Lattice-Based Group Signatures with Logarithmic Signature Size

Fabien Laguillaumie[1] **Adeline Langlois**[2] Benoît Libert[3]
Damien Stehlé[2]

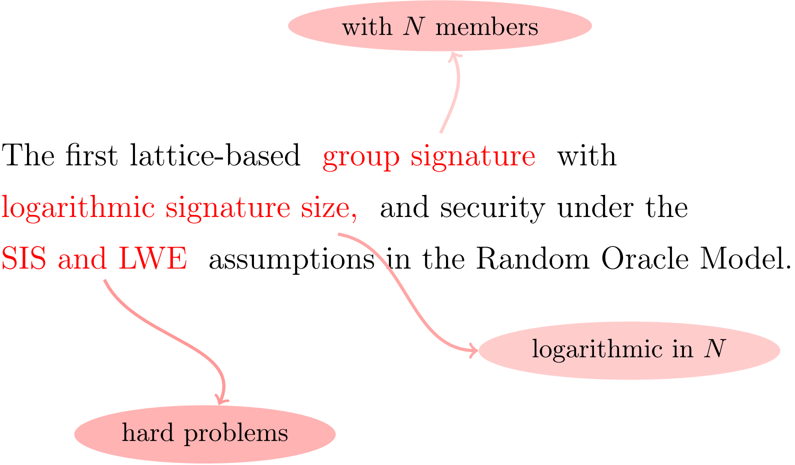
[1]LIP, Université Lyon 1

[2]LIP, ENS de Lyon

[3]Technicolor

December 4, 2013

Our main result



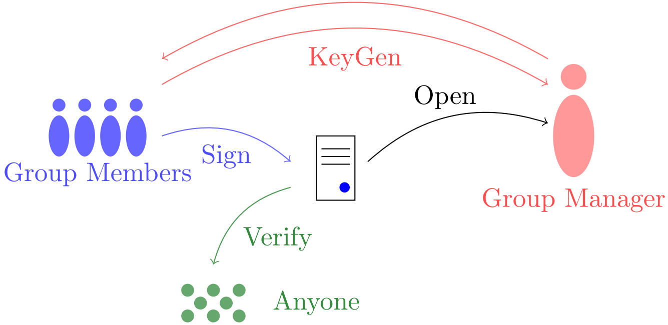
The first lattice-based group signature with logarithmic signature size, and security under the SIS and LWE assumptions in the Random Oracle Model.

Group Signatures

[ChaumVanHeyst91]

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.

  ⇝ 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 doesn't trace to someone not in the collusion (or nobody).

Applications

Need for authenticity *and* anonymity

- Anonymous credentials: anonymous use of certified attributes
  - E.g.: student card - name, picture, date, grade...
- Traffic management (Vehicle Safety Communications project of the U.S. Dept. of Transportation).
- Restrictive area access.

Prior works

- Introduced by [ChaumVanHest91],
- Generic construction [BellareMicciancioWarinschi03].

		signature size
Realization based on bilinear maps	[BoyenWaters07] and [Groth07]	constant number of elements of a large algebraic group
Lattice-based constructions	[GordonKatzVaikuntanathan10] [CamenischNevenRückert10]	linear in N (number of group members)
	Our result	logarithmic in N

Lattice-Based Cryptography

From basic to very advanced primitives

- Public key encryption [Regev05, ...],
- Lyubashevsky signature scheme [Lyubashevsky12],
- Identity-based encryption [GentryPeikertVaikuntanathan08, ...],
- Attribute-based encryption [Boyen13, GorbunovVaikuntanathanWee13],
- Fully homomorphic encryption [Gentry09, ...].

Advantages of lattice-based primitives

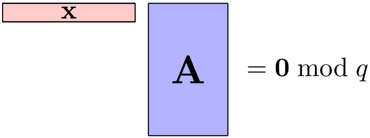
- (Asymptotically) efficient,
- Security proofs **from the hardness of LWE and SIS**,
- Likely to resist quantum attacks.

SIS_β and LWE_α

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

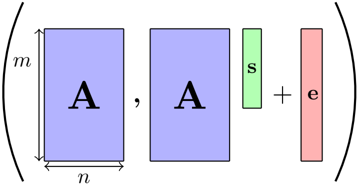
For $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m\times n})$:

Small Integer Solution



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

Learning With Errors



$\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$,

e a small error $\approx \alpha q$.

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

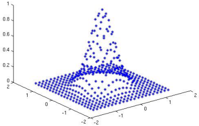
Lattice-Based Cryptography Toolbox: Trapdoors

- TrapGen $\rightsquigarrow (\mathbf{A}, \mathbf{T_A})$ such that $\mathbf{T_A}$ is a short basis of the lattice

$$\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{x}^T \cdot \mathbf{A} = \mathbf{0} \pmod{q}\}.$$

$$\begin{cases} \mathbf{A} \text{ public description of the lattice} \\ \mathbf{T_A} \text{ short basis, kept secret} \end{cases}$$

- Note that:
  1. Computing $\mathbf{T_A}$ *given* $\mathbf{A}$ is hard,
  2. Constructing $\mathbf{A}$ *together with* $\mathbf{T_A}$ is easy.



- With $\mathbf{T_A}$, we can sample short vectors in $\Lambda_q^\perp(\mathbf{A})$.
- Can add constraints:
  find $\mathbf{B}$ such that $\mathbf{B}^T \cdot \mathbf{A} = \mathbf{0}$ (with trapdoor for $\mathbf{A}$ and $\mathbf{B}$).

Group Signatures

A generic construction [BellareMicciancioWarinschi03]

Ingredients:

- Signature & Encryption schemes.
- Non-Interactive Zero Knowledge proof system.

Scheme:

- **Public key**: pk of Enc (pk_e) and Sign (pk_s).
- **Opening key**: secret key of Enc sk_e.
- **User sk**: signing key sk_i and $\mathrm{Sign}_{\mathrm{sk}_s}(i)$ from group manager.
- To sign a message m by a member i:
  1. $c = \mathrm{Enc}_{\mathsf{pk}_e}(i, \mathrm{Sign}_{\mathrm{sk}_s}(i), \mathrm{Sign}_{\mathsf{s}k_i}(m))$,
  2. π : ZKPoK of valid plaintext.
  3. Output $\Sigma = (c, \Pi)$.

Construction not efficient (Generic ZKPoK).
First attempt with lattices [GKV10]: size of signature $= O(N)$.

Our construction

Ingredients

- Certificate of users $\rightsquigarrow$ key to produce temporary certificate,
- [Boyen2010]'s signature (standard model),
- [GenPeiVai2008] variant of Dual-Regev encryption,
- ZKPoK adapted from Lyubashevsky's signature.

KeyGen

- $N = 2^{\ell}$ group members,
- ℓ public matrices $\mathbf{A}$, $\mathbf{A}_i$'s and $\mathbf{B}_i$'s such that $\mathbf{B}_i^T \cdot \mathbf{A}_i = 0 \bmod q$.
- Each user is given a *short* basis $\mathbf{T}_{\mathsf{id}}$ of a public lattice associated to its identity (using $\mathbf{T}_{\mathbf{A}}$):

$$\mathbf{A}_{\mathsf{id}} = \left(\frac{\mathbf{A}}{\mathbf{A}_0 + \sum_{i=1}^{\ell} \mathsf{id}[i]\mathbf{A}_i} \right).$$

- Group manager secret key is $\{\mathbf{T}_{\mathbf{B}_i}\}_i$.

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:** $\pi_0, \{\pi_{\mathrm{OR},i}\}_{1\leq i\leq \ell}, \pi_K$.

- **Message?**

$$\Sigma = \left(\{\mathbf{c}_i\}_{0\leq i\leq \ell}, \pi_0, \{\pi_{\mathrm{OR},i}\}_{1\leq i\leq \ell}, \pi_K\right)$$

Our construction

- Produce $(\mathbf{x}_1||\mathbf{x}_2)^T$ **short** such that:
$$\mathbf{x}_1{}^T \cdot \mathbf{A} + \mathbf{x}_2{}^T \cdot (\mathbf{A}_0 + \sum_{i=1}^{\ell} \mathsf{id}[i] \cdot \mathbf{A}_i) = 0 \pmod{q}$$

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

- **Prove that the ciphertext encrypts a valid certificate belonging to a group member:** $\pi_0, \{\pi_{\mathrm{OR},i}\}_{1 \le i \le \ell}, \pi_K$.

- **Message?**

$$\Sigma = \left(\{\mathbf{c}_i\}_{0 \le i \le \ell}, \pi_0, \{\pi_{\mathrm{OR},i}\}_{1 \le i \le \ell}, \pi_K \right)$$

Our construction

- Produce $(\mathbf{x}_1 || \mathbf{x}_2)^T$ **short** such that:
$$\mathbf{x}_1{}^T \cdot \mathbf{A} + \mathbf{x}_2{}^T \cdot (\mathbf{A}_0 + \sum_{i=1}^{\ell} \mathsf{id}[i] \cdot \mathbf{A}_i) = 0 \pmod q$$

- Encrypt $\mathbf{x}_2$ as $\mathbf{c}_0 = \mathbf{B}_0 \cdot \mathbf{s}_0 + \mathbf{x}_2$ $\qquad \mathbf{s}_0 \hookleftarrow U(\mathbb{Z}_q^n)$
- For all $i = 1, \ldots, \ell$ encrypt $\mathsf{id}_i \cdot \mathbf{x}_2$ as
$$\mathbf{c}_i = \mathbf{B}_i \cdot \mathbf{s} + p \cdot \mathbf{e}_i + \mathsf{id}_i \cdot \mathbf{x}_2 \qquad \mathrm{poly}(n) \ll p \ll q$$

- **Prove that the ciphertext encrypts a valid certificate belonging to a group member:** $\pi_0, \{\pi_{\mathrm{OR},i}\}_{1 \le i \le \ell}, \pi_K$.

- **Message?**

$$\Sigma = \left(\{\mathbf{c}_i\}_{0 \le i \le \ell}, \pi_0, \{\pi_{\mathrm{OR},i}\}_{1 \le i \le \ell}, \pi_K \right)$$

Our construction

- Produce $(\mathbf{x}_1||\mathbf{x}_2)^T$ **short** such that:
$$\mathbf{x}_1{}^T \cdot \mathbf{A} + \mathbf{x}_2{}^T \cdot (\mathbf{A}_0 + \sum_{i=1}^{\ell} \mathsf{id}[i] \cdot \mathbf{A}_i) = 0 \pmod q$$

- Encrypt $\mathbf{x}_2$ as $\mathbf{c}_0 = \mathbf{B}_0 \cdot \mathbf{s}_0 + \mathbf{x}_2$ $\qquad \mathbf{s}_0 \hookleftarrow U(\mathbb{Z}_q^n)$
- For all $i = 1, \ldots, \ell$ encrypt $\mathsf{id}_i \cdot \mathbf{x}_2$ as
$$\mathbf{c}_i = \mathbf{B}_i \cdot \mathbf{s} + p \cdot \mathbf{e}_i + \mathsf{id}_i \cdot \mathbf{x}_2 \qquad \text{poly}(n) \ll p \ll q$$

- **Generate a proof** π_0: $\mathbf{c}_0$ close to a point in the $\mathbb{Z}_q$-span of $\mathbf{B}_0$.

  We have that $\begin{cases} \mathbf{c}_i \text{ and } \mathbf{c}_0 \text{ encrypt the same } \mathbf{x}_2 & (\mathsf{id}_i = 1) \\ \text{or } \mathbf{c}_i \text{ encrypts } \mathbf{0} & (\mathsf{id}_i = 0) \end{cases}$

  Generate a proof $\pi_{\mathrm{OR},i}$ of these relations (disjunctions).

  Generate a proof π_K of knowledge of the $\mathbf{e}_i$'s and $\mathsf{id}_i \cdot \mathbf{x}_2$'s with their corresponding relation.

- **Message?**

$$\Sigma = \left(\{\mathbf{c}_i\}_{0 \leq i \leq \ell}, \pi_0, \{\pi_{\mathrm{OR},i}\}_{1 \leq i \leq \ell}, \pi_K \right)$$

Our construction

- Produce $(\mathbf{x}_1||\mathbf{x}_2)^T$ **short** such that:
$$\mathbf{x}_1{}^T \cdot \mathbf{A} + \mathbf{x}_2{}^T \cdot (\mathbf{A}_0 + \sum_{i=1}^{\ell} \mathsf{id}[i] \cdot \mathbf{A}_i) = 0 \pmod q$$

- Encrypt $\mathbf{x}_2$ as $\mathbf{c}_0 = \mathbf{B}_0 \cdot \mathbf{s}_0 + \mathbf{x}_2$ $\qquad \mathbf{s}_0 \hookleftarrow U(\mathbb{Z}_q^n)$
- For all $i = 1, \ldots, \ell$ encrypt $\mathsf{id}_i \cdot \mathbf{x}_2$ as
$$\mathbf{c}_i = \mathbf{B}_i \cdot \mathbf{s} + p \cdot \mathbf{e}_i + \mathsf{id}_i \cdot \mathbf{x}_2 \qquad \mathrm{poly}(n) \ll p \ll q$$

- **Generate a proof** π_0: $\mathbf{c}_0$ close to a point in the $\mathbb{Z}_q$-span of $\mathbf{B}_0$.

  We have that $\begin{cases} \mathbf{c}_i \text{ and } \mathbf{c}_0 \text{ encrypt the same } \mathbf{x}_2 & (\mathsf{id}_i = 1) \\ \text{or } \mathbf{c}_i \text{ encrypts } \mathbf{0} & (\mathsf{id}_i = 0) \end{cases}$

  Generate a proof $\pi_{\mathrm{OR},i}$ of these relations (disjunctions).

  Generate a proof π_K of knowledge of the $\mathbf{e}_i$'s and $\mathsf{id}_i \cdot \mathbf{x}_2$'s with their corresponding relation.

- ZKPoK ⇝ made non-interactive ZKPoK *via* Fiat-Shamir, (incorporating **the message** in π_K).

$$\Sigma = \left(\{\mathbf{c}_i\}_{0 \le i \le \ell}, \pi_0, \{\pi_{\mathrm{OR},i}\}_{1 \le i \le \ell}, \pi_K \right)$$

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, and the simulation of the ZKPoK.

Traceability

Traceability under SIS, and extraction of information in the ZKPoK.

- We also provide a variant with full-anonymity,
  ⇒ the adversary has an opening oracle.
  - Find a way to open adversarially chosen signatures,
    ⇒ using IND-CCA encryption.

Conclusion

Our result

- We give the first lattice-based signature with logarithmic signature and public key sizes.
- Weak and full anonymity (LWE), traceability (SIS).

Open problems

- Practice,
- Ring variants of LWE and SIS,
- Improving the sizes of the signature and public key,
- Removing the random oracle model.