Signature de Groupes et Réseaux Euclidiens

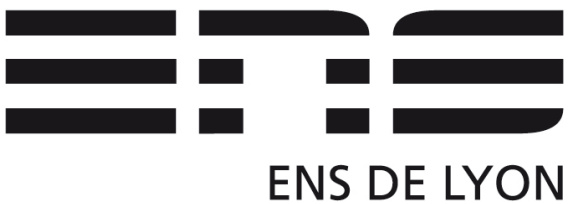
Fabrice Mouhartem

Avec Benoît Libert et Khoa Nguyen*

École Normale Supérieure de Lyon, France

*Nanyang Technological University, Singapour

8ème Rencontres Arithmétique de l'Informatique Mathématique
30 Juin 2016



Cryptography

Cryptanalysis | **Constructions**

Primitives: Encryption, Signature,. . .

Cryptography

Cryptanalysis	**Constructions**
Security Requirements $\longrightarrow$	Primitives: Encryption, Signature,...

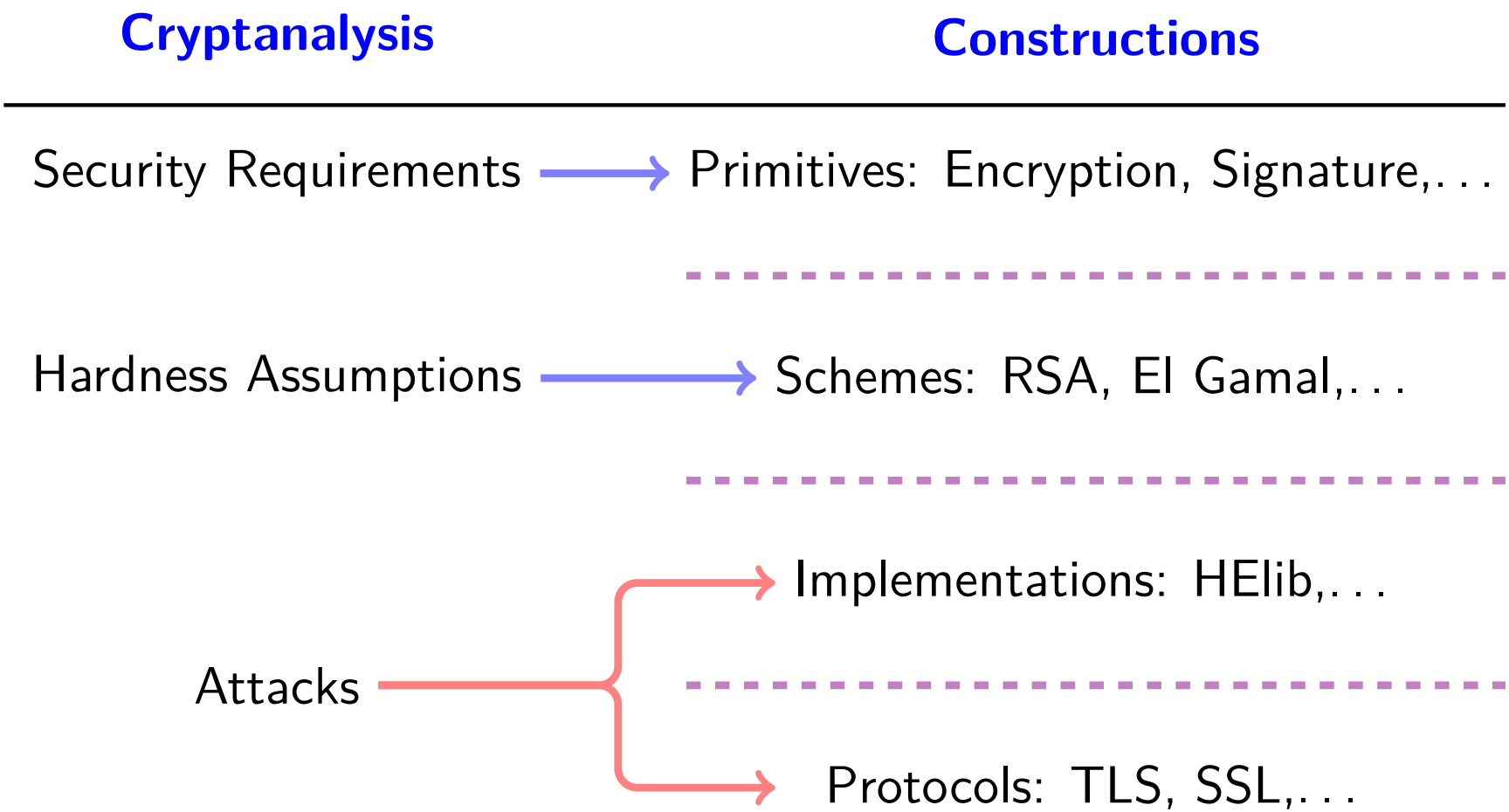
Cryptography

Cryptanalysis		**Constructions**
Security Requirements	$\longrightarrow$	Primitives: Encryption, Signature,...
Hardness Assumptions	$\longrightarrow$	Schemes: RSA, El Gamal,...

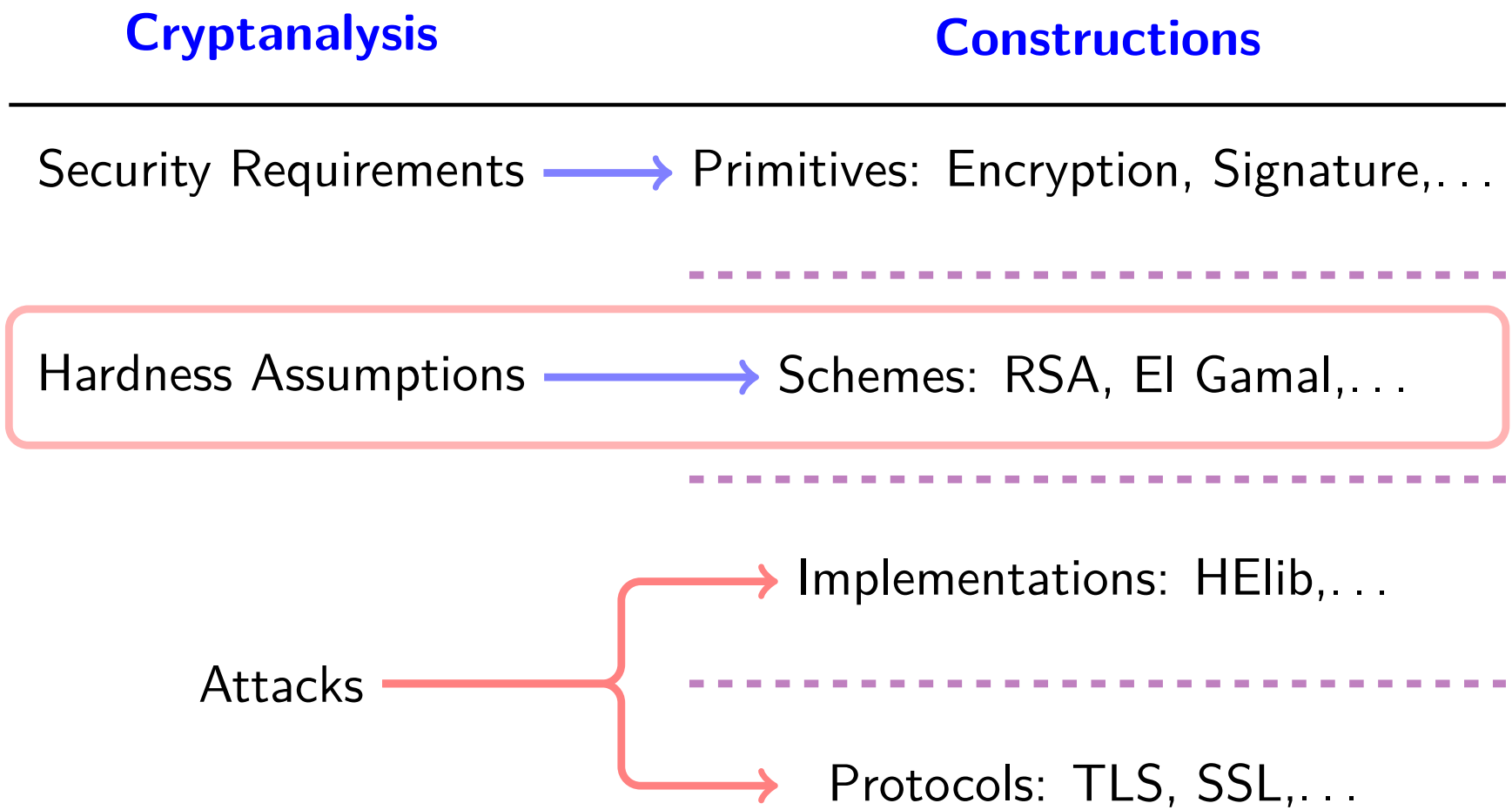
Cryptography

Cryptanalysis	**Constructions**
Security Requirements $\longrightarrow$	Primitives: Encryption, Signature,...
Hardness Assumptions $\longrightarrow$	Schemes: RSA, El Gamal,...
	Implementations: HElib,...
	Protocols: TLS, SSL,...

Cryptography



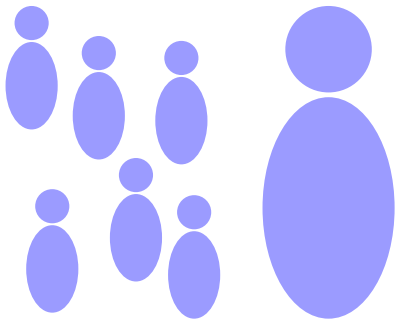
Cryptography



Group Signature

Example: Public Transportation

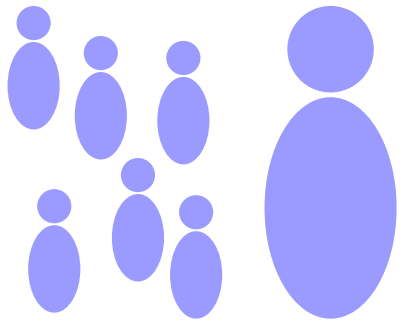
Some user wants to take public transportations.



Group Signature

Example: Public Transportation

Some user wants to take public transportations.

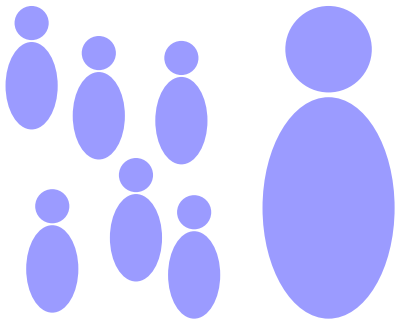


timestamp

Group Signature

Example: Public Transportation

Some user wants to take public transportations.



signature

- Authenticity & Integrity

Group Signature

Example: Public Transportation

Some user wants to take public transportations.

- Authenticity & Integrity
- Anonymity

Group Signature

Example: Public Transportation

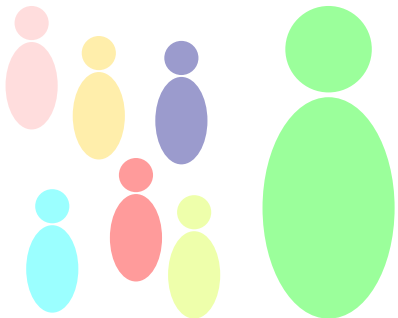
Some user wants to take public transportations.

- Authenticity & Integrity
- Anonymity
- Traceability

Group Signature

Example: Public Transportation

Some user wants to take public transportations.



signature

- Authenticity & Integrity
- Anonymity
- Traceability 

Group Signature

Example: Public Transportation

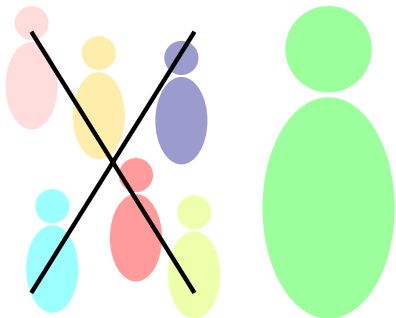
Some user wants to take public transportations.

- Authenticity & Integrity
- Anonymity
- Traceability
- Avoid opening abuses

Group Signature

Example: Public Transportation

Some user wants to take public transportations.



signature

- Authenticity & Integrity
- Anonymity
- Traceability 
- Avoid opening abuses
- Dynamicity  Join 

Group Signature

Motivations

Group Signature: A scheme to allow a member of a group to sign messages on behalf of the group

Group Signature

Motivations

Group Signature: A scheme to allow a member of a group to sign messages on behalf of the group

Accountability: Users remain accountable, an opening authority (OA) can unanonymize signatures

Group Signature

Motivations

Group Signature: A scheme to allow a member of a group to sign messages on behalf of the group

Accountability: Users remain accountable, an opening authority (OA) can unanonymize signatures

Applications

Control in public transportation, smart cars, anonymous access control (e.g. in company building), e-auction,...

Group Signature

Motivations

Group Signature: A scheme to allow a member of a group to sign messages on behalf of the group

Accountability: Users remain accountable, an opening authority (OA) can unanonymize signatures

Applications

Control in public transportation, smart cars, anonymous access control (e.g. in company building), e-auction,...

Extensions

- Dynamic: new users can join at any time
- Message Dependent Opening: add another authority to restrain the power of the OA

State of the art

- Introduction by Chaum and van Heyst (Eurocrypt'91)
- First scalable solution.
  Ateniese-Camenisch-Joye-Tsudik (Crypto'00)
- Formal model. Bellare-Micciancio-Warinschi (Eurocrypt'03)
- Dynamic Group Signature. Bellare-Shi-Zhang (CT-RSA'05),
  Kiayias-Yung (Eurocrypt'05)

- GS-MDO. Sakai *et al.* (Pairing'12)
  ↳ Relation with IBE

State of the art

- Introduction by Chaum and van Heyst (Eurocrypt'91)
- First scalable solution.
  Ateniese-Camenisch-Joye-Tsudik (Crypto'00)
- Formal model. Bellare-Micciancio-Warinschi (Eurocrypt'03)
- Dynamic Group Signature. Bellare-Shi-Zhang (CT-RSA'05),
  Kiayias-Yung (Eurocrypt'05)
- Lattice-based scheme.
  Gordon-Katz-Vaikuntanathan (Asiacrypt'10)
- GS-MDO. Sakai *et al.* (Pairing'12)
  ↳ Relation with IBE
- Efficient lattice-based signature (LNW and NZZ PKC'15)

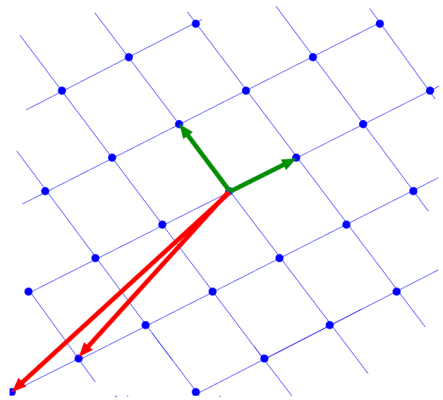
State of the art

- Introduction by Chaum and van Heyst (Eurocrypt'91)
- First scalable solution.
  Ateniese-Camenisch-Joye-Tsudik (Crypto'00)
- Formal model. Bellare-Micciancio-Warinschi (Eurocrypt'03)
- Dynamic Group Signature. Bellare-Shi-Zhang (CT-RSA'05), Kiayias-Yung (Eurocrypt'05)
- Lattice-based scheme.
  Gordon-Katz-Vaikuntanathan (Asiacrypt'10)
- GS-MDO. Sakai *et al.* (Pairing'12)
  ↳ Relation with IBE
- Efficient lattice-based signature (LNW and NZZ PKC'15)
- This work: dynamic + with GS-MDO

Lattice-Based Cryptography

A **Lattice** is the set of integer linear combination of independent vectors called a basis

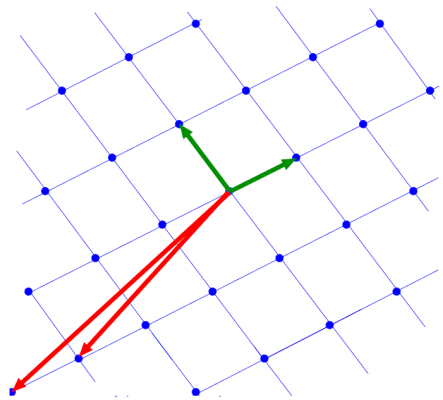
$$\Lambda(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \left\{ \sum_{i \leq n} a_i \mathbf{b}_i \;\middle|\; \forall i, a_i \in \mathbb{Z} \right\}$$



Lattice-Based Cryptography

A **Lattice** is the set of integer linear combination of independent vectors called a basis

$$\Lambda(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \left\{ \sum_{i \leq n} a_i \mathbf{b}_i \;\middle|\; \forall i, a_i \in \mathbb{Z} \right\}$$

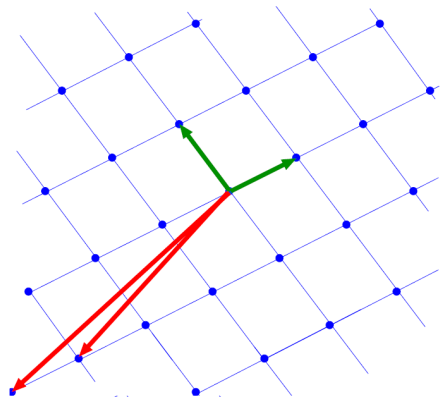


Idea: Find a short non-zero vector in a lattice without a short basis is hard

Lattice-Based Cryptography

A **Lattice** is the set of integer linear combination of independent vectors called a basis

$$\Lambda(\mathbf{b}_1, \ldots, \mathbf{b}_n) = \left\{ \sum_{i \leq n} a_i \mathbf{b}_i \;\middle|\; \forall i, a_i \in \mathbb{Z} \right\}$$



Idea: Find a short non-zero vector in a lattice without a short basis is hard

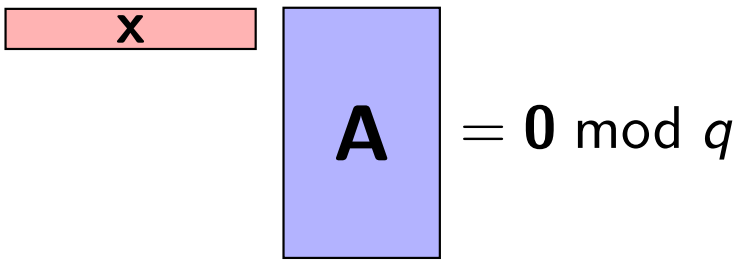
Advantages

Simple, efficient, conjectured resistant to a quantum adversary, secure under worst-case hardness assumptions, expressive...

Hardness Assumptions: SIS and LWE

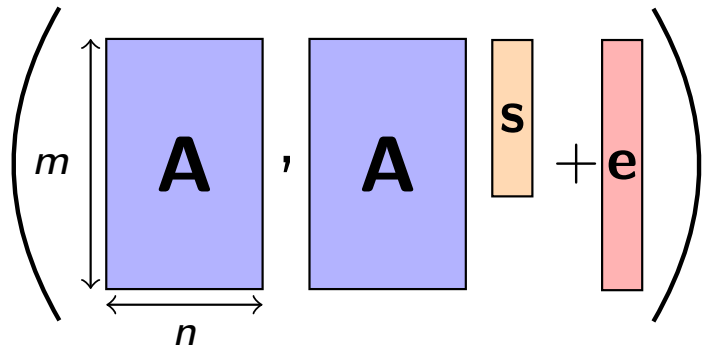
Parameters: Dimension n, $m \geq n$, modulus q, 'smallness' β

Small Integer Solution



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

Learning With Errors



$\mathbf{s} \hookleftarrow \mathbb{Z}_q^n$ $\mathbf{e}$ small error

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

$\rightarrow$ Standard, Well-Studied Assumptions.

Outline

q-ary Lattices

Given $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, let us define the following lattice

$$\Lambda_q\left(\mathbf{A}\right) = \left\{\mathbf{e} \in \mathbb{Z}^m \mid \exists \mathbf{s} \in \mathbb{Z}_q^n \text{ s.t. } \mathbf{A}^T \cdot \mathbf{s} = \mathbf{e}\right\}$$

q-ary Lattices

Given $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, let us define the following lattices

$$\Lambda_q\left(\mathbf{A}\right) = \left\{\mathbf{e} \in \mathbb{Z}^m \mid \exists \mathbf{s} \in \mathbb{Z}_q^n \text{ s.t. } \mathbf{A}^T \cdot \mathbf{s} = \mathbf{e}\right\}$$

$$\Lambda_q^{\perp}\left(\mathbf{A}\right) = \left\{\mathbf{e} \in \mathbb{Z}^m \mid \text{ s.t. } \mathbf{A} \cdot \mathbf{e} = \mathbf{0}\right\}$$

q-ary Lattices

Given $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, let us define the following lattices

$$\Lambda_q\left(\mathbf{A}\right) = \left\{\mathbf{e} \in \mathbb{Z}^m \mid \exists \mathbf{s} \in \mathbb{Z}_q^n \text{ s.t. } \mathbf{A}^T \cdot \mathbf{s} = \mathbf{e}\right\}$$
$$\Lambda_q^\perp\left(\mathbf{A}\right) = \left\{\mathbf{e} \in \mathbb{Z}^m \mid \text{ s.t. } \mathbf{A} \cdot \mathbf{e} = \mathbf{0}\right\}$$

Given $\mathbf{u} \in \mathbb{Z}_q^n$ let us define the shifted lattice

$$\Lambda_q^{\mathbf{u}}\left(\mathbf{A}\right) = \left\{\mathbf{e} \in \mathbb{Z}^m \mid \mathbf{A}^T \cdot \mathbf{e} = \mathbf{u}\right\}$$

Trapdoors

(Cash-Hofheinz-Kiltz-Peikert; Eurocrypt'10. Genty-Peikert-Vaikuntanathan; STOC'08)

Trapdoor: Short basis $\mathbf{T}_{\mathbf{A}} \in \mathbb{Z}_{m \times m}$ for a lattice $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$

- There is a PPT algorithm to sample $\mathbf{A}$ with a trapdoor $\mathbf{T}_{\mathbf{A}}$

Trapdoors

(Cash-Hofheinz-Kiltz-Peikert; Eurocrypt'10. Genty-Peikert-Vaikuntanathan; STOC'08)

Trapdoor: Short basis $\mathbf{T}_{\mathbf{A}} \in \mathbb{Z}_{m \times m}$ for a lattice $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$

- There is a PPT algorithm to sample $\mathbf{A}$ with a trapdoor $\mathbf{T}_{\mathbf{A}}$

Given $\mathbf{A}$ and a trapdoor $\mathbf{T}_{\mathbf{A}}$, there are PPT algorithms to

- Sample a short $\mathbf{v}$ in $\Lambda_q^{\perp}\left(\mathbf{A}\right), \Lambda_q^{\mathbf{u}}\left(\mathbf{A}\right)$ or $\Lambda_q\left(\mathbf{A}\right)$

Trapdoors

(Cash-Hofheinz-Kiltz-Peikert; Eurocrypt'10. Genty-Peikert-Vaikuntanathan; STOC'08)

Trapdoor: Short basis $\mathbf{T}_{\mathbf{A}} \in \mathbb{Z}_{m \times m}$ for a lattice $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$

- There is a PPT algorithm to sample $\mathbf{A}$ with a trapdoor $\mathbf{T}_{\mathbf{A}}$

Given $\mathbf{A}$ and a trapdoor $\mathbf{T}_{\mathbf{A}}$, there are PPT algorithms to

- Sample a short $\mathbf{v}$ in $\Lambda_q^{\perp}(\mathbf{A}), \Lambda_q^{\mathbf{u}}(\mathbf{A})$ or $\Lambda_q(\mathbf{A})$
- Extract a short basis for the matrix $\widetilde{\mathbf{A}}$ given $\mathbf{A'} \in \mathbb{Z}_q^{n \times m'}$

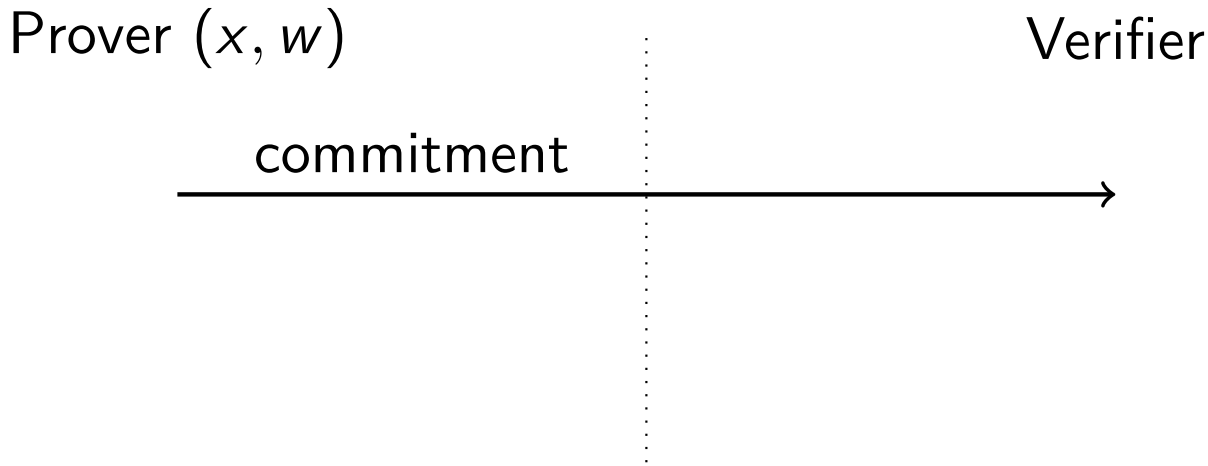
$$\widetilde{\mathbf{A}} = \left[\begin{array}{c|c} \mathbf{A} & \mathbf{A'} \end{array}\right] \in \mathbb{Z}_q^{n \times (m+m')}$$

Zero-Knowledge Argument

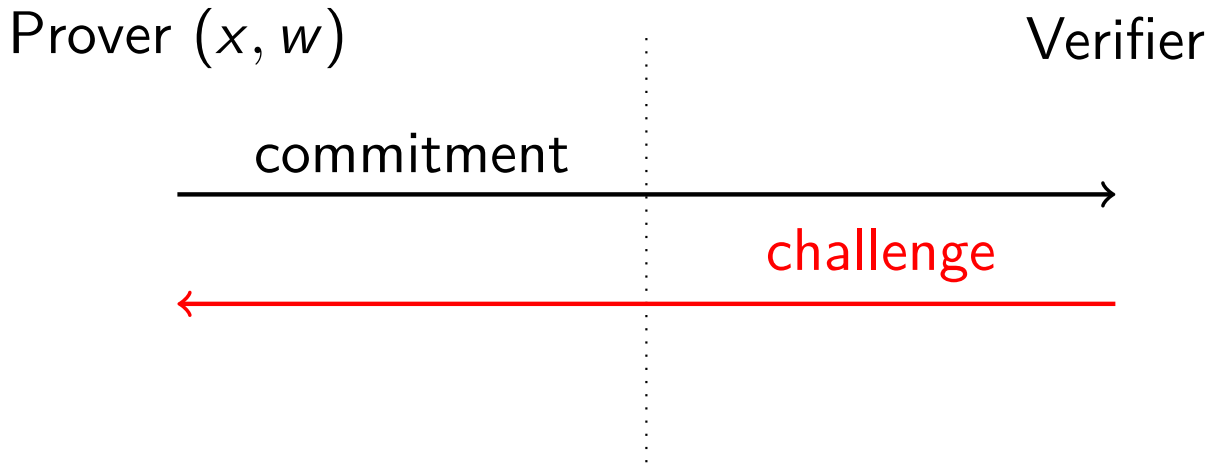
Prover (x, w)

Verifier

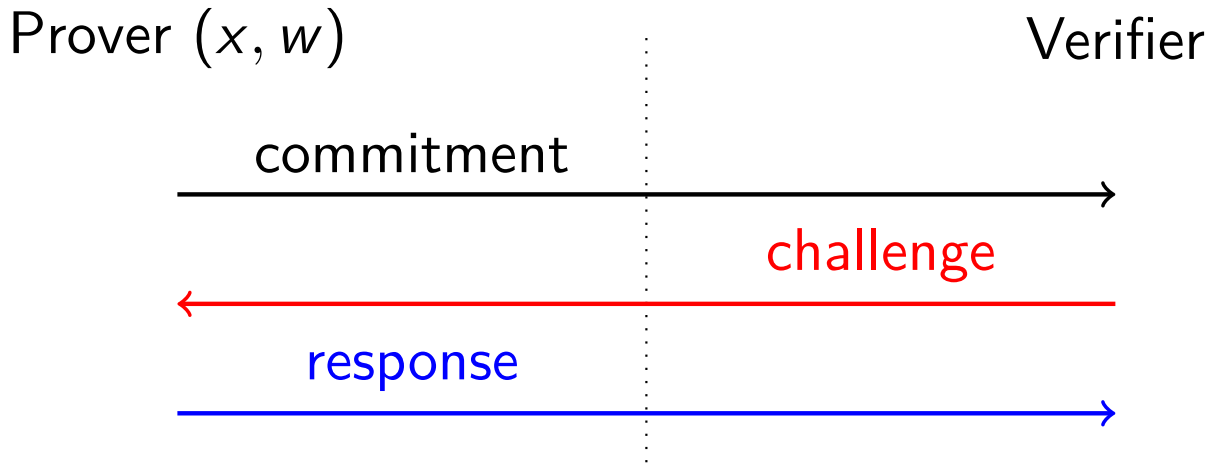
Zero-Knowledge Argument



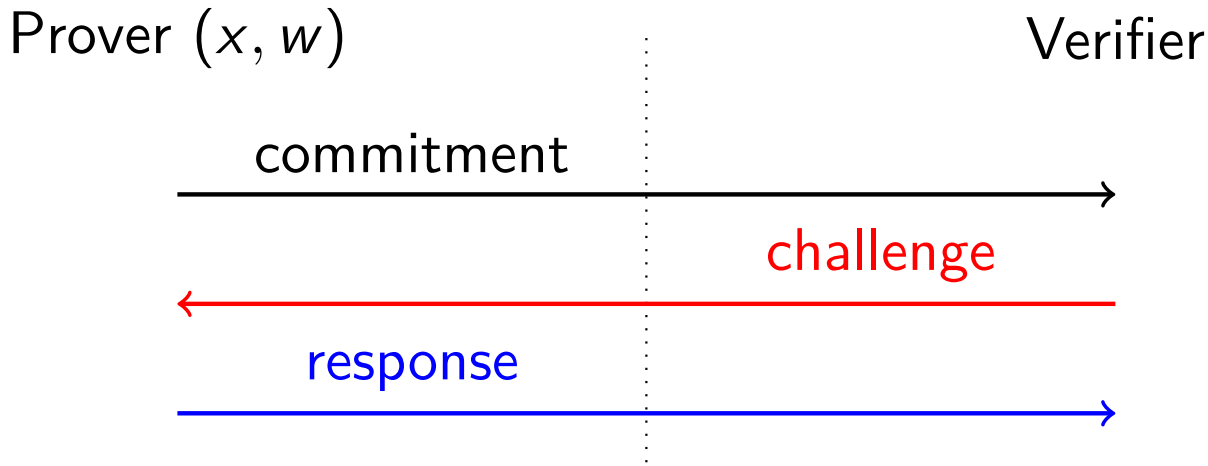
Zero-Knowledge Argument



Zero-Knowledge Argument

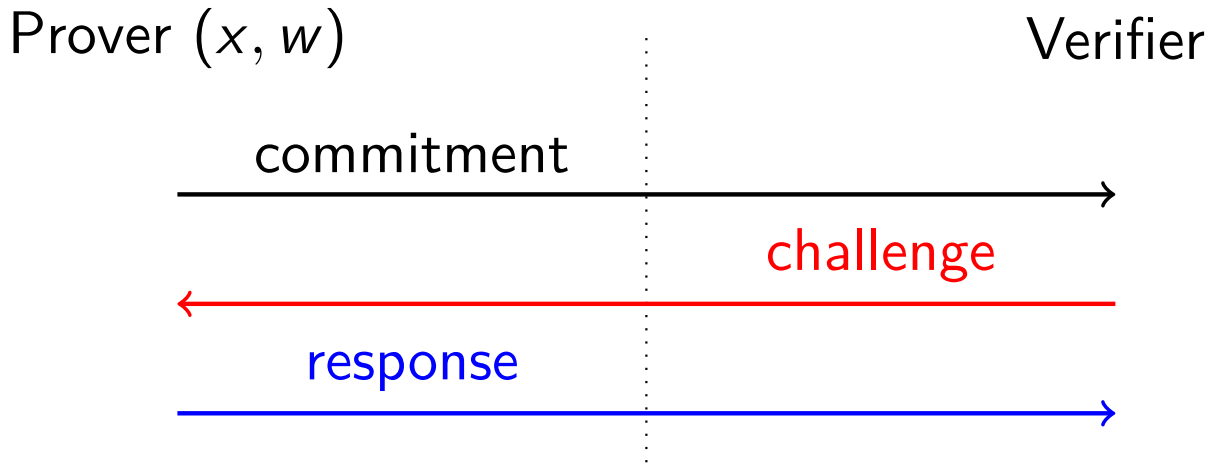


Zero-Knowledge Argument



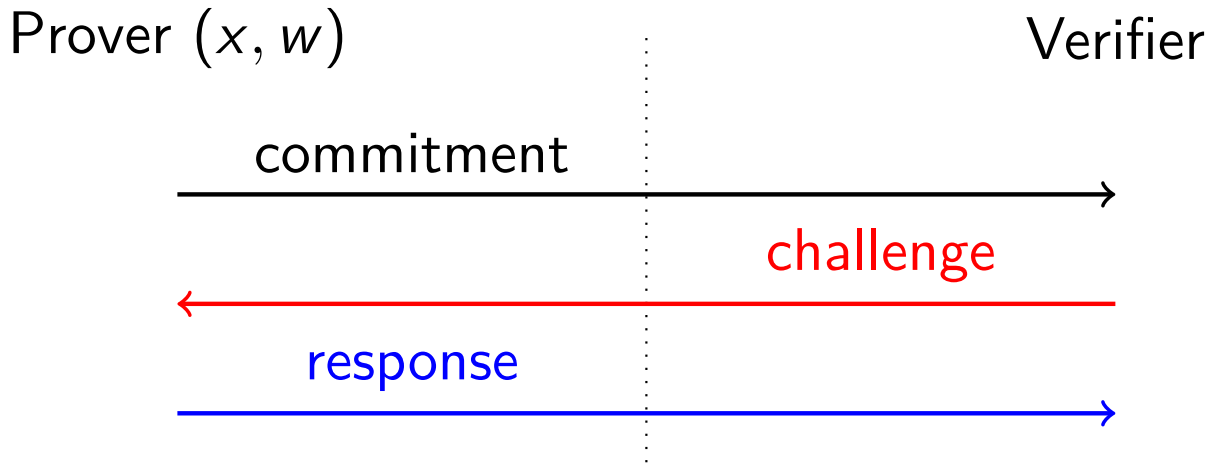
- **Completeness:** correctness of the protocol

Zero-Knowledge Argument



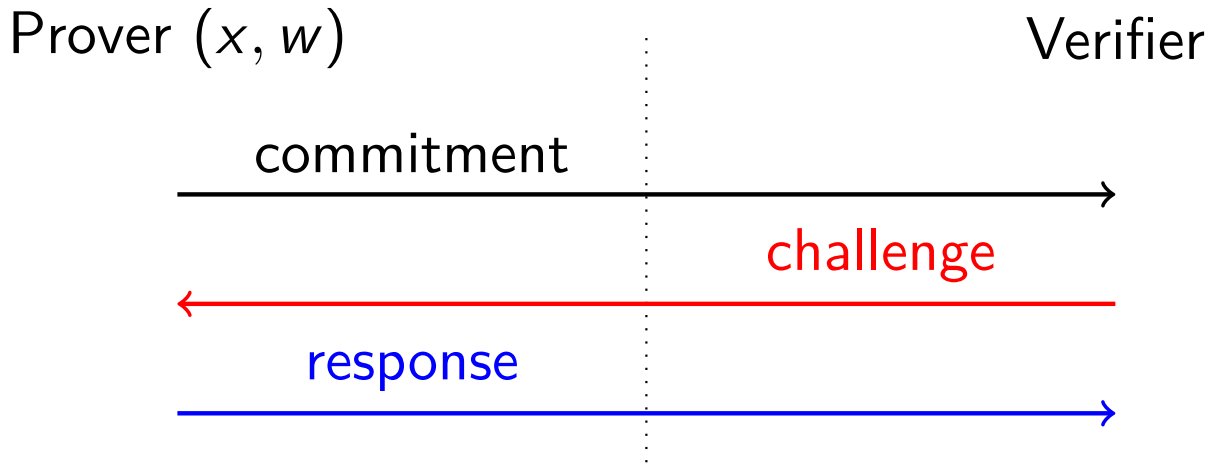
- **Completeness:** correctness of the protocol
- **Soundness:** no false statement can be proved

Zero-Knowledge Argument



- **Completeness:** correctness of the protocol
- **Soundness:** no false statement can be proved
- **Zero-Knowledge:** no information leaks except that "*the statement is true*"

Zero-Knowledge Argument



- **Completeness:** correctness of the protocol
- **Soundness:** no false statement can be proved
- **Zero-Knowledge:** no information leaks except that "*the statement is true*"

ZK Arguments are systems where soundness is computational.

Stern's Protocol

(Crypto'93)

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

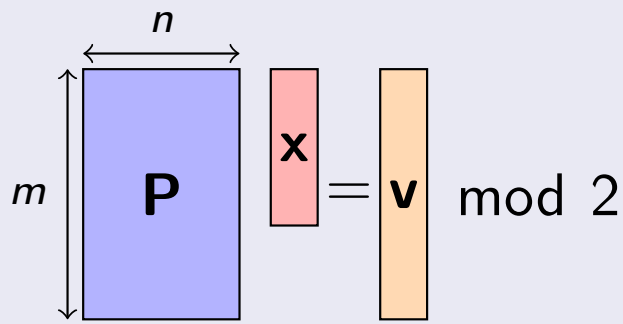
Stern's Protocol

(Crypto'93)

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

Syndrome Decoding Problem

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



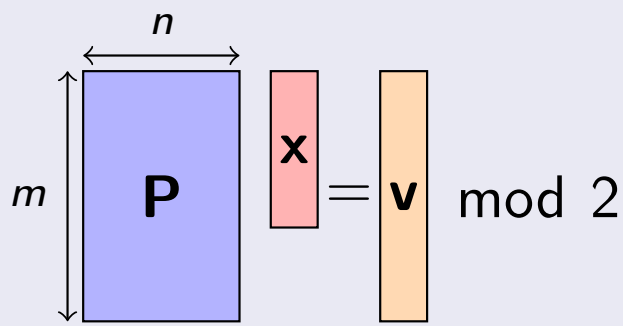
Stern's Protocol

(Crypto'93)

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

Syndrome Decoding Problem

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



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

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

Recent uses in cryptography: [LNW15], [LLNW16].

GPV IBE

(Gentry-Peikert-Vaikuntanathan; STOC'08)

Identity Based Encryption: To encrypt $\mathbf{m} \in \{0,1\}^\ell$ under id

Setup Generate $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ with a trapdoor $\mathbf{T_A} \in \mathbb{Z}^{m \times m}$

$$\text{mpk} = \mathbf{A}, \qquad \text{msk} = \mathbf{T_A}.$$

GPV IBE

(Gentry-Peikert-Vaikuntanathan; STOC'08)

Identity Based Encryption: To encrypt $\mathbf{m} \in \{0,1\}^\ell$ under id

Setup Generate $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ with a trapdoor $\mathbf{T_A} \in \mathbb{Z}^{m \times m}$

$$\text{mpk} = \mathbf{A}, \qquad \text{msk} = \mathbf{T_A}.$$

Extract Let $\mathbf{G} = \mathcal{H}(\text{id})$.

Use $\mathbf{T_A}$ compute small norm matrix $\mathbf{E} \in \mathbb{Z}^{m \times \ell}$ s.t.

$$\mathbf{A}\,\mathbf{E} = \mathbf{G} \bmod q$$

GPV IBE

(Gentry-Peikert-Vaikuntanathan; STOC'08)

Identity Based Encryption: To encrypt $\mathbf{m} \in \{0,1\}^\ell$ under id

Setup Generate $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ with a trapdoor $\mathbf{T_A} \in \mathbb{Z}^{m \times m}$

$$\text{mpk} = \mathbf{A}, \qquad \text{msk} = \mathbf{T_A}.$$

Extract Let $\mathbf{G} = \mathcal{H}(\text{id})$.
Use $\mathbf{T_A}$ compute small norm matrix $\mathbf{E} \in \mathbb{Z}^{m \times \ell}$ s.t.

$$\mathbf{A} \quad \mathbf{E} = \mathbf{G} \mod q$$

Encrypt Sample $(\mathbf{s}, \mathbf{e}_1, \mathbf{e}_2) \hookleftarrow \chi^n \times \chi^m \times \chi^\ell$ and output

$$\mathbf{c} = \left(\mathbf{A}^T \cdot \mathbf{s} + \mathbf{e}_1, \mathbf{G}^T \cdot \mathbf{s} + \mathbf{e}_2 + \lfloor q/2 \rfloor \cdot \mathbf{m} \right).$$

Decrypt $\mathbf{m}' = \boxed{1 \mid 2 \mid 4 \mid \cdots \mid 2^{\ell-1}} \cdot \left\lfloor (\mathbf{c}_2 - \mathbf{E}^T \cdot \mathbf{c}_1) \cdot (q/2) \right\rceil$

Boyen's Signature

(PKC'10)

To sign a message $M = m_1 \cdots m_\ell \in \{0,1\}^\ell$:

KeyGen: Generate matrix $\mathbf{A}$ with trapdoor $\mathbf{T_A}$, random matrices $\mathbf{A}_0, \ldots, \mathbf{A}_\ell \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{u} \in \mathbb{Z}_q^n$.

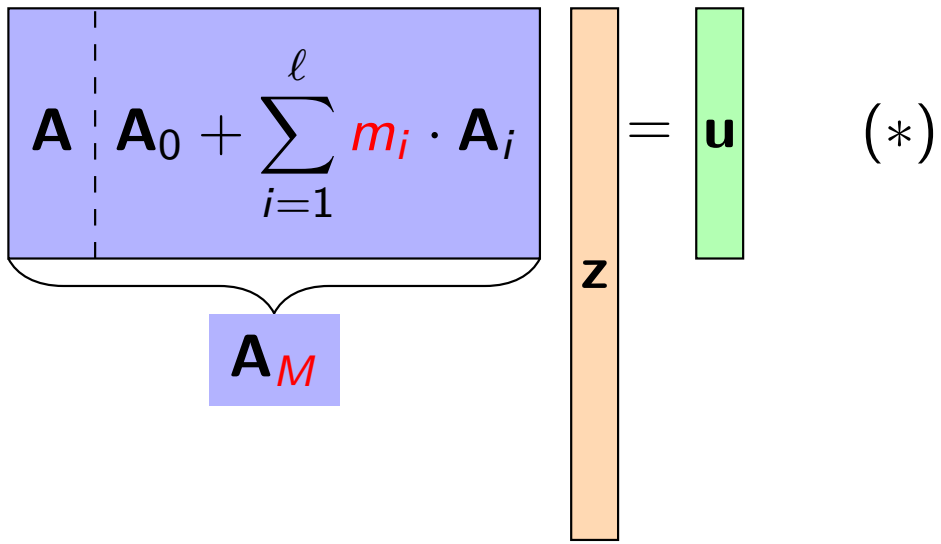
Boyen's Signature

(PKC'10)

To sign a message $M = m_1 \cdots m_\ell \in \{0,1\}^\ell$:

KeyGen: Generate matrix $\mathbf{A}$ with trapdoor $\mathbf{T_A}$, random matrices $\mathbf{A}_0, \ldots, \mathbf{A}_\ell \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{u} \in \mathbb{Z}_q^n$.

Sign: Using $\mathbf{T_A}$, compute short $\mathbf{z} \in \mathbb{Z}^{2m} = \sigma$ s.t.



$(*)$

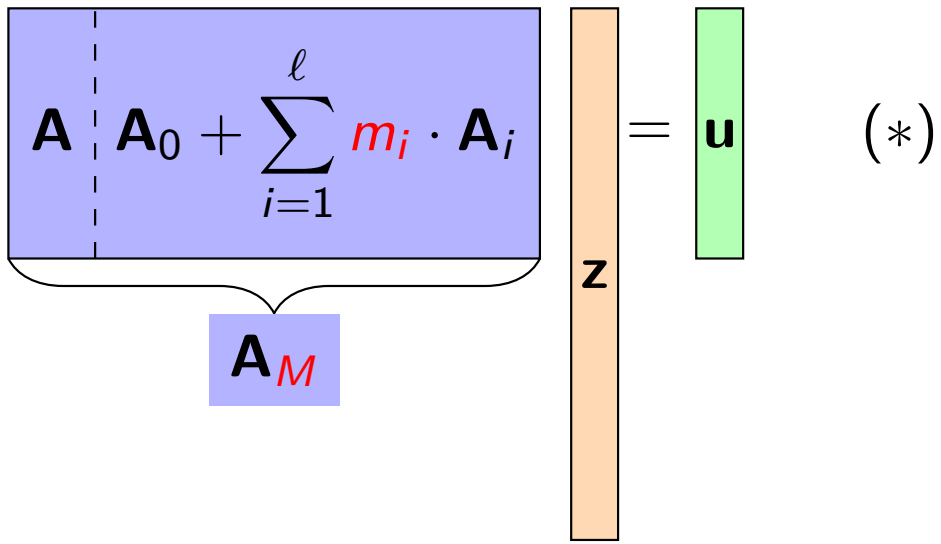
Boyen's Signature

(PKC'10)

To sign a message $M = m_1 \cdots m_\ell \in \{0,1\}^\ell$:

KeyGen: Generate matrix $\mathbf{A}$ with trapdoor $\mathbf{T_A}$, random matrices $\mathbf{A}_0, \ldots, \mathbf{A}_\ell \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{u} \in \mathbb{Z}_q^n$.

Sign: Using $\mathbf{T_A}$, compute short $\mathbf{z} \in \mathbb{Z}^{2m} = \sigma$ s.t.



$(*)$

Verify: Test $\|\mathbf{z}\| \leq \beta$.
Compute $\mathbf{A}_M$ to check relation $(*)$.

Generic Construction

(Bellare-Micciancio-Warinschi; Eurocrypt'03)

Group Signature

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

Generic Construction

(Bellare-Micciancio-Warinschi; Eurocrypt'03)

Group Signature

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

- **Keygen** provides user with a signature for its identity

Generic Construction

(Bellare-Micciancio-Warinschi; Eurocrypt'03)

Group Signature

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

- **Keygen** provides user with a signature for its identity
- **Sign** encrypt identity and prove knowledge of the above signature + correct encryption of identity

Generic Construction

(Bellare-Micciancio-Warinschi; Eurocrypt'03)

Group Signature

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

- **Keygen** provides user with a signature for its identity
- **Sign** encrypt identity and prove knowledge of the above signature + correct encryption of identity
- **Verify** verify the previous proof

Generic Construction

(Bellare-Micciancio-Warinschi; Eurocrypt'03)

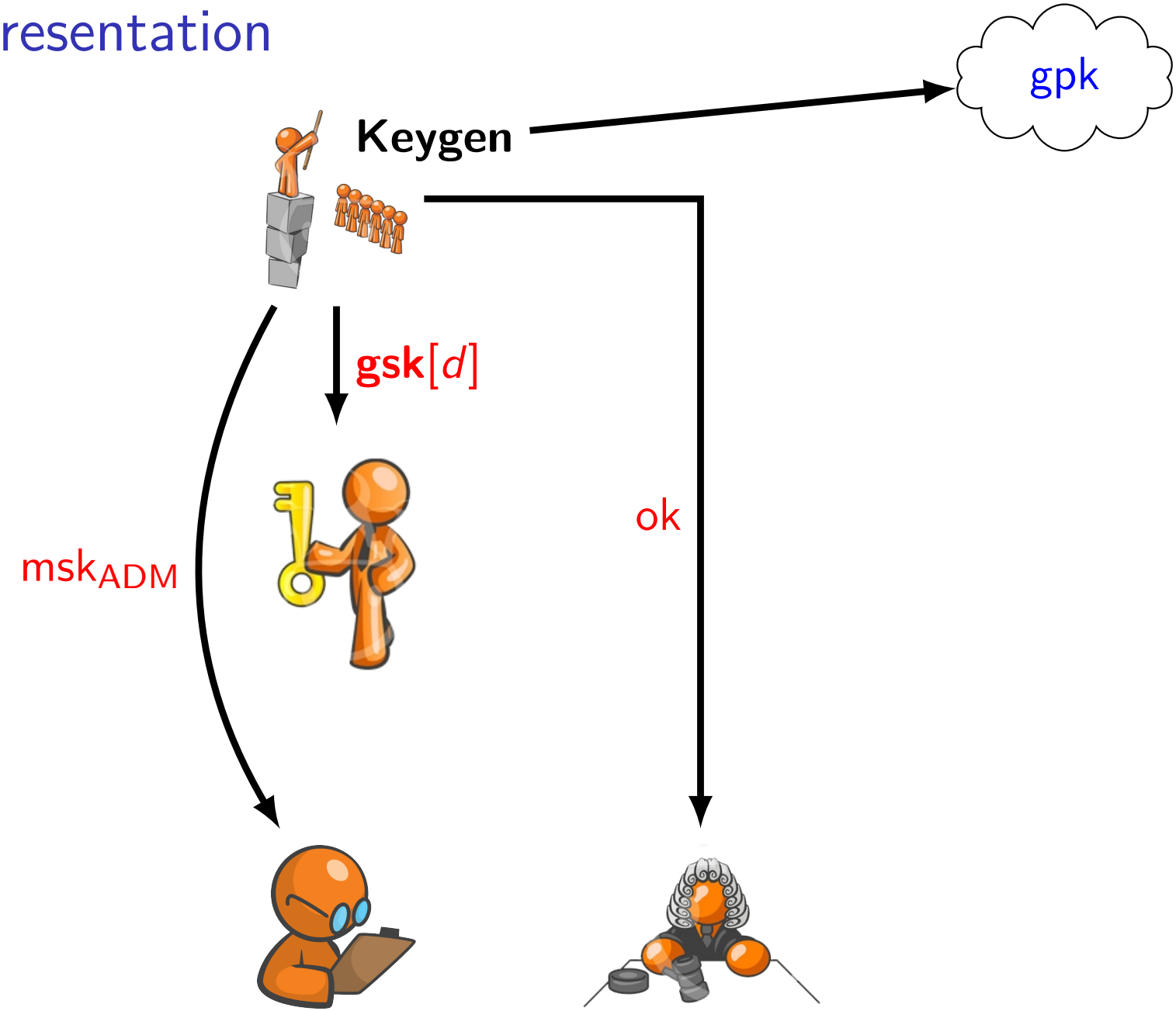
Group Signature

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

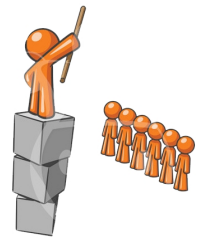
- **Keygen** provides user with a signature for its identity
- **Sign** encrypt identity and prove knowledge of the above signature + correct encryption of identity
- **Verify** verify the previous proof
- **Open** decrypt the identity

Outline

Presentation

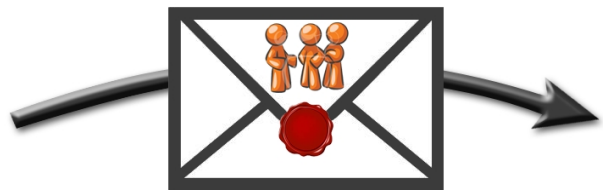


Presentation



Sign

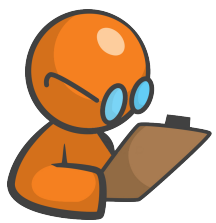
Verify



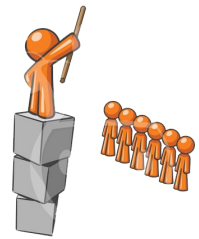
$\mathbf{gsk}[d]$

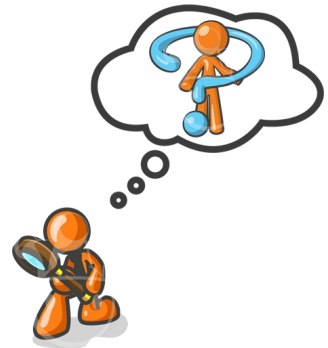
M, Σ

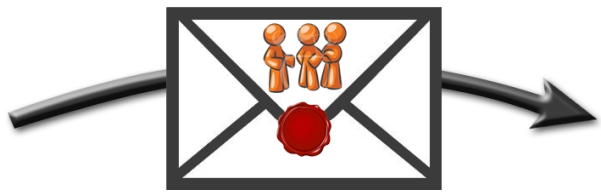
gpk



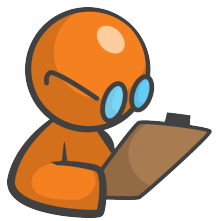
Presentation



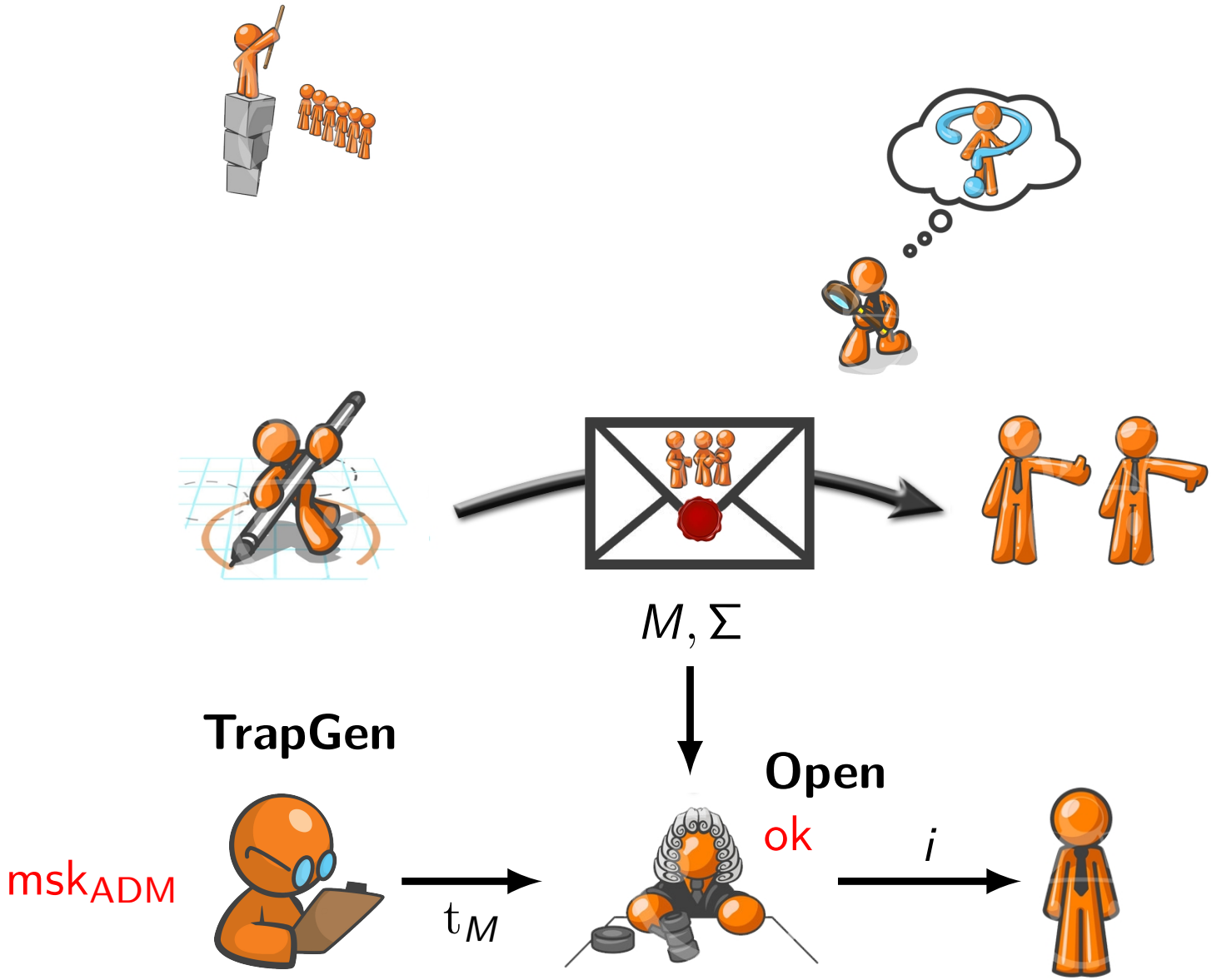




M, Σ



Presentation



Construction

(Sakai et al. Pairing'12)

- The scheme is built upon [LNW15] group signature scheme
  - It is a lattice-based scheme
  - Use GPV-IBE + CHK to encrypt identity

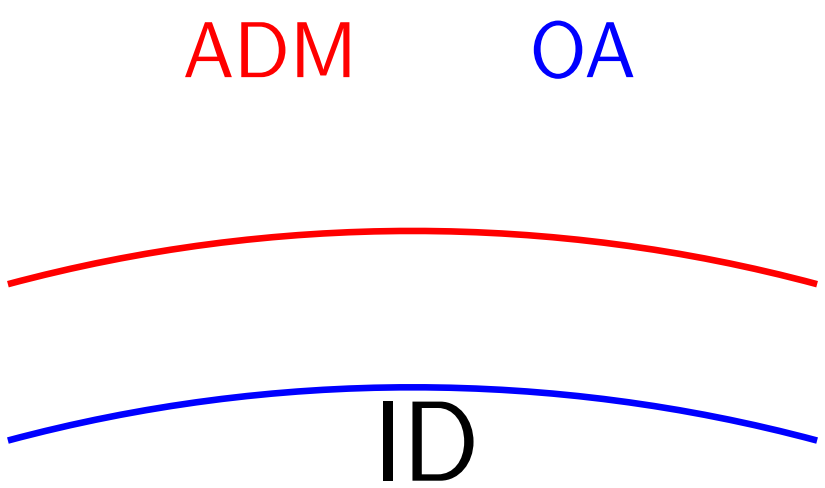
Construction

(Sakai et al. Pairing'12)

- The scheme is built upon [LNW15] group signature scheme
  - It is a lattice-based scheme
  - Use GPV-IBE + CHK to encrypt identity

Main Idea

Use two-layer encryption



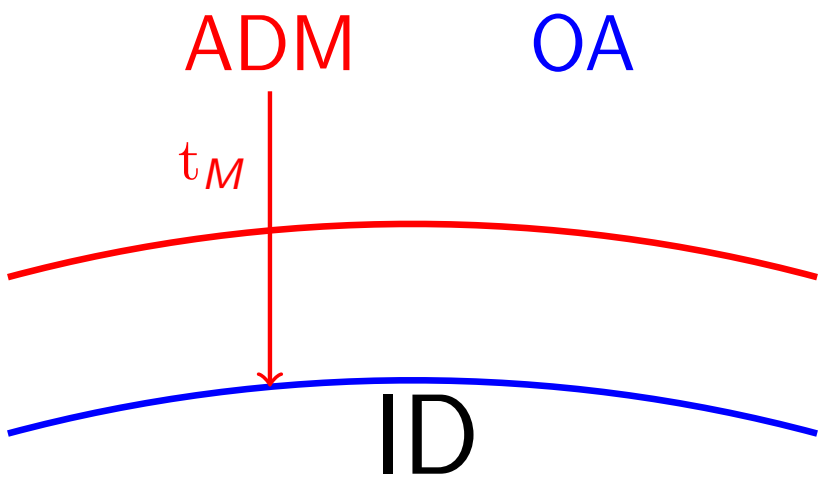
Construction

(Sakai et al. Pairing'12)

- The scheme is built upon [LNW15] group signature scheme
  - It is a lattice-based scheme
  - Use GPV-IBE + CHK to encrypt identity

Main Idea

Use two-layer encryption



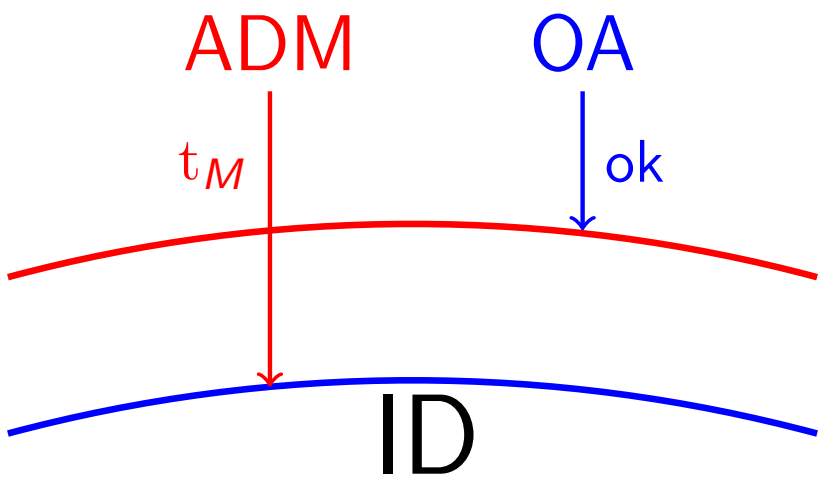
Construction

(Sakai et al. Pairing'12)

- The scheme is built upon [LNW15] group signature scheme
  - It is a lattice-based scheme
  - Use GPV-IBE + CHK to encrypt identity

Main Idea

Use two-layer encryption



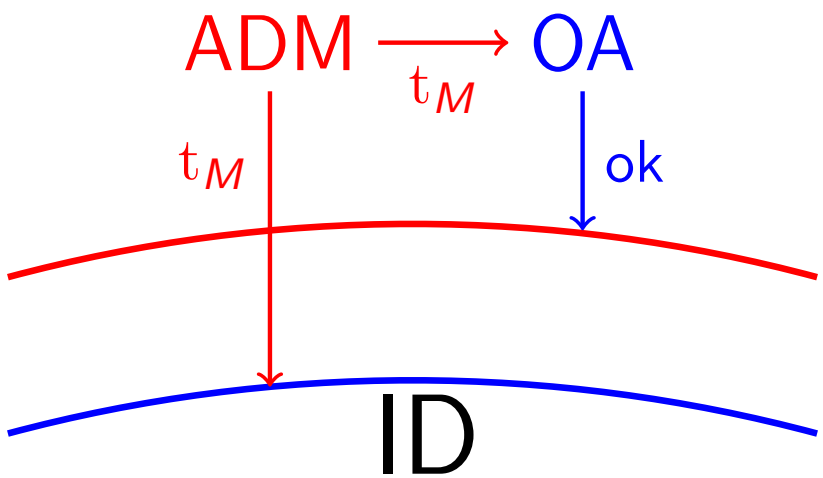
Construction

(Sakai et al. Pairing'12)

- The scheme is built upon [LNW15] group signature scheme
  - It is a lattice-based scheme
  - Use GPV-IBE + CHK to encrypt identity

Main Idea

Use two-layer encryption



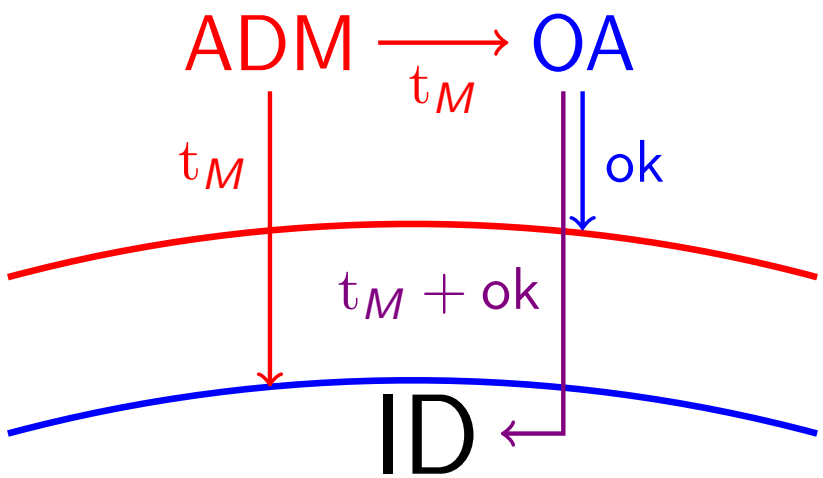
Construction

(Sakai et al. Pairing'12)

- The scheme is built upon [LNW15] group signature scheme
  - It is a lattice-based scheme
  - Use GPV-IBE + CHK to encrypt identity

Main Idea

Use two-layer encryption



Realization: Difficulties

Problem

We need to prove double-encryption relations in ZK

Realization: Difficulties

Problem

We need to prove double-encryption relations in ZK

Technique. Adapt Stern's protocol as in [LLMNW16]

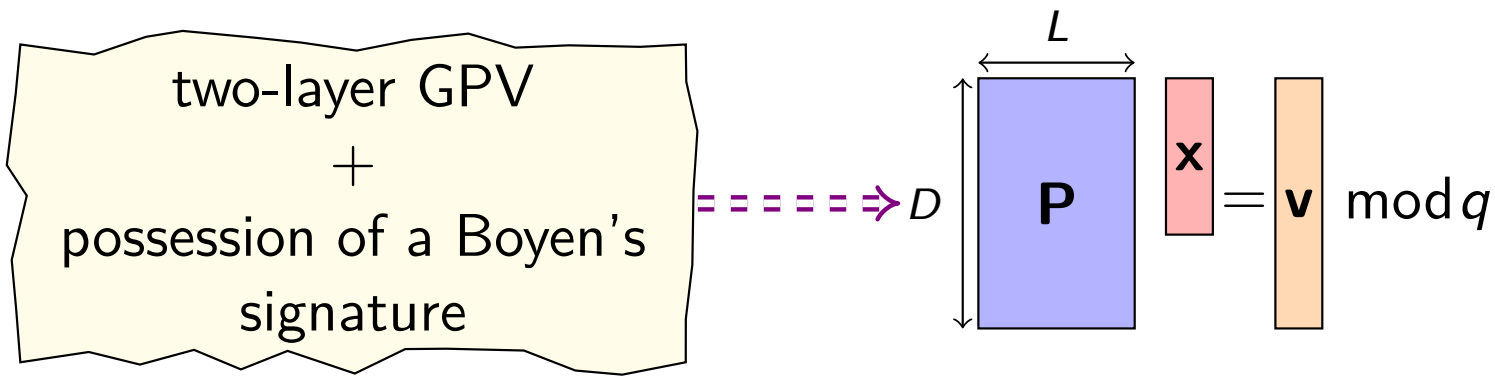
Realization: Difficulties

Problem

We need to prove double-encryption relations in ZK

Technique. Adapt Stern's protocol as in [LLMNW16]

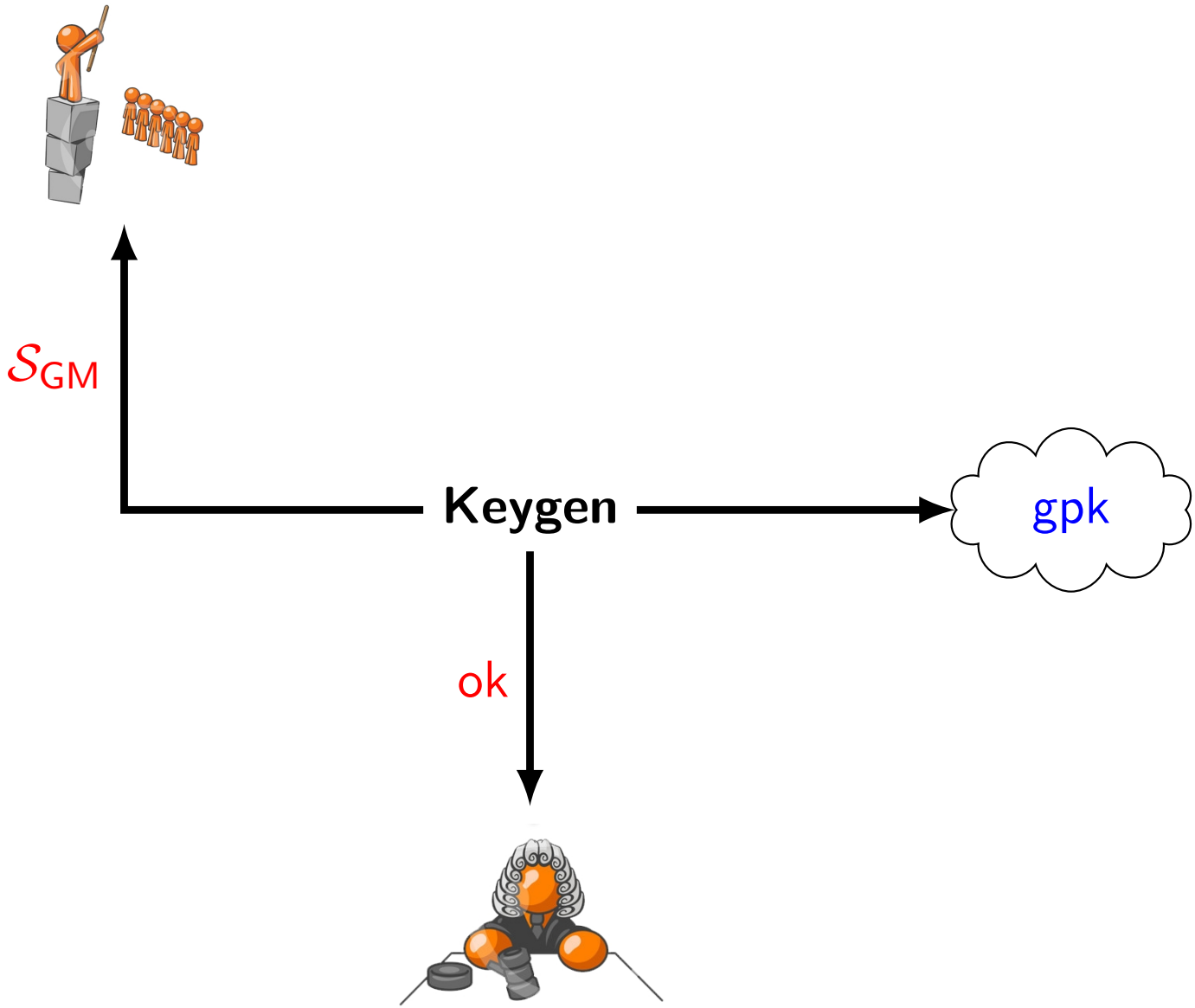
- Possible because relations can be transformed into



with $\mathbf{x} \in \{-1, 0, 1\}^L$ and $\mathbf{v} \in \mathbb{Z}_q^D$.

Outline

Presentation

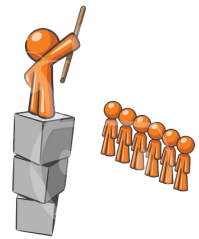


Presentation

Join

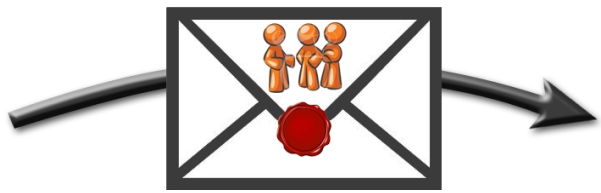
$(\mathsf{cert}_i, \mathsf{sec}_i)$

Presentation



Sign

$(\mathsf{cert}_i, \mathsf{sec}_i)$

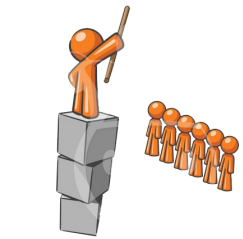


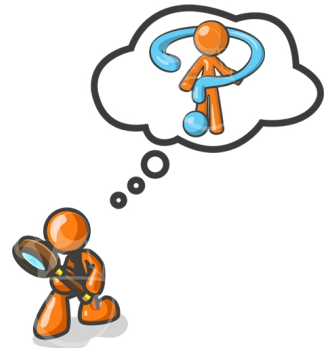
M, Σ

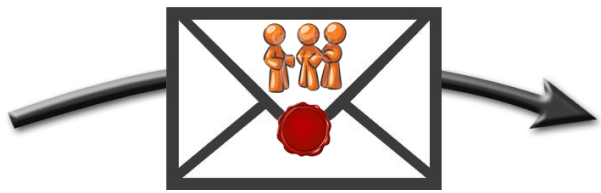
Verify

gpk

Presentation

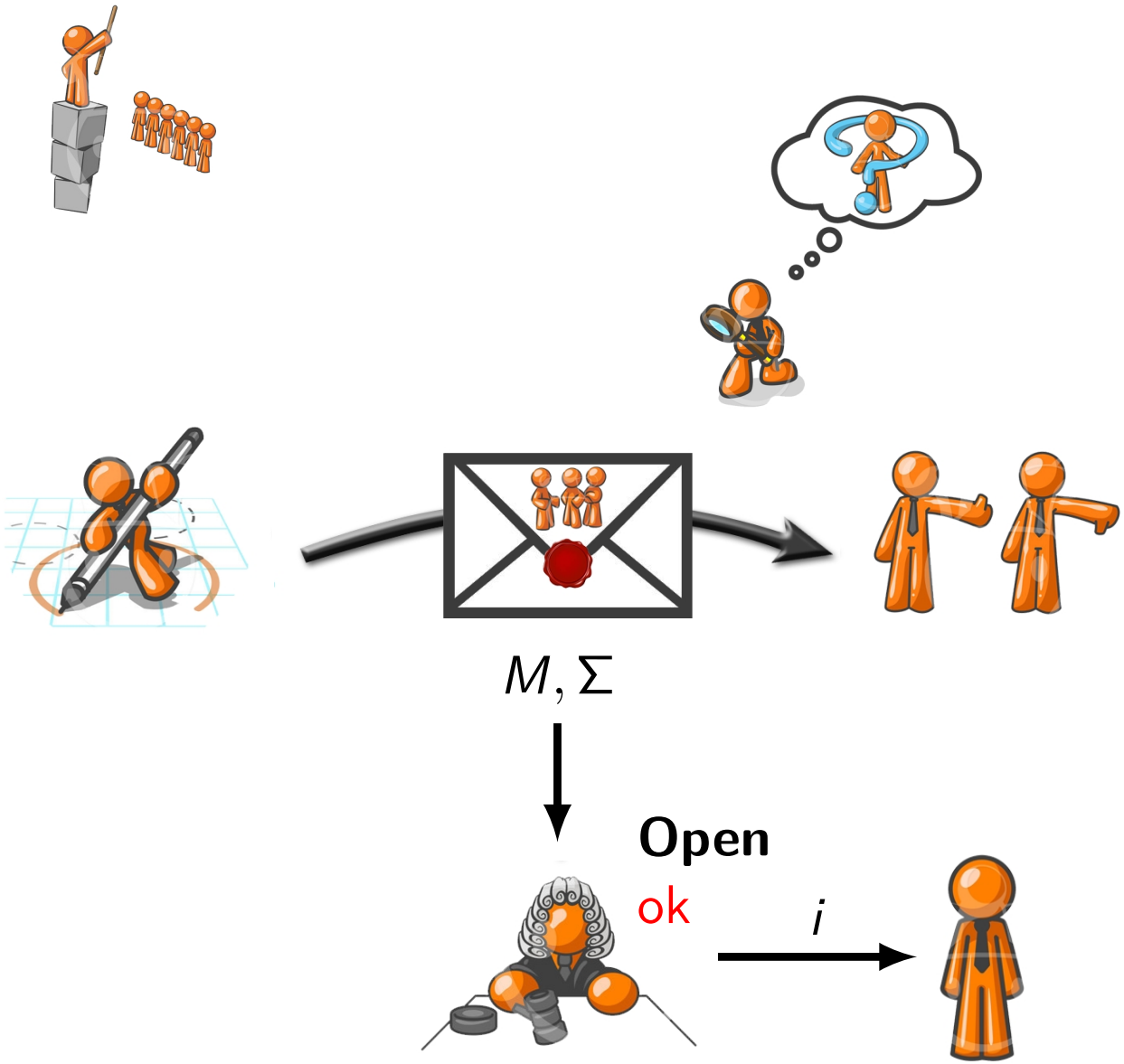




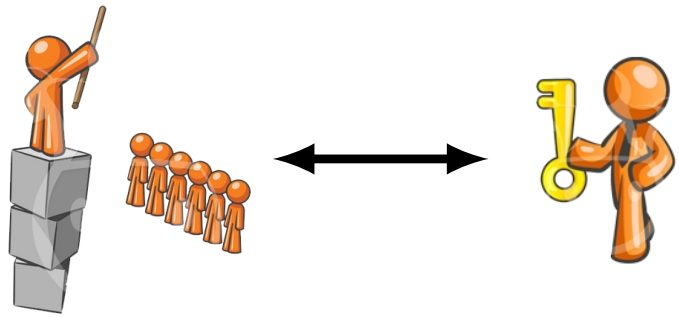


M, Σ

Presentation



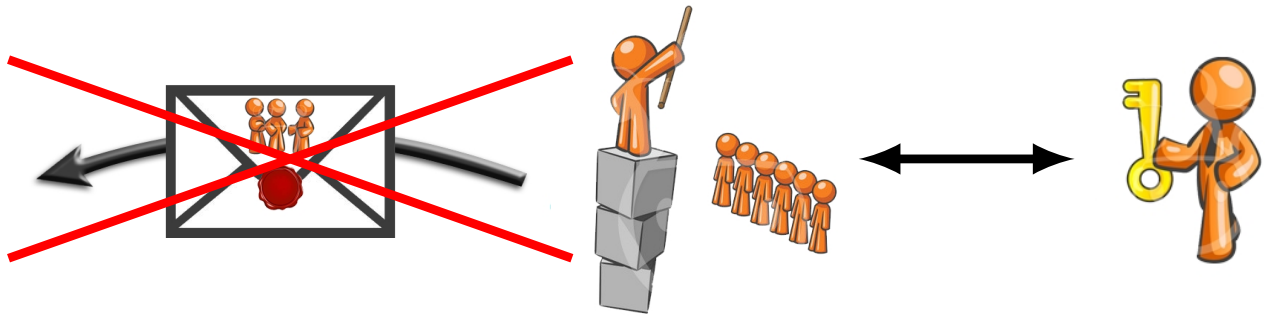
Difficulties



Differences with fixed-size group

The GM keeps a key to allow new users to enroll

Difficulties

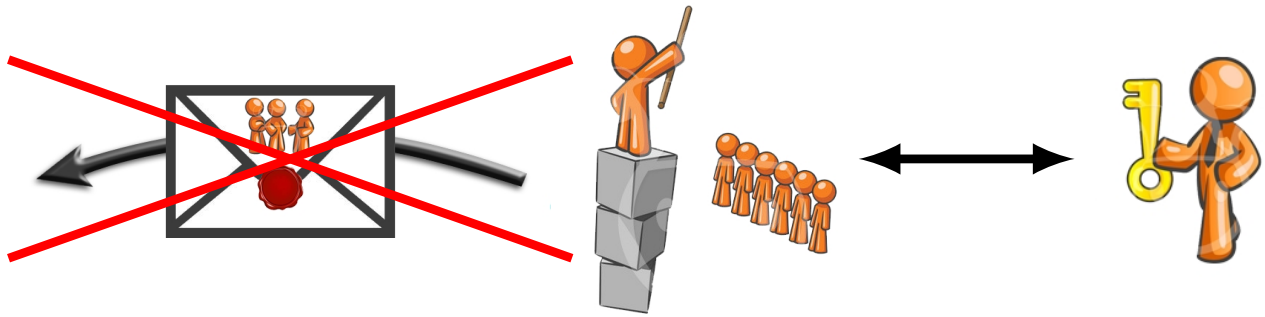


Differences with fixed-size group

The GM keeps a key to allow new users to enroll

Even with this key, authorities should not be able to sign in the name of an honest user *(non-frameability)*

Difficulties



Differences with fixed-size group

The GM keeps a key to allow new users to enroll

Even with this key, authorities should not be able to sign in the name of an honest user *(non-frameability)*

Idea: The GM has to **obliviously sign** a secret sec_i

Signature with Efficient Protocols

(Camenisch-Lysyanskaya; SCN'02)

Signatures compatible with advanced properties

Signature with Efficient Protocols

(Camenisch-Lysyanskaya; SCN'02)

Signatures compatible with advanced properties

Applications

Privacy-based primitives: anonymous credentials, e-cash,...

Signature with Efficient Protocols

(Camenisch-Lysyanskaya; SCN'02)

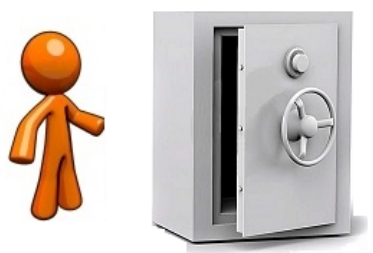
Signatures compatible with advanced properties

Applications

Privacy-based primitives: anonymous credentials, e-cash,...

Efficient Protocols :

- Sign a committed value ($\approx$ digital equivalent of a safe)
- Prove possession of a valid signature



Sign a committed value

Boyen's signature

Signature consists of a short vector in $\Lambda_q^{\mathbf{u}}\left(\mathbf{A}_M\right)$

We use a variant due to Böhl et al. (Journal of Cryptology 2015)

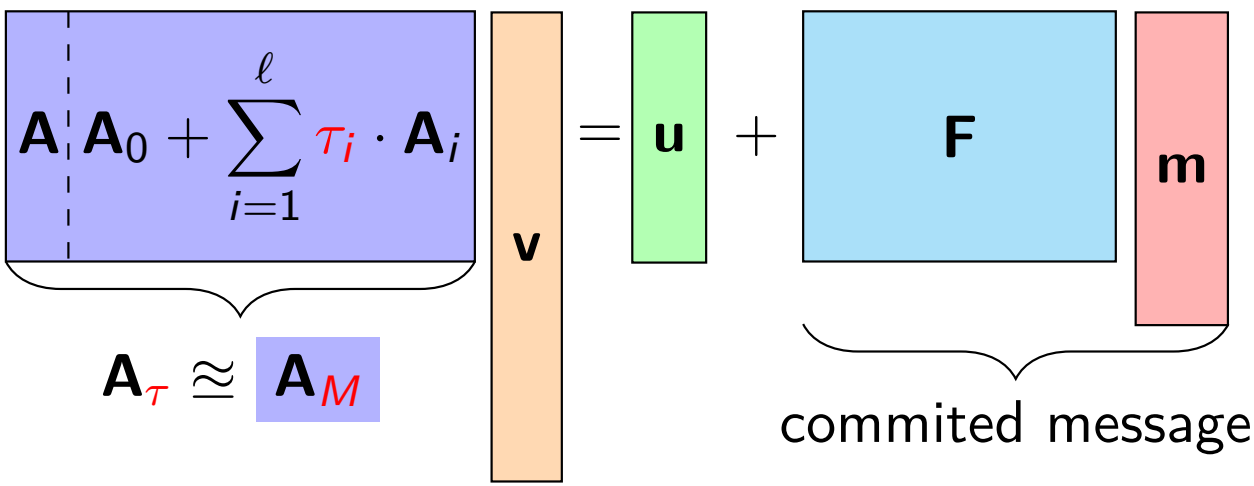
Sign a committed value

Boyen's signature

Signature consists of a short vector in $\Lambda_q^{\mathbf{u}}\left(\mathbf{A}_M\right)$

We use a variant due to Böhl et al. (Journal of Cryptology 2015)

The message is moved in the *shift*:



Conclusion

- We construct new primitives from existing techniques
- They are proven secure under standard assumptions
- Our approach is modular

There are other fields in lattice-based cryptography:

- Improve the tightness of the security proofs
  - At the level of assumptions
  - At the level of primitives
- Provide implementation with secure parameters

Thank you for your attention.