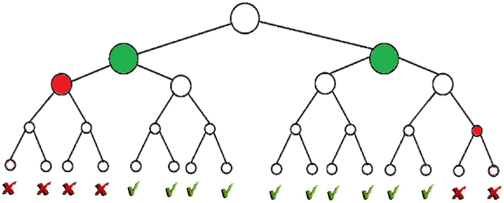
NNL-Based Revocation in Group Signatures

- Subset Difference (SD) method: each S_i is the difference between two subtrees; $m = \mathcal{O}(r)$ subsets are needed in the partition



- Public-key variant of NNL (Dodis-Fazio, DRM'02)
  - SD method uses Hierarchical Identity-Based Encryption (HIBE)
  - $\mathcal{O}(r)$-size ciphertexts and $\mathcal{O}(\log^3 N)$ private keys
  - Improvements (Halevy-Shamir, Crypto'02) give $\mathcal{O}(\log^{2+\epsilon} N)$-size 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 $C_1, \ldots, C_m$

- Signer shows the ability to decrypt *one* of these HIBE ciphertexts
  - Proof that he can decrypt a committed C_i, which is in the RL
  - Can be achieved with $\mathcal{O}(1)$-size signatures

NNL-Based Revocation in Group Signatures

- Using HIBE and the public-key NNL entails membership certificates of size $\mathcal{O}(\log^3 N)$.

  $\Rightarrow$ Important overhead w.r.t. schemes without revocation and ordinary signatures

  e.g., for $N = 1000$, private keys may contain > 1000 elements

- **This paper**: getting competitive with ordinary group signatures
  - $\mathcal{O}(1)$-size membership certificates in the NNL framework
  - Carrying out all operations in constant time

- How is it possible? $\mathcal{O}(\log N)$ dependency seems inevitable with a tree-based approach.

Construction with Short Private Keys

- Uses *concise* vector commitments (Libert-Yung, TCC 2010):

  Constant-size commitments to $(m_1, \ldots, m_\ell)$ that can be opened for individual coordinates $i \in \{1, \ldots, \ell\}$ using *short* openings

- Commitments to vectors of dimension $\ell = \log N$ are included in membership certificates

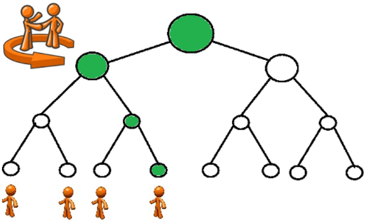
- Signatures prove properties about individual coordinates

  $\Rightarrow$ *Concise* openings give us constant-size signatures

- The "essential" $\mathcal{O}(\log N)$ factor is pushed to the public key size only!

Construction with Short Private Keys

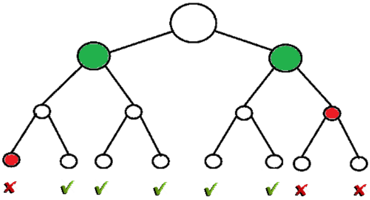
Combination of the SD method and vector commitments



- Each member is assigned to a leaf v and obtains a signature on C where $C = g_\ell^{I_1} \cdots g_1^{I_\ell}$ is a commitment to the path $I_1, \ldots, I_\ell$ to v
- $\mathcal{RL}$ encodes a cover $\{S_1, \ldots, S_m\}$ and specifies two node identifiers (L_{j,i_1}, L_{j,i_2}), with $i_1, i_2 \in \{1, \ldots, \ell\}$, for each S_j
- Unrevoked members prove their belonging to one of the S_j's by proving that $(I_1, \ldots, I_\ell)$ satisfies $I_{i_1} = L_{j,i_1}$ and $I_{i_2} \neq L_{j,i_2}$

Construction with Short Private Keys

Combination of the SD method and vector commitments



- Each member is assigned to a leaf v and obtains a signature on C where $C = g_\ell^{I_1} \cdots g_1^{I_\ell}$ is a commitment to the path $I_1, \ldots, I_\ell$ to v
- $\mathcal{RL}$ encodes a cover $\{S_1, \ldots, S_m\}$ and specifies two node identifiers (L_{j,i_1}, L_{j,i_2}), with $i_1, i_2 \in \{1, \ldots, \ell\}$, for each S_j
- Unrevoked members prove their belonging to one of the S_j's by proving that $(I_1, \ldots, I_\ell)$ satisfies $I_{i_1} = L_{j,i_1}$ and $I_{i_2} \neq L_{j,i_2}$

Efficiency Outcome

- Complexity is essentially optimal
  - $\mathcal{O}(1)$-size signatures and $\mathcal{O}(1)$ signing / verification time
  - $\mathcal{O}(r)$-size revocation lists at each period as in standard PKIs
  - $\mathcal{O}(\log N)$-size group public keys
  - $\mathcal{O}(1)$-size membership certificates
- Concrete signature length:
  - 144 group elements, or about 9 kB at the 128-bit security level
    Only 3 times as long as Groth's group signatures (Asiacrypt'07)

Security

- Security is proved under the same assumptions as in Eurocrypt'12 and an extra assumption (for $q = \mathcal{O}(\log N)$):

  The q-**Flexible Diffie-Hellman Exponent Problem**: given $(g, g_1, \ldots, g_q, g_{q+2}, \ldots, g_{2q})$ with $g_i = g^{(\alpha^i)}$, find a non-trivial triple $(g^\mu, g_{q+1}^\mu, g_{2q}^\mu) \in (\mathbb{G} \backslash \{1_\mathbb{G}\})^3$

- At the expense of $O(\log^2 N)$-size public keys, the Catalano-Fiore commitment allows using a weaker assumption:

  The **Flexible Squared Diffie-Hellman Problem**: given (g, g^a), find a non-trivial triple $(g^\mu, g^{a \cdot \mu}, g^{(a^2) \cdot \mu}) \in (\mathbb{G} \backslash \{1_\mathbb{G}\})^3$.

Conclusion

- Revocable schemes are now competitive with ordinary group signatures: only overhead is a $\mathcal{O}(\log N)$-size group public key
- Our revocation approach
  - Allows security proofs in the standard model
  - Applies in other settings: traceable signatures, anonymous credentials, ...
- Open problem: weakening the hardness assumptions without degrading the efficiency
  - Alternative construction relies on weaker assumptions but has $\mathcal{O}(\log^2 N)$-size public keys. Can we avoid this?

Thanks!