Signature Schemes with Efficient Protocols and Dynamic Group Signatures from Lattice Assumptions

Benoît Libert[1,2] San Ling[3] **Fabrice Mouhartem**[1]
Khoa Nguyen[3] Huaxiong Wang[3]

[1]É.N.S. de Lyon, France

[2]CNRS, France

[3]Nanyang Technological University, Singapore

Caen, 30/11/2016

Privacy-Preserving Cryptography

Important Goal: Anonymous authentication.

Privacy-Preserving Cryptography

Important Goal: Anonymous authentication.

e.g., e-voting, e-cash, group signatures, anonymous credentials. . .

Privacy-Preserving Cryptography

Important Goal: Anonymous authentication.

e.g., e-voting, e-cash, group signatures, anonymous credentials. . .

Ingredients

- A signature scheme
- Zero-knowledge (ZK) proofs

Privacy-Preserving Cryptography

Important Goal: Anonymous authentication.

e.g., e-voting, e-cash, group signatures, anonymous credentials. . .

Ingredients

- A signature scheme
- Zero-knowledge (ZK) proofs compatible with this signature (no hash functions)

Privacy-Preserving Cryptography

Important Goal: Anonymous authentication.

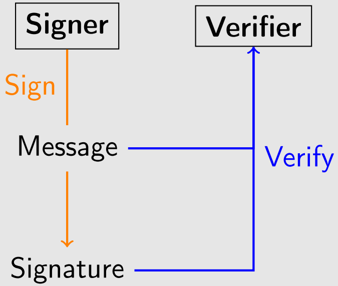
e.g., e-voting, e-cash, **group signatures**, anonymous credentials...

Ingredients

- A signature scheme
- Zero-knowledge (ZK) proofs compatible with this signature (no hash functions)

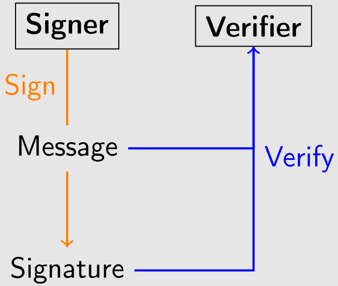
Digital Signatures

Signature Schemes



Digital Signatures

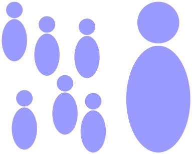
Signature Schemes



Guarantees authenticity and integrity.

Group Signatures

A user wants to take public transportations.



Group Signatures

A user wants to take public transportations.

Group Signatures

A user wants to take public transportations.

- Authenticity & Integrity

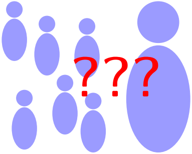
Group Signatures

A user wants to take public transportations.

- Authenticity & Integrity
- Anonymity

Group Signatures

A user wants to take public transportations.

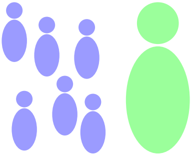


signature →

- Authenticity & Integrity
- Anonymity
- Dynamicity ⟷ Join

Group Signatures

A user wants to take public transportations.



signature

- Authenticity & Integrity
- Anonymity
- Dynamicity $\xleftrightarrow{\text{Join}}$ RATP
- Traceability

Why dynamic group signature?

Dynamic group signatures

In dynamic group signatures, new group members can be introduced at any time.

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

Why dynamic group signature?

Dynamic group signatures

In dynamic group signatures, new group members can be introduced at any time.

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

Main Differences

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

Motivation

Advantages of the dynamic group setting:

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

Motivation

Advantages of the dynamic group setting:

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

Motivation

Advantages of the dynamic group setting:

- Add users without re-running the **Setup** phase;
- Even if everyone, including authorities, is dishonest, no one can sign in your name;
- Most use cases inherently require dynamic groups (e.g., building's access control)

Commitments

Digital equivalent of a sealed box.

e.g., Pedersen Commitment
$pk = (g, h) \hookleftarrow \mathbb{G}^2$
$com = g^m \cdot h^r$
$open = (m, r)$

Commitments

Digital equivalent of a sealed box.

e.g., Pedersen Commitment
$pk = (g, h) \hookleftarrow \mathbb{G}^2$
$com = g^m \cdot h^r$
$open = (m, r)$

Properties

Commitments provide

- **Binding** property: once sealed, a value cannot be changed
- **Hiding** property: nobody is able tell what is inside the box without the key

Anonymous Credentials (Chaum'85, Camenisch-Lysyanskya'01)

Principle (e.g., U-Prove, Idemix)

Involves three parties: **Issuers**, **Users** and **Verifiers**.

- User dynamically obtains credentials from an issuer under a (pseudonym = commitment to a digital identity)
- ...and can dynamically prove possession of credentials using different (*unlinkable*) pseudonyms

Different flavors: one-show/multi-show credentials, attribute-based access control,...

Anonymous Credentials (Chaum'85, Camenisch-Lysyanskya'01)

Principle (e.g., U-Prove, Idemix)

Involves three parties: **Issuers**, **Users** and **Verifiers**.

- User dynamically obtains credentials from an issuer under a (pseudonym = commitment to a digital identity)
- ...and can dynamically prove possession of credentials using different (*unlinkable*) pseudonyms

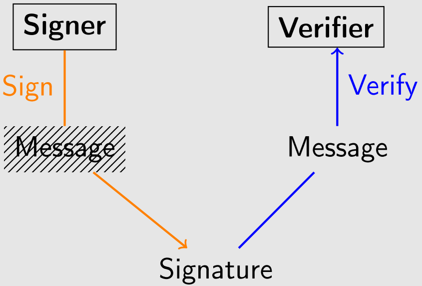
Different flavors: one-show/multi-show credentials, attribute-based access control,...

General construction from signature with efficient protocols:

- Issuer gives a user a signature on a committed message;
- User proves that same secret underlies different pseudonyms;
- User proves that he possesses a message-signature pair.

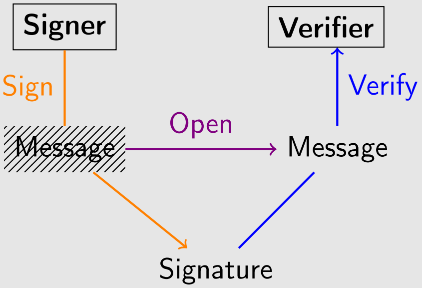
Signature with Efficient Protocols

Signature Scheme with Efficient Protocols (Camenisch-Lysyanskya, SCN'02)



Signature with Efficient Protocols

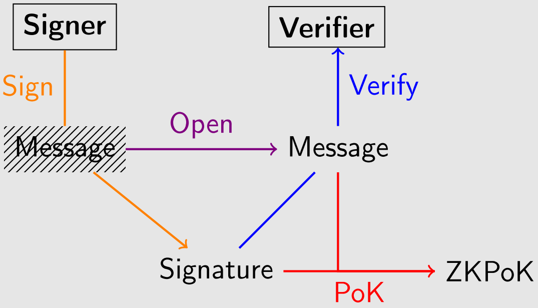
Signature Scheme with Efficient Protocols (Camenisch-Lysyanskya, SCN'02)



- Sign committed values

Signature with Efficient Protocols

Signature Scheme with Efficient Protocols (Camenisch-Lysyanskya, SCN'02)



- Sign committed values
- Proof of Knowledge (PoK) of (Message; Signature)

Lattice-Based Cryptography

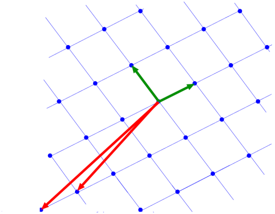
Lattice

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.



Why?

- Simple and efficient;
- **Still** conjectured quantum-resistant;
- Connection between average-case and worst-case problems;
- Powerful functionalities (e.g., FHE).

$\rightarrow$ Finding a non-zero short vector in a lattice is hard.

Hardness Assumptions: SIS and LWE

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

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

Small Integer Solution

$$\mathbf{x} \, \mathbf{A} = \mathbf{0} \ [q]$$

Goal: Given $\mathbf{A} \hookleftarrow \mathbb{Z}_q^{m \times n}$, find $\mathbf{x} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}$ small.

Learning With Errors

$$\left(\underbrace{\mathbf{A}}_{m \times n}, \ \mathbf{A}\mathbf{s} + \mathbf{e} \right)$$

$\mathbf{s} \hookleftarrow \mathbb{Z}_q^n$,

$\mathbf{e}$ a small error.

Goal: Given $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e})$, find $\mathbf{s} \in \mathbb{Z}_q^n$.

Provable Security

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

↓

Hardness assumptions
LWE, SIS.
Average-case

↓

Security properties
anonymity, traceability, non-frameability.

Group Signatures: History

1991 Chaum and Van Heyst: introduction

2000 Ateniese, Camenisch, Joye and Tsudik: first scalable solution

2003 Bellare, Micciancio and Warinschi: model for **static** groups

Group Signatures: History

1991 Chaum and Van Heyst: introduction

2000 Ateniese, Camenisch, Joye and Tsudik: first scalable solution

2003 Bellare, Micciancio and Warinschi: model for **static** groups

2004 Kiayias and Yung: model for **dynamic** groups

2004 Bellare, Shi and Zhang: model for **dynamic** groups

Group Signatures: History

1991 Chaum and Van Heyst: introduction

2000 Ateniese, Camenisch, Joye and Tsudik: first scalable solution

2003 Bellare, Micciancio and Warinschi: model for **static** groups

2004 Kiayias and Yung: model for **dynamic** groups

2004 Bellare, Shi and Zhang: model for **dynamic** groups

2010 Gordon, Katz and Vaikuntanathan: first **lattice**-based scheme

2013 Laguillaumie, Langlois, Libert and Stehlé: sub-linear signatures

Group Signatures: History

1991 Chaum and Van Heyst: introduction

2000 Ateniese, Camenisch, Joye and Tsudik: first scalable solution

2003 Bellare, Micciancio and Warinschi: model for **static** groups

2004 Kiayias and Yung: model for **dynamic** groups

2004 Bellare, Shi and Zhang: model for **dynamic** groups

2010 Gordon, Katz and Vaikuntanathan: first **lattice**-based scheme

2013 Laguillaumie, Langlois, Libert and Stehlé: sub-linear signatures

No dynamic group signature scheme based on lattices

Outline

Introduction

Definition

Presentation of the Scheme

Conclusion

Signature with Efficient Protocols (CL'02)

A signature scheme $(\mathbf{Keygen}, \mathbf{Sign}_{\mathsf{sk}}, \mathbf{Verif}_{\mathsf{vk}})$ with companion protocols:

- Sign a committed value;
- Prove possession of a signature.

Signature with Efficient Protocols (CL'02)

A signature scheme $(\mathbf{Keygen}, \mathbf{Sign}_{\mathsf{sk}}, \mathbf{Verif}_{\mathsf{vk}})$ with companion protocols:

- Sign a committed value;
- Prove possession of a signature.

Security

- Unforgeability;

Signature with Efficient Protocols (CL'02)

A signature scheme $(\mathbf{Keygen}, \mathbf{Sign}_{\mathsf{sk}}, \mathbf{Verif}_{\mathsf{vk}})$ with companion protocols:

- Sign a committed value;
- Prove possession of a signature.

Security

- Unforgeability;
- Security of the two protocols;
- Anonymity.

Signature with Efficient Protocols (CL'02)

A signature scheme $(\textbf{Keygen}, \textbf{Sign}_{\mathsf{sk}}, \textbf{Verif}_{\mathsf{vk}})$ with companion protocols:

- Sign a committed value;
- Prove possession of a signature.

Security

- Unforgeability;
- Security of the two protocols;
- Anonymity.

$\rightarrow$ many applications for privacy-based protocols

Signature with Efficient Protocols (CL'02)

A signature scheme $(\mathbf{Keygen}, \mathbf{Sign}_{sk}, \mathbf{Verif}_{vk})$ with companion protocols:

- Sign a committed value;
- Prove possession of a signature.

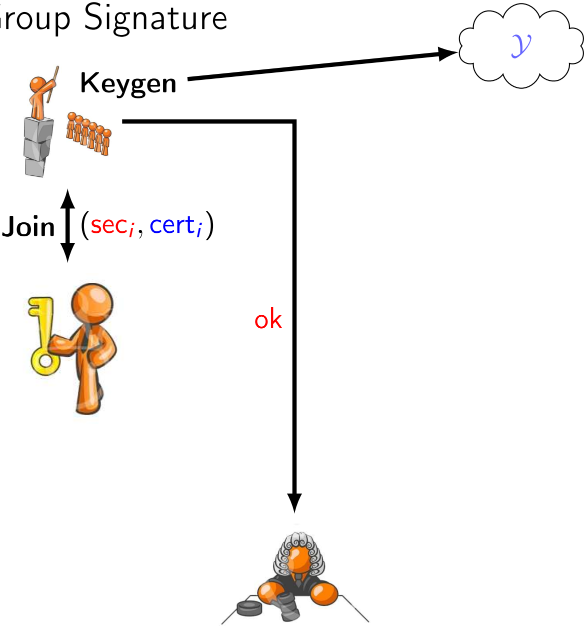
Security

- Unforgeability;
- Security of the two protocols;
- Anonymity.

$\rightarrow$ many applications for privacy-based protocols

Existing constructions rely on Strong RSA assumption or bilinear maps.

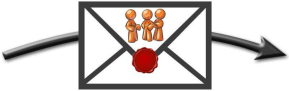
Dynamic Group Signature



Dynamic Group Signature

Sign

gsk[d]

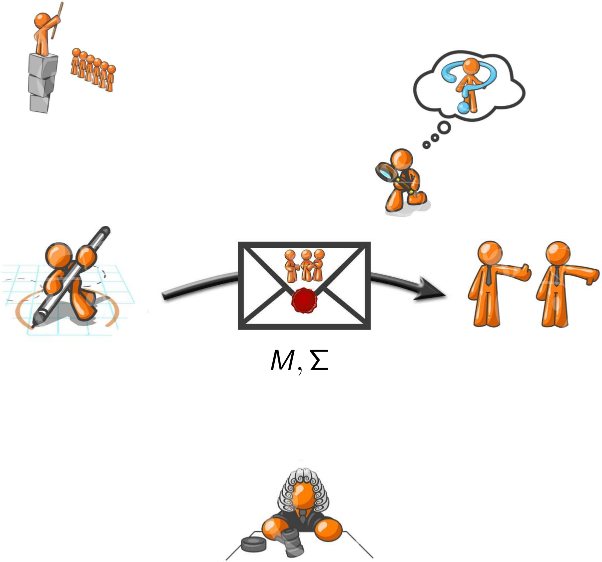


M, Σ

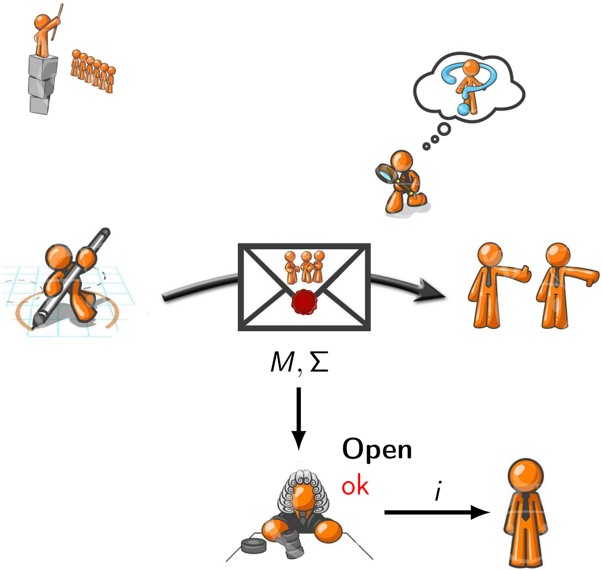
Verify

$\mathcal{Y}$

Dynamic Group Signature



Dynamic Group Signature



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:**
  `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 $\mathcal{U}_i \rightleftarrows$ **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 in the obvious way;
- **Open:**
  `Input:` **OA**'s secret $\mathcal{S}_{\mathrm{OA}}$, M and Σ
  `Output:` i.

Security

Three security notions

- **Anonymity**: only **OA** can open a signature;

Security

Three security notions

- **Anonymity**: only **OA** can open a signature;
- **Traceability** (= security of honest **GM** against users): no coalition of malicious users can create a signature that cannot be traced to one of them;

Security

Three security notions

- **Anonymity**: only **OA** can open a signature;
- **Traceability** (= security of honest **GM** against users): no coalition of malicious users can create a signature that cannot be traced to one of them;
- **Non-frameability** (= security of honest members): colluding **GM** and **OA** cannot frame honest users.

Outline

Signature with Efficient Protocols

Based on a variant of Boyen's signature (PKC'10)

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

$$\mathbf{d} \in \mathbb{Z}^{2m} \text{ s.t. } \boxed{\mathbf{A} \mid \mathbf{A}_0 + \textstyle\sum_{j=1}^{\ell} \mathfrak{m}_j \mathbf{A}_j} \cdot \mathbf{d} = \mathbf{0} \; [q].$$

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

Signature with Efficient Protocols

Based on a variant of Boyen's signature (PKC'10)

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

$$\mathbf{d} \in \mathbb{Z}^{2m} \quad \text{s.t.} \quad \left[\, \mathbf{A} \mid \mathbf{A}_0 + \textstyle\sum_{j=1}^{\ell} \mathfrak{m}_j \mathbf{A}_j \,\right] \cdot \mathbf{d} = \mathbf{0} \; [q].$$

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

(A modification of) Böhl *et al.*'s variant (Eurocrypt'13)

$\tau \leftarrow \mathcal{U}(\{0,1\}^{\ell})$, $\mathbf{D}$ and $\mathbf{u}$ are public, $\mathfrak{m} \in \{0,1\}^{2m}$ encodes Msg.

$$\left[\, \mathbf{A} \mid \mathbf{A}_0 + \textstyle\sum_{j=1}^{\ell} \tau_j \mathbf{A}_j \,\right] \cdot \mathbf{d} = \mathbf{u} + \mathbf{D} \cdot \mathfrak{m} \; [q].$$

$\rightarrow \quad \sigma = (\tau, \mathbf{d})$

Our Signature with Efficient Protocols

To sign $M \in \{0,1\}^{2m}$

- Sample random $\tau \in \{0,1\}^{\ell}$, random $\mathbf{s} \in D_{\mathbb{Z}^{2m},\tilde{\sigma}}$
- Compute $\mathbf{C}_M = \mathbf{D}_0 \cdot \mathbf{s} + \mathbf{D}_1 \cdot M \in \mathbb{Z}_q^{2n}$

Our Signature with Efficient Protocols

To sign $M \in \{0,1\}^{2m}$

- Sample random $\tau \in \{0,1\}^{\ell}$, random $\mathbf{s} \in D_{\mathbb{Z}^{2m},\tilde{\sigma}}$
- Compute $\mathbf{C}_M = \mathbf{D}_0 \cdot \mathbf{s} + \mathbf{D}_1 \cdot M \in \mathbb{Z}_q^{2n}$
- Using $\mathbf{T}_{\mathbf{A}}$, sample a short $\mathbf{d}$ s.t.

$$\underbrace{\left[\, \mathbf{A} \;\middle|\; \mathbf{A}_0 + \textstyle\sum_{j=1}^{\ell} \tau_j \cdot \mathbf{A}_j \,\right]}_{2m} \cdot \mathbf{d} = \mathbf{u} + \mathbf{D} \cdot \mathrm{bin}(\mathbf{C}_M) \qquad (*)$$

n

$\Sigma = (\tau, \mathbf{d}, \mathbf{s}) \in \{0,1\}^{\ell} \times \mathbb{Z}^{2m} \times \mathbb{Z}^{2m}$

Our Signature with Efficient Protocols

To sign $M \in \{0,1\}^{2m}$

- Sample random $\tau \in \{0,1\}^{\ell}$, random $\mathbf{s} \in D_{\mathbb{Z}^{2m},\tilde{\sigma}}$
- Compute $\mathbf{C}_M = \mathbf{D}_0 \cdot \mathbf{s} + \mathbf{D}_1 \cdot M \in \mathbb{Z}_q^{2n}$
- Using $\mathbf{T_A}$, sample a short $\mathbf{d}$ s.t.

$$n \Big\{ \underbrace{\left[\, \mathbf{A} \;\middle|\; \mathbf{A}_0 + \textstyle\sum_{j=1}^{\ell} \tau_j \cdot \mathbf{A}_j \,\right]}_{2m} \cdot \mathbf{d} = \mathbf{u} + \mathbf{D} \cdot \mathrm{bin}(\mathbf{C}_M) \quad (*)$$

$\Sigma = (\tau, \mathbf{d}, \mathbf{s}) \in \{0,1\}^{\ell} \times \mathbb{Z}^{2m} \times \mathbb{Z}^{2m}$

To verify: check that $\mathbf{d}$ is short and that Σ satisfies $(*)$.

Our Signature **with Efficient Protocols**

Kawachi *et al.* (Asiacrypt'08) commitment:

$$\mathbf{C}_M = \mathbf{D}_0 \cdot \mathbf{s} + \mathbf{D}_1 \cdot M$$

Is already embedded in Böhl *et al.* signature.

Our Signature **with Efficient Protocols**

Kawachi *et al.* (Asiacrypt'08) commitment:

$$\mathbf{C}_M = \mathbf{D}_0 \cdot \mathbf{s} + \mathbf{D}_1 \cdot M$$

Is already embedded in Böhl *et al.* signature.

Difficulty: In the proof, for one of the message, the signature has a different distribution.

Our Signature **with Efficient Protocols**

Kawachi *et al.* (Asiacrypt'08) commitment:

$$\mathbf{C}_M = \mathbf{D}_0 \cdot \mathbf{s} + \mathbf{D}_1 \cdot M$$

Is already embedded in Böhl *et al.* signature.

Difficulty: In the proof, for one of the message, the signature has a different distribution.

Solution: Use Rényi divergence instead of statistical distance to bound adversary's advantage [BLLSS15].

Rényi Divergence

Presentation

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

Rényi Divergence

Presentation

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

- 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
  - Only use it once in the proof

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
  - Only use it once in the proof
- **Probability preservation**:

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

Our Signature with efficient protocol**s**

Kawachi *et al.* (Asiacrypt'08) commitment:

For $\mathbf{D}_0, \mathbf{D}_1 \in \mathbb{Z}_q^{2n \times 2m}, \mathbf{s} \hookleftarrow D_{\mathbb{Z}^{2m},\sigma}, M \in \{0,1\}^{2m}$

$$\mathbf{C}_M = \mathbf{D}_0 \cdot \mathbf{s} + \mathbf{D}_1 \cdot M \; [q]$$

Compatible with Stern's protocol (Crypto'93, [LNSW; PKC'13])

$\Longrightarrow$ ZK proof compatible with the signature

Stern's Protocol (Crypto'93)

Stern's protocol is a ZK proof for Syndrome Decoding Problem.

Stern's Protocol (Crypto'93)

Stern's protocol is a ZK proof for Syndrome Decoding Problem.

Syndrome Decoding Problem

Given $\mathbf{P} \in \mathbb{Z}_2^{n \times m}$ and $\mathbf{v} \in \mathbb{Z}_2^{n}$, find $\mathbf{x}$ s.t. $\mathrm{w}(\mathbf{x}) = w$ and

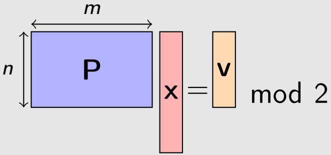
$$\underbrace{\mathbf{P}}_{n \times m} \cdot \mathbf{x} = \mathbf{v} \mod 2$$

Stern's Protocol (Crypto'93)

Stern's protocol is a ZK proof for Syndrome Decoding Problem.

Syndrome Decoding Problem

Given $\mathbf{P} \in \mathbb{Z}_2^{n \times m}$ and $\mathbf{v} \in \mathbb{Z}_2^{n}$, find $\mathbf{x}$ s.t. $\mathrm{w}(\mathbf{x}) = w$ and



[KTX08]: mod 2 $\rightarrow$ mod q

[LNSW13]: Extend Stern's protocol for SIS and LWE statements

Recent uses of Stern-like protocols in lattice-based crypto:
[LNW15], [LLNW16], [LLNMW16]

Unified Framework using Stern's Protocol

Problem: protocols using Stern's proofs build them "from scratch". [LNW15, LLNW16]

Unified Framework using Stern's Protocol

Problem: protocols using Stern's proofs build them "from scratch". [LNW15, LLNW16]

Provide a framework to construct ZKAoK:

- to prove knowledge of an $\mathbf{x} \in \{-1, 0, 1\}^n$ of a special form verifying $\mathbf{P} \cdot \mathbf{x} = \mathbf{v} \bmod q$
  - many lattice statements reduce to this
  - this captures various and complex statements

Unified Framework using Stern's Protocol

Problem: protocols using Stern's proofs build them "from scratch". [LNW15, LLNW16]

Provide a framework to construct ZKAoK:

- to prove knowledge of an $\mathbf{x} \in \{-1, 0, 1\}^n$ of a special form verifying $\mathbf{P} \cdot \mathbf{x} = \mathbf{v} \bmod q$
  - many lattice statements reduce to this
  - this captures various and complex statements
- that uses [LNSW13]'s decomposition-extension framework and is combinatoric in Stern's protocol manner

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];
- Non-frameability requires to introduce non-homogeneous terms in the SIS-based relations satisfied by membership certificates;

From Static to Dynamic

- Designed from a recent static group signature proposed by Ling, Nguyen and Wang [LNW15];
- Non-frameability requires to introduce non-homogeneous terms in the SIS-based relations satisfied by membership certificates;
- Other solutions [LLLS13, NZZ15] use membership certificates made of a complete basis. . .

  . . . which is problematic with non-homogeneous terms.

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's secret $\mathbf{z}_i$ to a unique public syndrome $\mathbf{v}_i = \mathbf{F} \cdot \mathbf{z}_i \in \mathbb{Z}_q^{4n}$ for some matrix $\mathbf{F} \in \mathbb{Z}_q^{4n \times 4m}$;

From Static to Dynamic

Difficulties

- Separate the secrets between **OA** and **GM**;
- Bind the user's secret $\mathbf{z}_i$ to a unique public syndrome $\mathbf{v}_i = \mathbf{F} \cdot \mathbf{z}_i \in \mathbb{Z}_q^{4n}$ for some matrix $\mathbf{F} \in \mathbb{Z}_q^{4n \times 4m}$;

  Use our signature scheme with efficient protocol:

$$\left[\, \mathbf{A} \;\middle|\; \mathbf{A}_0 + \sum_{j=1}^{\ell} \mathrm{id}_j \cdot \mathbf{A}_j \,\right] \cdot \mathbf{d} = \mathbf{u} + \mathbf{D} \cdot \mathrm{bin}(\mathbf{C}_{\mathbf{v}_i})$$

From Static to Dynamic

Difficulties

- **Difficulty**: achieving security against **framing attacks**:

From Static to Dynamic

Difficulties

- **Difficulty**: achieving security against **framing attacks**:
  - i.e., even a dishonest **GM** cannot create signatures that open to honest users;
  - Users need a membership secret with a corresponding secret key;
  - GM must certify that public key.

From Static to Dynamic

Difficulties

- **Difficulty**: achieving security against **framing attacks**:
  - i.e., even a dishonest **GM** cannot create signatures that open to honest users;
  - Users need a membership secret with a corresponding secret key;
  - GM must certify that public key.
- Be secure against **framing attacks** without compromising previous security properties;

From Static to Dynamic Our solution

Setup:

$$\text{group public key} \quad \mathcal{Y} = (\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{D}, \mathbf{D}_0, \mathbf{D}_1, \mathbf{F}, \mathbf{u})$$

$\ell = \log(N)$ (*e.g.* $\ell = 30$)

From Static to Dynamic Our solution

Setup:

group public key $\mathcal{Y} = (\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{D}, \mathbf{D}_0, \mathbf{D}_1, \mathbf{F}, \mathbf{u})$

$\ell = \log(N)$ (*e.g.* $\ell = 30$)

Join algorithm:

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

From Static to Dynamic Our solution

Setup:

group public key $\mathcal{Y} = (\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{D}, \mathbf{D}_0, \mathbf{D}_1, \mathbf{F}, \mathbf{u})$

$\ell = \log(N)$ (*e.g.* $\ell = 30$)

Join algorithm:

$\mathcal{U}_i$	**GM**
$\mathbf{z}_i \hookleftarrow$ short vector in $\mathbb{Z}^{4m}$	
$\mathbf{v}_i = \mathbf{F} \cdot \mathbf{z}_i$	

From Static to Dynamic Our solution

Setup:

group public key $\mathcal{Y} = (\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{D}, \mathbf{D}_0, \mathbf{D}_1, \mathbf{F}, \mathbf{u})$

$\ell = \log(N)$ (*e.g.* $\ell = 30$)

Join algorithm:

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

$\mathbf{z}_i \hookleftarrow$ short vector in $\mathbb{Z}^{4m}$

$\mathbf{v}_i = \mathbf{F} \cdot \mathbf{z}_i \xrightarrow{\mathbf{v}_i}$

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

$(\mathbf{d}_i, \mathbf{s}_i)$ is a signature under tag id_i

From Static to Dynamic Our solution

Setup:

group public key $\mathcal{Y} = (\mathbf{A}, \{\mathbf{A}_i\}_{i=0}^{\ell}, \mathbf{B}, \mathbf{D}, \mathbf{D}_0, \mathbf{D}_1, \mathbf{F}, \mathbf{u})$

$\ell = \log(N)$ (*e.g.* $\ell = 30$)

Join algorithm:

$\mathcal{U}_i$		**GM**
$\mathbf{z}_i \hookleftarrow$ short vector in $\mathbb{Z}^{4m}$		
$\mathbf{v}_i = \mathbf{F} \cdot \mathbf{z}_i$	$\xrightarrow{\mathbf{v}_i}$	
		$\mathrm{id}_i \hookleftarrow$ identity $\in \{0,1\}^{\ell}$
	$\xleftarrow{(\mathrm{id}_i, \mathbf{d}_i, \mathbf{s}_i)}$	$(\mathbf{d}_i, \mathbf{s}_i)$ is a signature under tag id_i
If $(\mathrm{id}_i, \mathbf{d}_i, \mathbf{s}_i)$ does not verify, abort		
$(\mathsf{sec}_i; \mathsf{cert}_i) = (\mathbf{z}_i; (\mathrm{id}_i, \mathbf{d}_i, \mathbf{s}_i))$		

From Static to Dynamic Our solution — further steps

Goal

CCA-Anonymity: anonymity under opening oracle.

From Static to Dynamic Our solution — further steps

Goal

CCA-Anonymity: anonymity under opening oracle.

$\uparrow$

Canetti-Halevi-Katz transformation (Eurocrypt'04)

Any IBE implies *IND-CCA*–secure public key encryption.

From Static to Dynamic Our solution — further steps

Goal

CCA-Anonymity: anonymity under opening oracle.

$\uparrow$

Canetti-Halevi-Katz transformation (Eurocrypt'04)

Any IBE implies *IND-CCA*–secure public key encryption.

Identity Based Encryption (Shamir'84, Boneh-Franklin'01)

- Encryption computes $C \leftarrow \textbf{Enc}(MPK, \text{ID}, M)$
- Decryption computes $M \leftarrow \textbf{Dec}(MPK, C, d_{\text{ID}})$ where $d_{\text{ID}} \leftarrow \textbf{Keygen}(MSK, ID)$

From Static to Dynamic Our solution

Sign algorithm:

$\mathbf{c} := \mathbf{Enc}(\mathbf{v}_i)$

From Static to Dynamic Our solution

Sign algorithm:

$\mathbf{c} := \mathbf{Enc}(\mathbf{v}_i) \quad \pi_K :=$ proof that $\mathbf{c}$ is correct and that

$$\left[\ \mathbf{A}\ \middle|\ \mathbf{A}_0 + \sum_{j=1}^{\ell} \mathrm{id}_j \cdot \mathbf{A}_j\ \right] \cdot \mathbf{d} = \mathbf{u} + \mathbf{D} \cdot \mathrm{bin}(\mathbf{C}_{\mathbf{v}_i})$$

From Static to Dynamic Our solution

Sign algorithm:

$\mathbf{c} := \mathbf{Enc}(\mathbf{v}_i)$ $\quad \pi_K :=$ proof that $\mathbf{c}$ is correct and that

$$\left[\,\mathbf{A} \;\middle|\; \mathbf{A}_0 + \sum_{j=1}^{\ell} \mathrm{id}_j \cdot \mathbf{A}_j \,\right] \cdot \mathbf{d} = \mathbf{u} + \mathbf{D} \cdot \mathrm{bin}(\mathbf{C}_{\mathbf{v}_i})$$

Where is the message? [BSZ04]

Inside π_K, encoded in the Fiat-Shamir transformation from **ZK**-proofs to **NIZK**-proofs.

From Static to Dynamic Our solution

Verify algorithm:

- A user verifies if π_K is correct.

From Static to Dynamic Our solution

Verify algorithm:

- A user verifies if π_K is correct.

Open algorithm:

- **OA** decrypts $\mathbf{c}$ to get $\mathbf{v}_i$;
- **OA** searchs for the associated i in the Join transcripts, and if so, returns i, otherwise abort.

Group Signatures: Comparative Table

Scheme	LLLS	NZZ	LNW	LLNW	Ours
Group PK	$\widetilde{\mathcal{O}}(\lambda^2) \cdot \log N_{\mathrm{gs}}$	$\widetilde{\mathcal{O}}(\lambda^2)$	$\widetilde{\mathcal{O}}(\lambda^2) \cdot \log N_{\mathrm{gs}}$	$\widetilde{\mathcal{O}}(\lambda^2)$	$\widetilde{\mathcal{O}}(\lambda^2) \cdot \log N_{\mathrm{gs}}$
User's SK	$\widetilde{\mathcal{O}}(\lambda^2)$	$\widetilde{\mathcal{O}}(\lambda^2)$	$\widetilde{\mathcal{O}}(\lambda)$	$\widetilde{\mathcal{O}}(\lambda) \cdot \log N_{\mathrm{gs}}$	$\widetilde{\mathcal{O}}(\lambda)$
Signature	$\widetilde{\mathcal{O}}(\lambda) \cdot \log N_{\mathrm{gs}}$	$\widetilde{\mathcal{O}}(\lambda + \log^2 N_{\mathrm{gs}})$	$\widetilde{\mathcal{O}}(\lambda) \cdot \log N_{\mathrm{gs}}$	$\widetilde{\mathcal{O}}(\lambda) \cdot \log N_{\mathrm{gs}}$	$\widetilde{\mathcal{O}}(\lambda) \cdot \log N_{\mathrm{gs}}$

Outline

Introduction

Definition

Presentation of the Scheme

Conclusion

Conclusion

Main Contributions:

- Lattice-based signature with efficient protocols;
  - for obtaining signatures on committed message
  - for proving possession of a message-signature pair
- First dynamic group signature based on lattice assumptions;
- Unified framework for proving modular linear equations using Stern's technique.

Technical contributions:

- Combine Böhl *et al.* signature + Ling *et al.* ZK proofs
  $\Longrightarrow$ signature with efficient protocols;
- A method of signing public keys so that knowledge of the secret key can be efficiently proved.

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 $H(\textbf{Commit}, \text{Public})$

From Static to Dynamic Our solution – Ingredients

Security proof of the Boyen signature

Lattice algorithms use short basis as *trapdoor* information.

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

SampleDown $\mathbf{A}' = \left[\frac{\mathbf{A}}{\mathbf{B}\cdot\mathbf{A}+\mathbf{C}}\right] \in \mathbb{Z}_q^{2m\times n}, \mathbf{C} \in \mathbb{Z}_q^{m\times n}, \mathbf{T}_\mathbf{C} \in \mathbb{Z}_q^{m\times m}, \sigma \mapsto$ 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. Set $\mathbf{A}_i = \mathbf{Q}_i \mathbf{A} + h_i \mathbf{C}$

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

$\Rightarrow$ 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

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

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

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

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

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

Problem

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

Problem

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

Consequence.

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

Rényi Divergence

Presentation

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

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

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

- 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 $\rightarrow$ **Game 1** $\rightarrow$ **Game 2** $\rightarrow$ **Hard Game**

Hardness assumptions

Bound winning probability.
Can be done through **probability preservation**!

Recall

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

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

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

Rényi Divergence

In Crypto

Consequence

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

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

→ Higher cost compared to usual lattice-based crypto parameters