Lattice-Based Group Signature for Dynamic Groups

Journées C2

Benoît Libert, **Fabrice Mouhartem**

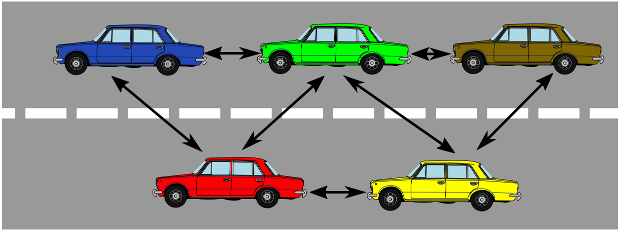
ÉNS de Lyon, LIP (AriC)

October 6, 2016

ENS DE LYON

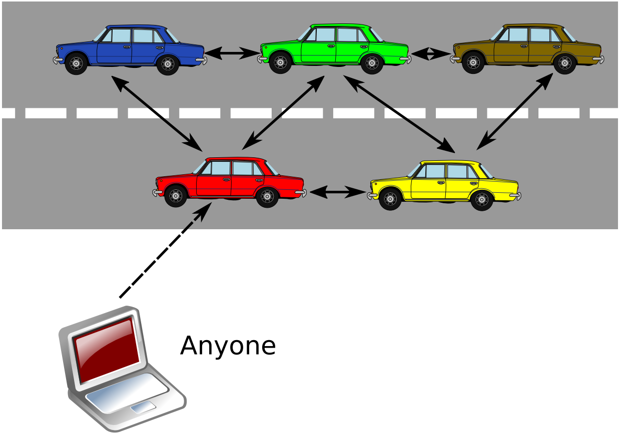
Example

Smart cars



Example

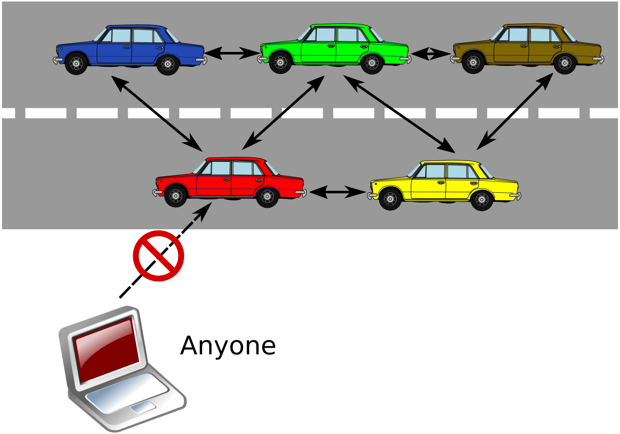
Smart cars



Example

Smart cars

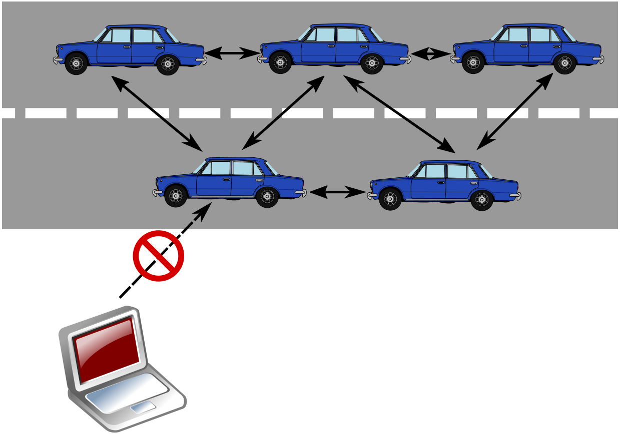
- Authenticity
- Integrity



Example

Smart cars

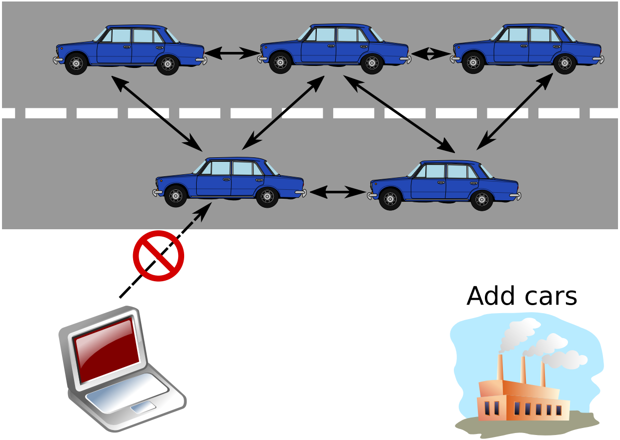
- Authenticity
- Integrity
- Anonymity



Example

Smart cars

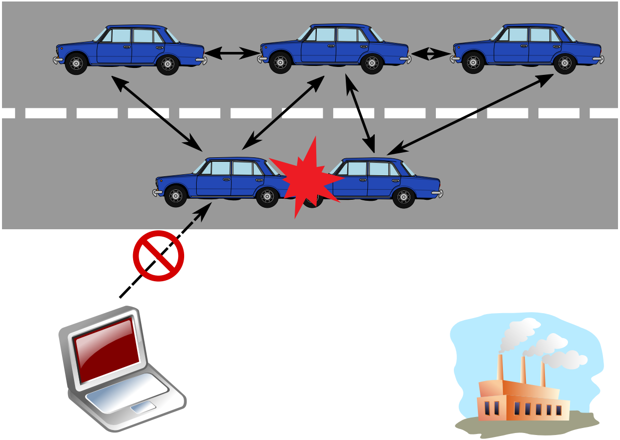
- Authenticity
- Integrity
- Anonymity
- Dynamicity



Example

Smart cars

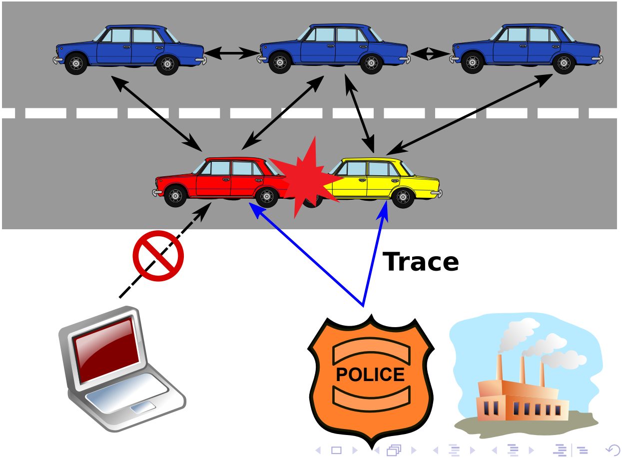
- Authenticity
- Integrity
- Anonymity
- Dynamicity



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 definition by Bellare-Micciancio-Warinschi for **static** groups.

History

- 1991 Introduced by Chaum and Van Heyst
- 2000 First scalable solution by Ateniese-Camenisch-Joye-Tsudik
- 2003 Formal definition by Bellare-Micciancio-Warinschi for **static** groups.
- 2004 Model for **dynamic** groups by Kiayias-Yung
- 2004 Model for **dynamic** groups by Bellare-Shi-Zhang

History

- 1991 Introduced by Chaum and Van Heyst
- 2000 First scalable solution by Ateniese-Camenisch-Joye-Tsudik
- 2003 Formal definition by Bellare-Micciancio-Warinschi for **static** groups.
- 2004 Model for **dynamic** groups by Kiayias-Yung
- 2004 Model for **dynamic** groups by Bellare-Shi-Zhang
- 2010 First scheme based on **lattices** by Gordon-Katz-Vaikuntanathan with linear size in the max. size of the group
- 2013 Down to log-size by Laguillaumie-Langlois-Libert-Stehlé
- 2015 More efficient schemes from Ling-Nguyen-Wang and Nguyen-Zhang-Zhang

History

- 1991 Introduced by Chaum and Van Heyst
- 2000 First scalable solution by Ateniese-Camenisch-Joye-Tsudik
- 2003 Formal definition by Bellare-Micciancio-Warinschi for **static** groups.
- 2004 Model for **dynamic** groups by Kiayias-Yung
- 2004 Model for **dynamic** groups by Bellare-Shi-Zhang
- 2010 First scheme based on **lattices** by Gordon-Katz-Vaikuntanathan with linear size in the max. size of the group
- 2013 Down to log-size by Laguillaumie-Langlois-Libert-Stehlé
- 2015 More efficient schemes from Ling-Nguyen-Wang and Nguyen-Zhang-Zhang

No dynamic group signature scheme based on lattices

Lattice-Based Cryptography

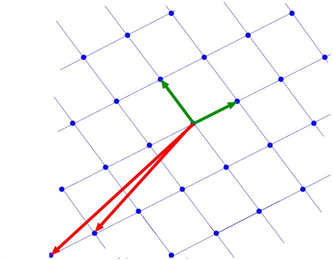
Lattice

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

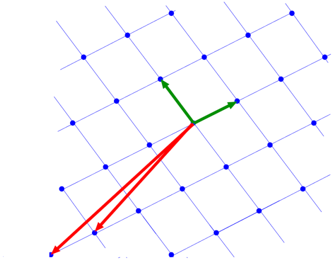
A lattice is a discrete subgroup of $\mathbb{R}^n$. Can be seen as integer linear combinations of a finite set of vectors.



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 non-zero short vector in a lattice is hard.

Lattice-Based Cryptography

Why?

- Simple and asymptotically efficient;

Lattice-Based Cryptography

Why?

- Simple and asymptotically efficient;
- Secure under well-studied assumptions;

Lattice-Based Cryptography

Why?

- Simple and asymptotically efficient;
- Secure under well-studied assumptions;
- Conjectured resistant to a quantum adversary;

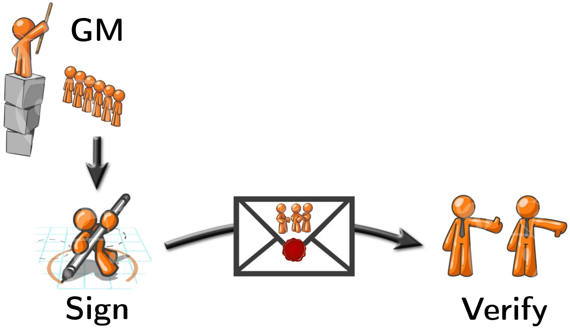
Lattice-Based Cryptography

Why?

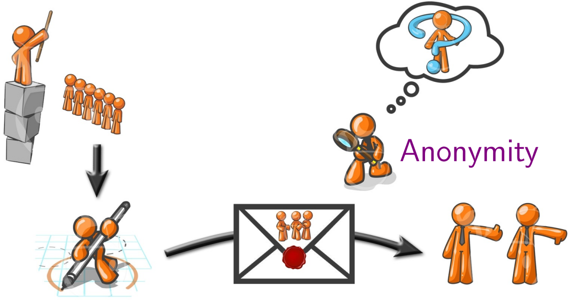
- Simple and asymptotically efficient;
- Secure under well-studied assumptions;
- Conjectured resistant to a quantum adversary;
- Powerful functionalities.

Outline

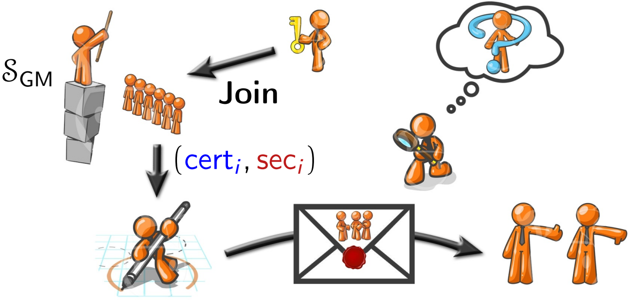
Presentation



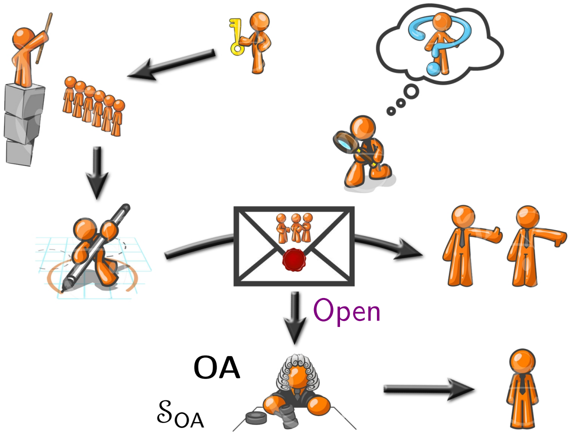
Presentation



Presentation



Presentation



Dynamic Group Signature

Dynamic Group Signature

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

Dynamic Group Signature

Dynamic Group Signature

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

- **Setup:** done in a trusted fashion
  `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 names.

- **Join:** interactive protocols between $\mathcal{U}_i \rightleftarrows \mathbf{GM}$. 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 names.

- **Sign** and **Verify** proceed as in standard digital signatures.
- **Open:**
  `Input:` **OA**'s secret $\mathcal{S}_{\mathrm{OA}}$, 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;

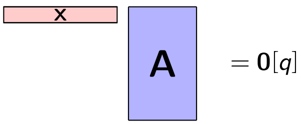
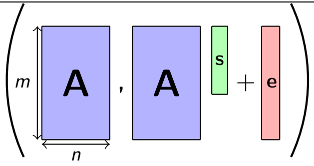
Security Notions

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.

Hardness 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 $\mathbf{x} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}$ 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
  (due to non-homogeneous SIS).

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 $\mathbf{v}_i^T = \underbrace{\mathbf{z}_i^T}_{\in \mathbb{Z}^m} \mathbf{D} \in \mathbb{Z}_q^n$ 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 $\mathbf{v}_i^T = \underbrace{\mathbf{z}_i^T}_{\in \mathbb{Z}^m} \mathbf{D} \in \mathbb{Z}_q^n$ for some matrix $\mathbf{D} \in \mathbb{Z}_q^{m \times n}$;

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

From Static to Dynamic

Difficulties

- 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

- 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**

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

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 $\mathbf{T}_{\mathbf{A}}$.

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**

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

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)

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

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: $\mathbf{A}, \mathbf{A}_0, \dots, \mathbf{A}_\ell, \mathbf{B}, \mathbf{D} \in \mathbb{Z}_q^{m \times n}$ 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. $\mathbf{d}_i^T \left[\dfrac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} \mathrm{id}_i \mathbf{A}_i}\right] = \mathbf{v}_i^T + \mathbf{u}^T\,[q]$
$(\text{cert}_i; \text{sec}_i) = ((\mathrm{id}_i, \mathbf{d}_i); \mathbf{z}_i)$	$\xleftarrow{\mathbf{d}_i}$	

From Static to Dynamic Our solution

Sign algorithm:

$\mathbf{c}_1 := \mathbf{Enc}(\mathrm{id}_i) \quad \mathbf{c}_2 := \mathbf{Enc}(\mathbf{d}_i)$

From Static to Dynamic Our solution

Sign algorithm:

$\mathbf{c}_1 := \mathbf{Enc}(\mathrm{id}_i) \quad \mathbf{c}_2 := \mathbf{Enc}(\mathbf{d}_i)$

$\pi_K :=$ proof that $\mathbf{c}_1$, $\mathbf{c}_2$ are 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:

$\mathbf{c}_1 := \mathbf{Enc}(\mathrm{id}_i) \quad \mathbf{c}_2 := \mathbf{Enc}(\mathbf{d}_i)$

$\pi_K :=$ proof that $\mathbf{c}_1$, $\mathbf{c}_2$ are correct and

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

Open algorithm:

- **OA** decrypts $\mathbf{c}_1, \mathbf{c}_2$ to get id and $\mathbf{d}$;
- Using id and $\mathbf{d}$, **OA** computes the associated syndrome $\mathbf{v}$;
- **OA** checks that $(\mathbf{v}, \mathrm{id}, i, \mathrm{upk}[i], \overbrace{sig}^{=Sign_{\mathbf{usk}[\mathrm{i}]}(\mathbf{v}_i, \mathrm{id}_i)})$ is in the records and that sig is correct.

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

Technical difficulties

Hybrid argument

Real game $\longrightarrow$ **Game 1** $\longrightarrow$ **Game 2** $\longrightarrow$ **Hard Game**

Hardness assumptions

- Similar to the proof of Böhl et al.

Technical difficulties

Hybrid argument

Real game $\longrightarrow$ **Game 1** $\longrightarrow$ **Game 2** $\longrightarrow$ **Hard Game**

Hardness assumptions

- Similar to the proof of Böhl et al.
- For one request: attacker's view differs from the real setting:

Technical difficulties

Hybrid argument

Real game $\longrightarrow$ **Game 1** $\longrightarrow$ **Game 2** $\longrightarrow$ **Hard Game**

Hardness assumptions

- Similar to the proof of Böhl et al.
- For one request: attacker's view differs from the real setting:
  - Possible solution: smudging (requires $q \sim \exp(\lambda)$)

Technical difficulties

Hybrid argument

Real game → Game 1 → Game 2 → Hard Game

Hardness assumptions

- Similar to the proof of Böhl et al.
- For one request: attacker's view differs from the real setting:
  - Possible solution: smudging (requires $q \sim \exp(\lambda)$)
  - Use of the Rényi Divergence:

    $\Pr[W_2] \geqslant \Pr[W_1]^2 / R_2(Game_1 \| Game_2)$.

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

- Easily support proofs of correct opening [BSZ05];
- Join protocol extends to certify hidden data (signature with efficient protocols [CL02]).

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

ZK Proofs

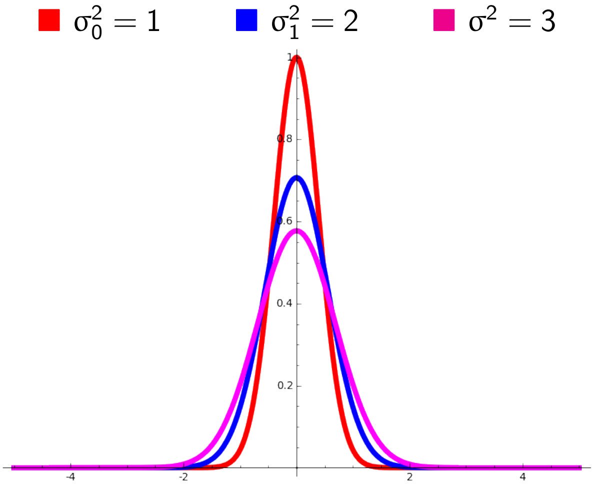
Σ-protocol [Dam10]

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

Fiat-Shamir Heuristic

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

Smudging



From Static to Dynamic Our solution — Ingredients

Goal

CCA-Anonymity: anonymity under opening oracle.

From Static to Dynamic Our solution — Ingredients

Goal

CCA-Anonymity: anonymity under opening oracle.

$\uparrow$

Canetti-Halevi-Katz transformation

From an IBE we can construct a *IND-CCA* public key encryption scheme.

From Static to Dynamic Our solution — Ingredients

Goal

CCA-Anonymity: anonymity under opening oracle.

$\uparrow$

Canetti-Halevi-Katz transformation

From an IBE we can construct a *IND-CCA* public key encryption scheme.

Identity Based Encryption

An asymmetric encryption scheme (*Setup*, *Keygen*, *Enc*, *Dec*) using identity as public key.

Canetti-Halevi-Katz idea

CCA security

M_0, M_1
$C = Enc(M_b), b \in \{0, 1\}$
Goal: find b, allowed to decrypt messages (all but C).

Canetti-Halevi-Katz idea

CCA security

M_0, M_1
$C = Enc(M_b), b \in \{0, 1\}$
Goal: find b, allowed to decrypt messages (all but C).

Enc(pk, M):

$(\mathrm{VK}, \mathrm{SK}) \leftarrow \mathbf{Gen}^{\mathrm{ots}}$
$C = \mathbf{Enc}^{IBE}(\mathrm{VK}, M)$
$\sigma \leftarrow \mathbf{Sign}^{\mathrm{ots}}(\mathrm{SK}, M)$
return (VK, C, σ)

Sketch of the security proofs – Traceability

$\mathcal{A}$ produces a forgery $M^\star, \Sigma^\star$ that verifies Böhl et al. signature scheme.

- Guess the identity $\mathrm{id}^\star$ that $\mathcal{A}$ used to forge $\Sigma^\star$;
- Program the parameters to solve an hard problem.

From Static to Dynamic Our solution – Ingredients

Security proof of the Boyen signature

Lattice based-scheme use short basis as *trapdoor* information.

From Static to Dynamic Our solution – Ingredients

Security proof of the Boyen signature

Lattice based-scheme use short basis as *trapdoor* information.

SampleUp $\mathbf{A}' = \left[\frac{\mathbf{A}}{\mathbf{B}\cdot\mathbf{A}+\mathbf{C}}\right] \in \mathbb{Z}_q^{2m\times n}, \mathbf{A} \in \mathbb{Z}_q^{m\times n}, \mathbf{T_A} \in \mathbb{Z}_q^{m\times m}, \sigma \mapsto$ gaussian $\mathbf{v} \in \mathbb{Z}_q^n$, s.t. $\mathbf{v}^T\mathbf{A}' = \mathbf{0}[q]$

SampleDown $\mathbf{A}' = \left[\frac{\mathbf{A}}{\mathbf{B}\cdot\mathbf{A}+\mathbf{C}}\right] \in \mathbb{Z}_q^{2m\times n}, \mathbf{C} \in \mathbb{Z}_q^{m\times n}, \mathbf{T_C} \in \mathbb{Z}_q^{m\times m}, \sigma \mapsto$ gaussian $\mathbf{v} \in \mathbb{Z}_q^n$, s.t. $\mathbf{v}^T\mathbf{A}' = \mathbf{0}[q]$

From Static to Dynamic Our solution – Ingredients

Security proof of the Boyen signature

Boyen's signature

$$\mathbf{d}^T \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} m_i \mathbf{A}_i}\right] = \mathbf{0}[q]$$

Idea.

From Static to Dynamic Our solution – Ingredients

Security proof of the Boyen signature

Boyen's signature

$$\mathbf{d}^T \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} m_i \mathbf{A}_i}\right] = \mathbf{0}[q]$$

Idea. Set $\mathbf{A}_i = \mathbf{Q}_i \mathbf{A} + h_i \mathbf{C}$

From Static to Dynamic Our solution – Ingredients

Security proof of the Boyen signature

Boyen's signature

$$\mathbf{d}^T \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} m_i \mathbf{A}_i} \right] = \mathbf{0}[q]$$

Idea. Set $\mathbf{A}_i = \mathbf{Q}_i \mathbf{A} + h_i \mathbf{C}$

$$\rightarrow \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} m_i \mathbf{A}_i} \right] = \left[\frac{\mathbf{A}}{(\mathbf{Q}_0 + \sum_{i=1}^{\ell} m_i \mathbf{Q_i})\mathbf{A} + h_M \mathbf{C}} \right]$$

From Static to Dynamic Our solution – Ingredients

Security proof of the Boyen signature

Boyen's signature

$$\mathbf{d}^T \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} m_i \mathbf{A}_i} \right] = \mathbf{0}[q]$$

Idea. Set $\mathbf{A}_i = \mathbf{Q}_i\mathbf{A} + h_i\mathbf{C}$

$$\rightarrow \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} m_i \mathbf{A}_i} \right] = \left[\frac{\mathbf{A}}{(\mathbf{Q}_0 + \sum_{i=1}^{\ell} m_i \mathbf{Q_i})\mathbf{A} + h_M \mathbf{C}} \right]$$

$\Rightarrow$ We can use SampleUp in the real setup and SampleDown in the reduction whenever $h_M \neq 0$.

From Static to Dynamic Our solution – Ingredients

Security proof of the Boyen signature

Recall

$$\mathbf{A}' := \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} m_i \mathbf{A}_i}\right] = \left[\frac{\mathbf{A}}{(\mathbf{Q}_0 + \sum_{i=1}^{\ell} m_i \mathbf{Q_i})\mathbf{A} + h_M \mathbf{C}}\right]$$

From Static to Dynamic Our solution – Ingredients

Security proof of the Boyen signature

Recall

$$\mathbf{A}' := \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} m_i \mathbf{A}_i}\right] = \left[\frac{\mathbf{A}}{(\mathbf{Q}_0 + \sum_{i=1}^{\ell} m_i \mathbf{Q_i})\mathbf{A} + h_M \mathbf{C}}\right]$$

Forgery. $\mathcal{A}$ outputs $\mathbf{d}^\star = [\mathbf{d}_1^{\star T} | \mathbf{d}_2^{\star T}]^T$ and $M^\star = m_1^\star \ldots m_\ell^\star$ such that $\mathbf{d}^{\star T}\mathbf{A}' = 0$.

From Static to Dynamic Our solution – Ingredients

Security proof of the Boyen signature

Recall

$$\mathbf{A}' := \left[\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} m_i \mathbf{A}_i}\right] = \left[\frac{\mathbf{A}}{(\mathbf{Q}_0 + \sum_{i=1}^{\ell} m_i \mathbf{Q_i})\mathbf{A} + h_M \mathbf{C}}\right]$$

Forgery. $\mathcal{A}$ outputs $\mathbf{d}^\star = [\mathbf{d}_1^{\star T} | \mathbf{d}_2^{\star T}]^T$ and $M^\star = m_1^\star \dots m_\ell^\star$ such that $\mathbf{d}^{\star T}\mathbf{A}' = 0$.
If $h_{M^\star} = 0$, then

$$\underbrace{\left(\mathbf{d}_1^{\star T} + \mathbf{d}_2^{\star T}\left(\mathbf{Q}_0 + \sum_{i=1}^{\ell} m_i^\star \mathbf{Q}_i\right)\right)}_{\text{valid } \textbf{SIS} \text{ solution}} \mathbf{A} = \mathbf{0}[q]$$

From Static to Dynamic Our solution

Remark

Boyen's signature: the reduction aborts if C vanishes.
Böhl et al.: answer the request by "programming" the vector

$$\mathbf{u}^T = \mathbf{d}^{\dagger\,T} \left[\frac{\mathbf{A}}{(\mathbf{Q}_0 + \sum_{i=1}^{\ell} \mathrm{id}_i^{\dagger} \mathbf{Q}_i)\mathbf{A}} \right] - \mathbf{z}_{i^\dagger}^T \mathbf{D}.$$

Problem

In this request, a sum of two discrete gaussian is generated differently from the real **Join** protocol.
$\Rightarrow$ Not the same standard deviation.

From Static to Dynamic Our solution

Problem

$$\mathbf{z}_{i,0}, \mathbf{z}_{i,1}, \mathbf{z}_i \in \mathbb{Z}^m$$

Consequence.

$$\{(\mathbf{z}_i, \mathbf{z}_{i,0}, \mathbf{z}_{i,1}) | \mathbf{z}_{i,0} \hookleftarrow D_{\sigma_0}, \mathbf{z}_{i,1} \hookleftarrow D_{\sigma_1}, \mathbf{z}_i = \mathbf{z}_{i,0} + \mathbf{z}_{i,1}\}$$
$$\approx \Delta$$
$$\{(\mathbf{z}_i, \mathbf{z}_{i,0}, \mathbf{z}_{i,1}) | \mathbf{z}_i \hookleftarrow D_{\sigma}, \mathbf{z}_{i,0} \hookleftarrow D_{\sigma_0}, \mathbf{z}_{i,1} = \mathbf{z}_i - \mathbf{z}_{i,0}\}$$

Rényi Divergence

Presentation

$$R_a(P\|Q) = \left(\sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{1/(a-1)}$$

Rényi Divergence

Presentation

$$R_a(P\|Q) = \left(\sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{1/(a-1)}$$

- Measurement of the distance between two distributions

Rényi Divergence

Presentation

$$R_a(P\|Q) = \left(\sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{1/(a-1)}$$

- Measurement of the distance between two distributions
- Multiplicative instead of additive
- Probability preservation:

$$Q(A) \geqslant P(A)^{\frac{a}{a-1}} / R_a(P\|Q)$$

Rényi Divergence

Presentation

$$R_a(P\|Q) = \left(\sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}} \right)^{1/(a-1)}$$

- Measurement of the distance between two distributions
- Multiplicative instead of additive
- Probability preservation:

$$Q(A) \geqslant P(A)^{\frac{a}{a-1}} / R_a(P\|Q)$$

Rényi Divergence

Hybrid argument:

Real game $\longrightarrow$ **Game 1** $\longrightarrow$ **Game 2** $\longrightarrow$ **Hard Game**

Hardness assumptions

Rényi Divergence

Hybrid argument:

Real game $\longrightarrow$ **Game 1** $\longrightarrow$ **Game 2** $\longrightarrow$ **Hard Game**

Hardness assumptions

Bound winning probability.

Rényi Divergence

Hybrid argument:

Real game $\longrightarrow$ **Game 1** $\longrightarrow$ **Game 2** $\longrightarrow$ **Hard Game**

Hardness assumptions

Bound winning probability.
Can be done through probability preservation!

Rényi Divergence

Hybrid argument:

Real game $\longrightarrow$ **Game 1** $\longrightarrow$ **Game 2** $\longrightarrow$ **Hard Game**

Hardness assumptions

Bound winning probability.
Can be done through probability preservation!

Recall

$$Q(A) \geqslant P(A)^{\frac{a}{a-1}} / R_a(P \| Q)$$

$$\Pr[W_2] \geqslant \Pr[W_1]^{\frac{a}{a-1}} / R_a(Game_1 \| Game_2)$$

For instance: $\Pr[W_2] \geqslant \Pr[W_1]^2 / R_2(Game_1 \| Game_2)$

Rényi Divergence

In Crypto

Consequence

Usually use *statistical distance* to measure distance between probabilities.

Rényi Divergence

In Crypto

Consequence

Usually use *statistical distance* to measure distance between probabilities.

→ In our setting, implies $q \sim \exp(\lambda)$ (smudging)

Rényi Divergence

In Crypto

Consequence

Usually use *statistical distance* to measure distance between probabilities.

$\rightarrow$ In our setting, implies $q \sim \exp(\lambda)$ (smudging)

$\rightarrow$ Higher cost compared to usual lattice-based crypto parameters