Group Signatures with Message-Dependent Opening in the Standard Model

Benoît Libert ▪ Marc Joye

technicolor

Group Signatures with Message-Dependent Opening in the Standard Model

Benoît Libert · Marc Joye

Outline

1 Background

- Group signatures: applications, history
- Group signatures with Message Dependent Opening
- The problem: GS-MDO in the standard model

2 Our results

- A partially structure-preserving IBE
- Construction of a GS-MDO scheme
- Security results

technicolor

Outline

1 Background

- Group signatures: applications, history
- Group signatures with Message Dependent Opening
- The problem: GS-MDO in the standard model

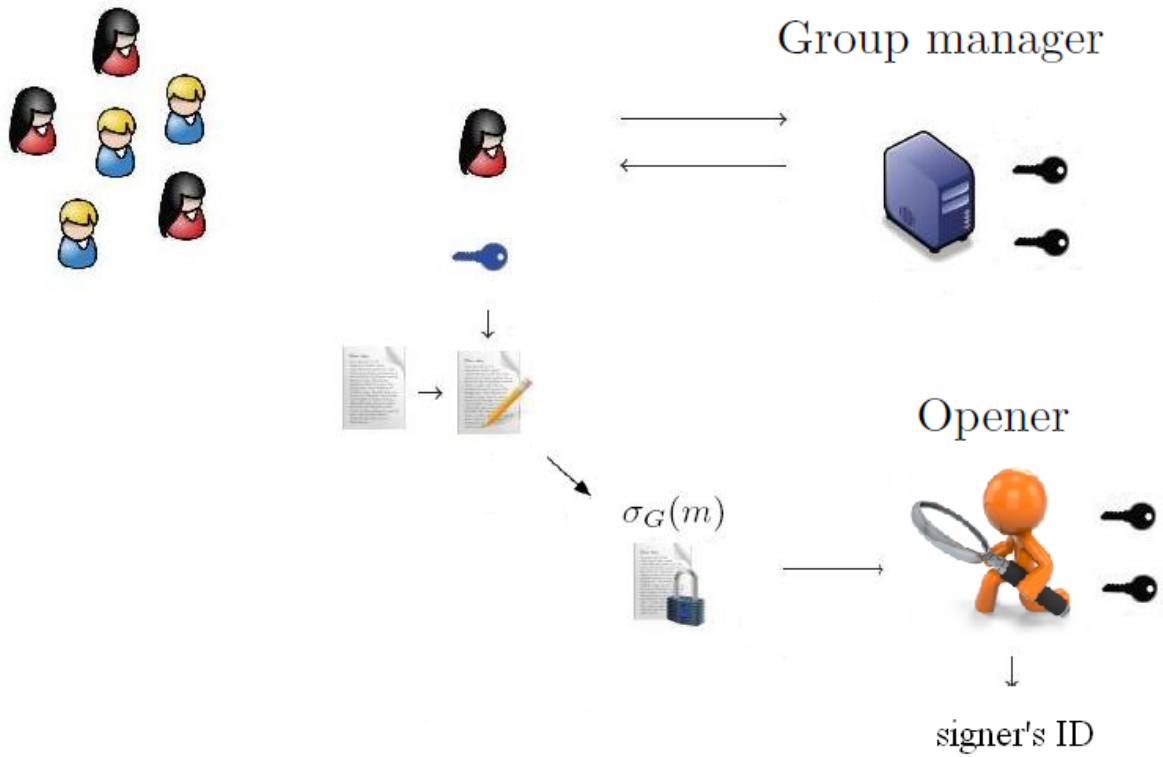
2 Our results

- A partially structure-preserving IBE
- Construction of a GS-MDO scheme
- Security results

technicolor

Group Signatures

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



- Applications in trusted computing platforms, can enhance the privacy of commuters in public transportation

technicolor

Group Signatures

- Chaum-van Heyst (Eurocrypt'91): introduction of the primitive
- Ateniese-Camenisch-Joye-Tsudik (Crypto'00):
  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 with Message-Dependent Opening

- Group signatures allow the opener to trace all signatures

  $\Rightarrow$ No privacy is possible against the opener

- Group signatures with message-dependent opening (Sakai-Emura-Hanaoka-Kawai-Matsuda-Omote, Pairing'12): Restrict the power of the opener

  - Signature openings must be approved by an *admitter* . . .
  - . . . and require a message-specific trapdoor t_M revealed by the admitter
  - Neither the opener or the admitter can open signatures alone

Group Signatures with Message-Dependent Opening

- Difference with threshold openings: given t_M, opener can open *all* signatures on M without interacting with the admitter
- More convenient when many signatures must be opened for the *same* message M
  - Find out who used a given metro line in a specific date / time
  - Identify the winner in auctions when many bids collide
- Existing solutions:
  - Sakai *et al.* (Pairing'12): general construction; efficient construction, but with anonymity against bounded collusions
  - Ohara *et al.* (AsiaCCS'13): efficent scheme in the ROM
  - Open problem: efficiency in the standard model

The problem: GS-MDO in the Standard Model

- In cyclic groups $(\mathbb{G}, \mathbb{G}_T)$ with a bilinear map (a.k.a. pairing)

$$e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$$

  such that $e(g^a, h^b) = e(g, h)^{ab}$ for all $a, b \in \mathbb{Z}$

- Groth-Sahai (Eurocrypt'08): efficient non-interactive proofs for
  - **Pairing-product equations:** committed variables $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$ satisfy

$$\prod_{i=1}^{n} e(\mathcal{A}_i, \mathcal{X}_i) \cdot \prod_{i=1}^{n} \cdot \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{X}_j)^{a_{ij}} = t_T,$$

    for constants $t_T \in \mathbb{G}_T$, $\mathcal{A}_1, \ldots, \mathcal{A}_n \in \mathbb{G}$, $a_{ij} \in \mathbb{Z}_p$.

  - Also for multi-exponentiation equations and quadratic equations

The problem: GS-MDO in the Standard Model

- **Our contribution:** efficient, fully anonymous GS-MDO scheme in the standard model
- Difficulties in the standard model:
  - Groth-Sahai proof systems (Eurocrypt'08) are needed
  - GS-MDO implies Identity-Based Encryption (showed by Sakai *et al.*, Pairing'12)
  - Need for a "Groth-Sahai-compatible" IBE scheme:

    In groups $(\mathbb{G}, \mathbb{G}_T)$ with a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$, the message space should be $\mathbb{G}$, instead of $\mathbb{G}_T$
  - Only q-resilient IBE schemes (*e.g.*, Heng-Kurosawa, CT-RSA'04) have this property so far, with parameters of size $O(q)$

technicolor

Our Solutions

- A partially structure-preserving IBE
  - Message space is $\mathbb{G}$ but identities are still binary strings
  - Allows efficient proving properties about IBE-encrypted data using Groth-Sahai
  - Downside: ciphertexts take $\mathcal{O}(\lambda)$ group elements
- An optimization to get $\mathcal{O}(\log N)$-size signatures
  - Combination of our IBE scheme and the Boyen-Waters group signature (Eurocrypt'06)
  - For groups of $N = 10^6$ members, signatures fit within 68 *kB* at the 128-bit security level (vs 32 *kB* in Sakai *et al.*'s system)

Outline

1 **Background**
- Group signatures: applications, history
- Group signatures with Message Dependent Opening
- The problem: GS-MDO in the standard model

2 **Our results**
- A partially structure-preserving IBE
- Construction of a GS-MDO scheme
- Security results

technicolor

Our Partially Structure-Preserving IBE

- Based on Waters' IBE (Eurocrypt'05):
  - Master key pair is obtained as $\mathsf{mpk} = \{g,\ h,\ g_1 = g^{\alpha}\}$; and $\mathsf{msk} = h^{\alpha}$
  - Private key is $(d_1, d_2) = \left(h^{\alpha} \cdot H_{\mathbb{G}}(\mathrm{ID})^{r}, g^{r}\right)$
  - Ciphertext is $(C_0, C_1, C_2) = \left(M \cdot e(g_1, h)^{s},\ g^{s},\ H_{\mathbb{G}}(\mathrm{ID})^{s}\right)$
- Our modification
  - Set $\mathsf{mpk} = \{g,\ h,\ g_0 = g^{\alpha_0},\ g_1 = g^{\alpha_1},\ \{Z_i\}_{i=1}^{\ell}\}$, with $\ell = \mathcal{O}(\lambda)$, and $\mathsf{msk} = \{h^{\alpha_0}, h^{\alpha_1}\}$
  - To encrypt $M \in \mathbb{G}$, set $C_0 = M \cdot \prod_{i=1}^{\ell} Z_i^{K[i]}$ where $K \xleftarrow{R} \{0,1\}^{\ell}$
  - Encode each $K[i] \in \{0,1\}$ by picking $s_i, \omega_i \xleftarrow{R} \mathbb{Z}_p$ and computing

$$(C_{1,i}, C_{2,i}, C_{3,i}, C_{4,i}) = (g^{s_i},\ H_{\mathbb{G}}(\mathrm{ID})^{s_i},\ g_{K[i]}^{s_i/\omega_i},\ h^{\omega_i})$$

Our Partially Structure-Preserving IBE

- Based on Waters' IBE (Eurocrypt'05):
  - Master key pair is obtained as $\mathsf{mpk} = \{g,\ h,\ g_1 = g^{\alpha}\}$; and $\mathsf{msk} = h^{\alpha}$
  - Private key is $(d_1, d_2) = \left(h^{\alpha} \cdot H_{\mathbb{G}}(\mathrm{ID})^{r}, g^{r}\right)$
  - Ciphertext is $(C_0, C_1, C_2) = \left(M \cdot e(g_1, h)^{s},\ g^{s},\ H_{\mathbb{G}}(\mathrm{ID})^{s}\right)$
- Our modification
  - Set $\mathsf{mpk} = \{g,\ h,\ g_0 = g^{\alpha_0},\ g_1 = g^{\alpha_1},\ \{Z_i\}_{i=1}^{\ell}\}$, with $\ell = \mathcal{O}(\lambda)$, and $\mathsf{msk} = \{h^{\alpha_0}, h^{\alpha_1}\}$
  - To encrypt $M \in \mathbb{G}$, set $C_0 = M \cdot \prod_{i=1}^{\ell} Z_i^{K[i]}$ where $K \xleftarrow{R} \{0,1\}^{\ell}$
  - Encode each $K[i] \in \{0,1\}$ by picking $s_i, \omega_i \xleftarrow{R} \mathbb{Z}_p$ and computing

$$(C_{1,i}, C_{2,i}, C_{3,i}, C_{4,i}) = (g^{s_i},\ H_{\mathbb{G}}(\mathrm{ID})^{s_i},\ g_{K[i]}^{s_i/\omega_i},\ h^{\omega_i})$$

Our GS-MDO Scheme

Desired security properties (based on the [BMW03] model):

- Full traceability

  No coalition of group members can create an untraceable signature

- Anonymity against the admitter

  Colluding admitter and group members cannot identify signers or link signatures, even with access to an opening oracle

- Anonymity against the opener

  Colluding opener and group members cannot identify signers or link signatures

Our GS-MDO Scheme

- Generically using our IBE requires signatures of $\mathcal{O}(\lambda)$ group elements (*i.e.* $\mathcal{O}(\lambda^2)$ bits)

  Inefficient as $\lambda \gg \log N$ (since $N \ll 2^\lambda$)

- **Problem:** we want $\mathcal{O}(\log N)$ group elements per signature

- **Idea:** exploit the similar bit-by-bit encodings of our IBE and the Boyen-Waters group signature (Eurocrypt'06)

  - In [BW06], membership certificate of user $\mathrm{id} = \mathrm{id}[1] \ldots \mathrm{id}[\ell]$ is

$$(d_1, d_2) = \left(h^\alpha \cdot (u_0 \cdot \prod_{i=1}^{\ell} u_i^{\mathrm{id}[i]})^r,\ g^r \right)$$

  - We use a bit-wise encoding of a key $K = K[1] \ldots K[\ell] \in \{0,1\}^\ell$ as

$$(g^{s_i},\ H_{\mathbb{G}}(\mathrm{ID})^{s_i},\ g_{K[i]}^{s_i/\omega_i},\ h^{\omega_i})$$

Construction Overview

- Each member has an identifier $\mathsf{id} = \mathsf{id}[1] \ldots \mathsf{id}[\ell]$ and a credential

$$(d_1, d_2) = \left(h^{\alpha} \cdot (u_0 \cdot \prod_{i=1}^{\ell} u_i^{\mathsf{id}[i]})^{r},\ g^{r} \right)$$

- Group signature consists of
  - A committed two-level hierarchical signature

$$(\sigma_1, \sigma_2, \sigma_3) = \left(h^{\alpha} \cdot (u_0 \cdot \prod_{i=1}^{\ell} u_i^{\mathsf{id}[i]})^{r} \cdot H_{\mathbb{G}}(M)^{s},\ g^{r},\ g^{s} \right)$$

  - Commitments to $\{\mathsf{id}[i]\}_{i=1}^{\ell}$ with proofs that $\mathsf{id}[i] \in \{0, 1\}$ for each i
  - An encrypted encoding of each $\mathsf{id}[i] \in \{0, 1\}$

$$(g^{s_i},\ H_{\mathbb{G}}(M)^{s_i},\ g_{\mathsf{id}[i]}^{s_i/\omega_i},\ h^{\omega_i})$$

  - NIWI / NIZK proofs that things are done correctly

Security Results

Theorem

The scheme provides

- *Full traceability under the standard* **Diffie-Hellman** *assumption*

  Given $(g, g^a, g^b) \in \mathbb{G}^3$*, no PPT algorithm can compute* g^{ab}

- *Anonymity properties assuming the hardness of*

  - *The* **Decision Linear** *problem*

    Given $(g, g^a, g^b, g^{ac}, g^{bd}) \in \mathbb{G}^5$*, distinguish* g^{c+d} *from random*

  - *The* **Decision 3-party Diffie-Hellman** *problem*

    Given $(g, g^a, g^b, g^c) \in \mathbb{G}^4$*, distinguish* g^{abc} *from random*

technicolor

Summary

We described:

- A “Groth-Sahai-compatible” IBE scheme, with plaintexts in $\mathbb{G}$
- First efficient, fully anonymous GS-MDO scheme in the standard model (with $\mathcal{O}(\log N)$-size signatures)

Open problems:

- Can we get a truly structure-preserving IBE?
- More efficient partially structure-preserving IBE
- GS-MDO scheme in the standard model with $\mathcal{O}(1)$ group elements per signature

technicolor

Questions?

technicolor