

Group Signatures with Message-Dependent Opening in the Standard Model



Benoît Libert • Marc Joye



Group Signatures with Message-Dependent Opening in the Standard Model

Benoît Libert • Marc Joye



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

1 Background

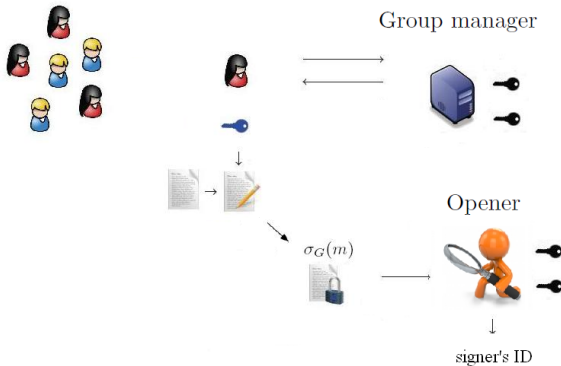
- Group signatures: applications, history
- Group signatures with Message Dependent Opening
- The problem: GS-MDO in the standard model

2 Our results

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

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

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
 - ⇒ 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): efficient 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)

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

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 $\mathcal{X}_1, \dots, \mathcal{X}_n \in \mathbb{G}$ 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 $t_T \in \mathbb{G}_T$, $\mathcal{A}_1, \dots, \mathcal{A}_n \in \mathbb{G}$, $a_{ij} \in \mathbb{Z}_p$.

- 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 $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, 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 $O(q)$

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

Our Partially Structure-Preserving IBE

■ Based on Waters' IBE (Eurocrypt'05):

- Master key pair is obtained as $\text{mpk} = \{g, h, g_1 = g^\alpha\}$; and $\text{msk} = h^\alpha$
- Private key is $(d_1, d_2) = (h^\alpha \cdot H_{\mathbb{G}}(\text{ID})^r, g^r)$
- Ciphertext is $(C_0, C_1, C_2) = (M \cdot e(g_1, h)^s, g^s, H_{\mathbb{G}}(\text{ID})^s)$

■ Our modification

- Set $\text{mpk} = \{g, h, g_0 = g^{\alpha_0}, g_1 = g^{\alpha_1}, \{Z_i\}_{i=1}^\ell\}$, with $\ell = \mathcal{O}(\lambda)$, and $\text{msk} = \{h^{\alpha_0}, h^{\alpha_1}\}$
- 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

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

Our Partially Structure-Preserving IBE

■ Based on Waters' IBE (Eurocrypt'05):

- Master key pair is obtained as $\text{mpk} = \{g, h, g_1 = g^\alpha\}$; and $\text{msk} = h^\alpha$
- Private key is $(d_1, d_2) = (h^\alpha \cdot H_{\mathbb{G}}(\text{ID})^r, g^r)$
- Ciphertext is $(C_0, C_1, C_2) = (M \cdot e(g_1, h)^s, g^s, H_{\mathbb{G}}(\text{ID})^s)$

■ Our modification

- Set $\text{mpk} = \{g, h, g_0 = g^{\alpha_0}, g_1 = g^{\alpha_1}, \{Z_i\}_{i=1}^\ell\}$, with $\ell = \mathcal{O}(\lambda)$, and $\text{msk} = \{h^{\alpha_0}, h^{\alpha_1}\}$
- 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

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

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 $\text{id} = \text{id}[1] \dots \text{id}[\ell]$ is

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

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

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

Construction Overview

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

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

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

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

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

$$(g^{s_i}, H_G(M)^{s_i}, g_{\text{id}[i]}^{s_i/\omega_i}, h^{\omega_i})$$

- 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

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

Questions?



Practical Distributed Signatures in the Standard Model

SESSION ID: CRYPT-R01

Yujue Wang

Wuhan University

Duncan S. Wong

City University
of Hong Kong

Qianhong Wu

Beihang University

Sherman S.M. Chow

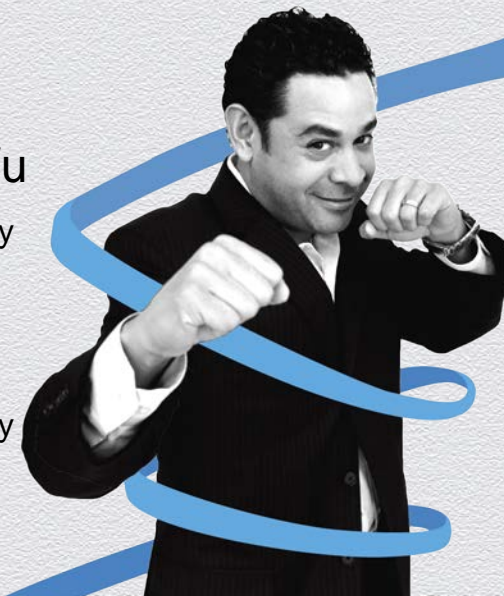
Chinese University
of Hong Kong

Bo Qin

Renmin University

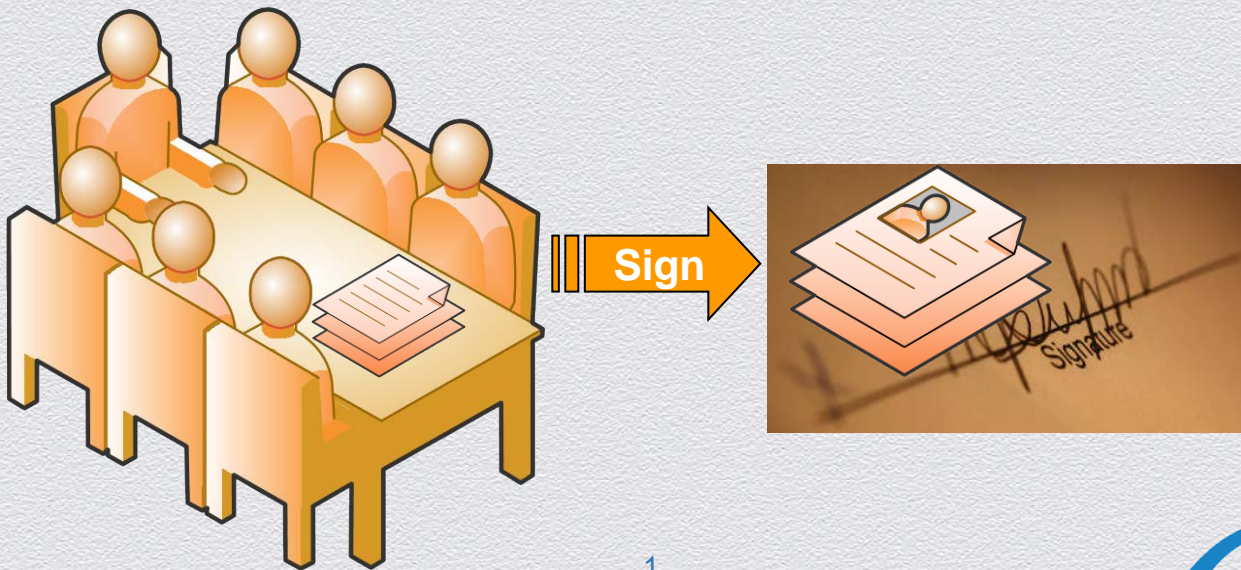
Jianwei Liu

Beihang University



Distributed Signing of Data

- ◆ Multiple managers issue a signature
 - ◆ Any individual manager cannot do it on behalf of the company
 - ◆ Only qualified sets of managers can jointly do so



Applications

- ◆ Secure digital signatures without single point of failure
 - ◆ E.g.: Digital certificates, signing of documents for a company
- ◆ Web-browsing records
 - ◆ E.g.1: Web-page counter [Daza-Herranz-Sáez@IJIS'04]
 - ◆ E.g.2: Promotion campaign: when an ad banner has been shown to the client via a number of different websites, the client can enter a lucky draw



Rundown

- ◆ Definition of Distributed Signature Schemes
- ◆ Related Notions of Signatures
- ◆ Overview of Existing Distributed Signature Schemes
- ◆ Our Proposed Scheme
- ◆ Extensions
- ◆ Conclusions

Standard Signature (SS) Scheme

- ◆ $(pk, sk) \leftarrow \text{KGen}(\kappa)$
 - ◆ Generate random public/private key-pair
- ◆ $\sigma \leftarrow \text{Sig}_{sk}(m)$
 - ◆ Sign on a message with the private key
- ◆ $0/1 \leftarrow \text{Ver}_{pk}(m, \sigma)$
 - ◆ Validate a message-signature pair under the public key



Distributed Signature (DS) Scheme

- ◆ $(pk, sk_1, \dots, sk_n, vp) \leftarrow \text{DKGen}(\kappa, \Gamma)$
 - ◆ takes as input an access structure (Γ) and a security parameter (κ)
 - ◆ generates a random public key (pk)
 - ◆ then private key shares $(\{sk_i\})$, and verification parameters (vp)
 - ◆ $\approx \text{SS.KGen}$ + Secret sharing of private key
- ◆ $\sigma_i \leftarrow \text{SFGen}(m, sk_i, pk, vp)$
 - ◆ generates a signature fragment with her private key share



Distributed Signature (DS) Scheme (cont.)

- ◆ $\sigma / \perp \leftarrow \text{SReCon}(m, \{\sigma_i\}, pk, vp, \Gamma)$
 - ◆ Reconstruct the signature from fragments
 - ◆ First discard all the invalid σ_i
 - ◆ Succeed if valid ones are qualified w.r.t. Γ
- ◆ $1 / 0 \leftarrow \text{Ver}(m, \sigma, pk)$
 - ◆ Indistinguishability: $\text{DS.Ver} = \text{SS.Ver}$



Related Signature Schemes

- ◆ Threshold signature (TS)
 - ◆ E.g.: any **two** out of four managers $\{P_1, P_2, P_3, P_4\}$ is qualified
 - ◆ Case not supported by TS: above threshold, but excluding, say, $\{P_1, P_4\}$
- ◆ Mesh signatures
 - ◆ each first generates an "atomic signature"
 - ◆ the final signature is their "concatenation"
- ◆ Attributed-based signatures
 - ◆ care about the attributes / qualifications of an individual



Desirable Properties of Distributed Signing

- ◆ Robustness: Signature fragments' (in)validity can be checked
- ◆ Non-interactive signing
- ◆ Non-interactive re-construction of the final signature
 - ◆ can be done by anyone who obtained enough qualified fragments
 - ◆



Comparison

Schemes	Key	Key Share	Signature /Fragment	Assumption	Standard Model	Non-Interactive
Herranz-Saez@FC'03	224	448	2272	Dis. Log.	X	X
Herranz <i>et al.</i> @ISC'03	2048	2048	2052	RSA	X	X
Damgård-Thorbek@PKC'06	2048	2048	2048	RSA	✓	X
Our Proposal	224-255	224-255	448-510	CDH	✓	✓



Key Ideas in Our Construction

- ◆ Extending Waters Signatures
- ◆ Utilizing linear secret sharing scheme to realize the access structure



Our Basic Scheme (DKGen)

- ◆ Bilinear map $e: \mathbf{G} \times \mathbf{G} \rightarrow \mathbf{G}_T$
- ◆ Monotone span program (MSP) which realizes access structure Γ :
 - ◆ τ : Target vector in \mathbf{Z}_p to share
 - ◆ M : A matrix representing the policy
 - ◆ ρ : Label each row of M with a participant, ρ^1 : Return a row of M
- ◆ Secret key $sk = k \in \mathbf{Z}_p$ and Public key $pk = (g, g_0, \dots, g_\ell, e(g, g)^k)$
- ◆ Select a random vector v that satisfies $v\tau = k$. Compute $k_i = v\rho^1(P_i)$
- ◆ Secret key shares $sk_i = k_i$ and Verification parameters $vp = \{e(g, g)^{k_i}\}$



Our Basic Scheme (SFGen, SReCon, and Ver)

- ◆ SFGen: $\sigma_i = (\alpha_i = g^{k_i} (g_0 g_1^{m_1} \dots g_\ell^{m_\ell})^{r_i}, \beta_i = g^{r_i})$
 - ◆ $m = m_1 \dots m_\ell \in \{0, 1\}^\ell$, r_i is randomly chosen from \mathbf{Z}_p
- ◆ A valid fragment should satisfy $e(\alpha_i, \beta_i) = e(g, g)^{k_i} e(g_0 g_1^{m_1} \dots g_\ell^{m_\ell}, \beta_i)$
- ◆ SReCon: Solves the system of equations to find the coefficients $\{d_i\}$ w.r.t the valid $\{\sigma_i\}$, such that τ can be spanned in MSP M
- ◆ Output $(\alpha = \prod s_i^{d_i}, \beta = \prod \beta_i^{d_i})$
- ◆ Ver: Output 1 if $e(\alpha, \beta) = e(g, g)^k e(g_0 g_1^{m_1} \dots g_\ell^{m_\ell}, \beta)$



Simulatability and Unforgeability

- ◆ Probabilistic poly. time adversary controls an unqualified set and see
 - ◆ all the public information
 - ◆ all the (intermediate) information of corrupted participants
- ◆ Her view on the execution of DKGen, SFGGen, and SReCon can be **simulated**
- ◆ If the distributed signature scheme **DS** is **simulatable** and the underlying signature scheme **SS** is **unforgeable**
- ◆ then DS is also **unforgeable**



Extension 1: Dynamic Join without a Central Dealer

- ◆ Threshold signature scheme, such that a new participant can join when he talked with at least t of the existing signers.
- ◆ Use **symmetric bivariate polynomial** $f(x, y)$ to secret-share private key
- ◆ Each share is an **univariate polynomial** $f(x, i)$, i.e., an evaluation on y
- ◆ For SFGGen, just use $f(0, i)$
- ◆ For new participant j , obtain $f(j, i)$ from signer P_i
- ◆ When enough $\{f(j, i) = f(i, j)\}$ are obtained, can interpolate to get $f(x, j)$
- ◆ Originally for Dynamic Threshold RSA [Gennaro *et al.* @Eurocrypt'08]



Extension 2: Compartment with Upper Bounds

- ◆ A special **multipartite** access structure: there exists a threshold for all the participants, and an upper bound for each separate group
 - ◆ i.e., there is a quorum for signature issuing, but any group can not contribute more than the given upper bound
- ◆ Participant set **P** comprises several disjoint subset **G_i**
- ◆ Requires at least **t** signers from **P** *and* at most **t_i** signers from **G_i**
- ◆ Replace the linear secret sharing scheme with [Tassa-Dyn@JoC'09]

Summary

- ◆ Distributed signature is a powerful tool in multi-user setting
- ◆ Existing schemes are interactive and not efficient enough
- ◆ We propose a practical scheme in the standard model, which is
 - ◆ non-interactive
 - ◆ robust
 - ◆ and secure under Computational Diffie-Hellman assumption
- ◆ We show two extensions useful for specific application scenarios



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Practical Distributed Signatures in the Standard Model

DECENTRALIZED TRACEABLE ATTRIBUTE-BASED SIGNATURES

Essam Ghadafi¹ **Ali El Kaafarani**² **Dalia Khader**³

¹University of Bristol, ²University of Bath, ³University of Luxembourg

`ghadafi@cs.bris.ac.uk`

CT-RSA 2014

- 1 BACKGROUND
- 2 A SECURITY MODEL
- 3 GENERIC CONSTRUCTIONS
- 4 INSTANTIATIONS
- 5 EFFICIENCY COMPARISON
- 6 SUMMARY & OPEN PROBLEMS

- 1 BACKGROUND
- 2 A SECURITY MODEL
- 3 GENERIC CONSTRUCTIONS
- 4 INSTANTIATIONS
- 5 EFFICIENCY COMPARISON
- 6 SUMMARY & OPEN PROBLEMS

- 1 BACKGROUND
- 2 A SECURITY MODEL
- 3 GENERIC CONSTRUCTIONS
- 4 INSTANTIATIONS
- 5 EFFICIENCY COMPARISON
- 6 SUMMARY & OPEN PROBLEMS

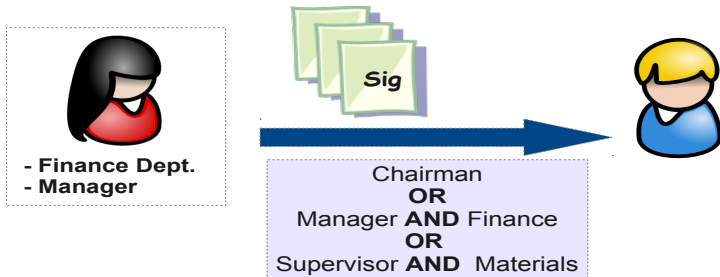
- 1 BACKGROUND
- 2 A SECURITY MODEL
- 3 GENERIC CONSTRUCTIONS
- 4 INSTANTIATIONS
- 5 EFFICIENCY COMPARISON
- 6 SUMMARY & OPEN PROBLEMS

- 1 BACKGROUND
- 2 A SECURITY MODEL
- 3 GENERIC CONSTRUCTIONS
- 4 INSTANTIATIONS
- 5 EFFICIENCY COMPARISON
- 6 SUMMARY & OPEN PROBLEMS

- 1 BACKGROUND
- 2 A SECURITY MODEL
- 3 GENERIC CONSTRUCTIONS
- 4 INSTANTIATIONS
- 5 EFFICIENCY COMPARISON
- 6 SUMMARY & OPEN PROBLEMS

Attribute-Based Signatures [Maji et al. 2008].

- Users have attributes (e.g. “Departmental Manager”, “Chairman”, “Finance Department”, etc.).
- Signing is w.r.t. a signing policy Ψ .
- A user can sign a message w.r.t. a policy Ψ only if she owns attributes \mathcal{A} s.t. $\Psi(\mathcal{A}) = 1$.



Example applications:

- **Attribute-Based Messaging:** Recipients are assured the sender satisfies a certain policy.
- **Leaking Secrets:** Allows more expressive predicates for leaking a secret than, e.g. traditional ring signatures [RST01].
- **Many other applications:** ...

Security of Attribute-Based Signatures [Maji et al. 2008]

► **(Perfect) Privacy (Anonymity):**

The signature hides:

- 1 The identity of the signer.
- 2 The attributes used in the signing (i.e. how Ψ was satisfied).

► **Unforgeability:** A signer cannot forge signatures w.r.t. signing policies her attributes do not satisfy even if she colludes with other signers.

- ▶ Maji et al. 2008 & 2011.
- ▶ Shahandashti and Safavi-Naini 2009.
- ▶ Li et al. 2010.
- ▶ Okamoto and Takashima 2011 & 2012.
- ▶ Gagné et al. 2012.
- ▶ Herranz et al. 2012.

Traceable Attribute-Based Signatures (TABS) [Escala et al. 2011]:

Extend ABS by adding an anonymity revocation mechanism.

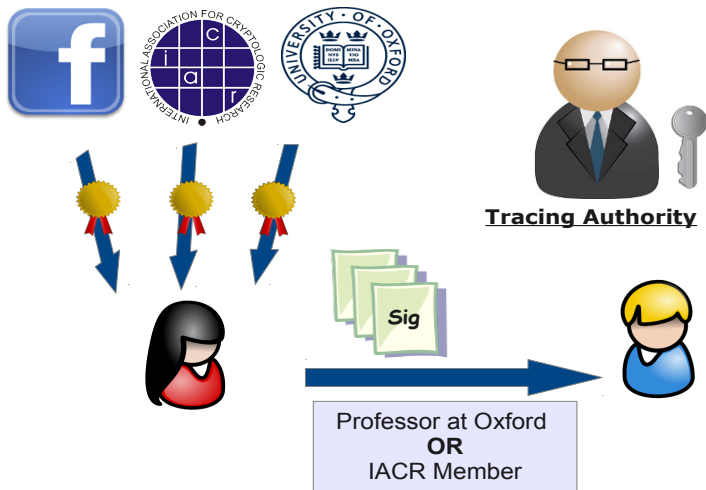
- A tracing authority can reveal the identity of the signer.
- Crucial in enforcing accountability and deterring abuse.

- 1 A security model for Decentralized Traceable Attribute-Based Signatures (DTABS).
- 2 Two generic constructions for DTABS.
- 3 Example instantiations in the standard model.

Features of Our Model:

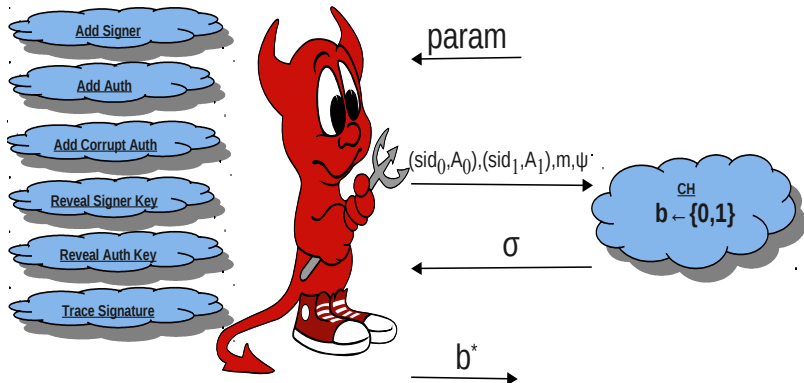
- Multiple attribute authorities, e.g. Company A, University B, Organization C, Government D, etc.
 - ▶ Need not trust one another or even be aware of each other.
- Signers and attribute authorities can join the system at any time.
- A tracing authority can reveal the identity of the signer.
- Tracing correctness is publicly verifiable.

DECENTRALIZED TRACEABLE ATTRIBUTE-BASED SIGNATURES



- ▶ **Correctness:** If all parties are honest:
 - Signatures verify correctly.
 - The tracing authority can identify the signer.
 - The **Judge** algorithm accepts the tracing decision.

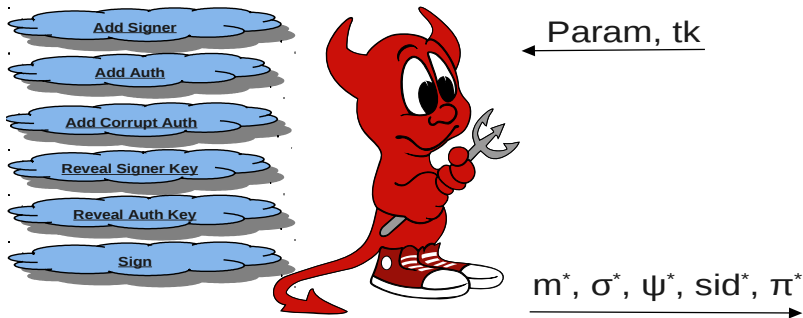
- **Anonymity:** Signatures do not reveal the identity of the signer or the attributes used.



Adversary wins if: $b = b^*$.

- The CH oracle returns \perp if $\Psi(A_0) \neq 1$ or $\Psi(A_1) \neq 1$.
- The Trace oracle returns \perp if queried on σ .

- **Full Unforgeability:** Even if signers collude, they cannot produce a signature on behalf of a signer whose attributes do not satisfy the policy. Covers non-frameability.



Adversary wins if:

- σ^* is valid and π^* accepted by Judge.
- No corrupt subset of attributes $\mathcal{A}_{\text{sid}^*}^*$ s.t. $\Psi^*(\mathcal{A}_{\text{sid}^*}^*)=1$.
- $(\text{sid}^*, \cdot, m^*, \sigma^*, \Psi^*)$ was not obtained from the signing oracle.

- **Traceability:** Signatures are traceable, i.e. the tracing authority can always identify the signer.



Adversary wins if all the following holds:

- σ^* is a valid signature on m^* w.r.t. Ψ^* **and either:**
 - σ^* opens to a signer who was never added.
 - The Judge algorithm rejects the tracing proof.

Construction I

► Tools used:

- Two NIZK systems \mathcal{NIZK}_1 and \mathcal{NIZK}_2 .
 - \mathcal{NIZK}_1 needs to be *simulation-sound* and a *proof of knowledge*.
- A tagged signature scheme \mathcal{TS} : a digital signature scheme that signs a tag and a message.
- A digital signature scheme \mathcal{DS} .
- An IND-CCA2 public key encryption scheme \mathcal{PKE} .

► **Setup:**

- Generate (epk, esk) for $\mathcal{PK}\mathcal{E}$, (vk, sk) for \mathcal{DS} , crs_1 for \mathcal{NIZK}_1 , and crs_2 for \mathcal{NIZK}_2 .
- Set $\text{tk} := \text{esk}$ and $\text{param} := (\text{crs}_1, \text{crs}_2, \text{vk}, \text{epk}, \mathcal{H})$.

► **Attribute Authority Join:**

Generate $(\text{aavk}_{\text{aid}}, \text{assk}_{\text{aid}})$ for \mathcal{TS} .

► **Attribute Key Generation:**

To generate a key $\text{sk}_{\text{sid},a}$ for attribute a for signer sid , compute $\text{sk}_{\text{sid},a} \leftarrow \mathcal{TS}.\text{Sign}(\text{assk}_{\text{aid}(a)}, \text{sid}, a)$.

► **Signing:** To sign m w.r.t. Ψ :

- 1 $C \leftarrow \mathcal{PK}\mathcal{E}.\text{Enc}(\text{epk}, \text{sid})$.
 - 2 Produce a proof π of A and sid that:
 - 1 C is an encryption of sid .
 - 2 Either owns attributes A s.t. $\Psi(A) = 1$
 \Rightarrow Has a valid tagged signature on (sid, a) for each $a \in A$
- OR**
- Has a special digital signature on $\mathcal{H}(\Psi, m, C)$, i.e. a pseudo-attribute.

The signature is $\sigma := (C, \pi)$.

► **Tracing:**

- The tracing authority uses esk to decrypt C to obtain sid .
- Produces a proof π_{Trace} of esk that decryption was done correctly.

Security of the Construction:

► Anonymity:

- NIZK of \mathcal{NIZK}_1 and \mathcal{NIZK}_2 .
- Simulation-soundness of \mathcal{NIZK}_1 .
- IND-CCA of $\mathcal{PK}\mathcal{E}$.
- Collision-resistance of \mathcal{H} .

► Full Unforgeability:

- Soundness of \mathcal{NIZK}_1 and \mathcal{NIZK}_2 .
- Unforgeability of \mathcal{TS} and \mathcal{DS} .
- Collision-resistance of \mathcal{H} .

► Traceability:

- Soundness of \mathcal{NIZK}_1 .
- Unforgeability of \mathcal{TS} and \mathcal{DS} .

Construction II

► Changes from Construction I:

- \mathcal{NIZK}_1 need not be simulation-sound.
- Replace $\mathcal{PK}\mathcal{E}$ with a selective-tag weakly IND-CCA tag-based encryption scheme \mathcal{TPKE} .
- Need a strongly unforgeable one-time signature \mathcal{OTS} .
- Another collision-resistant hash function $\hat{\mathcal{H}}$ to hash into the tag space of \mathcal{TPKE} .

► **Signing:** To sign m w.r.t. Ψ :

1 Choose a fresh key pair $(\text{otsvk}, \text{otssk})$ for \mathcal{OTS} .

2 $C_{\text{tbe}} \leftarrow \mathcal{TPKE}.\text{Enc}(\text{epk}, \hat{\mathcal{H}}(\text{otsvk}), \text{sid})$.

3 Produce a proof π of A and sid that:

① C_{tbe} is an encryption of sid under tag $\hat{\mathcal{H}}(\text{otsvk})$.

② Either owns attributes A s.t. $\Psi(A) = 1$

\Rightarrow Has a valid tagged signature on (sid, a) for each $a \in A$

OR

Has a special digital signature on $\mathcal{H}(\Psi, m, C_{\text{tbe}}, \hat{\mathcal{H}}(\text{otsvk}))$.

4 Compute $\sigma_{\text{ots}} \leftarrow \mathcal{OTS}.\text{Sign}(\text{otssk}, (\pi, C_{\text{tbe}}, \text{otsvk}))$.

The signature is $\sigma := (\sigma_{\text{ots}}, \pi, C_{\text{tbe}}, \text{otsvk})$.

► **Tracing:**

■ The tracing authority uses esk to decrypt C_{tbe} to obtain sid .

■ Produces a proof π_{Trace} of esk that decryption was done correctly.

Security of the Construction:

► Anonymity:

- NIZK of \mathcal{NIZK}_1 and \mathcal{NIZK}_2 .
- ST-IND-CCA of \mathcal{TPKE} .
- Unforgeability of \mathcal{OTS} .
- Collision-resistance of \mathcal{H} and $\hat{\mathcal{H}}$.

► Full Unforgeability:

- Soundness of \mathcal{NIZK}_1 and \mathcal{NIZK}_2 .
- Unforgeability of \mathcal{TS} , \mathcal{DS} and \mathcal{OTS} .
- Collision-resistance of \mathcal{H} and $\hat{\mathcal{H}}$.

► Traceability:

- Soundness of \mathcal{NIZK}_1 .
- Unforgeability of \mathcal{TS} and \mathcal{DS} .

How to prove that one owns A s.t. $\Psi(A) = 1$?

- ▶ Use a span program.
 - Represent Ψ by a $|\Psi| \times \beta$ span matrix \mathbf{Z} .
 - Prove you know a vector \vec{s} s.t. $\vec{s}\mathbf{Z} = [1, 0, \dots, 0]$
 $\Rightarrow \{a_i | s_i \neq 0\}$ satisfies Ψ .

- ▶ $\text{NIZKs} \Rightarrow$ Groth-Sahai proofs [GS08] secure under DLIN (or SXDH).
- ▶ $\mathcal{TS} \Rightarrow$ A variant of the automorphic signature scheme [Fuc09,Fuc10]: tag space is $\mathbb{G}_1 \times \mathbb{G}_2$ and message space is \mathbb{Z}_p secure under q -ADHSDH and WFCDH (or q -ADHSDH and AWFCDH).
- ▶ $\mathcal{TPKE} \Rightarrow$ Kiltz [Kil06] tag-based encryption scheme secure under DLIN or (SDLIN in group \mathbb{G}_i).
- ▶ $\mathcal{DS} \Rightarrow$ The full Boneh-Boyen signature scheme secure under q -SDH. Need not hide the integer component.
- ▶ $\mathcal{OTS} \Rightarrow$ The full Boneh-Boyen signature scheme secure under q -SDH.

Con.	Signature Size	Model	Set.	No. of Auth.
[EHM11]	$\mathbb{G}^{ \Psi +\beta+7}$	ROM	C	Single
I	$\mathbb{G}^{69 \Psi +69} + \mathbb{Z}_p^{2\cdot\beta+1}$	STD	P	Multiple
II	$\mathbb{G}_1^{34\cdot \Psi +28} + \mathbb{G}_2^{32\cdot \Psi +32} + \mathbb{Z}_p^{\beta+1}$	STD	P	Multiple
[MPR11] I	$\mathbb{G}^{51\cdot \Psi +2\cdot\beta+18\cdot\lambda\cdot \Psi +51}$	STD	P	Multiple
[MPR11] II	$\mathbb{G}^{36\cdot \Psi +2\cdot\beta+9\cdot\lambda+48}$	STD	P	Multiple

TABLE: Efficiency comparison

- ▶ A security model for decentralized traceable attribute-based signatures.
- ▶ Two generic constructions.
- ▶ Instantiations in the standard model.

- ▶ More efficient constructions without idealized assumptions.
- ▶ Efficient constructions from standard assumptions.

Thank you for your attention!
Questions?