Pseudorandomness of Ring-LWE for Any Ring and Modulus

Chris Peikert
University of Michigan

Oded Regev  Noah Stephens-Davidowitz

(to appear, STOC’17)

10 March 2017
Lattice-Based Cryptography

\[ y = g^x \mod p \]

\[ m^e \mod N \]

\[ e(g^a, g^b) \]

\[ N = p \cdot q \]

(Images courtesy xkcd.org)
Lattice-Based Cryptography

\[ N = pq \]
\[ y = g^x \mod p \]
\[ m^e \mod N = e(g^a, g^b) \]

Main Attractions

▶ Efficient: linear, embarrassingly parallel operations
▶ Resists quantum attacks (so far)
▶ Security from worst-case assumptions
▶ Solutions to 'holy grail' problems in crypto: FHE and related

(Images courtesy xkcd.org)
Lattice-Based Cryptography

Main Attractions

▶ **Efficient**: linear, embarrassingly parallel operations

(Images courtesy xkcd.org)
Lattice-Based Cryptography

Main Attractions

▶ **Efficient**: linear, embarrassingly parallel operations
▶ **Resists quantum attacks** (so far)
Lattice-Based Cryptography

\[ N = p \cdot q \]
\[ y = g^x \mod p \]
\[ m = e \mod N \]
\[ e(g^a, g^b) = \Rightarrow \]

Main Attractions

▶ Efficient: linear, embarrassingly parallel operations
▶ Resists quantum attacks (so far)
▶ Security from worst-case assumptions

(Images courtesy xkcd.org)
Lattice-Based Cryptography

\[ N = p \cdot q \]
\[ y = g^x \mod p \]
\[ m^e \mod N \]
\[ e(g^a, g^b) \Rightarrow \]

Main Attractions

- **Efficient**: linear, embarrassingly parallel operations
- **Resists** quantum attacks (so far)
- **Security from** worst-case assumptions
- **Solutions to** ‘holy grail’ problems in crypto: FHE and related

(Images courtesy xkcd.org)
Learning With Errors  [Regev'05]

- Parameters: dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$
Learning With Errors \cite{Regev'05}

- **Parameters:** dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$

- **Search:** find secret $s \in \mathbb{Z}_q^n$ given many ‘noisy inner products’

\[
\begin{align*}
a_1 & \leftarrow \mathbb{Z}_q^n, & b_1 & \approx \langle a_1, s \rangle \in \mathbb{Z}_q \\
a_2 & \leftarrow \mathbb{Z}_q^n, & b_2 & \approx \langle a_2, s \rangle \in \mathbb{Z}_q \\
& \vdots
\end{align*}
\]
Learning With Errors  [Regev'05]

- Parameters: dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$

- **Search:** find secret $s \in \mathbb{Z}_q^n$ given many ‘noisy inner products’

\[
\begin{align*}
a_1 & \leftarrow \mathbb{Z}_q^n, \quad b_1 = \langle a_1, s \rangle + e_1 \in \mathbb{Z}_q \\
a_2 & \leftarrow \mathbb{Z}_q^n, \quad b_2 = \langle a_2, s \rangle + e_2 \in \mathbb{Z}_q \\
\vdots & \\
\end{align*}
\]

width $\alpha q$
Learning With Errors  [Regev'05]

- **Parameters:** dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$
- **Search:** find secret $s \in \mathbb{Z}_q^n$ given many ‘noisy inner products’

\[
\begin{align*}
\mathbf{a}_1 & \leftarrow \mathbb{Z}_q^n, \quad b_1 = \langle \mathbf{a}_1 , s \rangle + e_1 \in \mathbb{Z}_q \\
\mathbf{a}_2 & \leftarrow \mathbb{Z}_q^n, \quad b_2 = \langle \mathbf{a}_2 , s \rangle + e_2 \in \mathbb{Z}_q \\
\vdots
\end{align*}
\]

- **Decision:** distinguish $(a_i, b_i)$ from uniform $(a_i, b_i)$

width $\alpha q$
Learning With Errors \[\text{[Regev'05]}\]

- **Parameters**: dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$

- **Search**: find secret $s \in \mathbb{Z}_q^n$ given many ‘noisy inner products’

\[
\begin{align*}
    a_1 &\leftarrow \mathbb{Z}_q^n, \quad b_1 = \langle a_1, s \rangle + e_1 \in \mathbb{Z}_q \\
    a_2 &\leftarrow \mathbb{Z}_q^n, \quad b_2 = \langle a_2, s \rangle + e_2 \in \mathbb{Z}_q \\
    \vdots
\end{align*}
\]

- **Decision**: distinguish $(a_i, b_i)$ from uniform $(a_i, b_i)$

---

**LWE is Hard and Versatile**

- **worst case**
  - \((n/\alpha)\)-SIVP on \(n\)-dim lattices \[\leq\] search-LWE \[\leq\] decision-LWE \[\leq\] much crypto

- (quantum [R'05]) \[\uparrow\] [BFKL'93,R'05,...]
Learning With Errors [Regev'05]

- **Parameters:** dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$

- **Search:** find secret $s \in \mathbb{Z}_q^n$ given many ‘noisy inner products’

  $$a_1 \leftarrow \mathbb{Z}_q^n, \quad b_1 = \langle a_1, s \rangle + e_1 \in \mathbb{Z}_q$$
  $$a_2 \leftarrow \mathbb{Z}_q^n, \quad b_2 = \langle a_2, s \rangle + e_2 \in \mathbb{Z}_q$$
  $$\vdots$$

- **Decision:** distinguish $(a_i, b_i)$ from uniform $(a_i, b_i)$

LWE is Hard and Versatile

- **worse case**
  - $(n/\alpha)$-SIVP on $\leq$ search-LWE $\leq$ decision-LWE $\leq$ much crypto
  - $n$-dim lattices $\uparrow$ (quantum [R'05]) $\uparrow$ [BFKL'93,R'05, …]

- **Classically,** GapSVP $\leq$ search-LWE (worse params) [P’09,BLPRS’13]
LWE Hardness and Parameters

- Parameters: dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$

**Worst case SIVP $\leq$ Search-LWE**

- One reduction for best known parameters: any $q \geq \sqrt{n/\alpha}$ [R’05]
LWE Hardness and Parameters

- Parameters: dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$

**Worst case SIVP $\leq$ Search-LWE**
- One reduction for best known parameters: any $q \geq \sqrt{n/\alpha}$ [R’05]

**Search-LWE $\leq$ Decision-LWE**
- Messy. Many incomparable reductions for different forms of $q$: 

  - Any prime $q = \text{poly}(n)$ [R’05]
  - Any “somewhat smooth” $q = p_1 \cdots p_t$ (large enough primes $p_i$) [P’09]
  - Any $q = p^e$ for large enough prime $p$ [ACPS’09]
  - Any $q = p^e$ with uniform error mod $p^i$ [MM’11]
  - Any $q$ via “mod-switching” — but increases $\alpha$ [P’09, BV’11, BLPRS’13]
LWE Hardness and Parameters

- Parameters: dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$

Worst case SIVP $\leq$ Search-LWE

- One reduction for best known parameters: any $q \geq \sqrt{n/\alpha}$ [R'05]

Search-LWE $\leq$ Decision-LWE

- Messy. Many incomparable reductions for different forms of $q$:
  - Any prime $q = \text{poly}(n)$ [R'05]
LWE Hardness and Parameters

- Parameters: dimension \( n \), integer modulus \( q \), error ‘rate’ \( \alpha \)

Worst case SIVP \( \leq \) Search-LWE

- One reduction for best known parameters: any \( q \geq \sqrt{n}/\alpha \) [R’05]

Search-LWE \( \leq \) Decision-LWE

- Messy. Many incomparable reductions for different forms of \( q \):
  - Any prime \( q = \text{poly}(n) \) [R’05]
  - Any “somewhat smooth” \( q = p_1 \cdots p_t \) (large enough primes \( p_i \)) [P’09]
LWE Hardness and Parameters

- Parameters: dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$

**Worst case SIVP $\leq$ Search-LWE**

- One reduction for best known parameters: any $q \geq \sqrt{n/\alpha}$  
  [R'05]

**Search-LWE $\leq$ Decision-LWE**

- Messy. Many incomparable reductions for different forms of $q$:
  - Any prime $q = \text{poly}(n)$  
    [R'05]
  - Any “somewhat smooth” $q = p_1 \cdots p_t$ (large enough primes $p_i$)  
    [P'09]
  - Any $q = p^e$ for large enough prime $p$  
    [ACPS'09]
LWE Hardness and Parameters

- Parameters: dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$

Worst case SIVP $\leq$ Search-LWE

- One reduction for best known parameters: any $q \geq \sqrt{n/\alpha}$ [R’05]

Search-LWE $\leq$ Decision-LWE

- Messy. Many incomparable reductions for different forms of $q$:
  - Any prime $q = \text{poly}(n)$ [R’05]
  - Any “somewhat smooth” $q = p_1 \cdots p_t$ (large enough primes $p_i$) [P’09]
  - Any $q = p^e$ for large enough prime $p$ [ACPS’09]
  - Any $q = p^e$ with uniform error mod $p^i$ [MM’11]

Increasing $q, \alpha$ yields a weaker ultimate hardness guarantee.
LWE Hardness and Parameters

- Parameters: dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$

**Worst case SIVP $\leq$ Search-LWE**

- One reduction for best known parameters: any $q \geq \sqrt{n}/\alpha$ [R’05]

**Search-LWE $\leq$ Decision-LWE**

- Messy. Many incomparable reductions for different forms of $q$:
  - Any prime $q = \text{poly}(n)$ [R’05]
  - Any “somewhat smooth” $q = p_1 \cdots p_t$ (large enough primes $p_i$) [P’09]
  - Any $q = p^e$ for large enough prime $p$ [ACPS’09]
  - Any $q = p^e$ with uniform error mod $p^i$ [MM’11]
  - Any $q = p^e$ — but increases $\alpha$ [MP’12]
LWE Hardness and Parameters

- Parameters: dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$

Worst case SIVP $\leq$ Search-LWE

- One reduction for best known parameters: any $q \geq \sqrt{n/\alpha}$ [R’05]

Search-LWE $\leq$ Decision-LWE

- Messy. Many incomparable reductions for different forms of $q$:
  - Any prime $q = \text{poly}(n)$ [R’05]
  - Any “somewhat smooth” $q = p_1 \cdots p_t$ (large enough primes $p_i$) [P’09]
  - Any $q = p^e$ for large enough prime $p$ [ACPS’09]
  - Any $q = p^e$ with uniform error mod $p^i$ [MM’11]
  - Any $q = p^e$ — but increases $\alpha$ [MP’12]
  - Any $q$ via “mod-switching” — but increases $\alpha$ [P’09,BV’11,BLPRS’13]
LWE Hardness and Parameters

- Parameters: dimension $n$, integer modulus $q$, error ‘rate’ $\alpha$

### Worst case SIVP $\leq$ Search-LWE

- One reduction for best known parameters: any $q \geq \sqrt{n/\alpha}$ [R’05]

### Search-LWE $\leq$ Decision-LWE

- Messy. Many incomparable reductions for different forms of $q$:
  - Any prime $q = \text{poly}(n)$ [R’05]
  - Any “somewhat smooth” $q = p_1 \cdots p_t$ (large enough primes $p_i$) [P’09]
  - Any $q = p^e$ for large enough prime $p$ [ACPS’09]
  - Any $q = p^e$ with uniform error mod $p^i$ [MM’11]
  - Any $q = p^e$ — but increases $\alpha$ [MP’12]
  - Any $q$ via “mod-switching” — but increases $\alpha$ [P’09,BV’11,BLPRS’13]

- Increasing $q, \alpha$ yields a weaker ultimate hardness guarantee.
LWE is Efficient (Sort Of)

Getting one pseudorandom scalar requires an $n$-dim inner product mod $q$

$$(\cdots a_i \cdots) \begin{pmatrix} s \\ \vdots \end{pmatrix} + e = b \in \mathbb{Z}_q$$
LWE is Efficient (Sort Of)

\[
\begin{pmatrix}
\cdots a_i \cdots
\end{pmatrix}
\begin{pmatrix}
s \\
\vdots
\end{pmatrix} + e = b \in \mathbb{Z}_q
\]

- Getting one pseudorandom scalar requires an \( n \)-dim inner product mod \( q \)

- Can amortize each \( a_i \) over many secrets \( s_j \), but still \( \tilde{O}(n) \) work per scalar output.
LWE is Efficient (Sort Of)

\[(\cdots a_i \cdots) \begin{pmatrix} \vdots \\ s \\ \vdots \end{pmatrix} + e = b \in \mathbb{Z}_q\]

- Getting one pseudorandom scalar requires an \(n\)-dim inner product mod \(q\)
- Can amortize each \(a_i\) over many secrets \(s_j\), but still \(\tilde{O}(n)\) work per scalar output.

- Cryptosystems have rather large keys: \(\Omega(n^2 \log^2 q)\) bits:

\[pk = \begin{pmatrix} \vdots \\ A \\ \vdots \end{pmatrix}, \quad \begin{pmatrix} \vdots \\ b \\ \vdots \end{pmatrix} \Omega(n)\]
Wishful Thinking...

\[
\begin{pmatrix}
\vdots \\
a_i \\
\vdots
\end{pmatrix} \ast \begin{pmatrix}
\vdots \\
s \\
\vdots
\end{pmatrix} + \begin{pmatrix}
\vdots \\
e_i \\
\vdots
\end{pmatrix} = \begin{pmatrix}
\vdots \\
b_i \\
\vdots
\end{pmatrix} \in \mathbb{Z}_q^n
\]

- Get \( n \) pseudorandom scalars from just one cheap product operation?
Wishful Thinking... 

Get \( n \) pseudorandom scalars from just one cheap product operation?

**Question**

How to define the product ‘\( \star \)’ so that \((a_i, b_i)\) is pseudorandom?
Wishful Thinking... 

\[
\begin{pmatrix} \vdots \\ a_i \end{pmatrix} \ast \begin{pmatrix} \vdots \\ s \end{pmatrix} + \begin{pmatrix} \vdots \\ e_i \end{pmatrix} = \begin{pmatrix} \vdots \\ b_i \end{pmatrix} \in \mathbb{Z}_q^n
\]

Get \( n \) pseudorandom scalars from just one cheap product operation?

Question

▶ How to define the product ‘\( \ast \)’ so that \((a_i, b_i)\) is pseudorandom?

▶ Careful! With small error, coordinate-wise multiplication is insecure!
Get \( n \) pseudorandom scalars from just one cheap product operation?

Question

- How to define the product ‘\( \star \)’ so that \((a_i, b_i)\) is pseudorandom?
- Careful! With small error, coordinate-wise multiplication is insecure!

Answer

- ‘\( \star \)’ = multiplication in a polynomial ring: e.g., \( \mathbb{Z}_q[X]/(X^n + 1) \).
  - Fast and practical with FFT: \( n \log n \) operations mod \( q \).
Wishful Thinking...

\[
\begin{pmatrix}
\vdots \\
a_i \\
\vdots \\
\end{pmatrix} \star \begin{pmatrix}
\vdots \\
s \\
\vdots \\
\end{pmatrix} + \begin{pmatrix}
\vdots \\
e_i \\
\vdots \\
\end{pmatrix} = \begin{pmatrix}
\vdots \\
b_i \\
\vdots \\
\end{pmatrix} \in \mathbb{Z}_q^n
\]

▶ Get \( n \) pseudorandom scalars from just one cheap product operation?

Question
▶ How to define the product ‘\( \star \)’ so that \((a_i, b_i)\) is pseudorandom?
▶ Careful! With small error, coordinate-wise multiplication is insecure!

Answer
▶ ‘\( \star \)’ = multiplication in a polynomial ring: e.g., \( \mathbb{Z}_q[X]/(X^n + 1) \).

Fast and practical with FFT: \( n \log n \) operations mod \( q \).

▶ Same ring structures used in NTRU cryptosystem [HPS’98],
& in compact one-way / CR hash functions [Mic’02,PR’06,LM’06,...]
Wishful Thinking...

\[
\begin{pmatrix}
\vdots \\
a_i \\
\vdots 
\end{pmatrix} \star \begin{pmatrix}
\vdots \\
s \\
\vdots 
\end{pmatrix} + \begin{pmatrix}
\vdots \\
e_i \\
\vdots 
\end{pmatrix} = \begin{pmatrix}
\vdots \\
b_i \\
\vdots 
\end{pmatrix} \in \mathbb{Z}_q^n
\]

Get \( n \) pseudorandom scalars from just one cheap product operation?

IF YOU LWE IT

THEN YOU SHOULD PUT A RING ON IT

meme-generator.net
Learning With Errors over Rings (Ring-LWE) \[\text{[LPR'10]}\]

- **Ring** $R$, often $R = \mathbb{Z}[X]/(f(X))$ for irred. $f$ of degree $n$ (or $R = \mathcal{O}_K$)
Learning With Errors over Rings (Ring-LWE) [LPR’10]

- Ring $R$, often $R = \mathbb{Z}[X]/(f(X))$ for irred. $f$ of degree $n$ (or $R = \mathcal{O}_K$)
- Has a ‘dual ideal’ $R^\vee$ (w.r.t. ‘canonical’ geometry)
Learning With Errors over Rings (Ring-LWE) [LPR’10]

- Ring $R$, often $R = \mathbb{Z}[X]/(f(X))$ for irred. $f$ of degree $n$ (or $R = \mathcal{O}_K$)
  Has a ‘dual ideal’ $R^\vee$ (w.r.t. ‘canonical’ geometry)
- Integer modulus $q$ defining $R_q := R/qR$ and $R_q^\vee := R^\vee/qR^\vee$
Learning With Errors over Rings (Ring-LWE) [LPR’10]

- Ring $R$, often $R = \mathbb{Z}[X]/(f(X))$ for irred. $f$ of degree $n$ (or $R = \mathcal{O}_K$)
- Has a ‘dual ideal’ $R^\vee$ (w.r.t. ‘canonical’ geometry)
- Integer modulus $q$ defining $R_q := R/qR$ and $R_q^\vee := R^\vee/qR^\vee$
- Gaussian error of width $\approx \alpha q$ over $R^\vee$
Learning With Errors over Rings (Ring-LWE) [LPR'10]

- Ring $R$, often $R = \mathbb{Z}[X]/(f(X))$ for irred. $f$ of degree $n$ (or $R = \mathcal{O}_K$)
- Has a ‘dual ideal’ $R^\vee$ (w.r.t. ‘canonical’ geometry)
- Integer modulus $q$ defining $R_q := R/qR$ and $R_q^\vee := R^\vee/qR^\vee$
- Gaussian error of width $\approx \alpha q$ over $R^\vee$

**Search:** find secret ring element $s \in R_q^\vee$, given independent samples

\[
\begin{align*}
    a_1 & \leftarrow R_q, \quad b_1 = a_1 \cdot s + e_1 \in R_q^\vee \\
    a_2 & \leftarrow R_q, \quad b_2 = a_2 \cdot s + e_2 \in R_q^\vee \\
    \vdots
\end{align*}
\]
Learning With Errors over Rings (Ring-LWE) [LPR’10]

- Ring $R$, often $R = \mathbb{Z}[X]/(f(X))$ for irred. $f$ of degree $n$ (or $R = \mathcal{O}_K$)
  Has a ‘dual ideal’ $R^\vee$ (w.r.t. ‘canonical’ geometry)
- Integer modulus $q$ defining $R_q := R/qR$ and $R_q^\vee := R^\vee / qR^\vee$
- Gaussian error of width $\approx \alpha q$ over $R^\vee$

**Search:** find secret ring element $s \in R_q^\vee$, given independent samples

\[
\begin{align*}
a_1 &\leftarrow R_q, \quad b_1 = a_1 \cdot s + e_1 \in R_q^\vee \\
a_2 &\leftarrow R_q, \quad b_2 = a_2 \cdot s + e_2 \in R_q^\vee \\
\vdots
\end{align*}
\]

**Decision:** distinguish $(a_i, b_i)$ from uniform $(a_i, b_i) \in R_q \times R_q^\vee$
Hardness of Ring-LWE [LPR’10]

\[
\text{worst-case } (n^c / \alpha)\text{-SIVP on ideal lattices in } R \leq \text{search } R\text{-LWE}_{q,\alpha} \leq \text{decision } R\text{-LWE}_{q,\alpha}
\]

(quantum, any \( R = \mathcal{O}_K \))  
(classical, any Galois \( R \))
Hardness of Ring-LWE [LPR’10]

worst-case \((n^c/\alpha)\)-SIVP on \textit{ideal} lattices in \(R\) \(\leq\) search \(R\)-LWE\(_{q,\alpha}\) \(\leq\) decision \(R\)-LWE\(_{q,\alpha}\)

(quantum, any \(R = \mathcal{O}_K\)) (classical, any Galois \(R\))

(Ideal \(\mathcal{I} \subseteq R\): additive subgroup, \(x \cdot r \in \mathcal{I}\) for all \(x \in \mathcal{I}, r \in R\).)

\(R = \mathbb{Z}[X]/(1 + X + X^2)\)

ideal \(\mathcal{I} = 3R + (1 - X)R \subset R\)
Hardness of Ring-LWE [LPR’10]

Large disparity in known hardness of search versus decision:

\[
\text{worst-case } (n^c/\alpha)\text{-SIVP on ideal lattices in } R
\leq \text{search } R\text{-LWE}_{q,\alpha}
\leq \text{decision } R\text{-LWE}_{q,\alpha}
\]

(quantum, any } R = \mathcal{O}_K\)  
(classical, any Galois } R\)
## Hardness of Ring-LWE [LPR’10]

<table>
<thead>
<tr>
<th>worst-case $(n^c/\alpha)$-SIVP</th>
<th>( \leq )</th>
<th>search</th>
<th>( R\text{-LWE}_{q,\alpha} )</th>
<th>( \leq )</th>
<th>decision</th>
<th>( R\text{-LWE}_{q,\alpha} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>on \textit{ideal} lattices in ( R )</td>
<td>( \gamma )</td>
<td>( \gamma )</td>
<td>( (\text{quantum, any } R = \mathcal{O}_K) )</td>
<td>( (\text{classical, any Galois } R) )</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Large disparity in known hardness of search versus decision:

**Search:** any number ring, any \( q \geq n^c/\alpha \).
Hardness of Ring-LWE [LPR’10]

\[
\text{worst-case } \left(\frac{n^c}{\alpha}\right)\text{-SIVP on ideal lattices in } R \leq \text{search } R\text{-LWE}_{q,\alpha} \leq \text{decision } R\text{-LWE}_{q,\alpha}
\]

(quantum, any \( R = \mathcal{O}_K \))

(classical, any Galois \( R \))

Large disparity in known hardness of search versus decision:

**Search**: any number ring, any \( q \geq \frac{n^c}{\alpha} \).

**Decision**: any Galois number ring (e.g., cyclotomic), any highly splitting prime \( q = \text{poly}(n) \).
Hardness of Ring-LWE [LPR’10]

Large disparity in known hardness of search versus decision:

**Search:** any number ring, any $q \geq n^c/\alpha$.

**Decision:** any Galois number ring (e.g., cyclotomic), any highly splitting prime $q = \text{poly}(n)$.

Can then get any $q$ by mod-switching, but increases $\alpha$ [LS’15]
Hardness of Ring-LWE [LPR’10]

Large disparity in known hardness of search versus decision:

**Search:** any number ring, any \( q \geq n^c/\alpha \).

**Decision:** any Galois number ring (e.g., cyclotomic), any highly splitting prime \( q = \text{poly}(n) \).

Can then get any \( q \) by mod-switching, but increases \( \alpha \) [LS’15]

- Decision has no known worst-case hardness in non-Galois rings.
Hardness of Ring-LWE [LPR’10]

\[
\text{worst-case } \left(\frac{n^c}{\alpha}\right)\text{-SIVP} \leq \begin{array}{c}
\text{search } R\text{-LWE}_{q,\alpha} \\
\text{decision } R\text{-LWE}_{q,\alpha}
\end{array}
\]
\[
\leq \begin{array}{c}
\text{on } \text{ideal lattices in } R \\
\text{on } \text{ideal lattices in } R
\end{array}
\]
\[
\leq \begin{array}{c}
\text{on } \text{ideal lattices in } R \\
\text{on } \text{ideal lattices in } R
\end{array}
\]

\[
(\text{quantum, any } R = \mathcal{O}_K) \\
(\text{classical, any Galois } R)
\]

Large disparity in known hardness of search versus decision:

**Search:** any number ring, any \( q \geq \frac{n^c}{\alpha} \).

**Decision:** any Galois number ring (e.g., cyclotomic), any highly splitting prime \( q = \text{poly}(n) \).

Can then get any \( q \) by mod-switching, but increases \( \alpha \) [LS’15]

- Decision has no known worst-case hardness in non-Galois rings.
- But no examples of easy(er) decision when search is worst-case hard!
Our Results

Main Theorem: Ring-LWE is Pseudorandom in Any Ring

worst-case $(n^c/\alpha)$-SIVP on ideal lattices in $R$ \( \leq \) decision $R$-LWE$_{q,\alpha}$

quantum,
any $R = \mathcal{O}_K$, any $q \geq n^{c-1/2}/\alpha$
Our Results

Main Theorem: Ring-LWE is Pseudorandom in Any Ring

worst-case \((n^c/\alpha)\)-SIVP on ideal lattices in \(R\) \(\leq\) decision \(R\text{-LWE}_{q,\alpha}\)

quantum, any \(R = \mathcal{O}_K\), any \(q \geq n^{c-1/2}/\alpha\)

Bonus Theorem: LWE is Pseudorandom for Any Modulus

worst case \((n/\alpha)\)-SIVP on \(n\)-dim lattices \(\leq\) decision-LWE\(_{q,\alpha}\)

quantum, any \(q \geq \sqrt{n}/\alpha\)
Our Results

Main Theorem: Ring-LWE is Pseudorandom in Any Ring

\[
\text{worst-case } \left( \frac{n^c}{\alpha} \right) - \text{SIVP} \leq \text{decision } R\text{-LWE}_{q,\alpha} \\
\text{on ideal lattices in } R \\
\text{quantum, } R = O_K, \text{ any } q \geq n^{c-1/2}/\alpha
\]

Bonus Theorem: LWE is Pseudorandom for Any Modulus

\[
\text{worst case } \left( \frac{n}{\alpha} \right) - \text{SIVP on } n\text{-dim lattices} \leq \text{decision-LWE}_{q,\alpha} \\
\text{quantum, any } q \geq \sqrt{n}/\alpha
\]

- Both theorems match or improve the previous best params:
Our Results

Main Theorem: Ring-LWE is Pseudorandom in Any Ring

\[
\text{worst-case } (n^c/\alpha)\text{-SIVP on ideal lattices in } R \leq \text{decision } R\text{-LWE}_{q,\alpha}
\]

quantum, any \( R = \mathcal{O}_K \), any \( q \geq n^{c-1/2}/\alpha \)

Bonus Theorem: LWE is Pseudorandom for Any Modulus

\[
\text{worst case } (n/\alpha)\text{-SIVP on } n\text{-dim lattices} \leq \text{decision-LWE}_{q,\alpha}
\]

quantum, any \( q \geq \sqrt{n}/\alpha \)

- Both theorems match or improve the previous best params:
  
  One reduction to rule them all.
Our Results

Main Theorem: Ring-LWE is Pseudorandom in Any Ring

\[ \text{worst-case } (n^c/\alpha)\text{-SIVP on ideal lattices in } R \leq \text{ decision } R\text{-LWE}_{q,\alpha} \]

quantum, any \( R = \mathcal{O}_K \), any \( q \geq n^{c-1/2}/\alpha \)

Bonus Theorem: LWE is Pseudorandom for Any Modulus

\[ \text{worst case } (n/\alpha)\text{-SIVP on } n\text{-dim lattices} \leq \text{ decision-LWE}_{q,\alpha} \]

quantum, any \( q \geq \sqrt{n}/\alpha \)

- Both theorems match or improve the previous best params:
  
  One reduction to rule them all.

- Seems to adapt to ‘module’ lattices/LWE w/techniques from [LS’15]
Which Rings To Use?

Our results don’t give any guidance: they work within a single ring $R$, lower-bounding the hardness of $R$-LWE by $R$-Ideal-SIVP.

Progress on Ideal-SIVP
- Quantum poly-time $\exp(\tilde{O}(\sqrt{n}))$-Ideal-SIVP in prime-power cyclotomics modulo heuristics [CGS’14,BS’16,CDPR’16,CDW’17]
- Quite far from the (quasi-)poly $(n)$ factors typically used for crypto
- Doesn’t apply to $R$-LWE or NTRU (unknown if $R$-LWE $\leq$ Ideal-SIVP)

Options
- Keep using $R$-LWE over cyclotomics
- Use $R$-LWE over (slower) rings like $\mathbb{Z}[X] / (X^p - X - 1)$ [BCLvV’16]
- Use ‘higher rank’ problem Module-LWE over cyclotomics/others
Which Rings To Use?

- Our results don’t give any guidance: they work within a single ring $R$, lower-bounding the hardness of $R$-LWE by $R$-Ideal-SIVP.

- We have no nontrivial relations between lattice problems over different rings. (Great open question!)
Which Rings To Use?

- Our results don’t give any guidance: they work within a single ring $R$, lower-bounding the hardness of $R$-LWE by $R$-Ideal-SIVP
- We have no nontrivial relations between lattice problems over different rings. (Great open question!)

Progress on Ideal-SIVP

- Quantum poly-time $\exp(\tilde{O}(\sqrt{n}))$-Ideal-SIVP in prime-power cyclotomics (modulo heuristics) [CGS’14,BS’16,CDPR’16,CDW’17]
Which Rings To Use?

- Our results don’t give any guidance: they work within a single ring $R$, lower-bounding the hardness of $R$-LWE by $R$-Ideal-SIVP.
- We have no nontrivial relations between lattice problems over different rings. (Great open question!)

Progress on Ideal-SIVP

- Quantum poly-time $\exp(\tilde{O}(\sqrt{n}))$-Ideal-SIVP in prime-power cyclotomics (modulo heuristics) [CGS’14, BS’16, CDPR’16, CDW’17]
- Quite far from the (quasi-)poly($n$) factors typically used for crypto.
Which Rings To Use?

- Our results don’t give any guidance: they work within a single ring $R$, lower-bounding the hardness of $R$-LWE by $R$-Ideal-SIVP
- We have no nontrivial relations between lattice problems over different rings. (Great open question!)

Progress on Ideal-SIVP

- Quantum poly-time $\exp(\tilde{O}(\sqrt{n}))$-Ideal-SIVP in prime-power cyclotomies (modulo heuristics) [CGS’14, BS’16, CDPR’16, CDW’17]
- Quite far from the (quasi-)poly($n$) factors typically used for crypto
- Doesn’t apply to $R$-LWE or NTRU (unknown if $R$-LWE $\leq$ Ideal-SIVP)
Which Rings To Use?

- Our results don’t give any guidance: they work within a single ring $R$, lower-bounding the hardness of $R$-LWE by $R$-Ideal-SIVP.
- We have no nontrivial relations between lattice problems over different rings. (Great open question!)

Progress on Ideal-SIVP

- Quantum poly-time $\exp(\tilde{O}(\sqrt{n}))$-Ideal-SIVP in prime-power cyclotomics (modulo heuristics) [CGS’14,BS’16,CDPR’16,CDW’17]
- Quite far from the (quasi-)poly($n$) factors typically used for crypto
- Doesn’t apply to $R$-LWE or NTRU (unknown if $R$-LWE $\leq$ Ideal-SIVP)

Options

- Keep using $R$-LWE over cyclotomics
Which Rings To Use?

- Our results don’t give any guidance: they work within a single ring $R$, lower-bounding the hardness of $R$-LWE by $R$-Ideal-SIVP.
- We have no nontrivial relations between lattice problems over different rings. (Great open question!)

Progress on Ideal-SIVP

- Quantum poly-time $\exp(\tilde{O}(\sqrt{n}))$-Ideal-SIVP in prime-power cyclotomics (modulo heuristics) [CGS’14, BS’16, CDPR’16, CDW’17]
- Quite far from the (quasi-)poly($n$) factors typically used for crypto
- Doesn’t apply to $R$-LWE or NTRU (unknown if $R$-LWE $\leq$ Ideal-SIVP)

Options

- Keep using $R$-LWE over cyclotomics
- Use $R$-LWE over (slower) rings like $\mathbb{Z}[X]/(X^p - X - 1)$ [BCLvV’16]
Which Rings To Use?

- Our results don’t give any guidance: they work within a single ring $R$, lower-bounding the hardness of $R$-LWE by $R$-Ideal-SIVP.
- We have no nontrivial relations between lattice problems over different rings. (Great open question!)

Progress on Ideal-SIVP

- Quantum poly-time $\exp(\tilde{O}(\sqrt{n}))-\text{Ideal-SIVP}$ in prime-power cyclotomics (modulo heuristics) [CGS’14, BS’16, CDPR’16, CDW’17]
- Quite far from the (quasi-)poly$(n)$ factors typically used for crypto
- Doesn’t apply to $R$-LWE or NTRU (unknown if $R$-LWE $\leq$ Ideal-SIVP)

Options

- Keep using $R$-LWE over cyclotomics
- Use $R$-LWE over (slower) rings like $\mathbb{Z}[X]/(X^p - X - 1)$ [BCLvV’16]
- Use ‘higher rank’ problem Module-LWE over cyclotomics/others
Overview of LWE Reduction

Theorem: quantumly, \((n/\alpha)\text{-SIVP} \leq \text{decision-LWE}_{q,\alpha} \quad \forall \, q \geq \sqrt{n/\alpha}\)
Overview of LWE Reduction

- **Theorem:** quantumly, \((n/\alpha)\text{-SIVP} \leq \text{decision-}LWE_{q,\alpha} \quad \forall q \geq \sqrt{n/\alpha}

- **Reduction strategy:** ‘play with’ \(\alpha\), detect when it decreases.
Overview of LWE Reduction

▶ **Theorem:** quantumly, \((n/\alpha)\text{-SIVP} \leq \text{decision-LWE}_{q,\alpha} \quad \forall q \geq \sqrt{n/\alpha}\)

▶ **Reduction strategy:** ‘play with’ \(\alpha\), detect when it decreases.

Suppose \(\mathcal{O}\) solves \(\text{decision-LWE}_{q,\alpha}\) with non-negligible advantage. Define

\[
p(\beta) = \Pr[\mathcal{O} \text{ accepts on } \text{LWE}_{q,\exp(\beta)} \text{ samples}].
\]
Overview of LWE Reduction

- **Theorem:** quantumly, \((n/\alpha)\)-SIVP \(\leq\) decision-LWE\(_{q,\alpha}\) \(\forall q \geq \sqrt{n/\alpha}\)

- **Reduction strategy:** ‘play with’ \(\alpha\), detect when it decreases.

Suppose \(\mathcal{O}\) solves decision-LWE\(_{q,\alpha}\) with non-negl advantage. Define

\[p(\beta) = \Pr[\mathcal{O} \text{ accepts on } \text{LWE}_{q,\exp(\beta)} \text{ samples}].\]
Overview of LWE Reduction

**Theorem:** quantumly, \((n/\alpha)\text{-SIVP} \leq \text{decision-LWE}_{q,\alpha} \quad \forall q \geq \sqrt{n}/\alpha\)

**Reduction strategy:** ‘play with’ \(\alpha\), detect when it decreases.

Suppose \(\mathcal{O}\) solves decision-LWE\(_{q,\alpha}\) with non-negl advantage. Define

\[
p(\beta) = \Pr[\mathcal{O} \text{ accepts on } \text{LWE}_{q,\exp(\beta)} \text{ samples}].
\]

**Key Properties**

1. \(p(\beta)\) is ‘smooth’ (Lipschitz) because \(D_{\sigma}, D_{\tau}\) are \((\frac{\tau}{\sigma} - 1)\)-close.
Overview of LWE Reduction

▶ **Theorem:** quantumly, \((n/\alpha)\text{-SIVP} \leq \text{decision-LWE}_{q,\alpha} \quad \forall q \geq \sqrt{n/\alpha}

▶ **Reduction strategy:** ‘play with’ \(\alpha\), detect when it decreases.

Suppose \(O\) solves decision-LWE\(_{q,\alpha}\) with non-negl advantage. Define

\[
p(\beta) = \Pr[O \text{ accepts on LWE}_{q,\exp(\beta)} \text{ samples}].
\]

**Key Properties**

1. \(p(\beta)\) is ‘smooth’ (Lipschitz) because \(D_\sigma, D_\tau\) are \((\frac{\tau}{\sigma} - 1)\)-close.

2. For all \(\beta \geq \log n\), \(p(\beta) \approx p(\infty) = \Pr[O \text{ accepts on uniform samples}],\) because huge Gaussian error is near-uniform mod \(q\mathbb{Z}\).
Overview of LWE Reduction

- **Theorem:** quantumly, $(n/\alpha)$-SIVP $\leq$ decision-LWE$_{q,\alpha}$ $\forall q \geq \sqrt{n/\alpha}$

- **Reduction strategy:** ‘play with’ $\alpha$, detect when it decreases.

Suppose $\mathcal{O}$ solves decision-LWE$_{q,\alpha}$ with non-negl advantage. Define

$$p(\beta) = \Pr[\mathcal{O} \text{ accepts on } \text{LWE}_{q,\exp(\beta)} \text{ samples}].$$

**Key Properties**

1. $p(\beta)$ is ‘smooth’ (Lipschitz) because $D_\sigma, D_\tau$ are $(\frac{\tau}{\sigma} - 1)$-close.

2. For all $\beta \geq \log n$, $p(\beta) \approx p(\infty) = \Pr[\mathcal{O} \text{ accepts on uniform samples}]$, because huge Gaussian error is near-uniform mod $q\mathbb{Z}$.

3. $p(\log \alpha) - p(\infty)$ is noticeable, so there is a noticeable change in $p$ somewhere between $\log \alpha$ and $\log n$. 
Exploiting the Oracle

- **Theorem:** quantumly, $(n/\alpha)$-SIVP $\leq$ decision-LWE$_{q,\alpha}$ $\forall$ $q \geq \sqrt{n}/\alpha$
Exploiting the Oracle

**Theorem:** quantumly, \((n/\alpha)\text{-SIVP} \leq \text{decision-LWE}_{q,\alpha} \quad \forall \ q \geq \sqrt{n/\alpha}

**Classical part of [Regev’05] reduction:**

\[
\begin{align*}
\text{BDD}_{L^*}, \text{dist } d & \quad + \quad D_{L,r} \text{ samples} \\
\Rightarrow \quad \text{LWE}_{q,\alpha} \text{ samples} \\
\alpha &= dr/q
\end{align*}
\]
Exploiting the Oracle

▶ **Theorem:** quantumly, \((n/\alpha)\text{-SIVP} \leq \text{decision-LWE}_{q,\alpha} \quad \forall q \geq \sqrt{n/\alpha}\)

▶ Classical part of [Regev’05] reduction:

\[
\text{BDD}_{L^*, \text{dist } d} + \text{D}_{L,r} \text{ samples} \implies \text{LWE}_{q,\alpha} \text{ samples}
\]

\[\alpha = dr/q\]

\((\text{D}_{L,r} \text{ samples come from previous iteration, quantumly. They’re eventually narrow enough to solve SIVP on } L.\))
Exploiting the Oracle

▶ **Theorem:** quantumly, \((n/\alpha)\text{-SIVP} \leq \text{decision-LWE}_{q,\alpha} \forall q \geq \sqrt{n/\alpha}

▶ Classical part of [Regev’05] reduction:

\[ \text{BDD}_{\mathcal{L}^*}, \text{dist } d \quad + \quad D_{\mathcal{L},r} \text{ samples} \quad \Rightarrow \quad \text{LWE}_{q,\alpha} \text{ samples} \]

\[ \alpha = dr/q \]

▶ Idea: perturb \( t \), use \( \mathcal{O} \) to check whether we’re closer to \( \mathcal{L}^* \) by how \( \alpha = dr/q \) changes.

We get a ‘suffix’ of \( p(\cdot) \).
Extending to the Ring Setting

- The LWE proof relies on 1-parameter BDD distance $d \equiv$ error rate $\alpha$
Extending to the Ring Setting

- The LWE proof relies on 1-parameter BDD distance \( d \leftrightarrow \) error rate \( \alpha \)
- \( R \)-LWE proof has \( n \)-parameter BDD offset \( e \leftrightarrow \) params \( \alpha = (\alpha_i) \).
  Gaussian error rate of \( \alpha_i \) in the \( i \)th dimension.
Extending to the Ring Setting

- The LWE proof relies on 1-parameter BDD distance $d \Leftrightarrow$ error rate $\alpha$.
- $R$-LWE proof has $n$-parameter BDD offset $e \Leftrightarrow$ params $\alpha = (\alpha_i)$. Gaussian error rate of $\alpha_i$ in the $i$th dimension.
- Classical part of [LPR’10] reduction:

\[
\text{BDD}_{\mathcal{I}^*}, \text{offset } e \quad + \quad D_{\mathcal{I},r} \text{ samples} \quad \Longrightarrow \quad R\text{-LWE}_{q,\alpha} \text{ samples}
\]

\[
\alpha_i = |e_i| r_i / q
\]
Extending to the Ring Setting

- The LWE proof relies on 1-parameter BDD distance \( d \leftrightarrow \) error rate \( \alpha \)
- \( R \)-LWE proof has \( n \)-parameter BDD offset \( e \leftrightarrow \) params \( \alpha = (\alpha_i) \).
  Gaussian error rate of \( \alpha_i \) in the \( i \)th dimension.
- Classical part of \([LPR'10]\) reduction:

  \[
  BDD_{I^*}, \text{ offset } e + D_{I,r} \text{ samples} \implies R\text{-LWE}_{q,\alpha} \text{ samples}
  \]

  \( \alpha_i = |e_i| r_i/q \)

- Now oracle’s acceptance prob. is \( p(\beta) \), mapping \((\mathbb{R}^+)^n \rightarrow [0, 1] \).
  - \( \lim_{\beta_i \rightarrow \infty} p(\beta) = p(\infty) \): huge error in one dim is ‘smooth’ mod \( R^\vee \).
Extending to the Ring Setting

The LWE proof relies on 1-parameter BDD distance $d \Leftrightarrow$ error rate $\alpha$

$R$-LWE proof has $n$-parameter BDD offset $e \Leftrightarrow$ params $\alpha = (\alpha_i)$. Gaussian error rate of $\alpha_i$ in the $i$th dimension.

Classical part of [LPR’10] reduction:

Now oracle’s acceptance prob. is $p(\beta)$, mapping $(\mathbb{R}^+)^n \rightarrow [0, 1]$.

- $\lim_{\beta_i \rightarrow \infty} p(\beta) = p(\infty)$: huge error in one dim is ‘smooth’ mod $R^\vee$.
- **Problem:** Reduction never produces spherical error (all $\alpha_i$ equal), so it’s hard to get anything useful from $O$.
Extending to the Ring Setting

- The LWE proof relies on 1-parameter BDD distance $d \Leftrightarrow$ error rate $\alpha$
- $R$-LWE proof has $n$-parameter BDD offset $e \Leftrightarrow$ params $\alpha = (\alpha_i)$. Gaussian error rate of $\alpha_i$ in the $i$th dimension.

- Classical part of [LPR’10] reduction:

  \[
  \text{BDD}_{\mathcal{I}^*}, \text{offset } e \quad \quad D_{\mathcal{I},r} \text{ samples} \quad \quad R\text{-LWE}_{q,\alpha} \text{ samples}
  \]\[
  \alpha_i = |e_i| r_i / q
  \]

- Now oracle’s acceptance prob. is $p(\beta)$, mapping $(\mathbb{R}^+)^n \rightarrow [0, 1]$.
  - $\lim_{\beta_i \to \infty} p(\beta) = p(\infty)$: huge error in one dim is ‘smooth’ mod $R^\vee$.
  - **Problem**: Reduction never* produces spherical error (all $\alpha_i$ equal), so it’s hard to get anything useful from $\mathcal{O}$.
  - **Solution** from [LPR’10]: randomize the $\alpha_i$: increase by $n^{1/4}$ factor.
Extending to the Ring Setting

- The LWE proof relies on 1-parameter BDD distance $d \Leftrightarrow$ error rate $\alpha$
- $R$-LWE proof has $n$-parameter BDD offset $e \Leftrightarrow$ params $\alpha = (\alpha_i)$. Gaussian error rate of $\alpha_i$ in the $i$th dimension.
- Classical part of [LPR’10] reduction:

$$\begin{align*}
\text{BDD}_{I^*}, \text{offset } e & \quad + \quad D_{I,x} \text{ samples} \\
R\text{-LWE}_{q,\alpha} \text{ samples} & \quad \Rightarrow \\
\alpha_i & = |e_i|r_i/q
\end{align*}$$

- Now oracle’s acceptance prob. is $p(\beta)$, mapping $(\mathbb{R}^+)^n \rightarrow [0, 1]$.
  - $\lim_{\beta_i \rightarrow \infty} p(\beta) = p(\infty)$: huge error in one dim is ‘smooth’ mod $R^\vee$.
  - **Problem**: Reduction never* produces spherical error (all $\alpha_i$ equal), so it’s hard to get anything useful from $\mathcal{O}$.
  - **Solution** from [LPR’10]: randomize the $\alpha_i$: increase by $n^{1/4}$ factor.
  - **Improvement**: randomization increases $\alpha_i$ by only $\omega(1)$ factor.
Final Thoughts and Open Problems

- \text{decision-} R\text{-LWE}_{q,\alpha} \text{ is worst-case hard for any ring } R = \mathcal{O}_K, \text{ mod } q

Open Questions

1. Hardness for spherical error: ⋆ Avoid $n^{1/4}$ degradation in $\alpha$? ⋆ Support unbounded samples?
2. Nontrivially relate Ideal-SIVP or Ring-LWE for different rings?
3. Classical reduction matching params of quantum reductions?
Final Thoughts and Open Problems

- \texttt{decision-}R-L\textsc{we}_{q,\alpha} \text{ is worst-case hard for any ring } R = \mathcal{O}_K, \text{ mod } q

- \texttt{decision-}L\textsc{we}_{q,\alpha} \text{ is hard for any } q; \text{ approx factor independent of } q
Final Thoughts and Open Problems

- decision-$R$-LWE$_{q,\alpha}$ is worst-case hard for any ring $R = \mathcal{O}_K$, mod $q$
- decision-LWE$_{q,\alpha}$ is hard for any $q$; approx factor independent of $q$

Open Questions

1. Hardness for spherical error:
   - Avoid $n^{1/4}$ degradation in $\alpha$?

2. Support unbounded samples?

3. Nontrivially relate Ideal-SIVP or Ring-LWE for different rings?

4. Classical reduction matching params of quantum reductions?
Final Thoughts and Open Problems

- decision-$R$-LWE$_{q,\alpha}$ is worst-case hard for any ring $R = \mathcal{O}_K$, mod $q$
- decision-LWE$_{q,\alpha}$ is hard for any $q$; approx factor independent of $q$

Open Questions

1. Hardness for spherical error:
   - Avoid $n^{1/4}$ degradation in $\alpha_i$?
   - Support unbounded samples?
Final Thoughts and Open Problems

- decision-$R$-LWE$_{q,\alpha}$ is worst-case hard for any ring $R = \mathcal{O}_K$, mod $q$
- decision-LWE$_{q,\alpha}$ is hard for any $q$; approx factor independent of $q$

Open Questions

1. Hardness for spherical error:
   - Avoid $n^{1/4}$ degradation in $\alpha_i$?
   - Support unbounded samples?

2. Nontrivially relate Ideal-SIVP or Ring-LWE for different rings?
Final Thoughts and Open Problems

- decision-$R$-LWE$_{q,\alpha}$ is worst-case hard for any ring $R = \mathcal{O}_K$, mod $q$
- decision-LWE$_{q,\alpha}$ is hard for any $q$; approx factor independent of $q$

Open Questions

1. Hardness for spherical error:
   - Avoid $n^{1/4}$ degradation in $\alpha_i$?
   - Support unbounded samples?

2. Nontrivially relate Ideal-SIVP or Ring-LWE for different rings?

3. Classical reduction matching params of quantum reductions?