Lattice-Based Cryptography: Security Foundations and Constructions

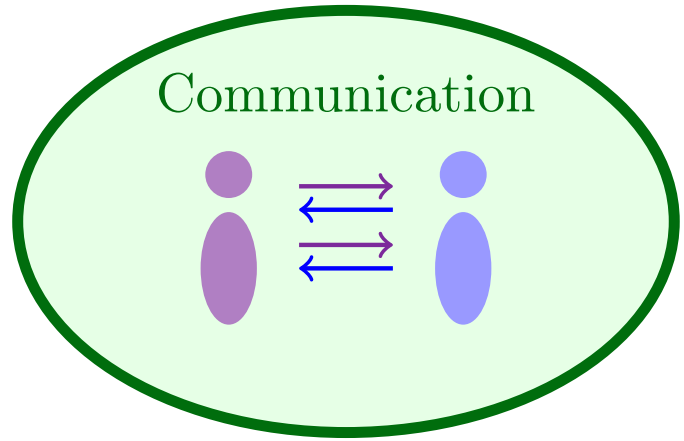
Adeline Langlois

École Normale Supérieure de Lyon,

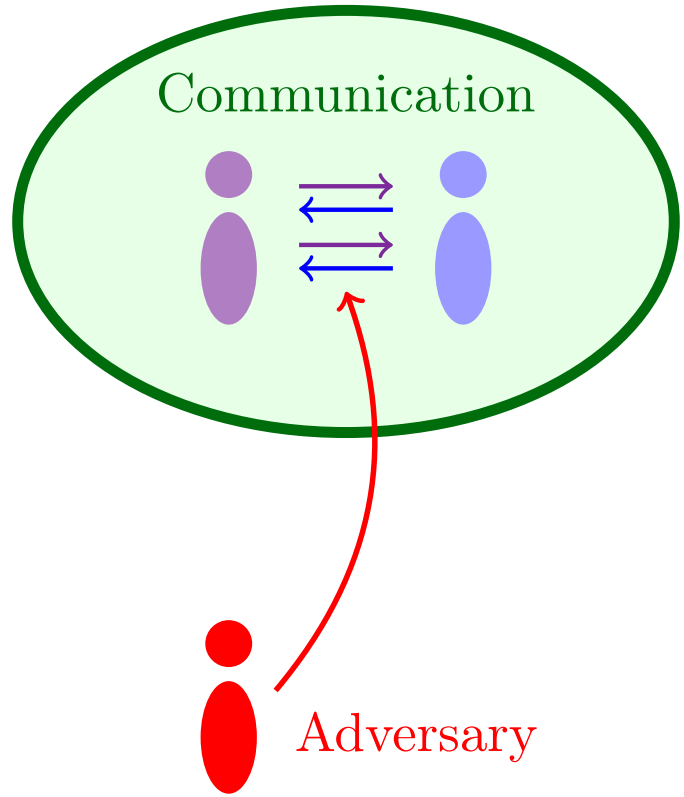
sous la direction de Damien Stehlé

Soutenance de thèse de doctorat – 17 octobre 2014

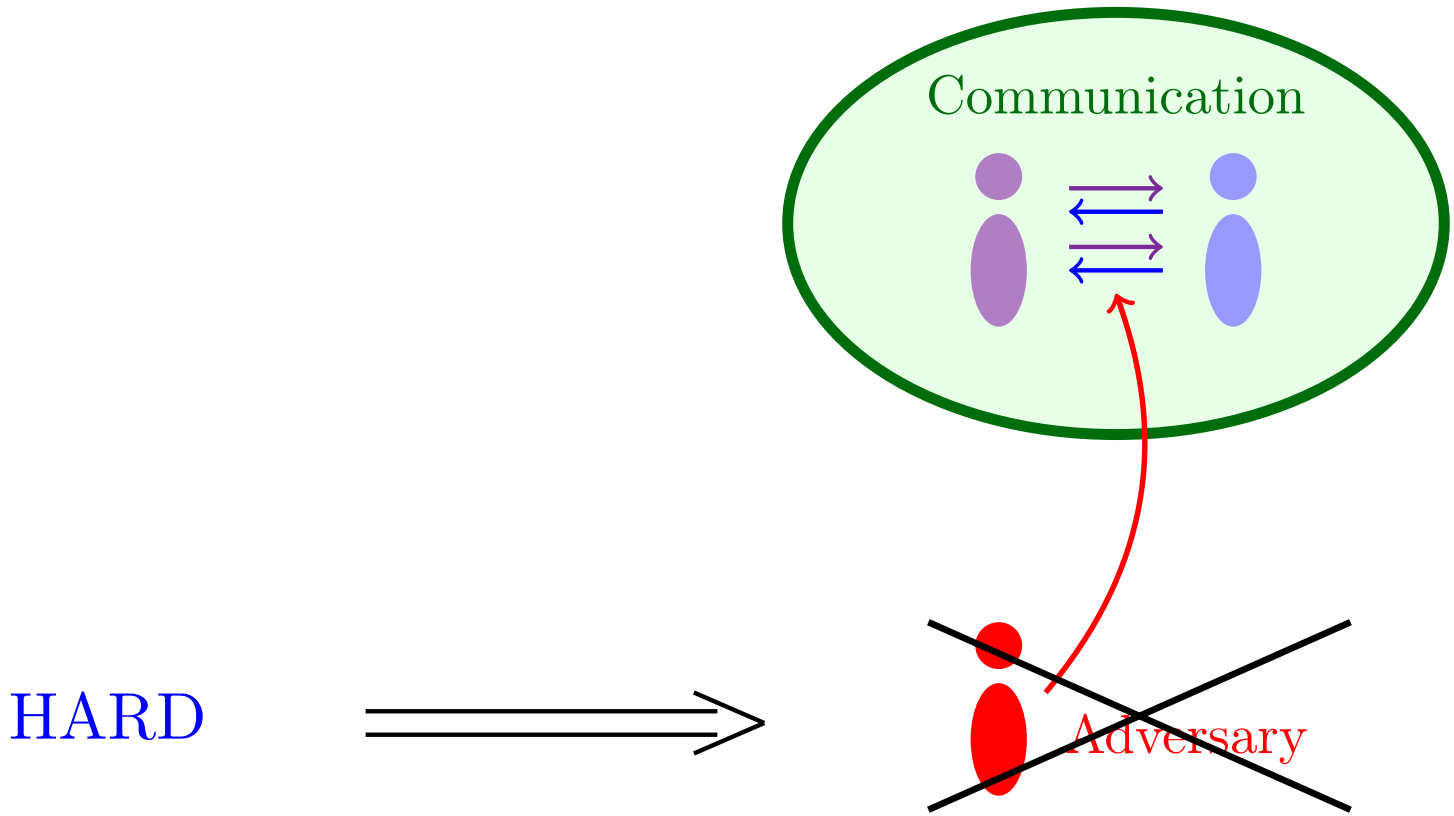
Lattice-based cryptography



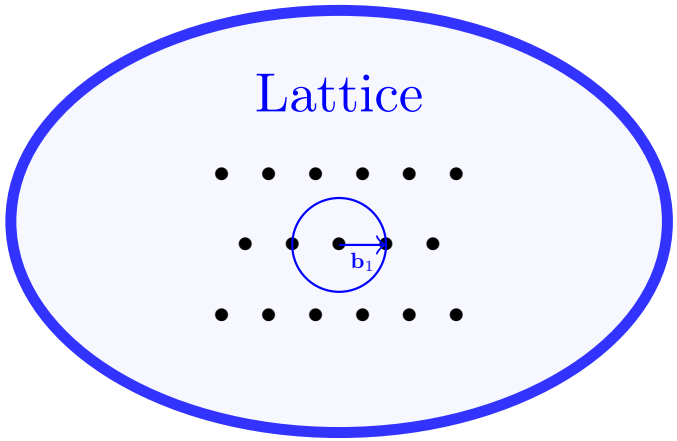
Lattice-based cryptography

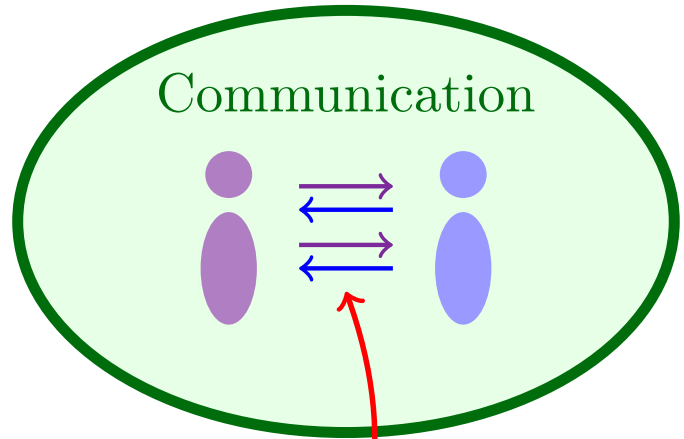


Lattice-based cryptography



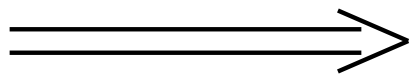
Lattice-based cryptography



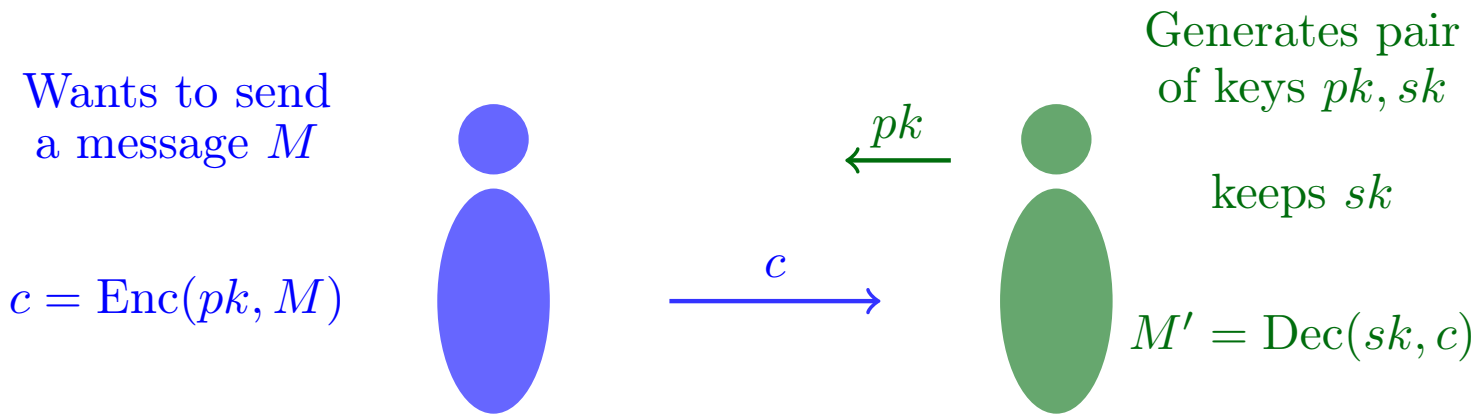


$\rightarrow$ solve an algorithmic problem

HARD



Encryption scheme



Two requirements:
Correctness
and Security

- $M = M'$ with high probability
- $c_0 = \mathrm{Enc}(pk, M_0)$ indistinguishable from $c_1 = \mathrm{Enc}(pk, M_1)$

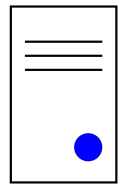
Signature scheme

Wants to authenticate a message M

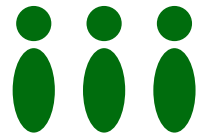
Generates a pair of keys (pk, sk)

$\sigma = \text{Sign}(sk, M)$

pk →



→ (M, σ)



Anyone can verify:
$\text{Verify}(pk, \sigma, M) = 1$?

Two requirements:
Correctness
and Security

→ Verify $= 1$ with high probability if σ is correct

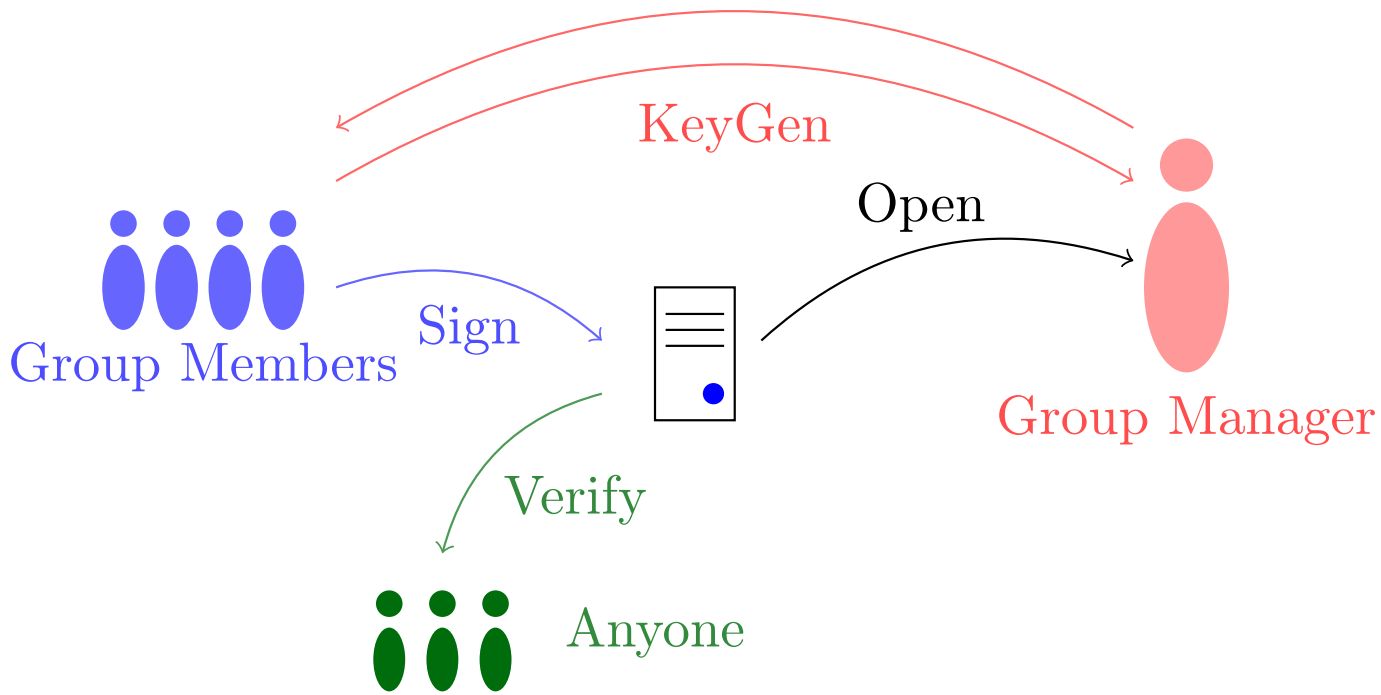
→ adversary cannot forge a signature σ^* for a new M^*

Group signatures

[Chaum, VanHeyst 91]

→ allow any member of a group to anonymously and accountably sign on behalf of this group.

- Group manager $(mpk, msk) + sk_i$ — KeyGen, Open
- Group members (sk_i) — Sign
- Anyone — Verify



Outline

Lattice-Based Cryptography

Security Foundations

- Z. Brakerski, **A. Langlois**, C. Peikert, O. Regev and D. Stehlé. Classical Hardness of Learning with Errors. In proc. of *STOC* 2013.
- **A. Langlois** and D. Stehlé. Worst-case to Average-case Reductions for Module Lattices. Accepted to *Designs, Codes and Cryptography*.

Group Signature Scheme

- F. Laguillaumie, **A. Langlois**, B. Libert and D. Stehlé. Lattice-based Group Signature with Logarithmic Signature Size. In proc. of *Asiacrypt* 2013.
- **A. Langlois**, S. Ling, K. Nguyen and H. Wang. Lattice-based Group Signature with Verifier Local Revocation. In proc. of *PKC* 2014.

Conclusion

Outline

Lattice-Based Cryptography

Security Foundations

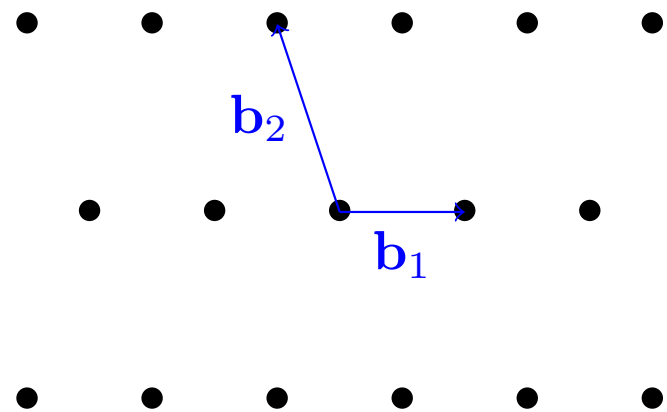
- Z. Brakerski, **A. Langlois**, C. Peikert, O. Regev and D. Stehlé. Classical Hardness of Learning with Errors. In proc. of *STOC* 2013.
- **A. Langlois** and D. Stehlé. Worst-case to Average-case Reductions for Module Lattices. Accepted to *Designs, Codes and Cryptography*.

Group Signature Scheme

- F. Laguillaumie, **A. Langlois**, B. Libert and D. Stehlé. Lattice-based Group Signature with Logarithmic Signature Size. In proc. of *Asiacrypt* 2013.
- **A. Langlois**, S. Ling, K. Nguyen and H. Wang. Lattice-based Group Signature with Verifier Local Revocation. In proc. of *PKC* 2014.

Conclusion

Lattices



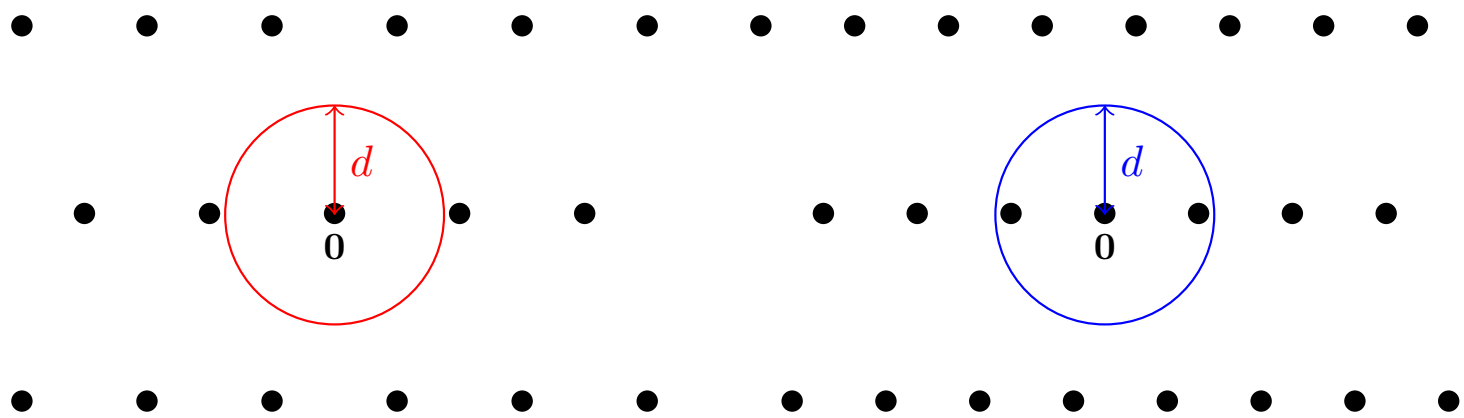
Lattice

$\mathcal{L}(\mathbf{B}) = \{\sum_{1=i}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$, where the $(\mathbf{b}_i)_{1 \leq i \leq n}$'s, linearly independent vectors, are a basis of $\mathcal{L}(\mathbf{B})$.

Shortest Vector Problem (GapSVP)

Given a lattice $\mathcal{L}(\mathbf{B})$ of dimension n and $d > 0$:

Output:
- YES: there is $\mathbf{z} \in \mathcal{L}(\mathbf{B})$ non-zero such that $\|\mathbf{z}\| < d$,
- NO: for all non-zero vectors $\mathbf{z} \in \mathcal{L}(\mathbf{B})$: $\|\mathbf{z}\| \geq d$.



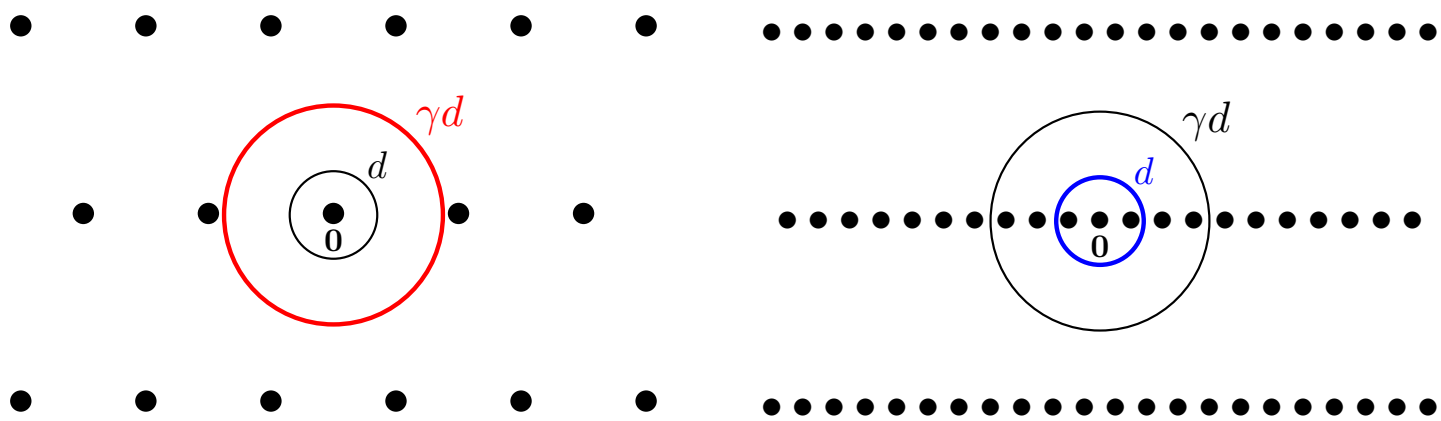
Lattice

$\mathcal{L}(\mathbf{B}) = \{\sum_{1=i}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$, where the $(\mathbf{b}_i)_{1 \leq i \leq n}$'s, linearly independent vectors, are a basis of $\mathcal{L}(\mathbf{B})$.

Gap Shortest Vector Problem (GapSVP$_\gamma$)

Given a lattice $\mathcal{L}(\mathbf{B})$ of dimension n and $d > 0$:

Output:
- YES: there is $\mathbf{z} \in \mathcal{L}(\mathbf{B})$ non-zero such that $\|\mathbf{z}\| < d$,
- NO: for all non-zero vectors $\mathbf{z} \in \mathcal{L}(\mathbf{B})$: $\|\mathbf{z}\| \geq \gamma d$.



Conjecture

There is no algorithm that approximates these lattice problems to within polynomial factors $\gamma = \text{poly}(n)$ with time polynomial in n.

Lattice-based cryptography

From basic to very advanced primitives

- Public key encryption and Signature scheme (practical),
  [Regev 05, Gentry, Peikert and Vaikuntanathan 08, Lyubashevsky 12 ...];
- Identity/Attribute-based encryption, [GPV 08
  Gorbunov, Vaikuntanathan and Wee 13 ...];
- Fully homomorphic encryption,
  [Gentry 09, Brakerski and Vaikuntanathan 11, ...].

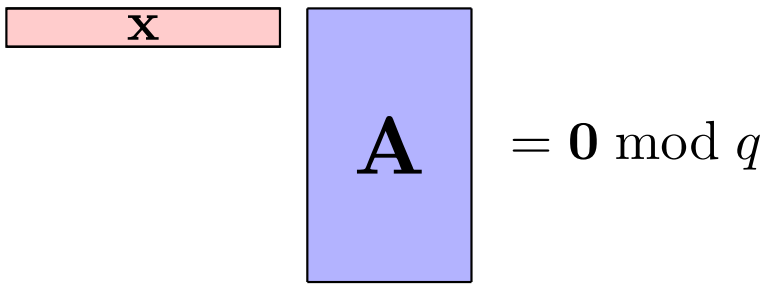
Advantages

- (Asymptotically) efficient;
- Security proofs **from the hardness of lattice problems**;
- Likely to resist attacks from quantum computers.

SIS_β

Parameters: n dimension, $m \geq n$, q modulus.
For $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$:

Small Integer Solution



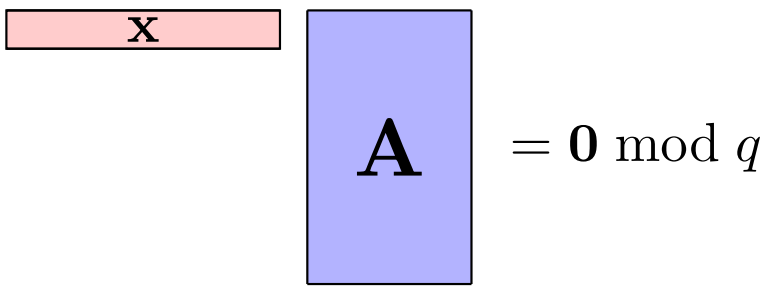
Goal: Given $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$,
find $\mathbf{x}$ s.t. $0 < \|\mathbf{x}\| \leq \beta$.

[Ajtai 96]

SIS_β and LWE_α

Parameters: n dimension, $m \geq n$, q modulus.
For $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$:

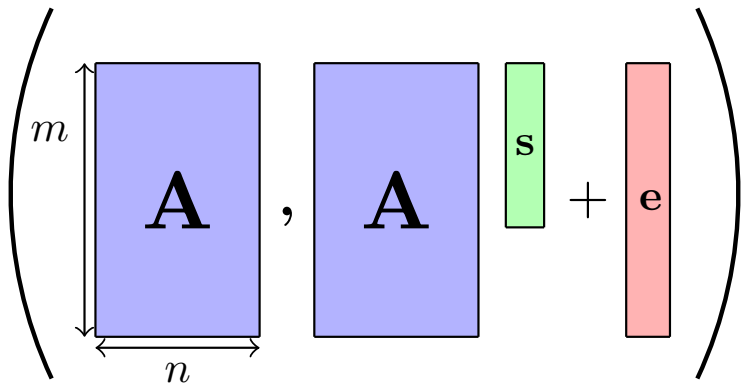
Small Integer Solution



Goal: Given $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$,
find $\mathbf{x}$ s.t. $0 < \|\mathbf{x}\| \leq \beta$.

[Ajtai 96]

Learning With Errors

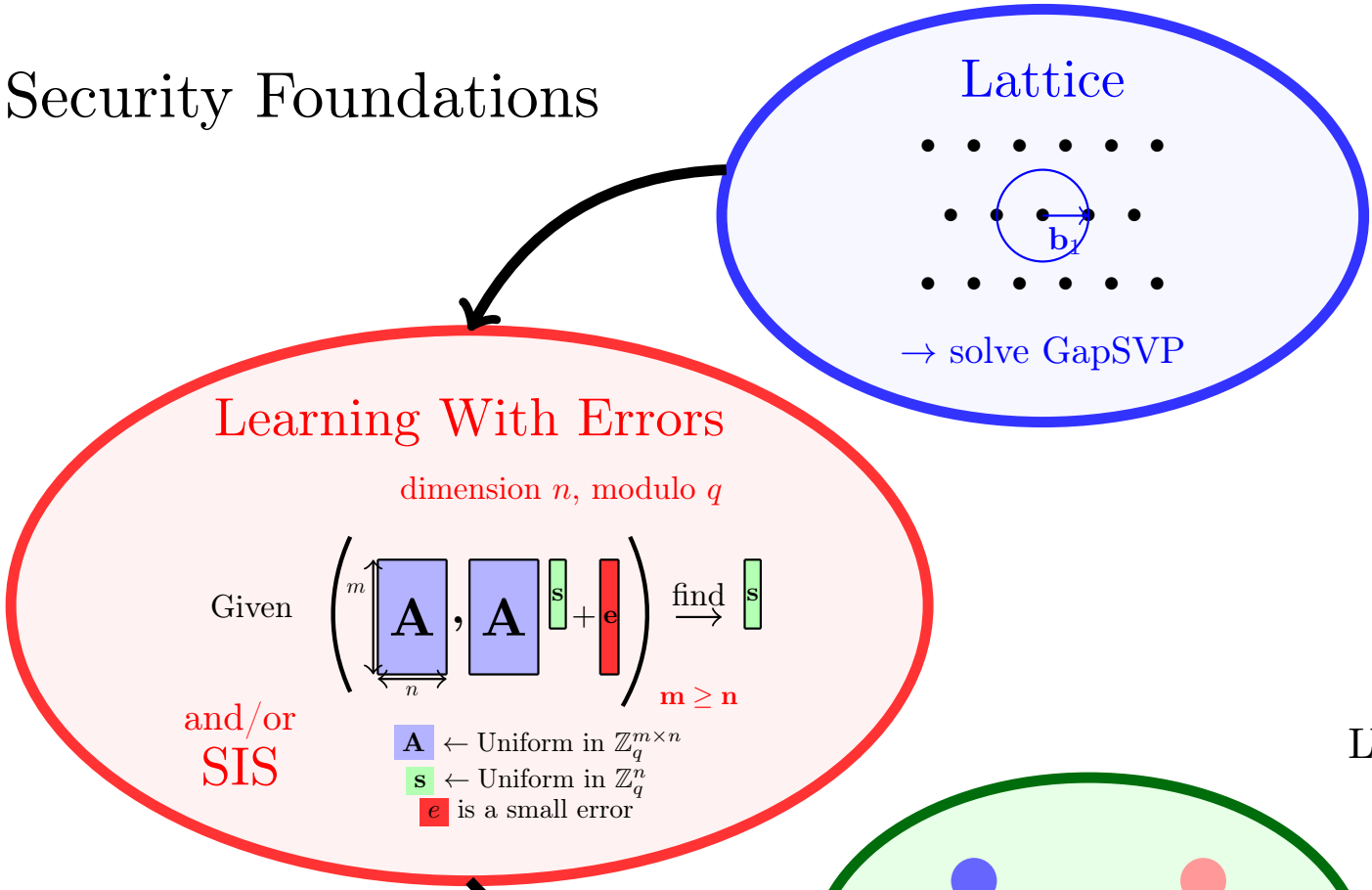


$\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$,
$\mathbf{e}$ a small error $\approx \alpha q$.

Goal: Given $(\mathbf{A}, \mathbf{A}\,\mathbf{s} + \mathbf{e})$,
find $\mathbf{s}$.

[Regev 05]

1. Security Foundations



LWE-based Encryption

SIS-based Signature

LWE and SIS-based Group signature

2. Constructions

Outline

Lattice-Based Cryptography

Security Foundations

- Z. Brakerski, **A. Langlois**, C. Peikert, O. Regev and D. Stehlé. Classical Hardness of Learning with Errors. In proc. of *STOC* 2013.
- **A. Langlois** and D. Stehlé. Worst-case to Average-case Reductions for Module Lattices. Accepted to *Designs, Codes and Cryptography*.

Group Signature Scheme

- F. Laguillaumie, **A. Langlois**, B. Libert and D. Stehlé. Lattice-based Group Signature with Logarithmic Signature Size. In proc. of *Asiacrypt* 2013.
- **A. Langlois**, S. Ling, K. Nguyen and H. Wang. Lattice-based Group Signature with Verifier Local Revocation. In proc. of *PKC* 2014.

Conclusion

Outline

Lattice-Based Cryptography

Security Foundations

- Z. Brakerski, **A. Langlois**, C. Peikert, O. Regev and D. Stehlé. Classical Hardness of Learning with Errors. In proc. of *STOC* 2013.
- **A. Langlois** and D. Stehlé. Worst-case to Average-case Reductions for Module Lattices. Accepted to *Designs, Codes and Cryptography*.

Group Signature Scheme

- F. Laguillaumie, **A. Langlois**, B. Libert and D. Stehlé. Lattice-based Group Signature with Logarithmic Signature Size. In proc. of *Asiacrypt* 2013.
- **A. Langlois**, S. Ling, K. Nguyen and H. Wang. Lattice-based Group Signature with Verifier Local Revocation. In proc. of *PKC* 2014.

Conclusion

Main result

Not quantum

GapSVP in dimension $\sqrt{n}$

A classical reduction from a worst-case lattice problem to the Learning With Errors problem with small modulus.

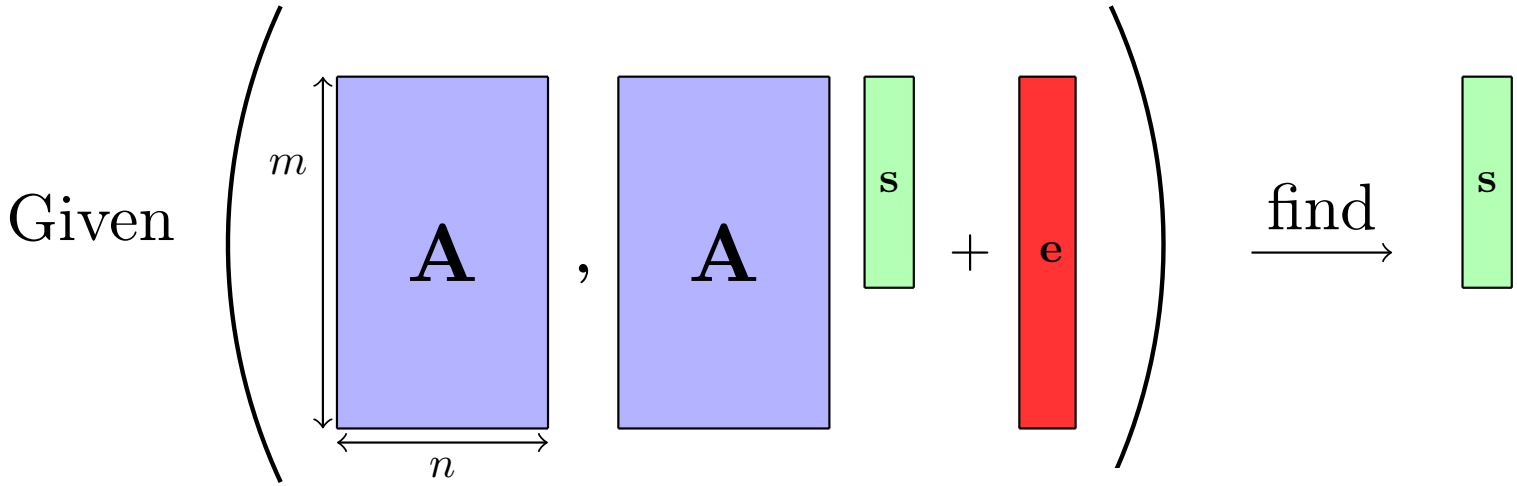
Dimension n

Polynomial in n

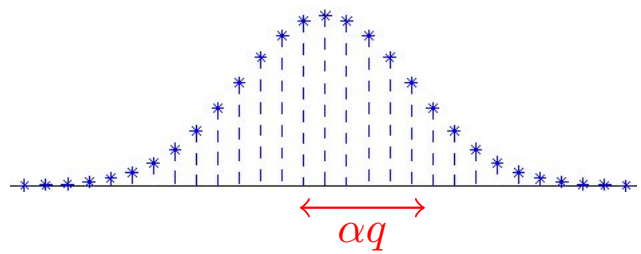
- Z. Brakerski, **A. Langlois**, C. Peikert, O. Regev and D. Stehlé. Classical Hardness of Learning with Errors. In the proceedings of *STOC* 2013.

The Learning With Errors problem [Regev 05]

LWE_q^n (with m arbitrarily large)



- $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$,
- $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$,
- $e \sim D_{\mathbb{Z}^m, \alpha q}$ small with $\alpha = o(1)$.



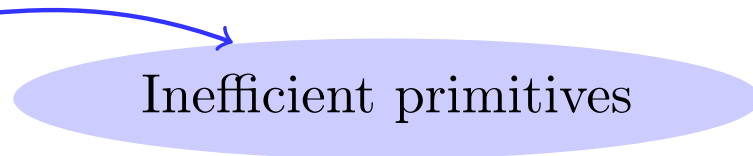
Discrete Gaussian error

Decision version: Distinguish from $(\mathbf{A}, \mathbf{b})$ with $\mathbf{b}$ uniform.

Prior reductions from worst-case lattice problem to LWE

- **[Regev 05]**
  - A **quantum** reduction;
  - with q polynomial.

- **[Peikert 09]**
  - A **classical** reduction;
  - with q exponential.



- **[Peikert 09]**
  - A **classical** reduction;
  - with q polynomial;
  - based on a non-standard lattice problem.

Prior reductions from worst-case lattice problem to LWE

- **[Regev 05]**
  - A **quantum** reduction;
  - with q polynomial.
- **[Peikert 09]**
  - A **classical** reduction;
  - with q exponential.
- **[Peikert 09]**
  - A **classical** reduction;
  - with q polynomial;
  - based on a non-standard lattice problem.

Our main result

- A **classical** reduction,
- from a standard worst-case lattice problem,
- with q polynomial.

Main component in the proof: a self reduction

- Recall that [Peikert09] already showed hardness of LWE with q exponential.

How do we obtain a hardness proof for p polynomial?

Main component in the proof: a self reduction

- Recall that [Peikert09] already showed hardness of LWE with q exponential.

How do we obtain a hardness proof for p polynomial?

- All we have to do is show the following reduction:

  A reduction from LWE with modulus q exponential to LWE with modulus p polynomial.

Modulus Switching

A reduction from LWE with modulus q to LWE with modulus p.

How to map $(\mathbf{A}, \mathbf{As} + \mathbf{e}) \bmod q$ to $(\mathbf{A}', \mathbf{A}'\mathbf{s} + \mathbf{e}') \bmod p$?

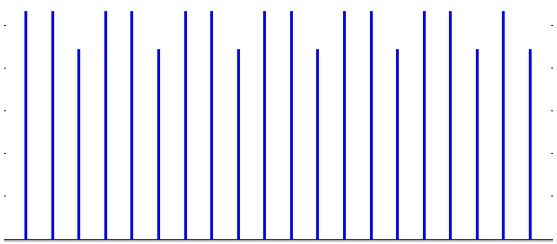
- Transform $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$ to $\mathbf{A}' \hookleftarrow U(\mathbb{Z}_p^{m \times n})$;
  First idea: $\mathbf{A}' = \lfloor \frac{p}{q} \mathbf{A} \rceil$?

Modulus Switching

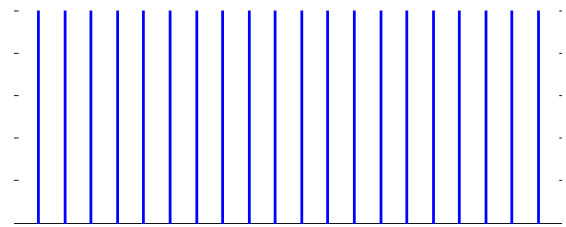
A reduction from LWE with modulus q to LWE with modulus p.

How to map $(\mathbf{A}, \mathbf{As} + \mathbf{e}) \bmod q$ to $(\mathbf{A}', \mathbf{A}'\mathbf{s} + \mathbf{e}') \bmod p$?

- Transform $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$ to $\mathbf{A}' \hookleftarrow U(\mathbb{Z}_p^{m \times n})$;
  First idea: $\mathbf{A}' = \lfloor \frac{p}{q} \mathbf{A} \rceil$?
- Two main difficulties:
  1. The distribution is not uniform:



A naive rounding introduces artefacts.



Add a **Gaussian rounding** to smooth the distribution:

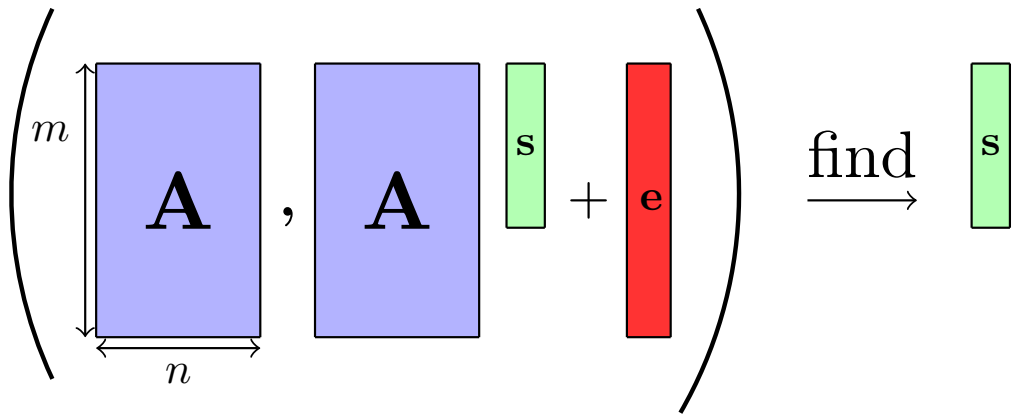
$\mathbf{A}' = \frac{p}{q} \mathbf{A} + \mathbf{R}$.

  2. In $\mathbf{A}'\mathbf{s} + \mathbf{e}'$, the rounding errors gets multiplied by the secret $\mathbf{s}$ (which is too large: uniform is $\mathbb{Z}_q^n$).

From large to small secret

From LWE with arbitrary secret to LWE with binary secret.

- Inspired by ideas from cryptography (prior reduction by [Goldwasser, Kalai, Peikert and Vaikuntanathan 10]); but different and stronger techniques.



- From $\mathbf{s}$ uniform in $\mathbb{Z}_q^n$ to $\mathbf{s}$ uniform in $\{0,1\}^n$.
- **Consequence:** it expands the dimension from n to $n \log q$.

Summary of our new hardness proof of LWE

Our main result

A classical reduction from GapSVP in dimension $\sqrt{n}$ to LWE in dimension n with poly(n) modulus.

Reductions of the proof

Problem	Dimension	Modulus	Secret	
GapSVP	$\sqrt{n}$			
$\downarrow_0$				**[Peikert 09]**
LWE	$\sqrt{n}$	large	$\mathbb{Z}_q^{\sqrt{n}}$	
$\downarrow_1$				**New**
LWE	n	large	small	
$\downarrow_2$				**New**
LWE	n	poly(n)	in $\mathbb{Z}_q^n$	

Summary of our new hardness proof of LWE

Our main result

A classical reduction from GapSVP in dimension $\sqrt{n}$
to LWE in dimension n with poly(n) modulus.

Other results

The hardness of LWE_q^n is a function of $n \log q$.

Open problems

Is there a classical reduction as good as the one in **[Regev 05]**?

1. We lose a quadratic term in the dimension;
2. We do not have the same hard problem on lattices as Regev.

Outline

Lattice-Based Cryptography

Security Foundations

- Z. Brakerski, **A. Langlois**, C. Peikert, O. Regev and D. Stehlé. Classical Hardness of Learning with Errors. In proc. of *STOC* 2013.
- **A. Langlois** and D. Stehlé. Worst-case to Average-case Reductions for Module Lattices. Accepted to *Designs, Codes and Cryptography*.

Group Signature Scheme

- F. Laguillaumie, **A. Langlois**, B. Libert and D. Stehlé. Lattice-based Group Signature with Logarithmic Signature Size. In proc. of *Asiacrypt* 2013.
- **A. Langlois**, S. Ling, K. Nguyen and H. Wang. Lattice-based Group Signature with Verifier Local Revocation. In proc. of *PKC* 2014.

Conclusion

Outline

Lattice-Based Cryptography

Security Foundations

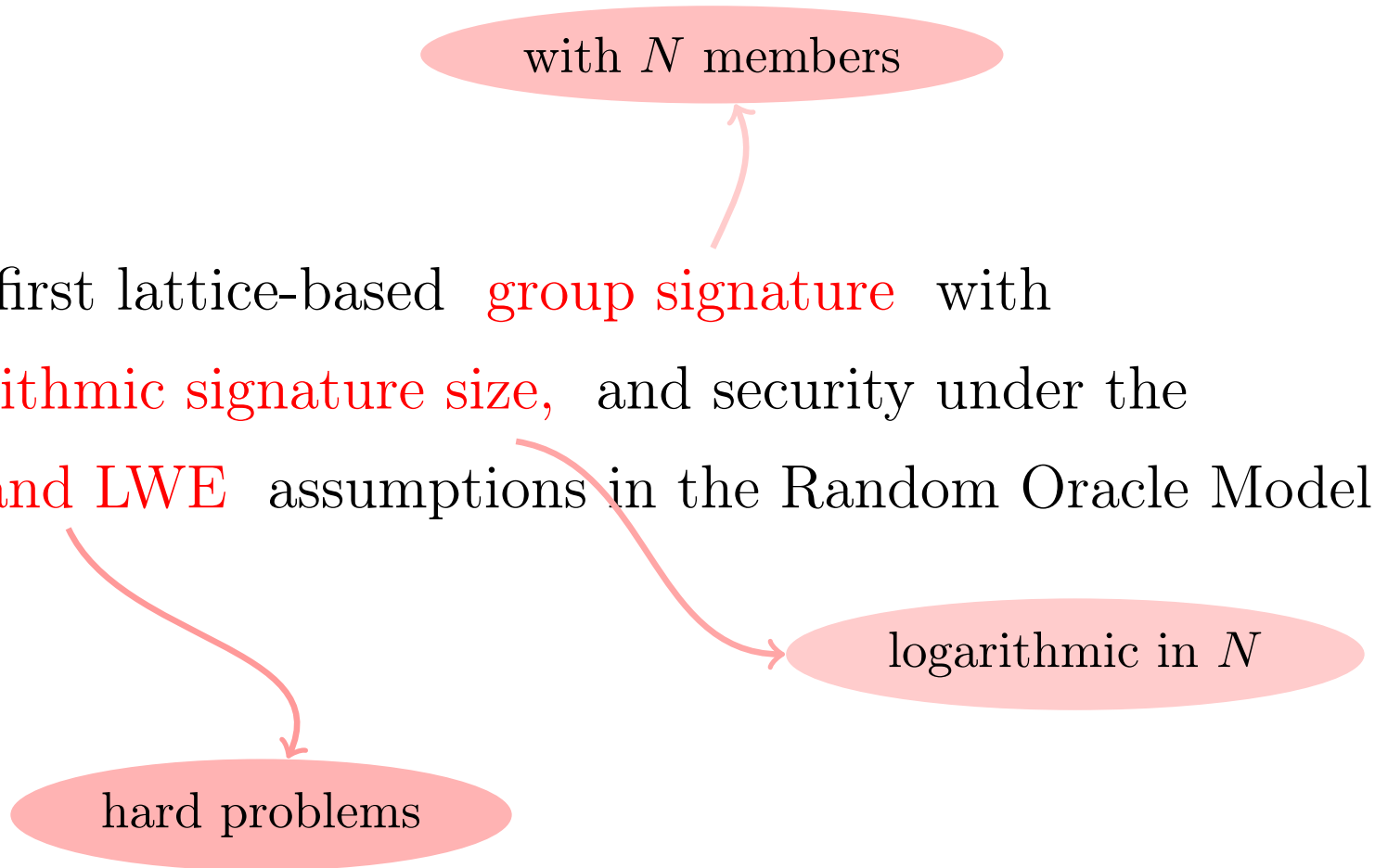
- Z. Brakerski, **A. Langlois**, C. Peikert, O. Regev and D. Stehlé. Classical Hardness of Learning with Errors. In proc. of *STOC* 2013.
- **A. Langlois** and D. Stehlé. Worst-case to Average-case Reductions for Module Lattices. Accepted to *Designs, Codes and Cryptography*.

Group Signature Scheme

- F. Laguillaumie, **A. Langlois**, B. Libert and D. Stehlé. Lattice-based Group Signature with Logarithmic Signature Size. In proc. of *Asiacrypt* 2013.
- **A. Langlois**, S. Ling, K. Nguyen and H. Wang. Lattice-based Group Signature with Verifier Local Revocation. In proc. of *PKC* 2014.

Conclusion

Main result



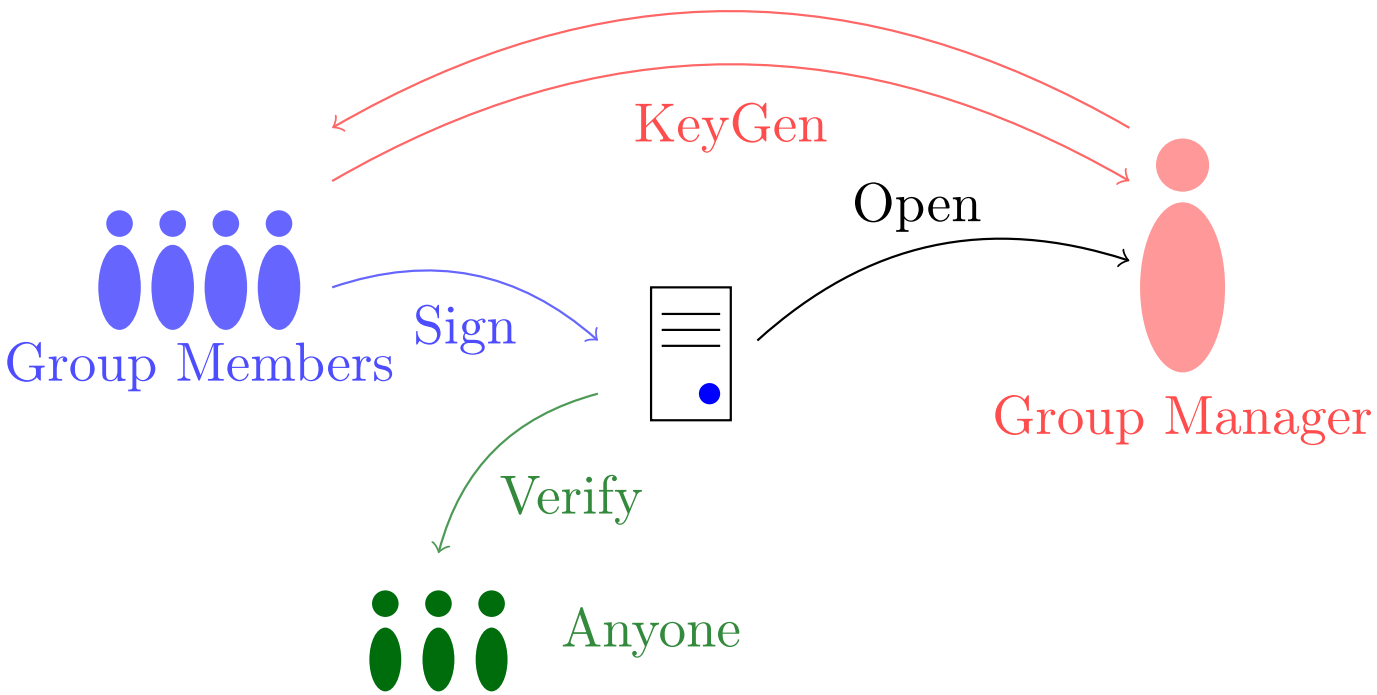
- F. Laguillaumie, **A. Langlois**, B. Libert and D. Stehlé. Lattice-based Group Signature with Logarithmic Signature Size. In the proc. of *Asiacrypt* 2013.

Group Signatures

[Chaum, VanHeyst 91]

Group signatures allow any member of a group to anonymously and accountably sign on behalf of this group.

- Group manager $(mpk, msk) + sk_i$ — KeyGen, Open
- Group members (sk_i) — Sign
- Anyone — Verify



Security:

- Anonymity
- Traceability

Security: Anonymity and Traceability

Security requirements [BellareMicciancioWarinschi03]

- Anonymity

  A given signature does not leak the identity of its originator.

  $\rightsquigarrow$ Two types: weak and full.

	weak	full
Given	sk_i for all users	opening oracle
Goal	distinguish between two users	

- Traceability

  No collusion of malicious users can produce a valid signature that cannot be traced to one of them.

Given	msk and sk_i of users in the collusion
Goal	create a valid signature that traces to someone not in the collusion

Prior works

- Introduced by [Chaum, VanHeyst 91],
- Generic construction [Bellare, Micciancio, Warinschi 03].

		signature size
Realization based on bilinear maps	[Boyen, Boneh, Shacham 04]	constant number of elements of a large algebraic group
Lattice-based constructions	[Gordon, Katz, Vaikuntanathan 10] [Camenisch, Neven, Rückert 10]	linear in N (number of group members)
	Our result	logarithmic in N

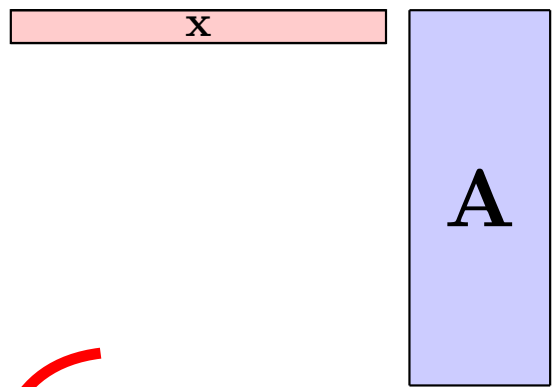
Our construction

Ingredients

- [Boyen 10]'s signature based on lattice trapdoors,
- Dual-Regev encryption [Gentry, Peikert, Vaikuntanathan 08],
- ZKPoK (proof of knowledge) adapted from [Lyubashevsky 12].

Trapdoor

- TrapGen $\rightsquigarrow (\mathbf{A}, \mathbf{T_A})$ such that $\mathbf{T_A}$ allows to find short $\mathbf{x}$('s)



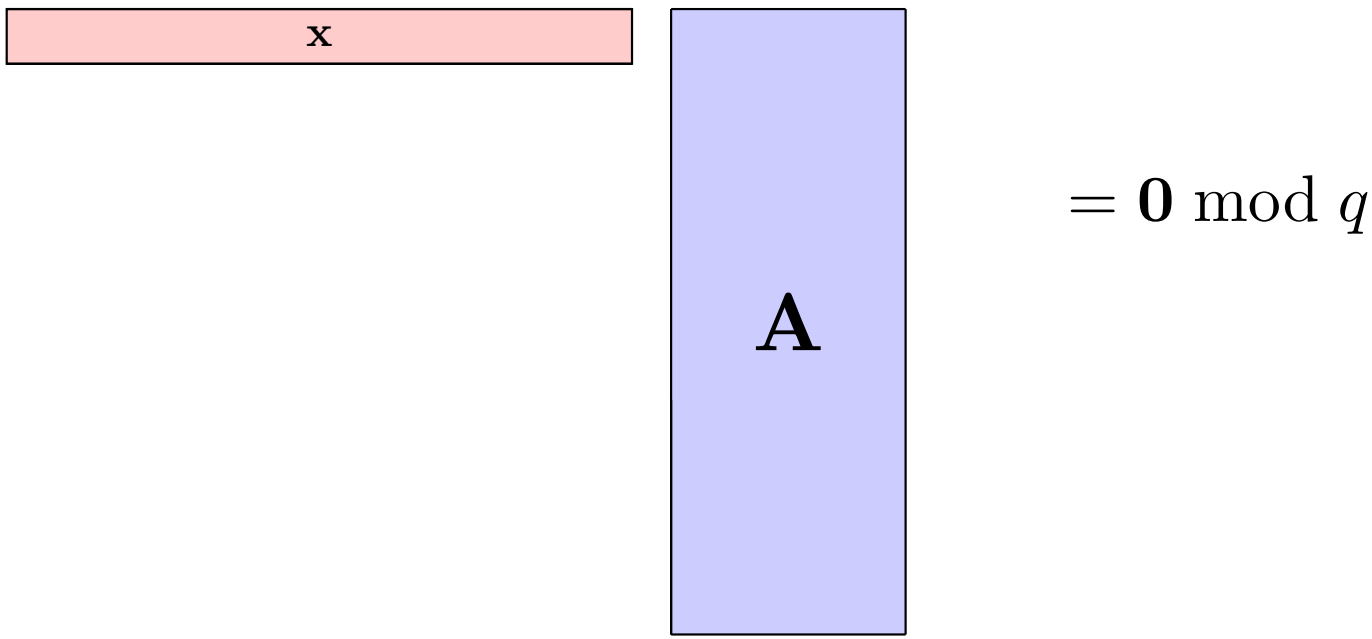
$= \mathbf{0} \bmod q$

With $\mathbf{T_A}$, we can solve SIS.

Computing $\mathbf{T_A}$ *given* $\mathbf{A}$ is hard,
Constructing $\mathbf{A}$ *and* $\mathbf{T_A}$ is easy.

Signature using trapdoors

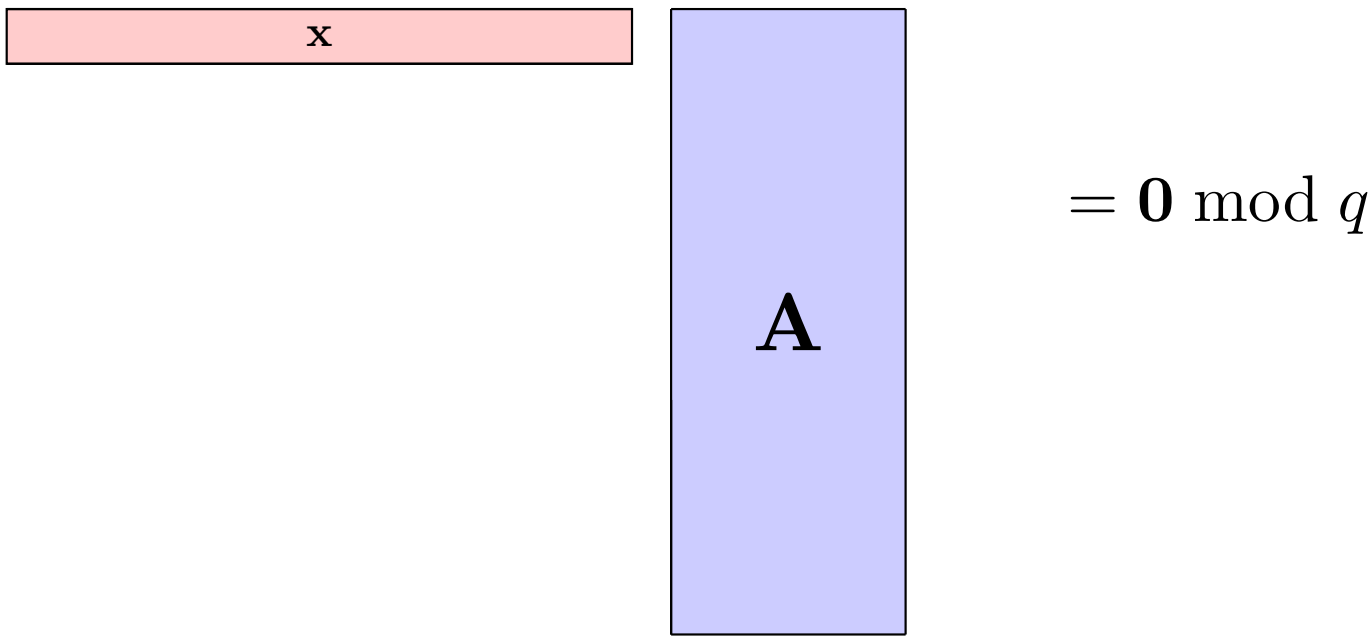
Given $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$, find $\mathbf{x}$ s.t. $0 < \|\mathbf{x}\| \leq \beta$ and



- Hard to solve given $\mathbf{A}$ $\Leftrightarrow$ solve SIS
- Easy to solve given $\mathbf{T_A}$

Signature using trapdoors

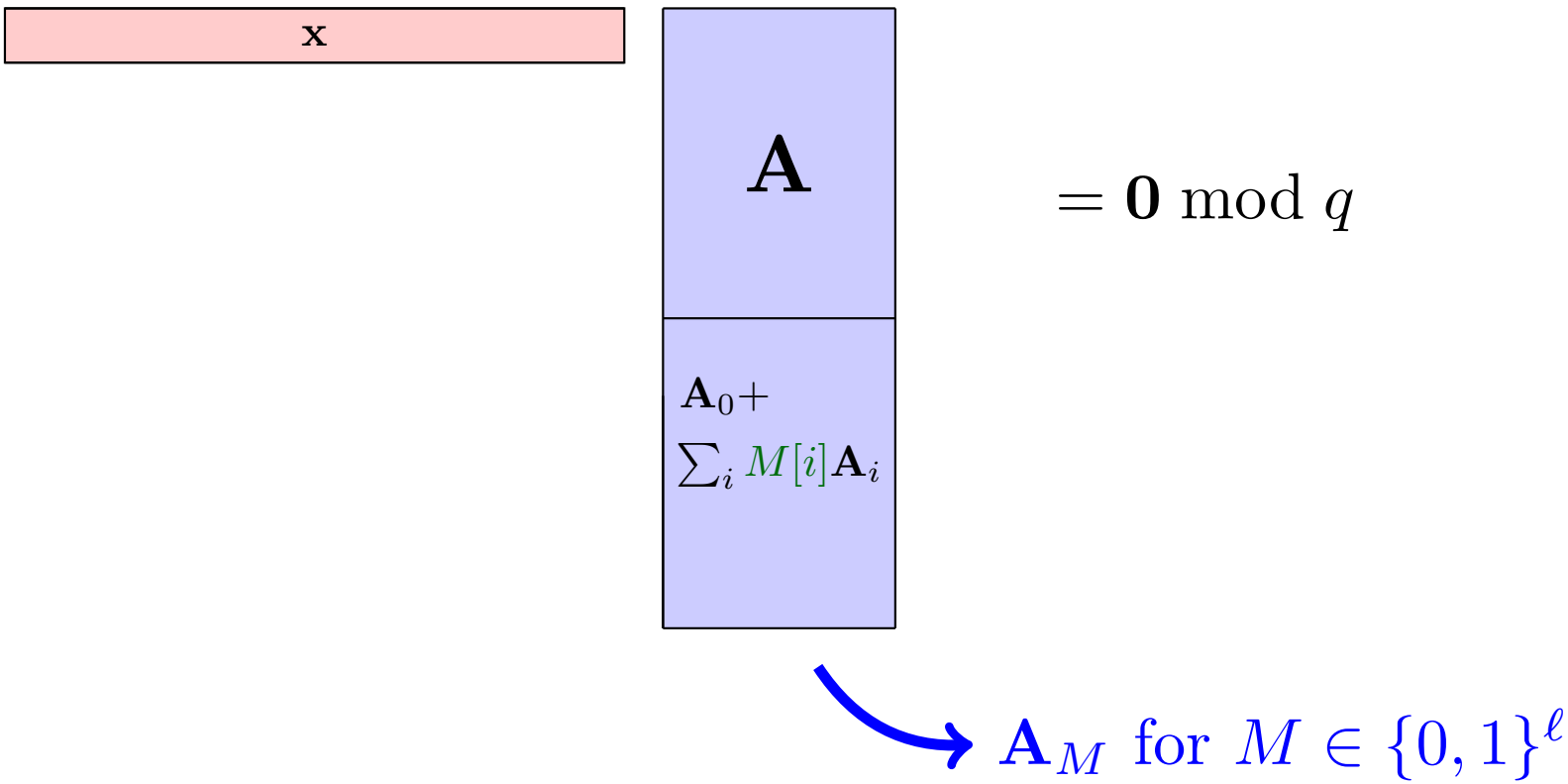
Given $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$, find $\mathbf{x}$ s.t. $0 < \|\mathbf{x}\| \leq \beta$ and



- Hard to solve given $\mathbf{A}$ $\Leftrightarrow$ solve SIS $\rightarrow$ $pk = \mathbf{A}$
- Easy to solve given $\mathbf{T_A}$ $\rightarrow$ $sk = \mathbf{T_A}$

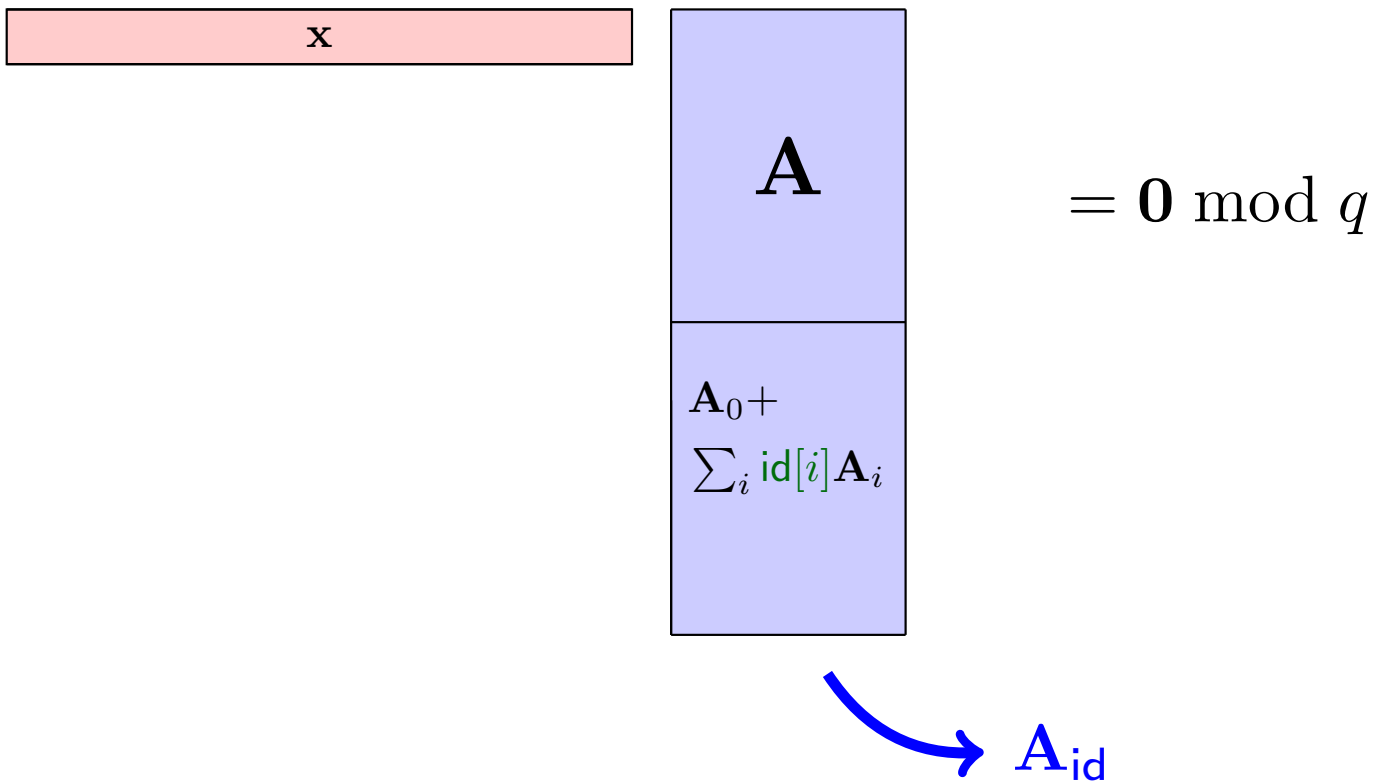
Signature using trapdoors [Boyen 10]

- $pk = (\mathbf{A}, (\mathbf{A}_i)_{0 \le i \le \ell})$
- $sk = \mathbf{T}_{\mathbf{A}}$,



Application to group signature

- $pk = \left(\mathbf{A}, (\mathbf{A}_i)_{0 \le i \le \ell}, (\mathbf{B}_i)_{0 \le i \le \ell} \right)$ s.t. $\mathbf{B}_i^T \cdot \mathbf{A}_i = 0 \bmod q$
- $msk = \{\mathbf{T}_{\mathbf{B}_i}\}_i$ trapdoors for the $\mathbf{B}_i$'s
- $sk_{\mathsf{id}} = \mathbf{T}_{\mathbf{A}_{\mathsf{id}}}$



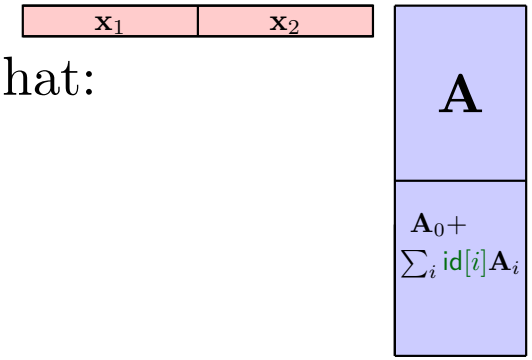
Our construction

- **Create a temporary membership certificate:** Boyen's signature of id (using $\mathbf{T}_{\mathsf{id}}$).
- **Encrypt this certificate:** $\{\mathbf{c}_i\}_{0 \leq i \leq \ell}$.
- **Prove that the ciphertext encrypts a valid certificate belonging to a group member:** π.
- **Message?**

$$\Sigma = \left(\{\mathbf{c}_i\}_{0 \leq i \leq \ell}, \pi \right)$$

Our construction

- Produce $(\mathbf{x}_1||\mathbf{x}_2)^T$ **short** such that:



$= \mathbf{0} \bmod q$

- **Encrypt this certificate:** $\{\mathbf{c}_i\}_{0 \leq i \leq \ell}$.

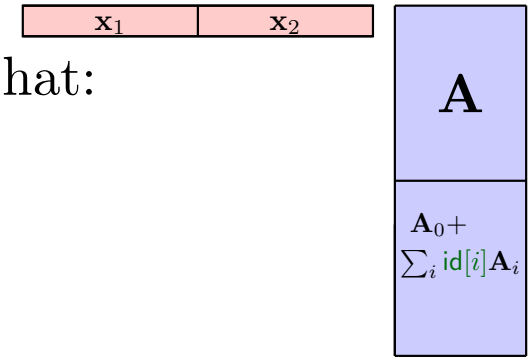
- **Prove that the ciphertext encrypts a valid certificate belonging to a group member:** π.

- **Message?**

$$\Sigma = \left(\{\mathbf{c}_i\}_{0 \leq i \leq \ell}, \pi\right)$$

Our construction

- Produce $(\mathbf{x}_1||\mathbf{x}_2)^T$ **short** such that:



$= \mathbf{0} \bmod q$

- Encrypt $\begin{cases} \mathbf{x}_2 \\ \mathsf{id}_i \cdot \mathbf{x}_2 \end{cases}$ in $\mathbf{c}_i$'s using LWE-based encryption with $\mathbf{B}_i$'s

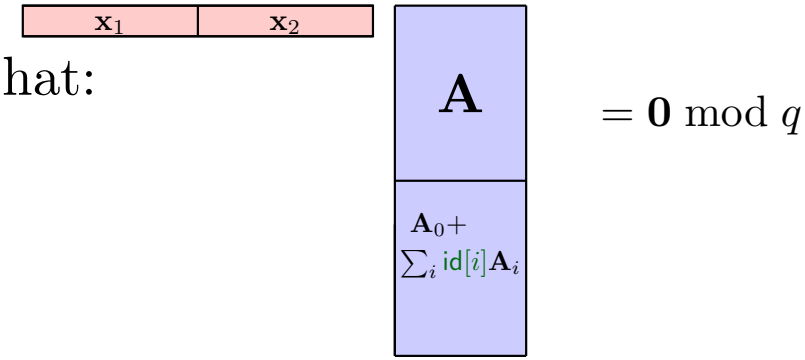
- **Prove that the ciphertext encrypts a valid certificate belonging to a group member: π.**

- **Message?**

$$\Sigma = \left(\{\mathbf{c}_i\}_{0 \leq i \leq \ell}, \pi\right)$$

Our construction

- Produce $(\mathbf{x}_1||\mathbf{x}_2)^T$ **short** such that:



$= \mathbf{0} \bmod q$

- Encrypt $\begin{cases} \mathbf{x}_2 \\ \mathsf{id}_i \cdot \mathbf{x}_2 \end{cases}$ in $\mathbf{c}_i$'s using LWE-based encryption with $\mathbf{B}_i$'s

- Prove that the ciphertext encrypts a valid certificate belonging to a group member: π.

- ZKPoK $\rightsquigarrow$ made non-interactive ZKPoK *via* Fiat-Shamir, (incorporating **the message** in π).

$$\Sigma = \left(\{\mathbf{c}_i\}_{0 \leq i \leq \ell}, \pi\right)$$

Our construction

Verify:

- Check the proofs.

Open:

- Decrypt $\mathbf{c}_0$ ($\rightsquigarrow \mathbf{x_2}$)
  and check whether $p^{-1}\mathbf{c}_i$ or $p^{-1}(\mathbf{c}_i - \mathbf{x}_2)$ is close to the $\mathbb{Z}_q$-span of $\mathbf{B}_i$.

Our construction

Verify:

- Check the proofs.

Open:

- Decrypt $\mathbf{c}_0$ ($\rightsquigarrow \mathbf{x_2}$)
  and check whether $p^{-1}\mathbf{c}_i$ or $p^{-1}(\mathbf{c}_i - \mathbf{x}_2)$ is close to the $\mathbb{Z}_q$-span of $\mathbf{B}_i$.

- Size of the signatures: $\tilde{\mathcal{O}}(\lambda \cdot \log(N))$.
- Size of the key of member i: $\tilde{\mathcal{O}}(\lambda^2)$.
- $\lambda = \Theta(n)$ is the security parameter.

Anonymity and Traceability

In the random oracle model

Anonymity

Weak anonymity under LWE.

Traceability

Traceability under SIS.

- We also provide a variant with full-anonymity.

Open problems

- Making it practical,
- Improving the sizes of the signature and public key,
- Removing the Random Oracle Model.

Outline

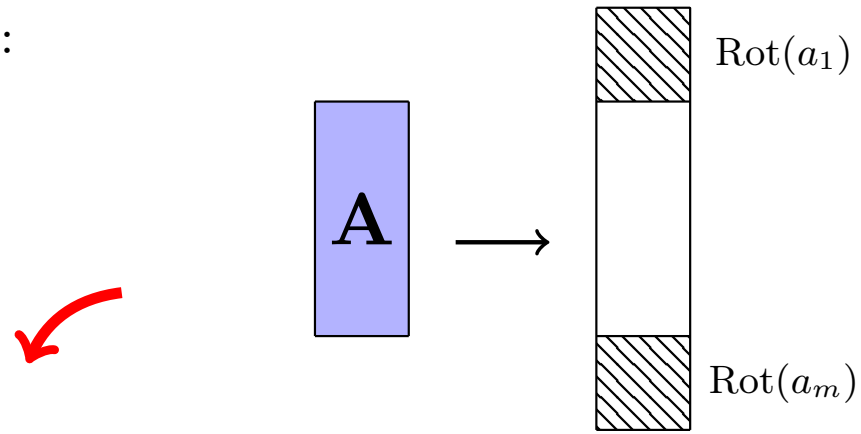
Main contributions

- Classical hardness of LWE,
- Hardness of LWE_q^n is a function of $n \log q$,
- First lattice-based group signature with logarithmic signature size (and a second scheme with verifier local revocation).

- **A. Langlois**, D. Stehlé, R. Steinfeld. GGHLite: More Efficient Multilinear Maps from Ideal Lattices. In proc. of Eurocrypt 2014.

Practical lattice-based cryptography

- Practical?
  - Ring variants since 2006:



  - Structured $\mathbf{A} \in \mathbb{Z}_q^{m \cdot n \times n}$ represented by $m \cdot n$ elements,
  - Product with a vector more efficient,
  - Hardness of Ring-SIS, [Lyubashevsky and Micciancio 06] and [Peikert and Rosen 06]
  - Hardness of Ring-LWE [Lyubashevsky, Peikert and Regev 11].

Open problems

- Security foundations
  - Hardness of LWE without quadratic loss,
  - Classical hardness of Ring-LWE.
- Constructions
  - Practical group signature scheme,
  - Removing the Random Oracle Model.
  - Practical and secure cryptographic multilinear maps.

Open problems

- Security foundations
  - Hardness of LWE without quadratic loss,
  - Classical hardness of Ring-LWE.
- Constructions
  - Practical group signature scheme,
  - Removing the Random Oracle Model.
  - Practical and secure cryptographic multilinear maps.

Thank You