Lattice-based cryptography: security foundations and constructions

Adeline Langlois

EPFL, Lausanne, Switzerland
Cryptography

New challenges in cryptography

- Need of new functionalities,
- Quantum computers.

Lattice-based cryptography

- Is it a credible alternative to modern cryptography?
  - Functionality
  - Security
  - Efficiency

- Study of the new functionalities:
  - Fully homomorphic encryption,
  - Cryptographic multilinear maps.
Learning With Errors

\[ A \leftarrow \text{Uniform in } \mathbb{Z}_m \times \mathbb{Z}_n \]
\[ s \leftarrow \text{Uniform in } \mathbb{Z}_n \]
e is a small error

\[ m \geq n \]

Given \( A \), find \( s \)

Lattice

\[ b_1 \quad b_2 \]

Cryptographic constructions

Adeline Langlois Journées du GDR IM 3/8
Learning With Errors

\[ \begin{align*}
A & \leftarrow \text{Uniform in } \mathbb{Z}^{m \times nq} \\
s & \leftarrow \text{Uniform in } \mathbb{Z}^{nq} \\
e & \text{is a small error}
\end{align*} \]

\[ m \geq n \]

Given \( A \), find \( s \) is the shortest vector problem (SVP) in \( \mathbb{Z}^m \):

\[ \text{Shortest Vector Problem} \]
Learning With Errors

dimension $n$, modulo $q$

Given $A \leftarrow \text{Uniform in } \mathbb{Z}_{q}^{m\times n}$, $s \leftarrow \text{Uniform in } \mathbb{Z}_{q}^{n}$, $e$ is a small error

A → solve hard problems on lattice

Security Foundations

Constructions

Cryptographic constructions
Lattice-based cryptography

Advantages

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

From basic to very advanced primitives

- Public key encryption and signature scheme (practical) ...
- New functionalities
  - Fully homomorphic encryption,
  - Cryptographic multilinear maps and applications.
My results

Classical hardness of LWE

Learning With Errors

dimension $n$, modulo $q$

Given:

\[
\begin{pmatrix}
A, & A' \\
\end{pmatrix} + e
\]

and/or

SIS

$m \geq n$

find

$s$

→ solve hard problem on lattice

Lattice

Improving cryptographic multilinear maps

Construction of group signatures

Cryptographic constructions

Adeline Langlois

Journées du GDR IM
My results

Classical hardness of LWE

Learning With Errors

\[ \begin{pmatrix} A \end{pmatrix} \left[ \begin{array}{c} s \end{array} \right] + e \]

Given \( A \) Uniform in \( \mathbb{Z}_q^{m \times n} \)

\( s \) Uniform in \( \mathbb{Z}_q^n \)

\( e \) is a small error

find \( s \) when \( m \geq n \)

Lattice

\[ \rightarrow \text{solve hard problem on lattice} \]

? Improving cryptographic multilinear maps

Construction of group signatures

Cryptographic constructions

Adeline Langlois Journées du GDR IM
Diffie-Hellman Key Exchange (1976)

\[ \mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z} \text{ with } q \text{ prime, } g \text{ public generator of } \mathbb{Z}_q^*. \]

Choose

\[ x_1 \leftarrow U(\mathbb{Z}_q) \]

\[ y_1 = g^{x_1} \]

Alice

Bob

\[ x_2 \leftarrow U(\mathbb{Z}_q) \]

\[ y_2 = g^{x_2} \]

Agreed secret key: \[ K = g^{x_1x_2} = y_1^{x_2} = y_2^{x_1} \]

- **Security:** Decisional Diffie-Hellman problem.
Cryptographic Multilinear Maps – 21st Century variant

Group of $N > 2$ parties want to communicate privately via cloud.

Choose $x_1 \in \mathbb{Z}_q$

$y_1 = g^{x_1}$

Choose $x_2 \in \mathbb{Z}_q$

$y_2 = g^{x_2}$

Choose $x_3 \in \mathbb{Z}_q$

$y_3 = g^{x_3}$

Choose $x_N \in \mathbb{Z}_q$

$y_N = g^{x_N}$

Secret key (using $e$: "cryptographic multilinear map"):

$K = e(g, \ldots, g)^{x_1 \cdots x_N} = e(y_2, y_3, \ldots, y_N)^{x_1}$

$= e(y_1, y_3, \ldots, y_N)^{x_2}$
Cryptographic Multilinear Maps

- **2013**: [Garg, Gentry, Halevi 13]
  - First plausible realization for $N > 3$, via ideal lattices,

- **2014**: GGHLite – More efficient variant of GGH,
  - [Langlois, Stehlé, Steinfeld 14]

- Improving and implementing GGHLite – *work in progress.*
  - [Albrecht, Cocis, Laguillaumie, Langlois]

| $N$  | $n$   | log $q$ | Setup  | Publish | KeyGen  | |\[\text{params}]|
|------|-------|---------|--------|---------|---------|---------|
| 7    | 65536 | 3605    | 2457s  | 12.58s  | 6.03s   | 112.7MB |
| 26   | 262144| 15410   | 29407s | 465.36s | 530.27s | 1.4GB   |

- **Open problems**
  - Construction with a security proof?
  - Efficient for large $N$?
Cryptographic Multilinear Maps

- 2013: [Garg, Gentry, Halevi 13]
  - First plausible realization for $N > 3$, via ideal lattices,

- 2014: GGHLite – More efficient variant of GGH,
  [Langlois, Stehlé, Steinfeld 14]

- Improving and implementing GGHLite – work in progress.
  [Albrecht, Cocis, Laguillaumie, Langlois]

| $N$  | $n$   | log $q$ | Setup  | Publish | KeyGen  | |params|
|------|-------|---------|--------|---------|---------|-------|
| 7    | 65536 | 3605    | 2457s  | 12.58s  | 6.03s   | 112.7MB |
| 26   | 262144| 15410   | 29407s | 465.36s | 530.27s | 1.4GB   |

- Open problems
  - Construction with a security proof?
    - Efficient for large $N$?

Thank You