Designing a Dynamic Group Signature Scheme using Lattices

M2 Internship Defense

Fabrice Mouhartem
Supervised by Benoît Libert

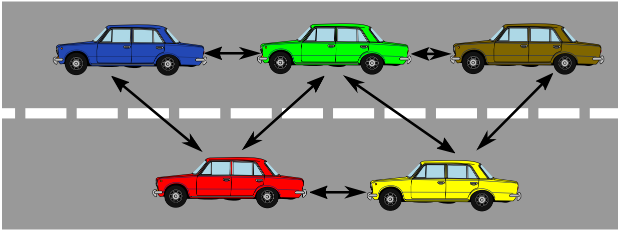
ÉNS de Lyon, Team AriC, LIP

06/24/2015

ENS DE LYON

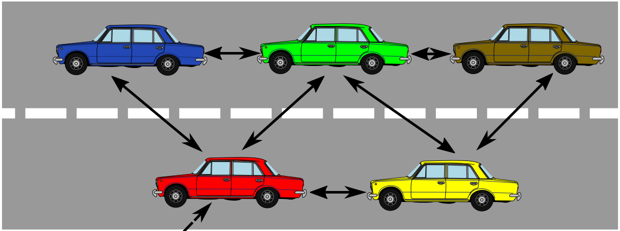
Example

Smart cars



Example

Smart cars

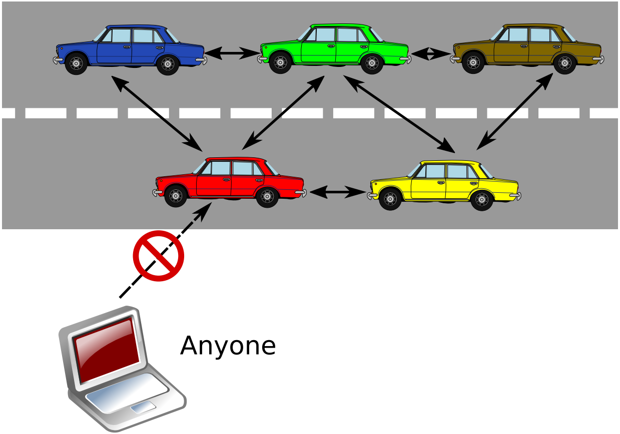


Anyone

Example

Smart cars

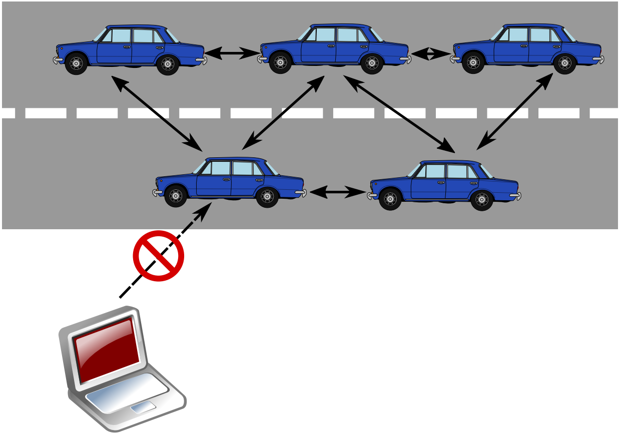
- Authenticity
- Integrity



Example

Smart cars

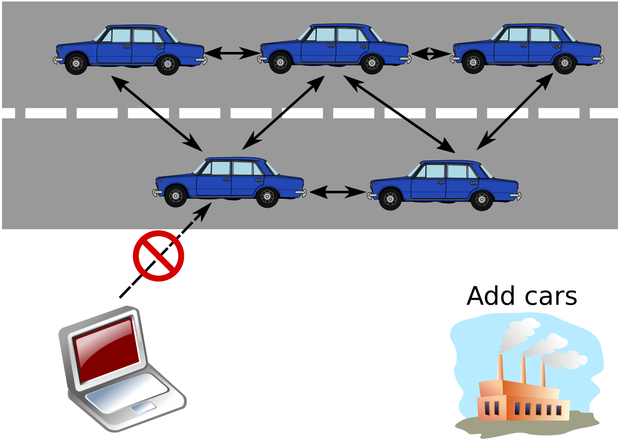
- Authenticity
- Integrity
- Anonymity



Example

Smart cars

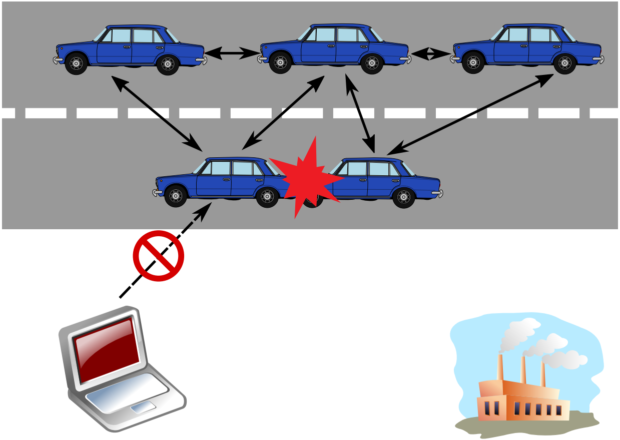
- Authenticity
- Integrity
- Anonymity
- Dynamicity



Example

Smart cars

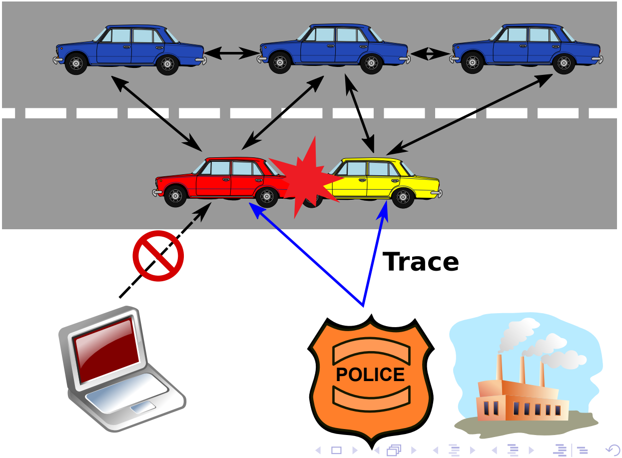
- Authenticity
- Integrity
- Anonymity
- Dynamicity



Example

Smart cars

- Authenticity
- Integrity
- Anonymity
- Dynamicity
- Traceability



Motivation

Definition

A *dynamic* group signature allows a member of a group to anonymously sign a message on behalf of the group, and allow new users to join at any time.

Applications: smart cars, control in public transportation, anonymous access control (*e.g.* in public transportation)...

Motivation

Definition

A *dynamic* group signature allows a member of a group to anonymously sign a message on behalf of the group, and allow new users to join at any time.

Applications: smart cars, control in public transportation, anonymous access control (*e.g.* in public transportation)...

Main Differences

Static Group	Dynamic Group
GM distributes keys	$\mathcal{U}_i$ makes his secret certified
GM must be trusted	Even colluding **GM**/**OA** cannot sign on behalf of a honest group member
Cannot add new users	

Motivation

Advantages of dynamically growing groups:

- Add users without re-running the **Setup** phase;

Motivation

Advantages of dynamically growing groups:

- Add users without re-running the **Setup** phase;
- Even if everyone, including authorities, is dishonest, no one can sign in your name.

History

1991 Introduced by Chaum and Van Heyst

2003 Formal model and definitions by Bellare, Micciancio and Warinschi for **static** groups.

History

1991 Introduced by Chaum and Van Heyst

2000 First scalable solution by Ateniese, Camenisch, Joye and Tsudik

2003 Formal model and definitions by Bellare, Micciancio and Warinschi for **static** groups.

2005 Model for **dynamic** groups by Bellare, Shi and Zhang

2006 Model for **dynamic** groups by Kiayias and Yung

History

- 1991 Introduced by Chaum and Van Heyst
- 2000 First scalable solution by Ateniese, Camenisch, Joye and Tsudik
- 2003 Formal model and definitions by Bellare, Micciancio and Warinschi for **static** groups.
- 2005 Model for **dynamic** groups by Bellare, Shi and Zhang
- 2006 Model for **dynamic** groups by Kiayias and Yung
- 2010 First scheme based on **lattices** by Gordon, Katz and Vaikuntanathan with *linear size* in the max. size of the group
- 2013 Down to *log-size* by Laguillaumie, Langlois, Libert and Stehlé

History

- 1991 Introduced by Chaum and Van Heyst
- 2000 First scalable solution by Ateniese, Camenisch, Joye and Tsudik
- 2003 Formal model and definitions by Bellare, Micciancio and Warinschi for **static** groups.
- 2005 Model for **dynamic** groups by Bellare, Shi and Zhang
- 2006 Model for **dynamic** groups by Kiayias and Yung
- 2010 First scheme based on **lattices** by Gordon, Katz and Vaikuntanathan with *linear size* in the max. size of the group
- 2013 Down to *log-size* by Laguillaumie, Langlois, Libert and Stehlé

No dynamic group signature scheme based on lattices

Lattice-Based Cryptography

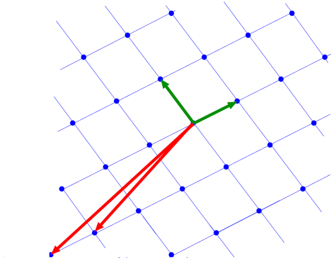
Lattice

A lattice is a discrete subgroup of $\mathbb{R}^n$. Can be seen as integer linear combinations of a finite set of vectors.

Lattice-Based Cryptography

Lattice

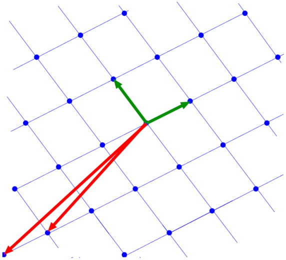
A lattice is a discrete subgroup of $\mathbb{R}^n$. Can be seen as integer linear combinations of a finite set of vectors.



Lattice-Based Cryptography

Lattice

A lattice is a discrete subgroup of $\mathbb{R}^n$. Can be seen as integer linear combinations of a finite set of vectors.



Find a short vector in a lattice is hard.

Lattice-Based Cryptography

Why?

- Simple and efficient;

Lattice-Based Cryptography

Why?

- Simple and efficient;
- Conjectured resistant to a quantum adversary;

Lattice-Based Cryptography

Why?

- Simple and efficient;
- Conjectured resistant to a quantum adversary;
- Secure under worst-case hardness assumptions;

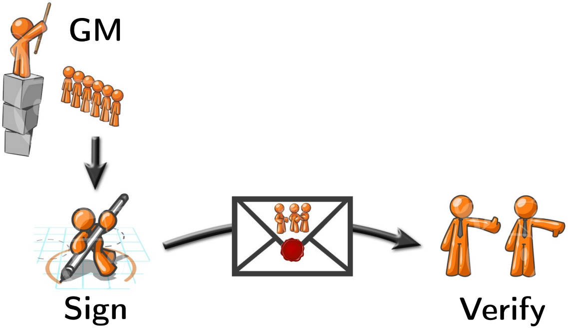
Lattice-Based Cryptography

Why?

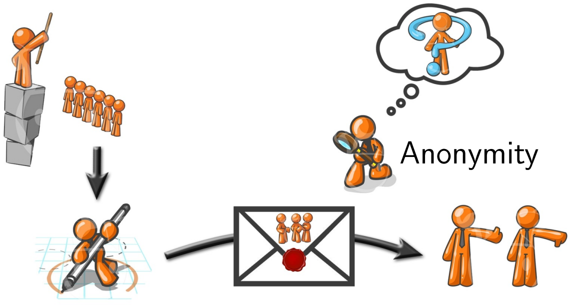
- Simple and efficient;
- Conjectured resistant to a quantum adversary;
- Secure under worst-case hardness assumptions;
- Powerful functionalities.

Outline

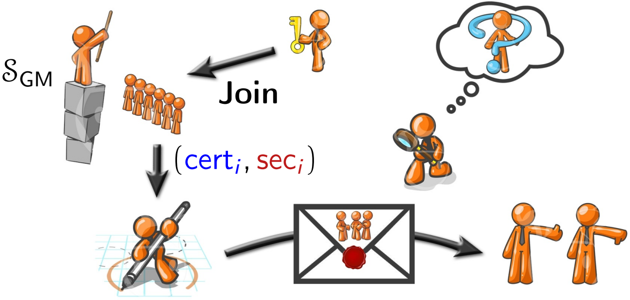
Presentation



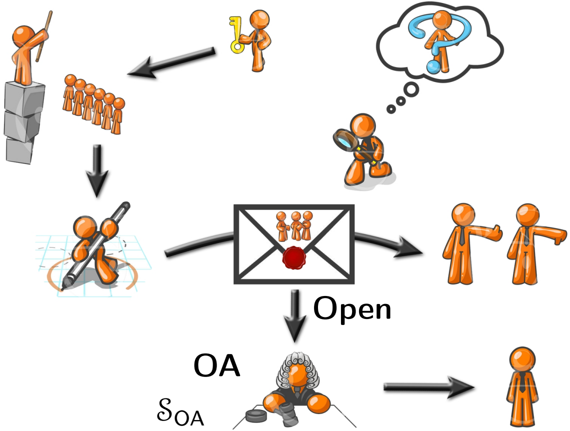
Presentation



Presentation



Presentation



Dynamic Group Signature

Dynamic Group Signature

It is a tuple of algorithms (**Setup**, **Join**, **Sign**, **Verify**, **Open**) acting according to their name.

Dynamic Group Signature

Dynamic Group Signature

It is a tuple of algorithms (**Setup**, **Join**, **Sign**, **Verify**, **Open**) acting according to their name.

- **Setup:**
  `Input:` security parameter λ, bound on group size N
  `Output:` public parameters $\mathcal{Y}$, group manager's secret key $\mathcal{S}_{\mathsf{GM}}$, the opening authority's secret key $\mathcal{S}_{\mathsf{OA}}$;

Dynamic Group Signature

Dynamic Group Signature

It is a tuple of algorithms (**Setup**, **Join**, **Sign**, **Verify**, **Open**) acting according to their name.

- **Join:** interactive protocols between $\mathcal{U}_i \rightleftarrows$ **GM**. Provide $(\mathsf{cert}_i, \mathsf{sec}_i)$ to $\mathcal{U}_i$. Where cert_i attests the secret sec_i. Update the user list along with the certificates;

Dynamic Group Signature

Dynamic Group Signature

It is a tuple of algorithms (**Setup**, **Join**, **Sign**, **Verify**, **Open**) acting according to their name.

- **Sign** and **Verify** proceed in the obvious way;
- **Open**:
  `Input`: **OA**'s secret $\mathcal{S}_{\mathsf{OA}}$, M and Σ
  `Output`: i.

Security Notions

Three security notions

- **Anonymity** Only **OA** can open a signature;

Security Notions

Three security notions

- **Anonymity** Only **OA** can open a signature;
- **Traceability** Security of honest **GM** against malicious users who want to escape from traceability;

Security Notions

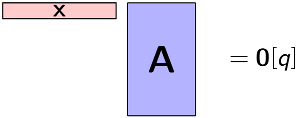
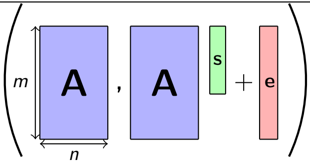
Three security notions

- **Anonymity** Only **OA** can open a signature;
- **Traceability** Security of honest **GM** against malicious users who want to escape from traceability;
- **Non-frameability** Security of honest members against malicious **GM**/**OA** authorities.

Security Assumptions: SIS and LWE

Parameters: n dimension, $m \geqslant n$, q modulus.

For $\mathbf{A} \hookleftarrow \mathbb{Z}_q^{m \times n}$:

Small Integer Solution	**Learning With Errors**
	
	$\mathbf{s} \hookleftarrow \mathbb{Z}_q^n$, $\mathbf{e}$ a small error.
Goal: Given $\mathbf{A} \hookleftarrow \mathbb{Z}_q^{m \times n}$, find $\mathbf{x} \in \mathbb{Z}^m$ small.	Goal: Given $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e})$, find $\mathbf{s} \in \mathbb{Z}_q^n$.

Lattice-based cryptography?

Lattice hard problems
find a short vector in a lattice.
Worst-case

↓

Hardness assumptions
LWE, SIS.
Average-case

↓

Security properties
anonymity, traceability, non-frameability.

Outline

From Static to Dynamic

- Designed from a recent static group signature proposed by Ling, Nguyen and Wang [LNW15].

From Static to Dynamic

- Designed from a recent static group signature proposed by Ling, Nguyen and Wang [LNW15].

- Other solutions [GKV10,LLLS13] use membership certificates made of a complete basis...

  ...which is problematic here.

From Static to Dynamic

Difficulties

- Separate the secrets between **OA** and **GM**;

From Static to Dynamic

Difficulties

- Separate the secrets between **OA** and **GM**;
- Bind the user to a unique public syndrome $\mathbf{v}_i = \mathbf{D}^T \mathbf{z}_i \in \mathbb{Z}_q^n$ for some matrix $\mathbf{D} \in \mathbb{Z}_q^{m \times n}$;

From Static to Dynamic

Difficulties

- Separate the secrets between **OA** and **GM**;
- Bind the user to a unique public syndrome $\mathbf{v}_i = \mathbf{D}^T \mathbf{z}_i \in \mathbb{Z}_q^n$ for some matrix $\mathbf{D} \in \mathbb{Z}_q^{m \times n}$;
- Previous schemes based on [LLLS13] do not interact well with the non-homogeneous terms $\mathbf{v}_i$ needed for *non-frameability* purposes;

From Static to Dynamic

Difficulties

- Separate the secrets between **OA** and **GM**;
- Bind the user to a unique public syndrome $\mathbf{v}_i = \mathbf{D}^T \mathbf{z}_i \in \mathbb{Z}_q^n$ for some matrix $\mathbf{D} \in \mathbb{Z}_q^{m \times n}$;
- Previous schemes based on [LLLS13] do not interact well with the non-homogeneous terms $\mathbf{v}_i$ needed for *non-frameability* purposes;
- Be secure against *framing attacks* without compromising previous security properties;

From Static to Dynamic Our solution – Ingredients

Boyen's signature (PKC'10)

Given $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and $\{\mathbf{A}_i\}_{i=0}^{\ell} \in \mathbb{Z}_q^{m \times n}$, the signature is a **small**

$$\mathbf{d} \in \mathbb{Z}_q^{2m} \;\; \text{s.t.} \;\; \mathbf{d}^T \cdot \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} m_i \mathbf{A}_i} \right] = 0[q].$$

The private key is a short $\mathbf{T_A} \in \mathbb{Z}_q^{m \times m}$ s.t. $\mathbf{T_A} \cdot \mathbf{A} = 0[q]$.

In our context: **GM**'s secret is $\mathbf{T_A}$.

From Static to Dynamic Our solution – Ingredients

Boyen's signature (PKC'10)

Given $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and $\{\mathbf{A}_i\}_{i=0}^{\ell} \in \mathbb{Z}_q^{m \times n}$, the signature is a **small**

$$\mathbf{d} \in \mathbb{Z}_q^{2m} \quad \text{s.t.} \quad \mathbf{d}^T \cdot \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} m_i \mathbf{A}_i} \right] = 0[q].$$

The private key is a short $\mathbf{T}_{\mathbf{A}} \in \mathbb{Z}_q^{m \times m}$ s.t. $\mathbf{T}_{\mathbf{A}} \cdot \mathbf{A} = 0[q]$.

In our context: **GM**'s secret is $\mathbf{T}_{\mathbf{A}}$.

The Böhl *et al.* variant (Eurocrypt'13)

$$\underset{\substack{\uparrow \\ \text{cert}_i}}{\mathbf{d}_i}^T \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} m_i \mathbf{A}_i} \right] = \underset{\substack{\uparrow \\ \text{sec}_i}}{\mathbf{z}_i}^T \mathbf{D} + \mathbf{u}^T [q]$$

From Static to Dynamic Our solution

Setup: $\mathcal{Y} = (\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{D}, \mathbf{u})$ $\quad \ell = \log(N)$ ($e.g.$ $\ell = 30$)
Where: $\mathbf{A}, \mathbf{A}_0, \ldots, \mathbf{A}_\ell, \mathbf{B}, \mathbf{D} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{u} \in \mathbb{Z}_q^n$

From Static to Dynamic Our solution

Setup: $\mathcal{Y} = (\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{D}, \mathbf{u})$ $\quad \ell = \log(N)$ (*e.g.* $\ell = 30$)
Where: $\mathbf{A}, \mathbf{A}_0, \ldots, \mathbf{A}_\ell, \mathbf{B}, \mathbf{D} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{u} \in \mathbb{Z}_q^n$

Join algorithm:

$\mathcal{U}_i$ GM

From Static to Dynamic Our solution

Setup: $\mathcal{Y} = (\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{D}, \mathbf{u})$ $\quad \ell = \log(N)$ (*e.g.* $\ell = 30$)
Where: $\mathbf{A}, \mathbf{A}_0, \ldots, \mathbf{A}_\ell, \mathbf{B}, \mathbf{D} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{u} \in \mathbb{Z}_q^n$

Join algorithm:

$\mathcal{U}_i$ **GM**

$\mathbf{z}_{i,0} \hookleftarrow$ short vector in $\mathbb{Z}^m$

$\mathbf{v}_{i,0}^T = \mathbf{z}_{i,0}^T \mathbf{D}$

From Static to Dynamic Our solution

Setup: $\mathcal{Y} = (\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{D}, \mathbf{u})$ $\quad \ell = \log(N)$ (*e.g.* $\ell = 30$)
Where: $\mathbf{A}, \mathbf{A}_0, \ldots, \mathbf{A}_\ell, \mathbf{B}, \mathbf{D} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{u} \in \mathbb{Z}_q^n$

Join algorithm:

$\mathcal{U}_i$ | **GM**

$\mathbf{z}_{i,0} \hookleftarrow$ short vector in $\mathbb{Z}^m$

$\mathbf{v}_{i,0}^T = \mathbf{z}_{i,0}^T \mathbf{D} \xrightarrow{\mathbf{v}_{i,0}}$

$\mathrm{id}_i \leftarrow$ identity $\in \{0,1\}^\ell$

$\mathbf{z}_{i,1} \hookleftarrow$ short vector in $\mathbb{Z}^m$

From Static to Dynamic Our solution

Setup: $\mathcal{Y} = (\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{D}, \mathbf{u})$ $\quad \ell = \log(N)$ (*e.g.* $\ell = 30$)
Where: $\mathbf{A}, \mathbf{A}_0, \ldots, \mathbf{A}_\ell, \mathbf{B}, \mathbf{D} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{u} \in \mathbb{Z}_q^n$

Join algorithm:

$\mathcal{U}_i$		**GM**
$\mathbf{z}_{i,0} \hookleftarrow$ short vector in $\mathbb{Z}^m$		
$\mathbf{v}_{i,0}^T = \mathbf{z}_{i,0}^T \mathbf{D}$	$\xrightarrow{\mathbf{v}_{i,0}}$	
		$\mathrm{id}_i \leftarrow$ identity $\in \{0,1\}^\ell$
	$\xleftarrow{(\mathrm{id}_i, \mathbf{z}_{i,1})}$	$\mathbf{z}_{i,1} \hookleftarrow$ short vector in $\mathbb{Z}^m$
$\mathbf{z}_i = \mathbf{z}_{i,0} + \mathbf{z}_{i,1}$		
$\mathbf{v}_i^T = \mathbf{z}_i^T \mathbf{D}$		
Authenticate $\mathbf{v}_i$, id_i and $\mathbf{z}_i$		

From Static to Dynamic Our solution

Setup: $\mathcal{Y} = (\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{D}, \mathbf{u})$ $\quad \ell = \log(N)$ (*e.g.* $\ell = 30$)
Where: $\mathbf{A}, \mathbf{A}_0, \ldots, \mathbf{A}_\ell, \mathbf{B}, \mathbf{D} \in \mathbb{Z}_q^{m\times n}$ and $\mathbf{u} \in \mathbb{Z}_q^n$

Join algorithm:

$\mathcal{U}_i$ | **GM**

$\mathbf{z}_{i,0} \hookleftarrow$ short vector in $\mathbb{Z}^m$

$\mathbf{v}_{i,0}^T = \mathbf{z}_{i,0}^T \mathbf{D} \xrightarrow{\mathbf{v}_{i,0}}$

$\mathrm{id}_i \leftarrow$ identity $\in \{0,1\}^\ell$

$\xleftarrow{(\mathrm{id}_i, \mathbf{z}_{i,1})}$ $\mathbf{z}_{i,1} \hookleftarrow$ short vector in $\mathbb{Z}^m$

$\mathbf{z}_i = \mathbf{z}_{i,0} + \mathbf{z}_{i,1}$

$\mathbf{v}_i^T = \mathbf{z}_i^T \mathbf{D}$

Authenticate $\mathbf{v}_i$, id_i and $\mathbf{z}_i$ $\xrightarrow{\mathbf{v}_i}$ $\mathbf{d}_i$, s.t.

$$\mathbf{d}_i^T \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} \mathrm{id}_i \mathbf{A}_i}\right] = \mathbf{v}_i^T + \mathbf{u}^T [q]$$

From Static to Dynamic Our solution

Setup: $\mathcal{Y} = (\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{D}, \mathbf{u})$ $\quad \ell = \log(N)$ (*e.g.* $\ell = 30$)
Where: $\mathbf{A}, \mathbf{A}_0, \ldots, \mathbf{A}_\ell, \mathbf{B}, \mathbf{D} \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{u} \in \mathbb{Z}_q^n$

Join algorithm:

$\mathcal{U}_i$		GM
$\mathbf{z}_{i,0} \hookleftarrow$ short vector in $\mathbb{Z}^m$		
$\mathbf{v}_{i,0}^T = \mathbf{z}_{i,0}^T \mathbf{D}$	$\xrightarrow{\mathbf{v}_{i,0}}$	
		$\mathrm{id}_i \leftarrow$ identity $\in \{0,1\}^\ell$
	$\xleftarrow{(\mathrm{id}_i, \mathbf{z}_{i,1})}$	$\mathbf{z}_{i,1} \hookleftarrow$ short vector in $\mathbb{Z}^m$
$\mathbf{z}_i = \mathbf{z}_{i,0} + \mathbf{z}_{i,1}$		
$\mathbf{v}_i^T = \mathbf{z}_i^T \mathbf{D}$		
Authenticate $\mathbf{v}_i$, id_i and $\mathbf{z}_i$	$\xrightarrow{\mathbf{v}_i}$	$\mathbf{d}_i$, s.t. $\mathbf{d}_i^T \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} \mathrm{id}_i \mathbf{A}_i}\right] = \mathbf{v}_i^T + \mathbf{u}^T \, [q]$
$(\mathrm{cert}_i; \mathrm{sec}_i) = ((\mathrm{id}_i, \mathbf{d}_i); \mathbf{z}_i)$	$\xleftarrow{\mathbf{d}_i}$	

From Static to Dynamic Our solution

Sign algorithm:
$\mathbf{c} := \mathbf{Enc}(\mathrm{id}_i, \mathbf{d}_i)$

From Static to Dynamic Our solution

Sign algorithm:

$\mathbf{c} := \mathbf{Enc}(\mathrm{id}_i, \mathbf{d}_i)$ $\pi_K :=$ proof that $\mathbf{c}$ is correct and

$$\mathbf{d}_i^T \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} \mathrm{id}_i \mathbf{A}_i} \right] = \mathbf{v}_i^T + \mathbf{u}^T [q]$$

From Static to Dynamic Our solution

Sign algorithm:

$\mathbf{c} := \mathbf{Enc}(\mathrm{id}_i, \mathbf{d}_i)$ $\quad \pi_K :=$ proof that $\mathbf{c}$ is correct and

$$\mathbf{d}_i^T \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} \mathrm{id}_i \mathbf{A}_i} \right] = \mathbf{v}_i^T + \mathbf{u}^T [q]$$

Difference with the Ling *et al.* scheme

We encrypt $\mathbf{d}$ and id_i not only id_i to enable signature openings.

From Static to Dynamic Our solution

Open algorithm:

- **OA** decrypts **c** to get $(\mathrm{id}, \mathbf{d})$;
- Using id and **d**, **OA** computes the associated syndrome **v**;
- **OA** checks that $(\mathbf{v}, \mathrm{id}, i, \mathsf{upk}[i], \overbrace{\mathit{sig}}^{=\mathit{Sign}_{\mathbf{usk}[i]}(\mathbf{v}_i, \mathrm{id}_i)})$ is in the records and that *sig* is correct.

  If so then return i; otherwise return $\perp$.

Efficiency

Remark

We use the "smudging" technique: making 2 distributions centered around 0 statistically close using a huge noise.

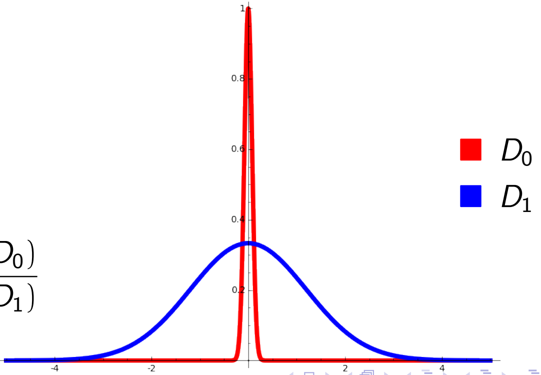
Goal:

$D_0 + D_1 \approx D_1$

in $\mathbb{Z}$ or $\mathbb{R}$

Statistical distance:

$$\Delta(D_0 + D_1, D_1) \approx \frac{\sigma(D_0)}{\sigma(D_1)}$$



Efficiency

Remark

We use the "smudging" technique: making 2 distributions centered around 0 statistically close using a huge noise.

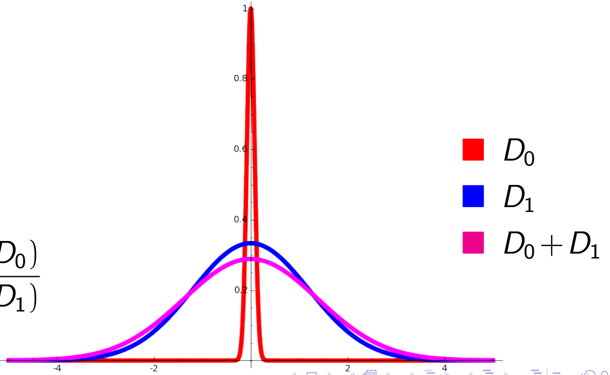
Goal:

$D_0 + D_1 \approx D_1$

in $\mathbb{Z}$ or $\mathbb{R}$

Statistical distance:

$$\Delta(D_0 + D_1, D_1) \approx \frac{\sigma(D_0)}{\sigma(D_1)}$$



Efficiency

Consequence

We need an exponential-size modulus q in the security parameter λ.

Efficiency

Consequence

We need an exponential-size modulus q in the security parameter λ.

Problem

Our protocol is somewhat costly.

Outline

Conclusion

Main contribution

First dynamic group signature based on lattice assumptions.

Technical contribution

We combine the Böhl *et al.* variant of Boyen's signature and the Ling *et al.* NIZK proofs.

Extensions

Possible extension supporting proofs of correct opening [BSZ05].
Possible use of the join protocol to certify hidden data.

Open problem

Prove the security without *smudging*: possibly more efficient parameters.

References

Mihir Bellare, Haixia Shi, Chong Zhang.
Foundations of group signatures: The case of dynamic groups
(CT-RSA'05)

Aggelos Kiayias and Moti Yung.
Secure scalable group signature with dynamic joins and separable authorities
(International Journal of Security and Networks)

Fabien Laguillaumie, Adeline Langlois, Benoit Libert, Damien Stehlé.
Lattice-based group signature scheme with verifier-local revocation
(Asiacrypt'13)

San Ling, Khoa Nguyen, and Huaxiong Wang.
Group Signatures from Lattices: Simpler, Tighter, Shorter, Ring-Based
(PKC'15)

Question Time

Thank you all for your attention!

One-Time Signature

Definition

A *one-time signature scheme* consists of a triple of algorithms $\Pi^{\mathrm{ots}} = (\mathcal{G}, \mathcal{S}, \mathcal{V})$. *Behaves like a digital signature scheme.*

Strong unforgeability: impossible to forge a valid signature *even for a previously signed message.*

Usage

We use one-time signature to provide CCA anonymity using Canetti-Halevi-Katz methodology.

CCA anonymity

Definition

No PPT adversary $\mathcal{A}$ can win the following game with non negligible probability:

- $\mathcal{A}$ makes open queries.
- $\mathcal{A}$ chooses $M^\star$ and two different $(\mathsf{cert}_i^\star, \mathsf{sec}_i^\star)_{i\in\{0,1\}}$
- $\mathcal{A}$ receives $\sigma^\star = Sign_{\mathsf{cert}_b^\star,\mathsf{sec}_b^\star}(M^\star)$ for some $b \in \{0, 1\}$
- $\mathcal{A}$ makes other open queries
- $\mathcal{A}$ returns b', and wins if $b = b'$

ZK Proofs

Σ-protocol [Dam10]

3-move scheme: (**Commit**, **Challenge**, **Answer**) *between 2 users*.

Fiat-Shamir Heuristic

Make the Σ-protocol non-interactive by setting the challenge to be $H(\mathbf{Commit}, \mathrm{Public})$

Smudging