Classical hardness of Learning with Errors

Adeline Langlois

Aric Team, LIP, ENS Lyon

Joint work with
Z. Brakerski, C. Peikert, O. Regev and D. Stehlé

Our main results

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.

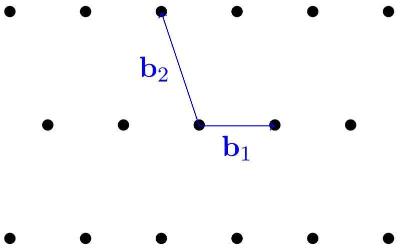
Dimension n

Polynomial in n

Outline

1. Lattices: definitions and problems
2. Lattice-based cryptography:
   LWE and a public-key encryption
3. Our main result:
   classical hardness of LWE for polynomial modulus

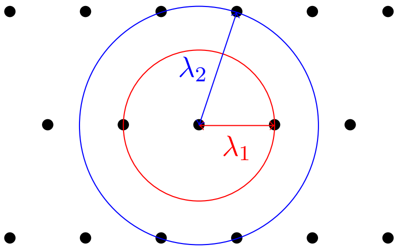
Lattices and problems



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 $\mathcal{L}(\mathbf{B})$.

Lattices and problems



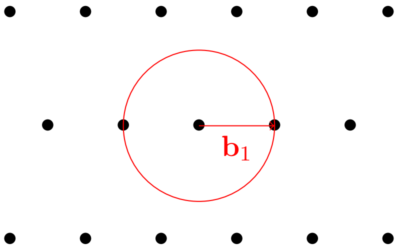
Definitions:

- 1st minimum;
- 2nd minimum.

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 $\mathcal{L}(\mathbf{B})$.

Lattices and problems



Definitions:

- 1st minimum;
- 2nd minimum.

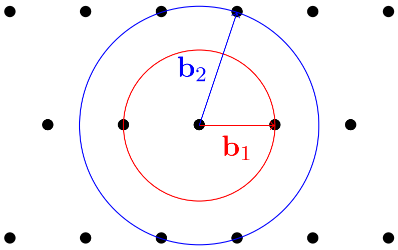
Problems :

- Shortest Vector Pbm. (computational or decisional version)

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 $\mathcal{L}(\mathbf{B})$.

Lattices and problems



Definitions:

- 1st minimum;
- 2nd minimum.

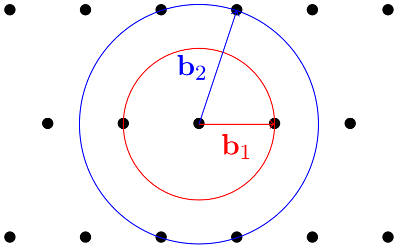
Problems :

- Shortest Vector Pbm. (computational or decisional version)
- Shortest Independent Vectors Pbm.

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 $\mathcal{L}(\mathbf{B})$.

Lattices and problems



Definitions:

- 1st minimum;
- 2nd minimum.

Problems :

- Shortest Vector Pbm. (computational or decisional version)
- Shortest Independent Vectors Pbm.
- Approximation factor: γ.

Conjecture

There is no polynomial time algorithm that approximates these lattice problems to within polynomial factors.

LWE-based cryptography

From basic to very advanced primitives

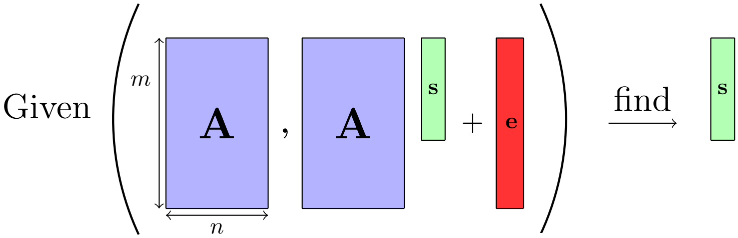
- Public key encryption
  [Regev 2005, ...];
- Identity-based encryption
  [Gentry, Peikert and Vaikuntanathan 2008, ...];
- Attribute-based encryption
  [Boyen 2013; Gorbunov, Vaikuntanathan and Wee 2013];
- Fully homomorphic encryption
  [Brakerski and Vaikuntanathan 2011, ...].

Advantages of LWE-based primitives

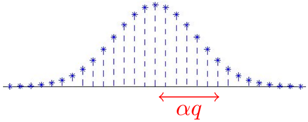
- Efficient, especially when the **modulus is polynomial**;
- Security proofs **from the hardness of LWE**;
- Likely to resist attacks from quantum computers.

The Learning With Errors problem [Regev05]

LWE_q^n (with m arbitrarily large)



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



Discrete Gaussian error

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

LWE: solve a linear system with noise

Find $(s_1, s_2, s_3, s_4, s_5)$ such that:

$$\begin{aligned}
s_1 + 22s_2 + 17s_3 + 2s_4 + s_5 &\approx 16 \mod 23 \\
3s_1 + 2s_2 + 11s_3 + 7s_4 + 8s_5 &\approx 17 \mod 23 \\
15s_1 + 13s_2 + 10s_3 + s_4 + 22s_5 &\approx 3 \mod 23 \\
17s_1 + 11s_2 + s_3 + 10s_4 + 3s_5 &\approx 8 \mod 23 \\
2s_1 + s_2 + 13s_3 + 6s_4 + 2s_5 &\approx 9 \mod 23 \\
4s_1 + 4s_2 + s_3 + 5s_4 + s_5 &\approx 18 \mod 23 \\
11s_1 + 12s_2 + 5s_3 + s_4 + 9s_5 &\approx 7 \mod 23
\end{aligned}$$

$\rightsquigarrow$ Arbitrary number of equations.

Other interpretation: decoding a uniform linear code for the Euclidean distance.

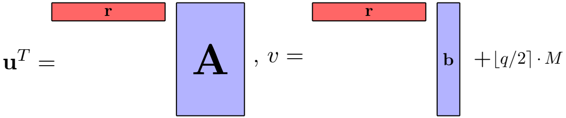
An example of Public-Key Encryption[Regev 2005]

- **Parameters**: $n, m, q \in \mathbb{Z}$, $\alpha \in \mathbb{R}$,
- **Keys**: $\mathrm{sk} = \mathbf{s}$ and $\mathrm{pk} = (\mathbf{A}, \mathbf{b})$, with $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ where $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$, $\mathbf{e} \hookleftarrow D_{\mathbb{Z}^m, \alpha q}$.
- **Encryption** $(M \in \{0,1\})$**:** Let $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

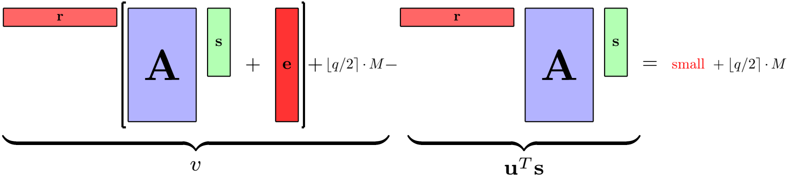
$$\mathbf{u}^T = \mathbf{r} \, \mathbf{A}, \quad v = \mathbf{r} \, \mathbf{b} + \lfloor q/2 \rceil \cdot M$$

An example of Public-Key Encryption [Regev 2005]

- **Parameters**: $n, m, q \in \mathbb{Z}$, $\alpha \in \mathbb{R}$,
- **Keys**: sk $=$ $\mathbf{s}$ and pk $= (\mathbf{A}, \mathbf{b})$, with $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ where $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$, $\mathbf{e} \hookleftarrow D_{\mathbb{Z}^m, \alpha q}$.
- **Encryption** $(M \in \{0, 1\})$**:** Let $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,



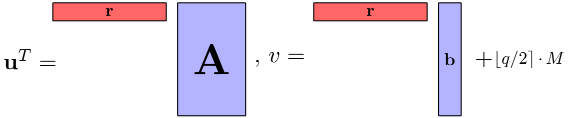
- **Decryption** of $(\mathbf{u}, v)$: compute $v - \mathbf{u}^T\mathbf{s}$,



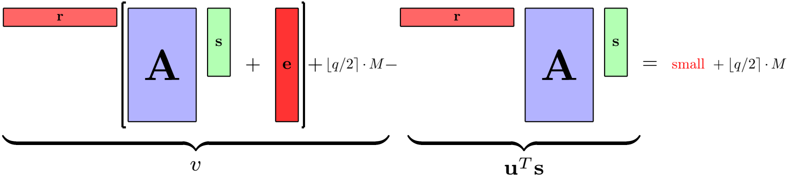
If close from 0: return 0, if close from $\lfloor q/2 \rceil$: return 1.

An example of Public-Key Encryption [Regev 2005]

- **Parameters**: $n, m, q \in \mathbb{Z}$, $\alpha \in \mathbb{R}$,
- **Keys**: sk $=$ $\mathbf{s}$ and pk $= (\mathbf{A}, \mathbf{b})$, with $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$ where $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$, $\mathbf{e} \hookleftarrow D_{\mathbb{Z}^m, \alpha q}$.
- **Encryption** $(M \in \{0,1\})$: Let $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,



- **Decryption** of $(\mathbf{u}, v)$: compute $v - \mathbf{u}^T\mathbf{s}$,



LWE hard $\Rightarrow$ Regev's scheme is "secure".

Prior reductions from worst-case lattice problem to LWE

- **[Regev05]**
  - A **quantum** reduction;
  - with q polynomial.

Quantum computer?

- **[Peikert09]**
  - A **classical** reduction;
  - with q exponential,

Inefficient primitives

- **[Peikert09]**
  - A **classical** reduction;
  - based on a non-standard lattice problem;
  - with q polynomial.

Hardness?

Prior reductions from worst-case lattice problem to LWE

- **[Regev05]**
  - A **quantum** reduction;
  - with q polynomial.
- **[Peikert09]**
  - A **classical** reduction;
  - with q exponential,
- **[Peikert09]**
  - A **classical** reduction;
  - based on a non-standard lattice problem;
  - with q polynomial.

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

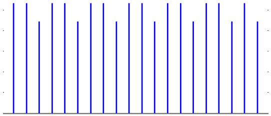
- Transform $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$ to $\mathbf{A}' \hookleftarrow U(\mathbb{Z}_p^{m \times n})$;
  First idea: $\mathbf{A}' = \lfloor \frac{p}{q} \mathbf{A} \rceil$?

Modulus Switching

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

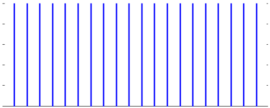
How to map $(\mathbf{A}, \mathbf{As} + \mathbf{e}) \bmod q$ to $(\mathbf{A}', \mathbf{A}'\mathbf{s} + \mathbf{e}') \bmod p$?

- 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 problems:
  1. The distribution is not uniform:



A naive rounding introduces artefacts.

solution



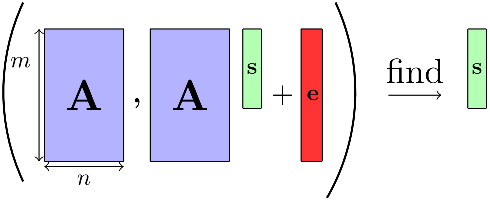
Add a **Gaussian rounding** to smooth the distribution: $\mathbf{A}' = \frac{p}{q}\mathbf{A} + \mathbf{R}$.

  2. In $\mathbf{A}'\mathbf{s} + \mathbf{e}'$, the rounding errors gets multiplied by the secret $\mathbf{s}$ (which is 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 2010]**) ; but different and stronger techniques.
- Definition of LWE:



- From $\mathbf{s}$ uniform in $\mathbb{Z}_q^n$ to $\mathbf{s}$ uniform in $\{0,1\}^n$.
- **Consequence:** this reduction 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	$\sqrt{n}$			
$\downarrow_0$				**[Peikert09]**
LWE	$\sqrt{n}$	large	$\mathbb{Z}_q^{\sqrt{n}}$	
$\downarrow_1$				**New**
LWE	n	large	small	
$\downarrow_2$				**New**
LWE	n	poly(n)	in $\mathbb{Z}_q^n$	

Conclusion

Our main result

A classical reduction from GapSVP in dimension $\sqrt{n}$ to LWE in dimension n with $\mathrm{poly}(n)$ 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 **[Regev05]**?

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