Classical hardness of Learning with Errors

Zvika Brakerski\textsuperscript{1}  Adeline Langlois\textsuperscript{2}  Chris Peikert\textsuperscript{3}  Oded Regev\textsuperscript{4}  Damien Stehlé\textsuperscript{2}

\textsuperscript{1}Stanford University  
\textsuperscript{2}ENS de Lyon  
\textsuperscript{3}Georgia Tech  
\textsuperscript{4}New York University
Our main results

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

- Not quantum
- GapSVP in dimension $\sqrt{n}$
- Dimension $n$
- Polynomial in $n$
The Learning With Errors problem [Regev05]

\[ \text{LWE}_q^n \]

Given

\[
\begin{pmatrix}
\text{A} \\
\text{A} \\
\text{s} \\
\text{e}
\end{pmatrix}
\]

find

\[ \text{s} \]

\[ \begin{aligned}
\text{A} &\leftarrow U(\mathbb{Z}_q^{m\times n}), \\
\text{s} &\leftarrow U(\mathbb{Z}_q^n), \\
\text{e} &\sim D_{\mathbb{Z}^m,\alpha q} \text{ with } \alpha = o(1).
\end{aligned} \]

Discrete Gaussian error

Decision version: Distinguish from \((\text{A}, \text{b})\) with \(\text{b}\) 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.

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

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

<table>
<thead>
<tr>
<th>From LWE in dimension $n$ with modulus $q^k$,</th>
</tr>
</thead>
<tbody>
<tr>
<td>to LWE in dimension $nk$ with modulus $q$.</td>
</tr>
</tbody>
</table>
Main contributions

Hardness of LWE:

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

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

⇒ The hardness of $\text{LWE}_{q}^n$ is a function of $n \log q$.

Consequences:

- Hardness of $\text{LWE}_{2^n}^1$ (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 $(A, As + e) \mod q$ to $(A', A's + e') \mod p$?

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

  First idea: $A' = \left\lfloor \frac{p}{q} A \right\rfloor$?
Modulus Switching

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

How to map $(A, As + e) \mod q$ to $(A', A's + e') \mod p$?

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

First idea: $A' = \left\lfloor \frac{p}{q} A \right\rfloor$?

- Two main problems:
  1. The distribution is not uniform:

A naive rounding introduces artefacts.

solution

Add a Gaussian rounding to smooth the distribution:

$$A' = \frac{p}{q} A + R.$$ 

2. In $A's + e'$, the rounding errors gets multiplied by the secret $s$ (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 $z \in \mathbb{Z}^m$ small:

\[
\begin{pmatrix}
  m \\
  A \\
  n \\
\end{pmatrix}, \begin{pmatrix}
  A \\
  s \\
  + \\
  e \\
\end{pmatrix}, \begin{pmatrix}
  z \\
  e \\
\end{pmatrix} \xrightarrow{\text{find}} s
\]
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:

<table>
<thead>
<tr>
<th>Problem</th>
<th>Dimension</th>
<th>Modulus</th>
<th>Secret</th>
</tr>
</thead>
<tbody>
<tr>
<td>GapSVP</td>
<td>$\sqrt{n}$</td>
<td></td>
<td>$\mathbb{Z}_{\sqrt{n}}$ [Peikert09]</td>
</tr>
<tr>
<td>$\downarrow^0$</td>
<td>$\sqrt{n}$</td>
<td>large</td>
<td>$\mathbb{Z}_{\sqrt{n}}$</td>
</tr>
<tr>
<td>LWE</td>
<td>$\sqrt{n}$</td>
<td>large</td>
<td>$\mathbb{Z}_{\sqrt{n}}$</td>
</tr>
<tr>
<td>$\downarrow^1$</td>
<td>$n$</td>
<td>large</td>
<td>small</td>
</tr>
<tr>
<td>LWE</td>
<td>$n$</td>
<td>large</td>
<td>$\mathbb{Z}^n$</td>
</tr>
<tr>
<td>$\downarrow^2$</td>
<td>$n$</td>
<td>poly($n$)</td>
<td>in $\mathbb{Z}_q^n$</td>
</tr>
<tr>
<td>LWE</td>
<td>$n$</td>
<td>poly($n$)</td>
<td>in $\mathbb{Z}_q^n$</td>
</tr>
</tbody>
</table>
Conclusion

**Our main result**

A classical reduction from \textsf{GapSVP} in dimension $\sqrt{n}$ to \textsf{LWE} in dimension $n$ with $\text{poly}(n)$ 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 \textsf{GapSVP} and not \textsf{SIVP}.
Conclusion

Our main result
A classical reduction from GapSVP in dimension $\sqrt{n}$ to LWE in dimension $n$ with $\text{poly}(n)$ 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 $\text{poly}(n)$ 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*