Classical hardness of the Learning with Errors problem

Adeline Langlois

Aric Team, LIP, ENS Lyon

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

August 12, 2013

Our 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.

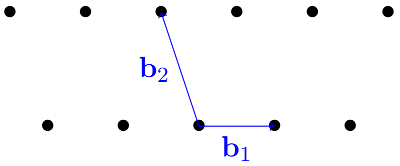
Dimension n

Polynomial in n

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
4. Other results on LWE.

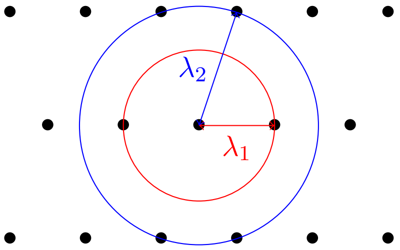
Lattices and problems



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



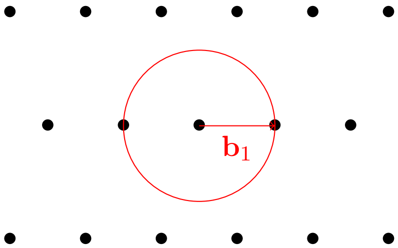
Definitions:

- 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.

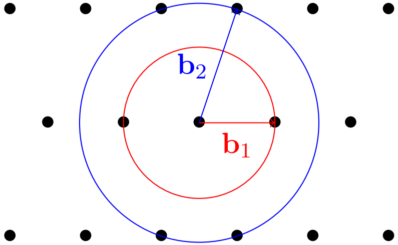
Problems :

- 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.

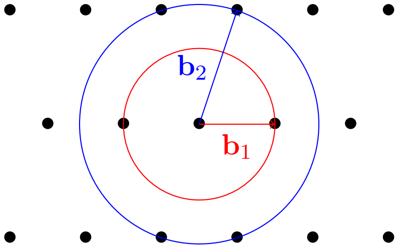
Problems :

- 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

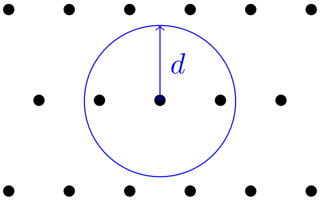
There is no polynomial time algorithm that approximates these lattice problems to within polynomial factors.

GapSVP

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

Input : a basis $\mathbf{B}$ of a lattice Λ and a number d,

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



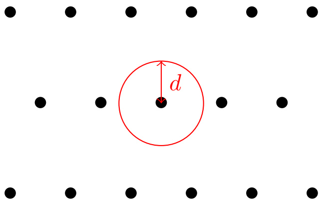
Best known algorithm: complexity $2^{\Omega\left(\frac{n \log\log n}{\log n}\right)}$.

GapSVP

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

Input : a basis $\mathbf{B}$ of a lattice Λ and a number d,

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



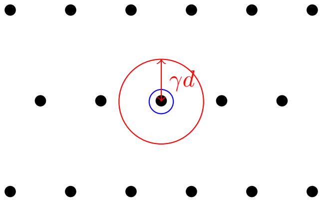
Best known algorithm: complexity $2^{\Omega(\frac{n \log\log n}{\log n})}$.

GapSVP

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

Input : a basis $\mathbf{B}$ of a lattice Λ and a number d,

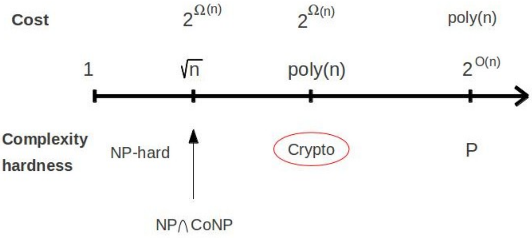
Output : • YES: there is $\mathbf{z} \in \Lambda$ non-zero such that $\|\mathbf{z}\| < d$,
• NO: for all non-zero vectors $\mathbf{z} \in \Lambda$: $\|\mathbf{z}\| \geq \gamma d$.



Approximation factor: γ.

Best known algorithm: complexity $2^{\Omega(\frac{n \log \log n}{\log n})}$.

Hardness of GapSVP$_\gamma$



Conjecture

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

LWE-based cryptography

From basic to very advanced primitives

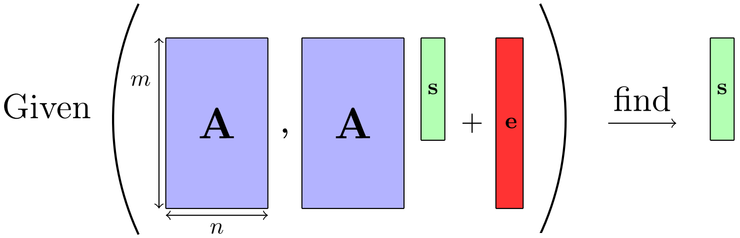
- Public key encryption
  [Regev 2005, ...];
- Identity-based encryption
  [Gentry, Peikert and Vaikuntanathan 2008, ...];
- Fully homomorphic encryption
  [Brakerski and Vaikuntanathan 2011, ...].

Advantages of LWE-based primitives

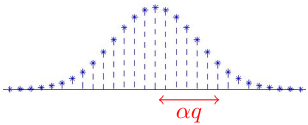
- Efficient, especially when the **modulus is polynomial**;
- Security proofs **from the hardness of LWE**;
- Likely to resist attacks from quantum computers.

The Learning With Errors problem [Regev05]

LWE_q^n



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



Discrete Gaussian error

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

Public key Encryption

- An user A has two keys:
  - one public pk_A
  - one secret sk_A
- To encrypt a message M, anyone can use pk_A.
- To decrypt a ciphertext C, only A can do it using sk_A.

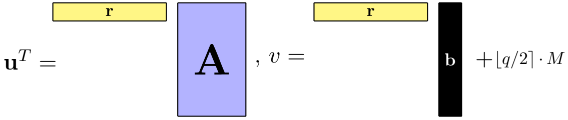
An example of Public-Key Encryption[Regev 2005]

- **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 $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

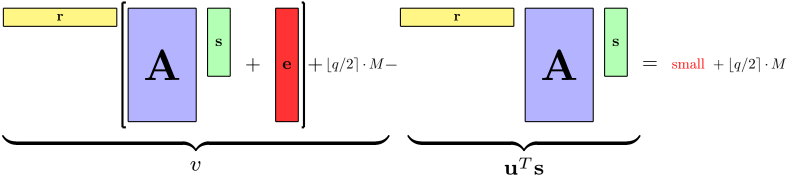
$$\mathbf{u}^T = \mathbf{r}\,\mathbf{A}, \quad v = \mathbf{r}\,\mathbf{b} + \lfloor q/2 \rceil \cdot M$$

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 $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,



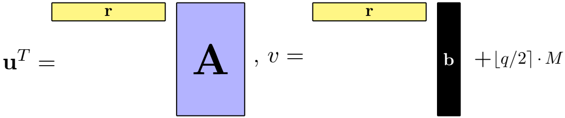
- **Decryption** of $(\mathbf{u}, v)$: compute $v - \mathbf{u}^T\mathbf{s}$,



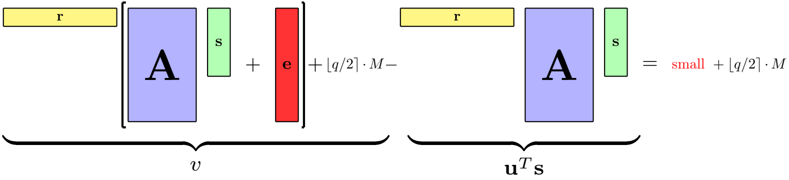
If close from 0: return 0, if close from $\lfloor q/2 \rceil$: return 1.

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".

Reminders

- Hard problem on lattices: GapSVP.
- Lattice-based cryptography:
  Security proof based on reduction from GapSVP to a problem (= a protocol attacker).
- Learning With Errors problem:
  Distinguish between $(\mathbf{A}, \mathbf{b})$ uniform and $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q)$, where $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m \times n})$, $\mathbf{s} \leftarrow U(\mathbb{Z}_q^n)$ is secret, and $\mathbf{e}$ Gaussian.
- Public-key encryption: security based on hardness of LWE.

Prior reductions from worst-case lattice problems 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 problems 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:

From LWE	in dimension n with modulus q^k,
to LWE	in dimension nk with modulus q.

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.

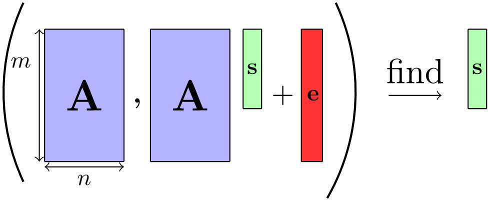
Add a **Gaussian rounding** to smooth the distribution: $\mathbf{A}' = \frac{p}{q}\mathbf{A} + \mathbf{R}$.

  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 $\mathbb{Z}_q^n$	

Other main contributions

Hardness of LWE:

- **Shrinking modulus / Expanding dimension**:
  A reduction from $\mathrm{LWE}_{q^k}^{n}$ to LWE_{q}^{nk}.
- **Expanding modulus / Shrinking dimension**:
  A reduction from LWE_{q}^{n} to $\mathrm{LWE}_{q^k}^{n/k}$.

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

Consequences:

- Hardness of $\mathrm{LWE}_{2^n}^{1}$ (Hidden Number Problem).
- The Ring-LWE problem in dimension n with exponential modulus is hard under hardness of general lattices (not ideal lattices).

Conclusion

Our main result

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

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 only get GapSVP and not SIVP.

Conclusion

Our main result

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

Open problems:

Is there a classical reduction as good as the one in **[Regev05]**?

1. We lose a quadratic term in the dimension;

   Recall that the **[Peikert09]** reduction is from GapSVP in dimension $\sqrt{n}$ to LWE with dimension $\times$ log(modulus) $= n$.

   Is this reduction sharp?

Conclusion

Our main result

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

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 only get GapSVP and not SIVP.

   In (quantum) **[Regev05]** the worst-case lattice problem is SIVP.

   SIVP feels like a harder problem than GapSVP