Classical hardness of Learning with Errors

Zvika Brakerski[1] Adeline Langlois[2] Chris Peikert[3]
Oded Regev[4] Damien Stehlé[2]

[1]Stanford University

[2]ENS de Lyon

[3]Georgia Tech

[4]New York University

Our main results

Not quantum

GapSVP in dimension $\sqrt{n}$

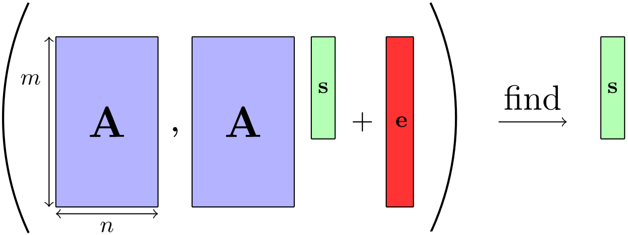
A classical reduction from a worst-case lattice problem to the Learning with Errors problem with small modulus.

Dimension n

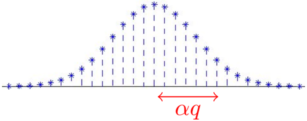
Polynomial in n

The Learning With Errors problem [Regev05]

LWE_q^n

Given 

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



Discrete Gaussian error

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

LWE-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.

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:

$$\text{From LWE} \left| \begin{array}{l} \text{in dimension } n \\ \text{with modulus } q^k, \end{array} \right.$$

$$\text{to LWE} \left| \begin{array}{l} \text{in dimension } nk \\ \text{with modulus } q. \end{array} \right.$$

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).

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: $\mathbf{A}' = \lfloor \frac{p}{q} \mathbf{A} \rceil$?

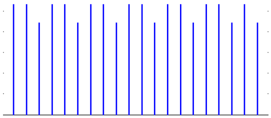
Modulus Switching

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

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

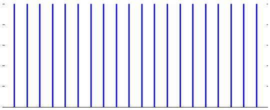
- Transform $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$ to $\mathbf{A}' \hookleftarrow U(\mathbb{Z}_p^{m \times n})$;

  First idea: $\mathbf{A}' = \lfloor \frac{p}{q} \mathbf{A} \rceil$?
- Two main problems:
  1. The distribution is not uniform:



A naive rounding introduces artefacts.

$\xrightarrow{\text{solution}}$



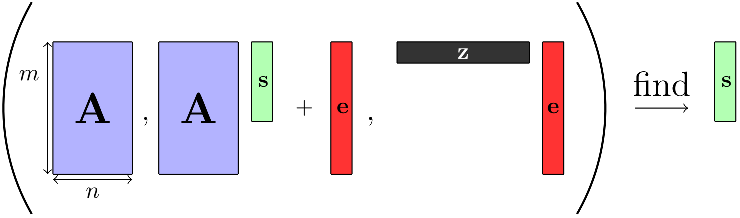
Add a **Gaussian rounding** to smooth the distribution:
$\mathbf{A}' = \frac{p}{q}\mathbf{A} + \mathbf{R}$.

  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.
- The improvement relies on Extended LWE **[Alperin-Sheriff and Peikert 2012]**.
  We give a hardness proof for Extended LWE.
  For a given $\mathbf{z} \in \mathbb{Z}^m$ small:



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 $\mathrm{poly}(n)$ 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	$\mathrm{poly}(n)$	in $\mathbb{Z}_q^n$	

Conclusion

Our main result

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

Open problems:

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

1. We lose a quadratic term in the dimension;

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

   Is this reduction sharp?

Conclusion

Our main result

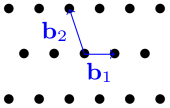
A classical reduction from GapSVP in dimension $\sqrt{n}$ to LWE in dimension n with $\mathrm{poly}(n)$ modulus.

Open problems:

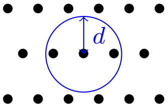
Is there a classical reduction as good as the one in **[Regev05]**?

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: search problem



GapSVP: decision problem

SIVP feels like a harder problem than GapSVP