Theoretical Hardness of Algebraically Structured Learning With Errors

PhD Defense

Katharina Boudgoust

Univ Rennes, CNRS, IRISA

16th November 2021
Provably secure **public-key** cryptography needs **well-defined** assumptions in the form of **mathematical problems**.

**Current problems:**
- **Discrete Logarithm**
- **Factoring**

⚠️ ∃ poly-time **quantum** algorithm [Sho97].

**Sources for assumedly quantum-resistant problems:**
- **Euclidean Lattices**
- **Codes**
- **Isogenies**
- **Multivariate Systems**
- ⚫️ my research
An Euclidean lattice $\Lambda$ of rank $n$ with a basis $B = (b_j)_{1 \leq j \leq n}$ is given by

$$\Lambda(B) = \left\{ \sum_{j=1}^{n} z_j b_j : z_j \in \mathbb{Z} \right\}.$$ 

The minimum of $\Lambda$ is

$$\lambda_1(\Lambda) := \min_{v \in \Lambda \backslash \{0\}} \|v\|.$$ 

The approximate shortest vector problem (SVP$_\gamma$) for $\gamma \geq 1$ asks to find a vector $w$ such that $\|w\| \leq \gamma \lambda_1(\Lambda)$.

**Conjecture:**
There is no polynomial-time classical or quantum algorithm that solves SVP$_\gamma$ and its variants to within polynomial factors.

⚠️ Hard to build cryptography on top of SVP$_\gamma$. 

---

Katharina Boudgoust
PhD Defense
16th November 2021 3 / 30
Lattice-Based Cryptography

💡 Idea: use intermediate problems!

(Main) Mathematical Problems:
- Short Integer Solution [Ajt96]
- NTRU [HPS98]
- Learning With Errors [Reg05]
  - Strong security guarantees
    At least as hard as variants of SVP\_γ
    for any Euclidean lattice
  - Efficiency
    Linear algebra & parallelizable
  - Many cryptographic applications
    Fully Homomorphic Encryption,
    E-Voting, Zero-Knowledge Proofs, ...
NIST Competition ♻

Started in 2016: NIST project to define new standards for post-quantum cryptography. A majority (5 out of 7) of the finalist candidates are based on lattice problems. Several among them (3 out of 5) are based on (variants of) Learning With Errors.

Public Key Encryption 🔐
- Kyber: (module variant of) Learning With Errors
- Saber: (deterministic module variant of) Learning With Errors

Digital Signature 🖋
- Dilithium: (module variant of) Learning With Errors

Observation ❞

Lattice-based cryptography, and in particular Learning With Errors, plays a key role in designing post-quantum cryptography.
Outline

1 Introduction

2 Learning With Errors

3 Module Learning With Errors
   • Binary Hardness
   • Classical Hardness

4 Partial Vandermonde Learning With Errors
   • Hard Problems
   • PASS Encrypt

5 Conclusion and Perspectives
Learning With Errors
The Learning With Errors (LWE) Problem [Reg05]

Set $\mathbb{Z}_q := \mathbb{Z}/q\mathbb{Z}$ for some integer $q$.

Given $A \sim \text{Unif}(\mathbb{Z}_q^{m \times d})$, $b \in \mathbb{Z}_q^m$, $s \sim \text{DistrS}$ over $\mathbb{Z}^d$, $e \sim \text{DistrE}$ over $\mathbb{Z}^m$ such that

$$A \cdot s + e = b \mod q.$$ 

Search: find secret $s$

Decision: distinguish from $(A, b)$, where $b \sim \text{Unif}(\mathbb{Z}_q^m)$

Standard: $\text{DistrS} = \text{Unif}(\mathbb{Z}_q^d)$, $\text{DistrE} = \text{Gauss}(\mathbb{Z}_q^m)$

Binary Secret: $\text{DistrS} = \text{Unif}(\{0, 1\}^d)$, $\text{DistrE} = \text{Gauss}(\mathbb{Z}_q^m)$

Rounding: $\text{DistrS} = \text{Unif}(\mathbb{Z}_q^d)$, $\text{DistrE} \equiv \text{deterministic}$ depends on $A$ & $s$

⚠️ Storage $m(d + 1) \log_2 q$ bits ~ $\tilde{O}(\lambda^2)$

⚠️ Computation $O(md)$ ~ $O(\lambda^2)$

$\lambda$ security parameter
Reduce needed storage of the public key and speed-up the computations by adding **structure**!

$\Rightarrow$ structured variants of Learning With Errors

$\Rightarrow$ my research
My Contributions

I. Study of existing structured variants
   1. Module Learning With Errors with a binary secret
   2. Classical hardness of Module Learning With Errors

II. Proposing new structured variants
   3. Middle-Product Learning With Rounding
   4. Partial Vandermonde Learning With Errors

III. Building public key encryption
   5. Based on MP-LWR (3.)
   6. PASS Encrypt, related to (4.)
Hardness of Module Learning With Errors

Joint work with C. Jeudy, A. Roux-Langlois and W. Wen
Ring of Integers over a Number Field

Idea: replace $\mathbb{Z}$ by the ring of integers $R$ of some number field $K$ of degree $n$.
Think of $R = \mathbb{Z}[x]/\langle x^n + 1 \rangle$ and $K = \mathbb{Q}[x]/\langle x^n + 1 \rangle$ with $n = 2^\ell$.

Before: multiplication of two integers $a \cdot s \in \mathbb{Z}$
Now: multiplication of two polynomials $a \cdot s \in R$ modulo $x^n + 1$

Note: defines matrix-vector multiplication over $\mathbb{Z}$, denoted by $\text{Rot}(a) \cdot s$.

Example: $n = 4$ thus $R = \mathbb{Z}[x]/\langle x^4 + 1 \rangle$

$$m = 4 \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \\ a_{41} & a_{42} \end{bmatrix}, \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} \in R$$

$n d = 8$

structured
Module Learning With Errors (Module-LWE, M-LWE) [BGV12, LS15]

Let \( R \) be the ring of integers of some number field \( K \) of degree \( n \), set \( R_q = R/qR \).

Given \( A \sim \text{Unif}(R_{q}^{m \times d}) \), \( b \in R_q^m \), \( s \sim \text{DistrS} \) over \( R^d \), \( e \sim \text{DistrE} \) over \( R^m \) such that

\[
A \cdot s + e = b \mod q.
\]

Search: find secret \( s \)
Decision: distinguish from \( (A, b) \), where \( b \sim \text{Unif}(R_{q}^m) \)

Standard: \( \text{DistrS} = \text{Unif}(R_q^d) \) \( \text{DistrE} = \text{Gauss}(R_q^m) \)
Binary Secret: \( \text{DistrS} = \text{Unif}\{0, 1\}^{dn} \) \( \text{DistrE} = \text{Gauss}(R^m) \)

For \( d = 1 \), we call this Ring-LWE [SSTX09, LPR10].
Motivation: Theory vs. Praxis

Lattice Problem
SVP$_{\gamma}$

[Reg05]

Standard LWE

[GKPV10] [BLP$^{+}$13, Mic18]

Binary Secret LWE

Public Key Crypto

Module Lattice Problem
Mod-SVP$_{\gamma}$

[LS15]

Standard M-LWE

Binary Secret M-LWE

Public Key Crypto

Contributions:

1. Extending and Improving [GKPV10] to M-LWE
2. Extending [BLP$^{+}$13] to M-LWE
3. Generalizing both proofs to bounded secrets

K number field with ring of integers $R$
$M$ module over $R \cong$ module lattice

$K$ number field with ring of integers $R$
$M$ module over $R \cong$ module lattice

Public Key Crypto

16th November 2021 14 / 30
Hardness of Module-LWE with Binary Secrets (Cyclotomics)

Standard M-LWE $\rightarrow$ Binary Secret M-LWE

- modulus $q$
- ring degree $n$
- secret $s' \mod q$
- Gaussian width $\alpha$
- rank $k$
- modulus $q$
- ring degree $n$
- secret $s \mod 2$
- Gaussian width $\beta$
- rank $d$

<table>
<thead>
<tr>
<th>Property</th>
<th>Contribution 1</th>
<th>Contribution 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>LWE analogue</td>
<td>[GKPV10] using RD*</td>
<td>[BLP+13]</td>
</tr>
<tr>
<td>minimal rank $d$</td>
<td>$k \log_2 q + \Omega(\log_2 n)$</td>
<td>$(k + 1) \log_2 q + \omega(\log_2 n)$</td>
</tr>
<tr>
<td>noise ratio $\beta/\alpha$</td>
<td>$O(n^2 \sqrt{md})$</td>
<td>$O(n^2 \sqrt{d})$</td>
</tr>
<tr>
<td>conditions on $q$</td>
<td>prime</td>
<td>number-theoretic restrictions</td>
</tr>
<tr>
<td>decision/search</td>
<td>search</td>
<td>decision</td>
</tr>
</tbody>
</table>

$\Rightarrow$ both proofs have their (dis)advantages

* Rényi Divergence

$q$ prime and $q = 5 \mod 8$
Proof of Hardness of Module-LWE with Binary Secrets

The secret $s \in \mathbb{R}^d_2$ is binary and the secret $s' \in \mathbb{R}^k_q$ is modulo $q$.
Improved Noise Flooding via Rényi Divergence 1/2

Let $P, Q$ be discrete probability distributions.

In [GKPV10]: Statistical Distance

$$\text{SD}(P, Q) = \frac{1}{2} \sum_{x \in \text{Supp}(P)} |P(x) - Q(x)|$$

In our work: Rényi Divergence

$$\text{RD}(P, Q) = \sum_{x \in \text{Supp}(P)} \frac{P(x)^2}{Q(x)}$$

Example: two Gaussians $D_\beta$ and $D_{\beta, s}$

$$\text{RD}(D_\beta, D_{\beta, s}) = \exp \left( \frac{2\pi \|s\|^2}{\beta^2} \right)$$

$$\text{SD}(D_\beta, D_{\beta, s}) = \frac{\sqrt{2\pi} \|s\|}{\beta}$$
Both fulfill the **probability preservation property** for an event $E$:

- **[GKPV10]:** $P(E) \leq SD(P, Q) + Q(E)$ (additive)
- **Our work:** $P(E)^2 \leq RD(P, Q) \cdot Q(E)$ (multiplicative)

We need: $Q(E)$ negligible $\Rightarrow P(E)$ negligible

Thus: $SD(P, Q) =^!$ negligible and $RD(P, Q) =^!$ constant

Back to example: two Gaussians $D_\beta$ and $D_\beta, s$ with $\|s\| \leq \alpha$

\[
SD(D_\beta, D_\beta, s) = \frac{\sqrt{2\pi}\|s\|}{\beta} \Rightarrow \frac{\alpha}{\beta} \leq \text{negligible}
\]
\[
RD(D_\beta, D_\beta, s) = \exp\left(\frac{2\pi\|s\|^2}{\beta^2}\right) \approx 1 + \frac{2\pi\|s\|^2}{\beta^2} \Rightarrow \frac{\alpha}{\beta} \leq \text{constant}
\]

⚠ Rényi Divergence only for search problems.
Contributions:

4. Classical reduction, modulus $q$ is poly-small, but linear rank extending [Pei09] and [BLP+13] to M-LWE and combining them with [PRS17]*

*Pseudorandomness of ring-LWE for any ring and modulus* C. Peikert, O. Regev and N. Stephen-Davidowitz
Classical Hardness of Module-LWE

High level idea following [BLP⁺13]:

- **Step 1**: Classical reduction from decision Mod-SVP_{γ} to decision Module-LWE with exponentially large modulus $q$
  - Extending [Pei09] (classical) and [PRS17] (decision) to the module variants.

- **Step 2**: Reduction from Module-LWE with uniform secret to Module-LWE with binary secret
  - Using either Contribution 1 or 2 presented before.
  - Leftover hash lemma requires rank $\geq \log(q) = \log(2^n) = n$.

- **Step 3**: Modulus reduction from exponentially large to polynomially small modulus for Module-LWE with binary secret
  - Using [AD17], computing bounds on singular values of rotation matrix, loss in the reduction depends on the norm of the secret.
Partial Vandermonde Learning With Errors

Joint work with A. Sakzad and R. Steinfeld
Under submission
Partial Vandermonde Transform \([HPS^{+}14, \text{LZA18}]\)

Again: Let \(R\) be the ring of integers of a number field \(K\) of degree \(n\).
Think of \(R = \mathbb{Z}[x]/\langle x^n + 1 \rangle\) and \(K = \mathbb{Q}[x]/\langle x^n + 1 \rangle\) with \(n = 2^\ell\).

Choose \(q\) prime such that \(q = 1 \mod 2n\):
- \(x^n + 1 = \prod_{j=1}^{n}(x - \omega_j)\), where \(\omega_j\) is a primitive \(2n\)-th root of unity in \(\mathbb{Z}_q\)

The set \(\{\omega_j\}_{j=1,...,n}\) defines the **Vandermonde transform** \(V: R \rightarrow \mathbb{Z}_q^n\), where

\[
V \cdot a = \begin{bmatrix}
1 & \omega_1 & \cdots & \omega_1^{n-1} \\
1 & \omega_2 & \cdots & \omega_2^{n-1} \\
1 & \omega_3 & \cdots & \omega_3^{n-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & \omega_n & \cdots & \omega_n^{n-1}
\end{bmatrix} \cdot \begin{bmatrix}
a_1 \\
a_2 \\
a_3 \\
\vdots \\
a_n
\end{bmatrix} = \begin{bmatrix}
b_1 \\
b_2 \\
b_3 \\
\vdots \\
b_n
\end{bmatrix} = b \mod q.
\]

**Observation:** \(b = (b_j)_{j=1,...,n}\) uniquely defines \(a\) and vice versa. \((V^{-1}\text{ exists})\)

**Question:** What happens if we only provide \(t\) out of \(n\) coefficients? (say half)

**Note:** For \(\Omega \subseteq \{\omega_j\}_{j=1,...,n}\) write \(V_\Omega \cdot a = b\). \((\text{partial Vandermonde transform})\)
Partial Vandermonde Problems

Choose a random subset $\Omega \subseteq \{\omega_j\}_{j=1,...,n}$ of size $|\Omega| = t$.

**Partial Vandermonde knapsack problem (PV-Knap):** Sample $e \sim \text{DistrE}$ over $\mathbb{Z}^n$ defining

$$V_{\Omega} \rightarrow e = b \pmod{q}.$$

Search: find $e$

**Partial Vandermonde Learning With Errors (PV-LWE):** Sample $s \sim \text{DistrS}$ over $\mathbb{Z}^t$ and $e \sim \text{DistrE}$ over $\mathbb{Z}^n$ defining

$$V_{\Omega}^T \rightarrow s + e = b \pmod{q}.$$

Search: find $e$ (and secret $s$)

**Conjecture:** Hard to solve if $\text{DistrE}$ provides elements of small norm.
Equivalence of PV-Knap and PV-LWE

Let $t = n/2$ and set $\mathcal{P}_t = \{\Omega \subseteq \{\omega_j\}_{j=1,\ldots,n} : |\Omega| = t\}$.

Property 1: $V_{\Omega}$ defines a ring homomorphism from $R$ to $\mathbb{Z}_q^t$:

$$V_{\Omega}(a \cdot b) = (V_{\Omega}a) \circ (V_{\Omega}b)$$

(component-wise multiplication $\circ$)

Property 2: $\Omega^c = \{\omega_j\}_{j \not\in \Omega}$ defines the complement partial Vandermonde transform $V_{\Omega^c}$.

Given $V_{\Omega}a$ and $V_{\Omega^c}a$, we can recover $a$.

Property 3: For every $\Omega \in \mathcal{P}_t$, there exists a $\Omega' \in \mathcal{P}_t$ such that

$$V_{\Omega'} \cdot V_{\Omega}^T = 0 \in \mathbb{Z}_q^{t \times t}.$$  

(parity check matrix, \(\triangle\) only for power-of-two cyclotomics)

Lemma (Adapted [MM11, Sec. 4.2])

Let $\psi$ denote a distribution over $\mathbb{Z}_n \cong R$. There is an efficient reduction from PV-LWE$\psi$ to PV-Knap$\psi$, and vice versa.

Idea: Given $(V_{\Omega}, b)$, with $b = V_{\Omega}^T s + e$. Compute $\Omega'$ such that $V_{\Omega'} \cdot V_{\Omega}^T = 0$.

Then, $b' := V_{\Omega'} b = V_{\Omega'} e$ is an instance of PV-Knap.
PASS Encrypt [HS15]

<table>
<thead>
<tr>
<th>[HS15]</th>
<th>Our work</th>
</tr>
</thead>
<tbody>
<tr>
<td>deterministic</td>
<td>randomized</td>
</tr>
<tr>
<td>without proof of security</td>
<td>with proof of security</td>
</tr>
<tr>
<td>fixed $V_{\Omega}$</td>
<td>random $V_{\Omega}$</td>
</tr>
</tbody>
</table>

Let $p \ll q$ be two primes, $m \in \{0, 1\}^n$, $\psi$ a distribution over $\mathbb{Z}^n$ and $t = n/2$.

KeyGen($1^\lambda$): sample $f \leftarrow \psi$ and $\Omega \leftarrow \text{Unif}(\mathcal{P}_t)$; return $sk = f$ and $pk = (\Omega, V_{\Omega}f)$

Enc($pk, m$): sample $r, s \leftarrow \psi$; set $r' = pr$ and $s' = m + ps$

\[ e_1 = (pk \circ V_{\Omega}r') + V_{\Omega}s' \]
\[ e_2 = V_{\Omega^c}r' \]
\[ e_3 = V_{\Omega^c}s' \]

return $c = (e_1, e_2, e_3)$

Dec($sk, c$): compute $c' = (V_{\Omega^c}sk \circ e_2) + e_3$ and combine with $e_1$ to $c'' \in \mathbb{Z}^n$; return $V^{-1}c'' \mod p$.

Recall: $V_{\Omega}$ and $V_{\Omega^c}$ define $V$ and $V^{-1}$.

Correctness:

\[
\begin{align*}
  e_1 &= (V_{\Omega}f \circ V_{\Omega}r') + V_{\Omega}s' = V_{\Omega}(f \cdot r' + s') \\
  c' &= (V_{\Omega^c}sk \circ (V_{\Omega^c}r')) + V_{\Omega^c}s' = V_{\Omega^c}(f \cdot r' + s') \\
  V^{-1}(e_1 || c') &= V^{-1}(V(f \cdot r' + s')) = f \cdot pr + ps + m = m \mod p \\
\end{align*}
\]

if $f, r$ and $s$ are small enough
**PASS Encrypt [HS15]**

<table>
<thead>
<tr>
<th>[HS15]</th>
<th>Our work</th>
</tr>
</thead>
<tbody>
<tr>
<td>deterministic</td>
<td>randomized</td>
</tr>
<tr>
<td>without proof of security</td>
<td>with proof of security</td>
</tr>
<tr>
<td>fixed $\mathbf{V}_\Omega$</td>
<td>random $\mathbf{V}_\Omega$</td>
</tr>
</tbody>
</table>

Let $p \ll q$ be two primes, $m \in \{0,1\}^n$, $\psi$ a distribution over $\mathbb{Z}^n$ and $t = n/2$.

**KeyGen($1^\lambda$):** sample $f \leftarrow \psi$ and $\Omega \leftarrow \text{Unif}(\mathcal{P}_t)$; return $\text{sk} = f$ and $\text{pk} = (\Omega, \mathbf{V}_\Omega f)$

**Enc(pk, m):** sample $r, s \leftarrow \psi$; set $r' = pr$ and $s' = m + ps$

- $e_1 = (pk \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s' = \mathbf{V}_\Omega (f \cdot r' + s')$
- $e_2 = \mathbf{V}_\Omega e r'$
- $e_3 = \mathbf{V}_\Omega e s'$

return $c = (e_1, e_2, e_3)$

**Dec(sk, c):** compute $c' = (\mathbf{V}_\Omega \circ \text{sk} \circ e_2) + e_3$ and combine with $e_1$ to $c'' \in \mathbb{Z}_q^n$; return $\mathbf{V}^{-1} c'' \mod p$.

**Security:**

$e_1 = \mathbf{V}_\Omega (f \cdot r' + s')$ defines an instance of $\text{PV-Knap}$ with $\text{pk}, e_2$ and $e_3$ as additional information.

⇒ leaky variant of $\text{PV-Knap}$, that we call the **PASS problem**.

⚠️ PASS problem is tailored to PASS Encrypt!

❓ Reduce it from some more general problem?
Properties of PASS Encrypt

**Homomorphic properties:**

- **Addition:** \( \text{Enc}(pk, m_1) + \text{Enc}(pk, m_2) = \text{Enc}(pk, m_1 + m_2) \)

- **Multiplication:** \( \text{Enc}(pk, m_1) \circ \text{Enc}(pk, m_2) = \text{Enc}(pk, m_1 \cdot m_2) \)

⚠️ For \( \circ \), need of 1 additional cross-term and the decryption algorithm has to be changed.

**Efficiency:**

<table>
<thead>
<tr>
<th>Scheme</th>
<th>NTRU [HPS98]</th>
<th>P-LWE Regev [LP11]</th>
<th>PASS Encrypt</th>
</tr>
</thead>
<tbody>
<tr>
<td>(</td>
<td>c</td>
<td>+</td>
<td>pk</td>
</tr>
</tbody>
</table>

**Concrete Security:**

- **Known:** key recovery and randomness recovery attacks [HS15, DHSS20]

- **New:** plaintext recovery using hints attacks

💡 make use of leaky LWE estimator of Dachman-Soled et al. [DDGR20]
Conclusion and Perspectives
Conclusion

I. Study of existing structured variants
1. Module Learning With Errors with a binary secret
2. Classical hardness of Module Learning With Errors

II. Proposing new structured variants
3. Middle-Product Learning With Rounding
4. Partial Vandermonde Learning With Errors & Knapsack

III. Building public key encryption
5. Based on MP-LWR (3.)
6. PASS Encrypt, related to (4.)
Open Questions and Perspectives

I. Module LWE

Follow-ups 🙀

- General secret distributions (Entropic Secret Module-LWE)
- Small noise distributions (extending [MP13])

Open questions ❓

- Classical and binary hardness for smaller ranks, in particular rank equals 1 (Ring-LWE)
  - Avoid leftover hash lemma in the reduction?
  - Avoid exponentially large modulus in [Pei09]?
- Narrow gap between theoretical reductions and practical attacks

II. Partial Vandermonde LWE

Follow-ups 🙀

- Construct encryption scheme based only on PV-LWE / PV-Knap

Questions ❓

- Hardness of partial Vandermonde problems
  - Cryptanalysis?
  - Worst-case average-case reductions as for LWE?
- More cryptographic applications
Contributions

Published:

**CT-RSA’21** "On the Hardness of Module-LWE with Binary Secret" [HAL]
Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois & Weiqiang Wen.

**Asiacrypt’20** "Towards Classical Hardness of Module-LWE: The Linear Rank Case" [HAL]
Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois & Weiqiang Wen.

**Asiacrypt’19** "Middle-Product Learning with Rounding Problem and its Applications" [HAL]

Under Submission:

- **Vandermonde meets Regev: Public Key Encryption Schemes Based on Partial Vandermonde Problems.** Katharina Boudgoust, Amin Sakzad and Ron Steinfeld.

E-Print:

- **Compressed Linear Aggregate Signatures Based on Module Lattices** [IACR ePrint]
  Katharina Boudgoust and Adeline Roux-Langlois.

Thank you.
Martin R. Albrecht and Amit Deo.
Large modulus ring-lwe $\geq$ module-lwe.

Miklós Ajtai.
Generating hard instances of lattice problems (extended abstract).

Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan.
(leveled) fully homomorphic encryption without bootstrapping.

Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen.
Towards classical hardness of module-lwe: The linear rank case.

Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen.
On the hardness of module-lwe with binary secret.

Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé.
Classical hardness of learning with errors.
Katharina Boudgoust.
Theoretical hardness of algebraically structured learning with errors, 2021.

Abhishek Banerjee, Chris Peikert, and Alon Rosen.
Pseudorandom functions and lattices.

Olivier Bernard and Adeline Roux-Langlois.
Twisted-phs: Using the product formula to solve approx-svp in ideal lattices.

Ronald Cramer, Léo Ducas, and Benjamin Wesolowski.
Short stickelberger class relations and application to ideal-svp.

Long Chen, Zhenfeng Zhang, and Zhenfei Zhang.
On the hardness of the computational ring-lwr problem and its applications.

Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi.
LWE with side information: Attacks and concrete security estimation.


Elie Gouzien and Nicolas Sangouard. Factoring 2048 rsa integers in 177 days with 13436 qubits and a multimode memory, 2021.


Jeffrey Hoffstein and Joseph H. Silverman. 
Pass-encrypt: a public key cryptosystem based on partial evaluation of polynomials. 

Richard Lindner and Chris Peikert. 
Better key sizes (and attacks) for lwe-based encryption. 

Vadim Lyubashevsky, Chris Peikert, and Oded Regev. 
On ideal lattices and learning with errors over rings. 

Adeline Langlois and Damien Stehlé. 
Worst-case to average-case reductions for module lattices. 

Xingye Lu, Zhenfei Zhang, and Man Ho Au. 
Practical signatures from the partial fourier recovery problem revisited: A provably-secure and gaussian-distributed construction. 
Daniele Micciancio.

Daniele Micciancio.

Daniele Micciancio and Petros Mol.

Daniele Micciancio and Chris Peikert.

Chris Peikert.

Alice Pellet-Mary, Guillaume Hanrot, and Damien Stehlé.
Approx-svp in ideal lattices with pre-processing.

Chris Peikert and Zachary Pepin.
Algebraically structured lwe, revisited.

Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz.
Pseudorandomness of ring-lwe for any ring and modulus.

Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.

Miruna Rosca, Amin Sakzad, Damien Stehlé, and Ron Steinfeld.
Middle-product learning with errors.

Peter W. Shor.
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.