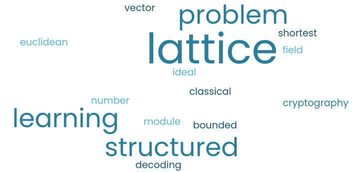
Theoretical Hardness of Algebraically Structured Learning With Errors

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

Hard Lattice Problems

An **Euclidean lattice** Λ of rank n with a basis $\mathbf{B} = (\mathbf{b}_j)_{1 \leq j \leq n}$ is given by

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

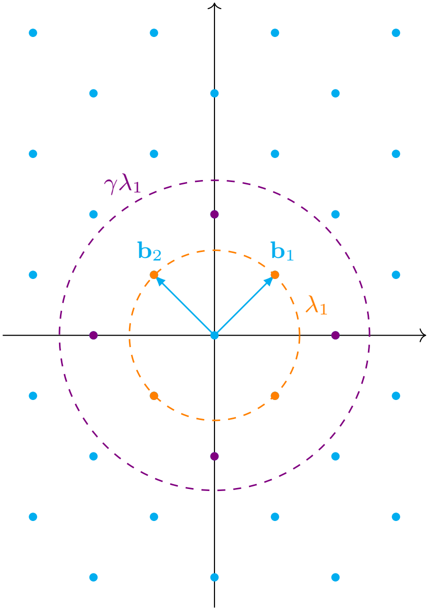
The **minimum** of Λ is

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

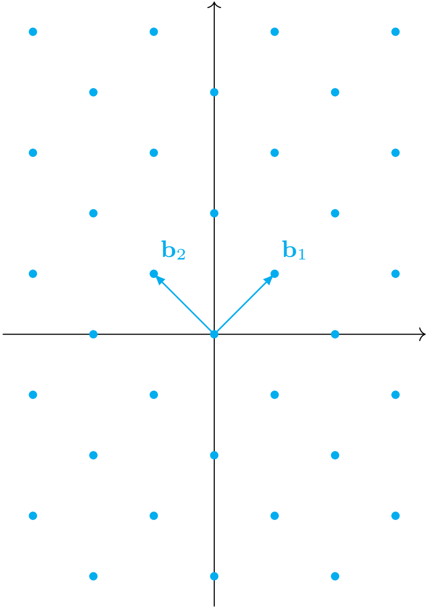
The **approximate shortest vector problem** (SVP_γ) for $\gamma \geq 1$ asks to find a vector $\mathbf{w}$ such that $\|\mathbf{w}\| \leq \gamma \lambda_1(\Lambda)$.

Conjecture:
There is no polynomial-time classical or quantum algorithm that solves SVP_γ and its variants to within polynomial factors.

⚠ Hard to build cryptography on top of SVP_γ.



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

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

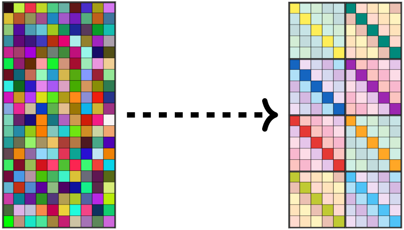
$$m\left\{ \underbrace{A}_{d} \right. , \quad A\, s + e = b \mod q.$$

Search:	find secret s	
Decision:	distinguish from (A , b),	where b $\sim$ Unif$(\mathbb{Z}_q^m)$
Standard:	DistrS $=$ Unif$(\mathbb{Z}_q^d)$	DistrE $=$ Gauss$(\mathbb{Z}^m)$
Binary Secret:	DistrS $=$ Unif$(\{0,1\}^d)$	DistrE $=$ Gauss$(\mathbb{Z}^m)$
Rounding:	DistrS $=$ Unif$(\mathbb{Z}_q^d)$	DistrE $\widehat{=}$ deterministic depends on A & s
⚠ Storage	$m(d+1)\log_2 q$ bits	$\sim \tilde{O}(\lambda^2)$
⚠ Computation	$O(md)$	$\sim O(\lambda^2)$

λ security parameter

Idea

Reduce needed storage of the public key
and speed-up the computations
by adding **structure**!



⇒ structured variants of Learning With Errors

my research

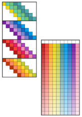
My Contributions

Asiacrypt'20
CT-RSA'21

I. Study of existing structured variants

1. **Module Learning With Errors with a binary secret**
2. **Classical hardness of Module Learning With Errors**

$$A \;,\; A \; s + e = b$$



II. Proposing new structured variants

3. Middle-Product Learning With Rounding
4. **Partial Vandermonde Learning With Errors**

Asiacrypt'19
& under submission

III. Building $\overbrace{\text{public key}}^{\textbf{provable secure}}$ 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 $x^n + 1$

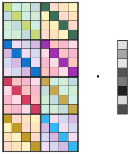
Note: defines matrix-vector multiplication over $\mathbb{Z}$, denoted by $\mathrm{Rot}(a) \cdot s$.

structured

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

$$m = 4 \left\{ \underbrace{\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \\ a_{41} & a_{42} \end{bmatrix}}_{d\,=\,2} \right. \cdot \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} \in R$$

$nm = 16$



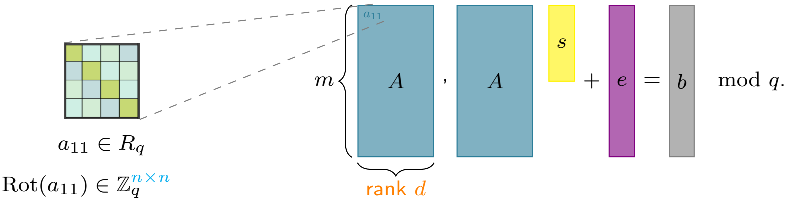
$\in \mathbb{Z}$

$nd = 8$

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 $\sim$ Unif$(R_q^{m\times d})$, b $\in R_q^m$, s $\sim$ DistrS over R^d, e $\sim$ DistrE over R^m such that

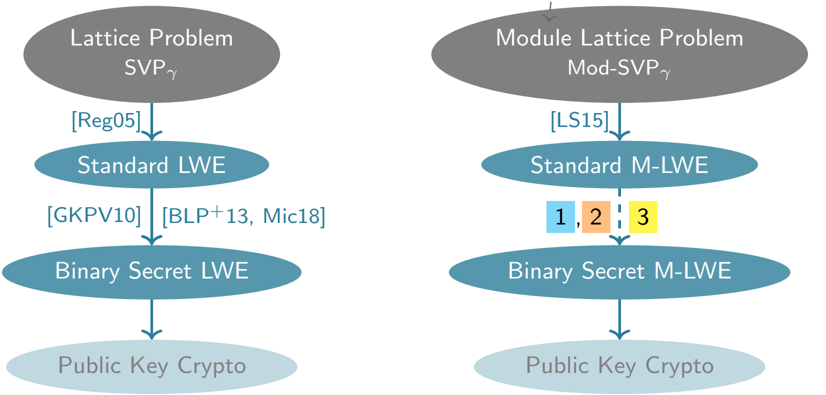


Search:	find secret s	
Decision:	distinguish from (A, b),	where b $\sim$ Unif(R_q^m)
Standard:	DistrS $=$ Unif(R_q^d)	DistrE $=$ Gauss(R^m)
Binary Secret:	DistrS $=$ Unif$(\{0,1\}^{dn})$	DistrE $=$ Gauss(R^m)

For $d = 1$, we call this Ring-LWE [SSTX09, LPR10].

Motivation: Theory vs. Praxis

K number field with ring of integers R
M module over $R \mathrel{\widehat{=}}$ module lattice



Contributions:

1	Extending and Improving [GKPV10] to M-LWE	[BJRW20] Asiacrypt'20
2	Extending [BLP$^+$13] to M-LWE	[BJRW21] CT-RSA'21
3	Generalizing both proofs to bounded secrets	[Bou21] PhD Thesis

Hardness of Module-LWE with Binary Secrets (Cyclotomics)

Standard M-LWE	$\rightarrow$	Binary Secret M-LWE
modulus q		modulus q
ring degree n		ring degree n
secret $\mathbf{s}'$ $\bmod q$		secret $\mathbf{s}$ $\bmod 2$
Gaussian width α		Gaussian width β
rank k		rank d

Property	Contribution 1	Contribution 2
LWE analogue	[GKPV10] using RD*	[BLP+13]
minimal rank d	$k \log_2 q + \Omega(\log_2 n)$	$(k+1) \log_2 q + \omega(\log_2 n)$
noise ratio β/α	$O(n^2\sqrt{m}d)$	$O(n^2\sqrt{d})$
conditions on q	prime	number-theoretic restrictions
decision/search	search	decision

$\gg$ **practice**

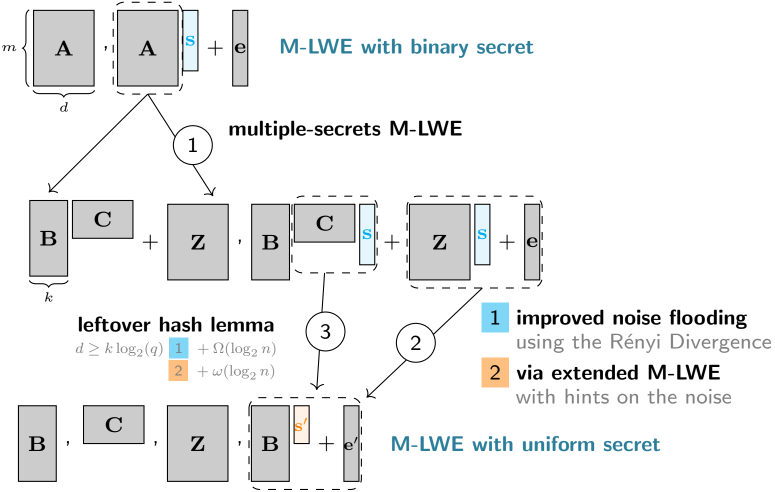
pow-of-two:
q prime and
$q = 5 \bmod 8$

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

* Rényi Divergence

Proof of Hardness of Module-LWE with Binary Secrets

The secret $\mathbf{s} \in R_2^d$ is binary and the secret $\mathbf{s}' \in R_q^k$ is modulo q.



Improved Noise Flooding via Rényi Divergence 1/2

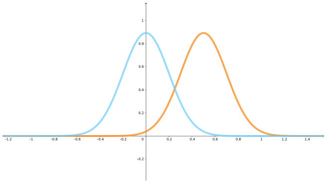
Let P, Q be discrete probability distributions.

In [GKPV10]: Statistical Distance

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

In our work: Rényi Divergence

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



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

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

$$\mathrm{SD}(D_\beta, D_{\beta,s}) = \frac{\sqrt{2\pi}\|s\|}{\beta}$$

Improving 2 by using Rényi Divergence 2/2

Both fulfill the **probability preservation property** for an event E:

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

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

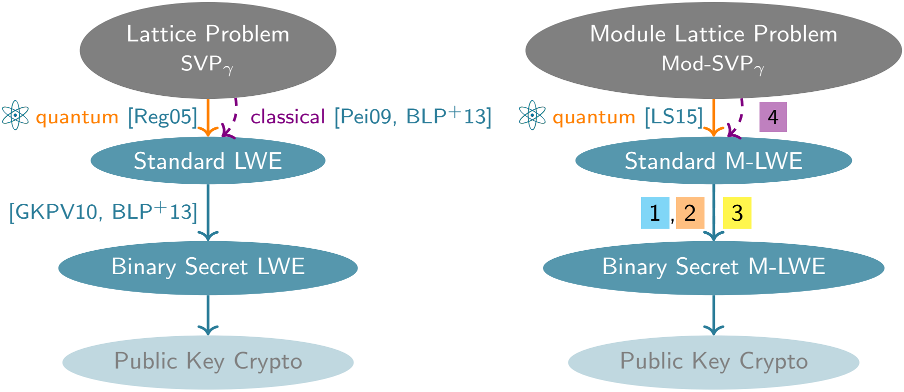
Thus: $\mathsf{SD}(P,Q) \stackrel{!}{=}$ negligible and $\mathsf{RD}(P,Q) \stackrel{!}{=}$ **constant**

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

$$\begin{aligned} \mathsf{SD}(D_\beta, D_{\beta,s}) &= \frac{\sqrt{2\pi}\|s\|}{\beta} && \Rightarrow \alpha/\beta \leq \text{negligible} \\ \mathsf{RD}(D_\beta, D_{\beta,s}) &= \exp\left(\frac{2\pi\|s\|^2}{\beta^2}\right) \approx 1 + \frac{2\pi\|s\|^2}{\beta^2} && \Rightarrow \alpha/\beta \leq \textbf{constant} \end{aligned}$$

⚠ Rényi Divergence only for search problems.

Motivation (Continued)



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]* [BJRW20]

* *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$_\gamma$ 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

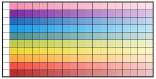
Partial Vandermonde Transform [HPS+14, LZA18]

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 $q = 1 \bmod 2n$:

- $x^n + 1 = \prod_{j=1}^{n}(x - \omega_j)$, where ω_j is a primitive $2n$-th root of unity in $\mathbb{Z}_q$

The set $\{\omega_j\}_{j=1,\dots,n}$ defines the **Vandermonde transform** $\mathbf{V}\colon R \to \mathbb{Z}_q^n$, where



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

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

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

Note: For $\Omega \subseteq \{\omega_j\}_{j=1,\dots,n}$ write $\mathbf{V}_\Omega \cdot a = b$. **(partial Vandermonde transform)**

Partial Vandermonde Problems

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

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

$$\mathbf{V}_\Omega \, e = b \mod q.$$

Search: find e

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

$$\mathbf{V}_\Omega^T \, s + e = b \mod q.$$

Search: find e (and secret s)

Conjecture: Hard to solve if DistrE provides elements of small norm.

Equivalence of PV-Knap and PV-LWE

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

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

$$\mathbf{V}_\Omega(a \cdot b) = (\mathbf{V}_\Omega a) \circ (\mathbf{V}_\Omega b)$$

(component-wise multiplication $\circ$)

Property 2: $\Omega^c = \{\omega_j\}_j \setminus \Omega$ defines the **complement** partial Vandermonde transform $\mathbf{V}_{\Omega^c}$. Given $\mathbf{V}_\Omega a$ and $\mathbf{V}_{\Omega^c} a$, we can recover a.

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

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

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

Lemma (Adapted [MM11, Sec. 4.2])

Let ψ 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 $(\mathbf{V}_\Omega, b)$, with $b = \mathbf{V}_\Omega^T s + e$. Compute Ω' such that $\mathbf{V}_{\Omega'} \cdot \mathbf{V}_\Omega^T = 0$.
Then, $b' := \mathbf{V}_{\Omega'} b = \mathbf{V}_{\Omega'} e$ is an instance of PV-Knap.

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

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

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

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

$$e_1 = (\mathsf{pk} \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s'$$
$$e_2 = \mathbf{V}_{\Omega^c} r'$$
$$e_3 = \mathbf{V}_{\Omega^c} s'$$

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

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

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

Correctness:

$$\left.\begin{aligned} e_1 &= (\mathbf{V}_\Omega f \circ \mathbf{V}_\Omega r') + \mathbf{V}_\Omega s' = \mathbf{V}_\Omega (f \cdot r' + s') \\ c' &= (\mathbf{V}_{\Omega^c} \mathsf{sk} \circ (\mathbf{V}_{\Omega^c} r') + \mathbf{V}_{\Omega^c} s' = \mathbf{V}_{\Omega^c} (f \cdot r' + s') \end{aligned}\right\} \text{ring homomorphism}$$

$$\mathbf{V}^{-1}(e_1 || c') = \mathbf{V}^{-1}(\mathbf{V}(f \cdot r' + s')) = f \cdot pr + ps + m = m \bmod p$$

if f, r and s are small enough

PASS Encrypt [HS15]

[HS15]	Our work
deterministic	randomized
without proof of security	with proof of security
fixed $\mathbf{V}_\Omega$	random $\mathbf{V}_\Omega$

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

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

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

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

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

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

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

$\Rightarrow$ leaky variant of **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: $\mathsf{Enc}(\mathsf{pk}, m_1) + \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 + m_2)$

Multiplication: $\mathsf{Enc}(\mathsf{pk}, m_1) \circ \mathsf{Enc}(\mathsf{pk}, m_2) = \mathsf{Enc}(\mathsf{pk}, m_1 \cdot m_2)$

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

Efficiency:

Scheme	NTRU [HPS98]	P-LWE Regev [LP11]	PASS Encrypt
$\frac{\lvert c\rvert + \lvert \mathsf{pk}\rvert}{\lvert m\rvert}$	$2\log_2 q$	$3\log_2 q$	$2.5\log_2 q$

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

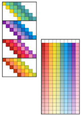
Asiacrypt'20
CT-RSA'21

I. Study of existing structured variants

1. Module Learning With Errors with a binary secret

2. Classical hardness of Module Learning With Errors

$$A \cdot A\, s + e = b$$



II. Proposing new structured variants

3. Middle-Product Learning With Rounding

4. Partial Vandermonde Learning With Errors & Knapsack

Asiacrypt'19
& under submission

provable secure

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]
Shi Bai, Katharina Boudgoust, Dipayan Das, Adeline Roux-Langlois, Weiqiang Wen & Zhenfei Zhang.

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.
In *ASIACRYPT (1)*, volume 10624 of *Lecture Notes in Computer Science*, pages 267–296. Springer, 2017.

Miklós Ajtai.
Generating hard instances of lattice problems (extended abstract).
In *STOC*, pages 99–108. ACM, 1996.

Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan.
(leveled) fully homomorphic encryption without bootstrapping.
In *ITCS*, pages 309–325. ACM, 2012.

Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen.
Towards classical hardness of module-lwe: The linear rank case.
In *ASIACRYPT (2)*, volume 12492 of *Lecture Notes in Computer Science*, pages 289–317. Springer, 2020.

Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen.
On the hardness of module-lwe with binary secret.
In *CT-RSA*, volume 12704 of *Lecture Notes in Computer Science*, pages 503–526. Springer, 2021.

Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé.
Classical hardness of learning with errors.
In *STOC*, pages 575–584. ACM, 2013.

Katharina Boudgoust.
Theoretical hardness of algebraically structured learning with errors, 2021.

Abhishek Banerjee, Chris Peikert, and Alon Rosen.
Pseudorandom functions and lattices.
In *EUROCRYPT*, volume 7237 of *Lecture Notes in Computer Science*, pages 719–737. Springer, 2012.

Olivier Bernard and Adeline Roux-Langlois.
Twisted-phs: Using the product formula to solve approx-svp in ideal lattices.
In *ASIACRYPT (2)*, volume 12492 of *Lecture Notes in Computer Science*, pages 349–380. Springer, 2020.

Ronald Cramer, Léo Ducas, and Benjamin Wesolowski.
Short stickelberger class relations and application to ideal-svp.
In *EUROCRYPT (1)*, volume 10210 of *Lecture Notes in Computer Science*, pages 324–348, 2017.

Long Chen, Zhenfeng Zhang, and Zhenfei Zhang.
On the hardness of the computational ring-lwr problem and its applications.
In *ASIACRYPT (1)*, volume 11272 of *Lecture Notes in Computer Science*, pages 435–464. Springer, 2018.

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

In *CRYPTO (2)*, volume 12171 of *Lecture Notes in Computer Science*, pages 329–358. Springer, 2020.

Yarkin Doröz, Jeffrey Hoffstein, Joseph H. Silverman, and Berk Sunar.
MMSAT: A scheme for multimessage multiuser signature aggregation.
IACR Cryptol. ePrint Arch., page 520, 2020.

Craig Gidney and Martin Ekerå.
How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.
Quantum, 5:433, 2021.

Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan.
Robustness of the learning with errors assumption.
In *ICS*, pages 230–240. Tsinghua University Press, 2010.

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

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman.
NTRU: A ring-based public key cryptosystem.
In *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.

Jeffrey Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William Whyte.
Practical signatures from the partial fourier recovery problem.

In *ACNS*, volume 8479 of *Lecture Notes in Computer Science*, pages 476–493. Springer, 2014.

Jeffrey Hoffstein and Joseph H. Silverman.
Pass-encrypt: a public key cryptosystem based on partial evaluation of polynomials.
Des. Codes Cryptogr., 77(2-3):541–552, 2015.

Richard Lindner and Chris Peikert.
Better key sizes (and attacks) for lwe-based encryption.
In *CT-RSA*, volume 6558 of *Lecture Notes in Computer Science*, pages 319–339. Springer, 2011.

Vadim Lyubashevsky, Chris Peikert, and Oded Regev.
On ideal lattices and learning with errors over rings.
In *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2010.

Adeline Langlois and Damien Stehlé.
Worst-case to average-case reductions for module lattices.
Des. Codes Cryptogr., 75(3):565–599, 2015.

Xingye Lu, Zhenfei Zhang, and Man Ho Au.
Practical signatures from the partial fourier recovery problem revisited: A provably-secure and gaussian-distributed construction.
In *ACISP*, volume 10946 of *Lecture Notes in Computer Science*, pages 813–820. Springer, 2018.

Daniele Micciancio.
Generalized compact knapsacks, cyclic lattices, and efficient one-way functions.
Comput. Complex., 16(4):365–411, 2007.

Daniele Micciancio.
On the hardness of learning with errors with binary secrets.
Theory Comput., 14(1):1–17, 2018.

Daniele Micciancio and Petros Mol.
Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions.
In *CRYPTO*, volume 6841 of *Lecture Notes in Computer Science*, pages 465–484. Springer, 2011.

Daniele Micciancio and Chris Peikert.
Hardness of SIS and LWE with small parameters.
In *CRYPTO (1)*, volume 8042 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 2013.

Chris Peikert.
Public-key cryptosystems from the worst-case shortest vector problem: extended abstract.
In *STOC*, pages 333–342. ACM, 2009.

Alice Pellet-Mary, Guillaume Hanrot, and Damien Stehlé.

Approx-svp in ideal lattices with pre-processing.
In *EUROCRYPT (2)*, volume 11477 of *Lecture Notes in Computer Science*, pages 685–716. Springer, 2019.

Chris Peikert and Zachary Pepin.
Algebraically structured lwe, revisited.
In *TCC (1)*, volume 11891 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2019.

Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz.
Pseudorandomness of ring-lwe for any ring and modulus.
In *STOC*, pages 461–473. ACM, 2017.

Oded Regev.
On lattices, learning with errors, random linear codes, and cryptography.
In *STOC*, pages 84–93. ACM, 2005.

Miruna Rosca, Amin Sakzad, Damien Stehlé, and Ron Steinfeld.
Middle-product learning with errors.
In *CRYPTO (3)*, volume 10403 of *Lecture Notes in Computer Science*, pages 283–297. Springer, 2017.

Peter W. Shor.
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.
SIAM J. Comput., 26(5):1484–1509, 1997.

Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa.
Efficient public key encryption based on ideal lattices.
In *ASIACRYPT*, volume 5912 of *Lecture Notes in Computer Science*, pages 617–635. Springer, 2009.