Practical "Signatures with Efficient Protocols" from Simple Assumptions

Benoît Libert[1] **Fabrice Mouhartem**[1]
Thomas Peters[2] Moti Yung[3]

[1]École Normale Supérieure de Lyon, France

[2]Université Catholique de Louvain, Belgium

[3]Snapchat & Columbia University, USA

AsiaCCS, Xi'an – June 2nd 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...

Requires

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

Privacy-Preserving Cryptography

Important Goal: Anonymous authentication.

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

Requires

- A signature scheme
- Zero-knowledge (ZK) proof compatible with this signature

Privacy-Preserving Cryptography

Important Goal: Anonymous authentication.

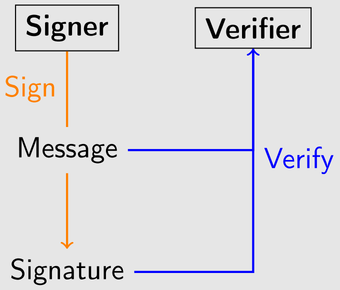
e.g. e-voting, e-cash, **group signatures**, anonymous credentials. . .

Requires

- A signature scheme
- Zero-knowledge (ZK) proof compatible with this signature

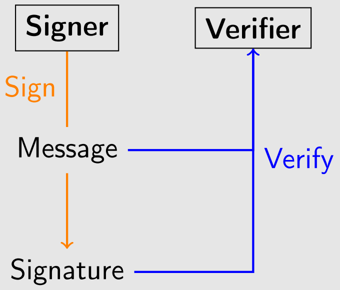
Digital Signatures

Signature Scheme



Digital Signatures

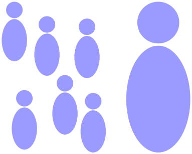
Signature Scheme



Guarantees authenticity and integrity.

Group Signatures

Bob wants to take public transportations.



Group Signatures

Bob wants to take public transportations.

Group Signatures

Bob wants to take public transportations.

- Authenticity & Integrity

Group Signatures

Bob wants to take public transportations.

- Authenticity & Integrity
- Anonymity

Group Signatures

Bob wants to take public transportations.

- Authenticity & Integrity
- Anonymity
- Dynamicity ⟷ Join

Group Signatures

Bob wants to take public transportations.

- Authenticity & Integrity
- Anonymity
- Dynamicity ↔ Join
- Traceability

Commitments

Digital equivalent of a sealed box.

Commitments

Digital equivalent of a sealed box.

Properties

Commitments provide

- **Binding** property: once sealed, a value cannot be changed

Commitments

Digital equivalent of a sealed box.

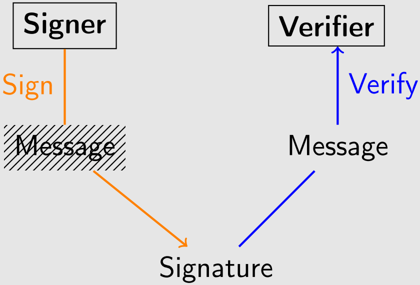
Properties

Commitments provide

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

Signature with Efficient Protocols

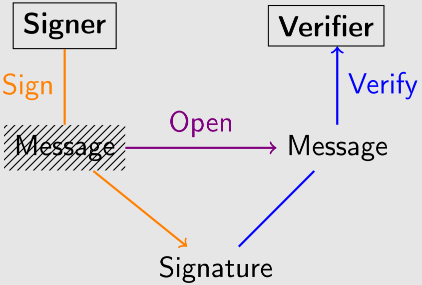
Signature Scheme with Efficient Protocols (Camenisch-Lysyanskya, SCN'02)



- Signature

Signature with Efficient Protocols

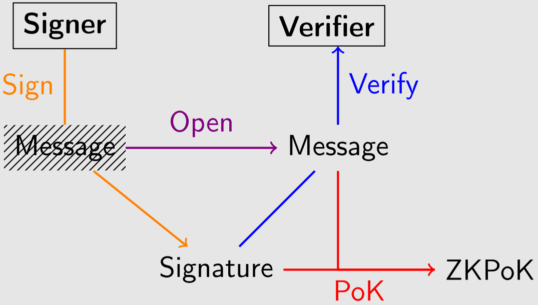
Signature Scheme with Efficient Protocols (Camenisch-Lysyanskya, SCN'02)



- Signature
- Sign committed values

Signature with Efficient Protocols

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



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

Pairing-Based Cryptography

Pairing

$$e : \mathbb{G} \times \hat{\mathbb{G}} \longrightarrow \mathbb{G}_T$$

s.t. for $g \in \mathbb{G}, \hat{g} \in \hat{\mathbb{G}}$

$$e(g^a, \hat{g}^b) = e(g, \hat{g})^{ab}$$

Pairing-Based Cryptography

Pairing

$$e : \mathbb{G} \times \hat{\mathbb{G}} \longrightarrow \mathbb{G}_T$$

s.t. for $g \in \mathbb{G}, \hat{g} \in \hat{\mathbb{G}}$

$$e(g^a, \hat{g}^b) = e(g, \hat{g})^{ab}$$

Hardness assumptions:

- **SXDH**: *DDH* holds in $\mathbb{G}$ and $\hat{\mathbb{G}}$ with $\mathbb{G} \neq \hat{\mathbb{G}}$
  - **DDH**: given (g, g^a, g^b, g^c), tells whether $c = a \cdot b$ or $c \in_R \mathbb{Z}_p$
- **SDL**: given $(g, \hat{g}, g^a, \hat{g}^a)$, compute $a \in \mathbb{Z}_p$ with $p = |\mathbb{G}|$

$\rightarrow$ Well studied, fixed-size assumptions.

Standard Assumptions

Standard assumptions are static and non-interactive assumptions.

Standard Assumptions

Standard assumptions are static and non-interactive assumptions.

vs

Static (or fixed-size) assumptions

- **DDH**: $(g^a, g^b, g^c) \mapsto$ tells if $c = ab$ or c random.

***q*-type** assumptions

- ***q*-DH-Inversion**: $(g^x, g^{x^2}, \ldots, g^{x^q}) \mapsto g^{x^{q+1}}$

Standard Assumptions

Standard assumptions are static and non-interactive assumptions.

vs

Static (or fixed-size) assumptions

- **DDH**: $(g^a, g^b, g^c) \mapsto$ tells if $c = ab$ or c random.

q-**type** assumptions

- q-**DH-Inversion**: $(g^x, g^{x^2}, \ldots, g^{x^q}) \mapsto g^{x^{q+1}}$

q usually represents the number of adversarial queries
Large values of q may lead to attacks (Cheon (Eurocrypt'06))

Standard Assumptions

Standard assumptions are static and non-interactive assumptions.

vs

Static (or fixed-size) assumptions

- **DDH**: $(g^a, g^b, g^c) \mapsto$ tells if $c = ab$ or c random.

***q*-type** assumptions

- ***q*-DH-Inversion**: $(g^x, g^{x^2}, \ldots, g^{x^q}) \mapsto g^{x^{q+1}}$

q usually represents the number of adversarial queries
Large values of q may lead to attacks (Cheon (Eurocrypt'06))

Non-interactive assumptions

- **DL**: $g^a \in \mathbb{G} \mapsto a \in \mathbb{Z}_p$

Interactive assumptions

- **One-more-DL**: given oracle access to $(g^{a_i} \mapsto a_i)$, finds $(b_i)_i$ given $(g^{b_i})_i$

Outline

Signature

Signature Scheme:

- Constant-size

Signature

Signature Scheme:

- Constant-size 4 group elements

Signature

Signature Scheme:

- Constant-size 4 group elements
- Multi-block

Signature

Signature Scheme:

- Constant-size 4 group elements
- Multi-block
- Randomizable

Signature with Efficient Protocols

Signature Scheme:

- Constant-size 4 group elements
- Multi-block
- Randomizable

Compatible with Efficient Protocols

Signature with Efficient Protocols

Signature Scheme:

- Constant-size 4 group elements
- Multi-block
- Randomizable

Compatible with Efficient Protocols

- Sign committed messages

Signature with Efficient Protocols

Signature Scheme:

- Constant-size 4 group elements
- Multi-block
- Randomizable

Compatible with Efficient Protocols

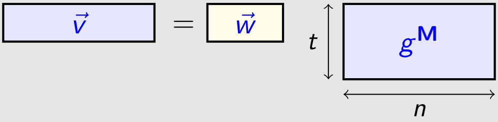
- Sign committed messages
- ZK-Prove the knowledge of a valid message-signature pair

Linear Subspace Membership

Linear Subspace Membership

We say that $\vec{v} \in \mathrm{Span}(\mathrm{Rows}(\mathbf{M}))$ if there exists $\vec{w} \in \mathbb{Z}_p^t$ satisfying

$$\vec{v} = g^{\vec{w} \cdot \mathbf{M}} \in \mathbb{G}^n$$

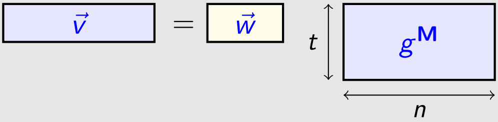


Linear Subspace Membership

Linear Subspace Membership

We say that $\vec{v} \in \mathrm{Span}(\mathrm{Rows}(\mathbf{M}))$ if there exists $\vec{w} \in \mathbb{Z}_p^t$ satisfying

$$\vec{v} = g^{\vec{w} \cdot \mathbf{M}} \in \mathbb{G}^n$$



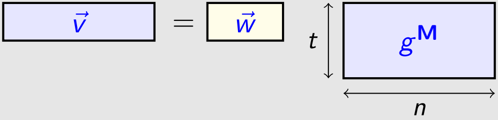
First **Quasi-Adaptive Non-Interactive-ZK** (QA-NIZK) proofs was proposed by Libert-Peters-Joye-Yung (Eurocrypt'14)

Linear Subspace Membership

Linear Subspace Membership

We say that $\vec{v} \in \mathrm{Span}(\mathrm{Rows}(\mathbf{M}))$ if there exists $\vec{w} \in \mathbb{Z}_p^t$ satisfying

$$\vec{v} = g^{\vec{w} \cdot \mathbf{M}} \in \mathbb{G}^n$$



First **Quasi-Adaptive Non-Interactive-ZK** (QA-NIZK) proofs was proposed by Libert-Peters-Joye-Yung (Eurocrypt'14)

Quasi-Adaptive (Jutla-Roy (Asiacrypt'13)) means that the *common reference string* (*crs*) may depend on the language (here the matrix $\mathbf{M}$)

Proof System for Linear Subspace Membership

Use of Kiltz-Wee Quasi-Adaptive Non-Interactive ZK proofs (QA-NIZK) to prove linear subspace membership.

Proof System for Linear Subspace Membership

Use of Kiltz-Wee Quasi-Adaptive Non-Interactive ZK proofs (QA-NIZK) to prove linear subspace membership.

Kiltz-Wee QA-NIZK (Eurocrypt'15)

Given $\mathbf{M} = (\vec{M}_1, \ldots, \vec{M}_t)^T \in \mathbb{G}^{t \times n}$,

$\pi \in \mathbb{G}$ prove that $\vec{v} \in \mathrm{Span}(\mathrm{Rows}(\mathbf{M}))$ for some witness $\vec{w}$.

Which is constant-size.

Our Signature Scheme

$$pk = (\mathsf{cp}, \mathsf{crs}, \vec{v} = (v_1, \ldots, v_\ell, w) \in_R \mathbb{G}^{\ell+1}, \Omega = h^\omega) \quad sk = \omega$$

$$\mathbf{M} = \begin{pmatrix} g & 1 & \cdots & 1 & 1 & 1 & 1 & \ldots & 1 & h \\ v_1 & g & 0 & \cdots & 0 & h & 0 & \cdots & 0 & 1 \\ \vdots & 0 & \ddots & 0 & \vdots & 0 & \ddots & 0 & \vdots & \vdots \\ v_\ell & 0 & \cdots & g & 0 & 0 & \cdots & h & 0 & 1 \\ w & 0 & \cdots & 0 & g & 0 & \cdots & 0 & h & 1 \end{pmatrix}$$

Our Signature Scheme

$$pk = (\mathsf{cp}, \mathsf{crs}, \vec{v} = (v_1, \ldots, v_\ell, w) \in_R \mathbb{G}^{\ell+1}, \Omega = h^\omega) \quad sk = \omega$$

$$\mathbf{M} = \begin{pmatrix} g & 1 & \cdots & 1 & 1 & 1 & 1 & \ldots & 1 & h \\ v_1 & g & 0 & \cdots & 0 & h & 0 & \cdots & 0 & 1 \\ \vdots & 0 & \ddots & 0 & \vdots & 0 & \ddots & 0 & \vdots & \vdots \\ v_\ell & 0 & \cdots & g & 0 & 0 & \cdots & h & 0 & 1 \\ w & 0 & \cdots & 0 & g & 0 & \cdots & 0 & h & 1 \end{pmatrix} \quad \begin{matrix} \omega \\ m_1 \cdot s \\ \vdots \\ m_\ell \cdot s \\ s \end{matrix}$$

$$\sigma_1 = g^\omega (v_1^{m_1} \cdots v_\ell^{m_\ell} w)^s \qquad \sigma_2 = g^s \qquad \sigma_3 = h^s$$

$+\ \pi$: ZK proof that

$$(\sigma_1, \sigma_2^{m_1}, \ldots, \sigma_2^{m_\ell}, \sigma_2, \sigma_3^{m_1}, \ldots, \sigma_3^{m_\ell}, \sigma_3, \Omega) \in \mathrm{Span}(\mathrm{Rows}(\mathbf{M}))$$

Our Signature Scheme

$$pk = (\mathsf{cp}, \mathsf{crs}, \vec{v} = (v_1, \ldots, v_\ell, w) \in_R \mathbb{G}^{\ell+1}, \Omega = h^\omega) \quad sk = \omega$$

$$\mathbf{M} = \begin{pmatrix} g & 1 & \cdots & 1 & 1 & 1 & 1 & \ldots & 1 & h \\ v_1 & g & 0 & \cdots & 0 & h & 0 & \cdots & 0 & 1 \\ \vdots & 0 & \ddots & 0 & \vdots & 0 & \ddots & 0 & \vdots & \vdots \\ v_\ell & 0 & \cdots & g & 0 & 0 & \cdots & h & 0 & 1 \\ w & 0 & \cdots & 0 & g & 0 & \cdots & 0 & h & 1 \end{pmatrix} \quad \begin{matrix} \omega & & \\ m_1 \cdot s & & m_1 \cdot s' \\ \vdots & + & \vdots \\ m_\ell \cdot s & & m_\ell \cdot s' \\ s & & s' \end{matrix}$$

$$\sigma_1 = g^\omega (v_1^{m_1} \cdots v_\ell^{m_\ell} w)^s \cdot (v_1^{m_1} \cdots v_\ell^{m_\ell} w)^{s'} \qquad \sigma_2 = g^s \cdot g^{s'} \qquad \sigma_3 = h^s \cdot h^{s'}$$

$+ \pi$: ZK proof that

$$(\sigma_1, \sigma_2^{m_1}, \ldots, \sigma_2^{m_\ell}, \sigma_2, \sigma_3^{m_1}, \ldots, \sigma_3^{m_\ell}, \sigma_3, \Omega) \in \mathrm{Span}(\mathrm{Rows}(\mathbf{M}))$$

Properties

Security

The signature scheme is secure under **chosen-message attack** under **SXDH**.

Properties

Security

The signature scheme is secure under **chosen-message attack** under **SXDH**.

Efficient protocols

There exist **practical** protocols for:

- signing committed messages

Properties

Security

The signature scheme is secure under **chosen-message attack** under **SXDH**.

Efficient protocols

There exist **practical** protocols for:

- signing committed messages
- proving knowledge of a valid message-signature pair

Outline

Definition

Dynamic Group Signature

It is a tuple of algorithms (**Setup**, **Join**, **Sign**, **Verify**, **Open**).

Definition

Dynamic Group Signature

It is a tuple of algorithms (**Setup**, **Join**, **Sign**, **Verify**, **Open**).

- **Setup:** done by a trusted entity

  `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 $\mathcal{S}_{\mathsf{OA}}$

Definition

Dynamic Group Signature

It is a tuple of algorithms (**Setup**, **Join**, **Sign**, **Verify**, **Open**).

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

  Provides $(\mathsf{cert}_i, \mathsf{sec}_i)$ to $\mathcal{U}_i$.

  Where cert_i attests the secret sec_i.

  Updates the list of users and membership certificates.

Definition

Dynamic Group Signature

It is a tuple of algorithms (**Setup**, **Join**, **Sign**, **Verify**, **Open**).

- **Sign** and **Verify** proceed as in standard digital signatures
- **Open:**

  `Input:` **OA**'s secret $\mathcal{S}_{\mathsf{OA}}$, M and Σ
  `Output:` i or $\perp$

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 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

CCA/CPA security refers to anonymity

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

CCA/CPA security refers to anonymity

$\rightarrow$ Decryption queries correspond to opening queries

Generic Construction

- **Keygen** $\rightarrow \mathcal{S}_{\mathsf{GM}}, \mathcal{S}_{\mathsf{OA}}, \mathcal{Y}$
  - $\mathcal{S}_{\mathsf{GM}} \leftarrow$ Sign.sk
  - $\mathcal{S}_{\mathsf{OA}} \leftarrow$ Enc.sk
  - $\mathcal{Y} \leftarrow$ (Sign.pk, Enc.pk)

Generic Construction

- **Keygen** $\rightarrow \mathcal{S}_{\mathsf{GM}}, \mathcal{S}_{\mathsf{OA}}, \mathcal{Y}$
  - $\mathcal{S}_{\mathsf{GM}} \leftarrow$ Sign.sk
  - $\mathcal{S}_{\mathsf{OA}} \leftarrow$ Enc.sk
  - $\mathcal{Y} \leftarrow$ (Sign.pk, Enc.pk)
- **Join**
  - $\mathsf{cert}_i \leftarrow$ GM obliviously sign identity $\mathsf{sec}_i = \mathsf{ID}$ chosen by $\mathcal{U}_i$

Generic Construction

- **Keygen** $\rightarrow \mathcal{S}_{\mathsf{GM}}, \mathcal{S}_{\mathsf{OA}}, \mathcal{Y}$
  - $\mathcal{S}_{\mathsf{GM}} \leftarrow$ Sign.sk
  - $\mathcal{S}_{\mathsf{OA}} \leftarrow$ Enc.sk
  - $\mathcal{Y} \leftarrow$ (Sign.pk, Enc.pk)
- **Join**
  - $\mathsf{cert}_i \leftarrow$ GM obliviously sign identity $\mathsf{sec}_i = \mathsf{ID}$ chosen by $\mathcal{U}_i$
- **Sign** $\rightarrow (C, \pi)$
  - $\widetilde{\mathsf{cert}} \leftarrow \mathcal{U}_i$ re-randomize cert_i
  - $C \leftarrow Encrypt(\widetilde{\mathsf{cert}};\ r)$
  - $\pi \leftarrow$ ZKoK of $(\mathsf{ID}; \widetilde{\mathsf{cert}}, r)$

Generic Construction

- **Keygen** $\rightarrow \mathcal{S}_{\mathsf{GM}}, \mathcal{S}_{\mathsf{OA}}, \mathcal{Y}$
  - $\mathcal{S}_{\mathsf{GM}} \leftarrow$ Sign.sk
  - $\mathcal{S}_{\mathsf{OA}} \leftarrow$ Enc.sk
  - $\mathcal{Y} \leftarrow$ (Sign.pk, Enc.pk)
- **Join**
  - $\mathsf{cert}_i \leftarrow$ GM obliviously sign identity $\mathsf{sec}_i =$ ID chosen by $\mathcal{U}_i$
- **Sign** $\rightarrow (C, \pi)$
  - $\widetilde{\mathsf{cert}} \leftarrow \mathcal{U}_i$ re-randomize cert_i
  - $C \leftarrow Encrypt(\widetilde{\mathsf{cert}};\ r)$
  - $\pi \leftarrow$ ZKoK of $(\mathsf{ID}; \widetilde{\mathsf{cert}}, r)$

Use of the previous signature with efficient protocols.

Results

Security

The scheme is traceable, resistant to framing attacks and CCA-anonymous in the ROM under **SXDH** and **SDL** assumptions.

Results

Security

The scheme is traceable, resistant to framing attacks and CCA-anonymous in the ROM under **SXDH** and **SDL** assumptions.

In the **random oracle model** for efficiency reasons.
(Libert-Peters-Yung'15 signature has 19+8 group elements)

Results

Security

The scheme is traceable, resistant to framing attacks and CCA-anonymous in the ROM under **SXDH** and **SDL** assumptions.

In the **random oracle model** for efficiency reasons.
(Libert-Peters-Yung'15 signature has 19+8 group elements)

Name	Signature length			Assumptions	Group Type	Anonymity
	$\mathbb{G}$	$\mathbb{Z}_p$	bitsize			
BBS04	3	6	2 304	q-SDH + DLIN	Static	CPA
DP06	4	5	2 304	q-SDH + XDH	Dynamic	CCA
BCNSW10	3	2	1 280	*interactive* + SDL	Dynamic	CCA-
PS16	2	2	1 024	*interactive*	Dynamic	CCA-
Ours	7	3	2 560	SXDH + SDL	Dynamic	CCA

Table: Comparison between different group signature schemes

CCA- means selfless-CCA-anonymity

Conclusion

We propose:

- A group signature built on **well studied assumptions** with comparable signature length with other schemes
  - Almost as efficient as Delerablée-Pointcheval'06
- A rather efficient signature with efficient protocols that can be used for other privacy-friendly protocols
- An implementation is in progress

Conclusion

We propose:

- A group signature built on **well studied assumptions** with comparable signature length with other schemes
  - Almost as efficient as Delerablée-Pointcheval'06
- A rather efficient signature with efficient protocols that can be used for other privacy-friendly protocols
- An implementation is in progress

Thank you for your attention.
Any Question?