USING STRUCTURED VARIANTS IN LATTICE-BASED CRYPTOGRAPHY

Adeline Roux-Langlois

Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, Caen, FRANCE

GREYC Electronics and Computer Science Laboratory

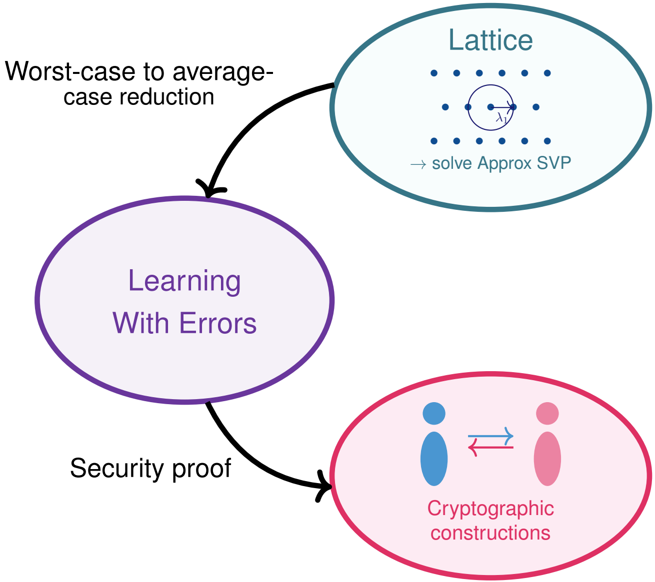
Normandie Université

UNICAEN

ENSI CAEN ÉCOLE PUBLIQUE D'INGÉNIEURS CENTRE DE RECHERCHE

cnrs

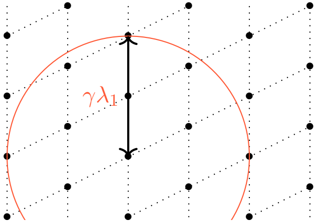
Using LWE to build provable constructions - theory



Approx Shortest Vector Problem (Approx SVP$_\gamma$)

Given a lattice $\mathcal{L}(\mathbf{B})$ of dimension n:

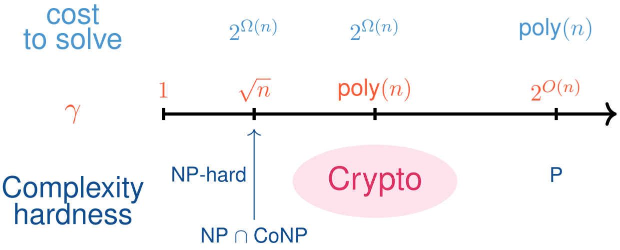
Output: find a non-zero vector $\mathbf{x} \in \mathcal{L}(\mathbf{B})$ such that $\|\mathbf{x}\| \leq \gamma \lambda_1(\mathcal{L}(\mathbf{B}))$



Lattice

$\mathcal{L}(\mathbf{B}) = \{\sum_{1=i}^{n} a_i \mathbf{b}_i, a_i \in \mathbb{Z}\}$, where the $(\mathbf{b}_i)_{1\leq i \leq n}$'s, linearly independent vectors, are a basis of $\mathcal{L}(\mathbf{B})$.

Hardness of Approx SVP$_\gamma$



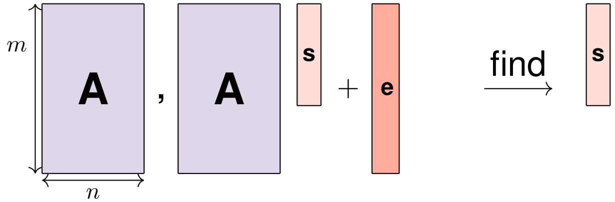
Conjecture

There is no polynomial time algorithm that approximates this lattice problem and its variants to within polynomial factors.

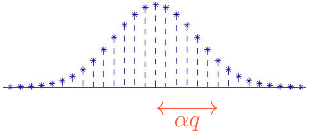
The Learning With Errors problem

$\mathsf{LWE}^n_{\alpha,q}$

Given



- $\mathbf{A} \leftarrow U(\mathbb{Z}_q^{m\times n})$,
- $\mathbf{s} \leftarrow U(\mathbb{Z}_q^{n})$,
- $\mathbf{e} \leftarrow D_{\mathbb{Z}^m,\alpha q}$, small compared to q.



Discrete Gaussian error $D_{\mathbb{Z},\alpha q}$

Search version: Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$, find $\mathbf{s}$.
Decision version: Distinguish from $(\mathbf{A}, \mathbf{b})$ with $\mathbf{b}$ uniform.

Regev's encryption scheme

- **Parameters**: $n, m, q \in \mathbb{Z}$, $\alpha \in \mathbb{R}$,
- **Keys**: sk = $\mathbf{s}$ and pk = $(\mathbf{A}, \mathbf{b})$, with $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \bmod q$
  where $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m \times n})$, $\mathbf{e} \hookleftarrow D_{\mathbb{Z}^m, \alpha q}$.
- **Encryption** $(M \in \{0,1\})$: Let $\mathbf{r} \hookleftarrow U(\{0,1\}^m)$,

$$\mathbf{u}^T = \mathbf{r}\,\mathbf{A}, \quad v = \mathbf{r}\,\mathbf{b} + \lfloor q/2 \rceil \cdot M$$

- **Decryption** of $(\mathbf{u}, v)$: compute $v - \mathbf{u}^T\mathbf{s}$,

$$\underbrace{\mathbf{r}\left[\mathbf{A}\,\mathbf{s} + \mathbf{e}\right] + \lfloor q/2 \rceil \cdot M}_{v} - \underbrace{\mathbf{r}\,\mathbf{A}\,\mathbf{s}}_{\mathbf{u}^T\mathbf{s}} = \text{small} + \lfloor q/2 \rceil \cdot M$$

If **close from** 0: return 0, if **close from** $\lfloor q/2 \rceil$: return 1.

LWE hard $\Rightarrow$ Regev's scheme is IND-CPA secure.

Using LWE

Hardness of LWE used as a foundation for many constructions.

Learning With Errors

Problem: constructions based on LWE enjoy a nice guarantee of security but are too costly in practice.

Security proof

Cryptographic constructions

Signature, encryption
Advanced schemes
Fully Homomorphic Encryption

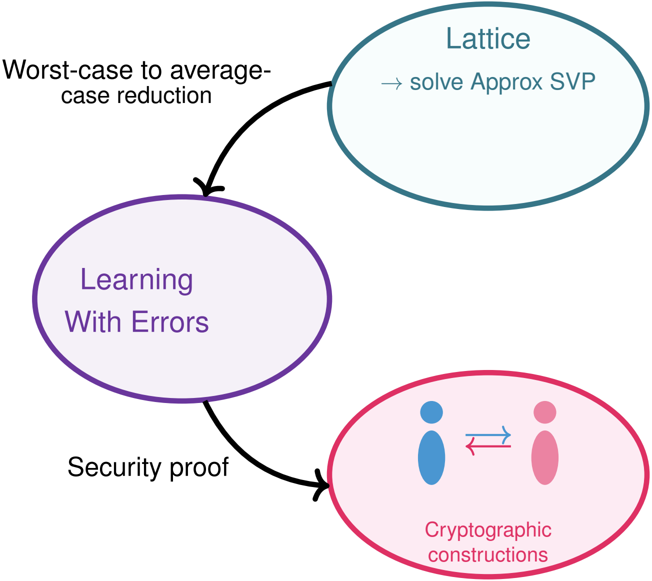
Solutions used today?

Lattice-based NIST finalists

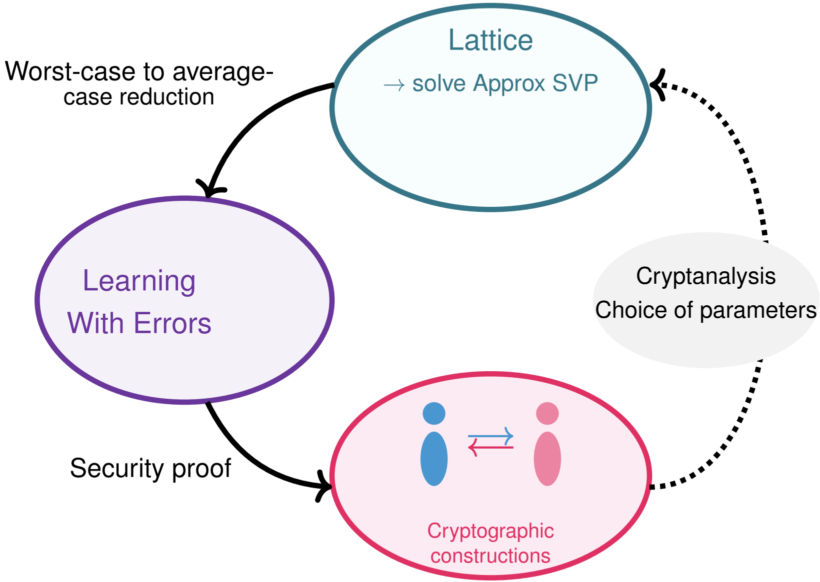
Among the 5 lattice-based finalists, 3 of them are based on (possibly structured) variants of LWE.

- Public Key Encryption
  - **Crystals - Kyber**: Module-LWE with both secret and noise chosen from a centered binomial distribution.
  - **Saber:** Module-LWR (deterministic variant).
  - **NTRU**
  - **FrodoKEM** (as alternate candidate): LWE but with smaller parameters.
- Signature
  - **Crystals - Dilithium**: Module-LWE with both secret and noise chosen in a small uniform interval, and Module-SIS.
  - **Falcon**: Ring-SIS on NTRU matrices.

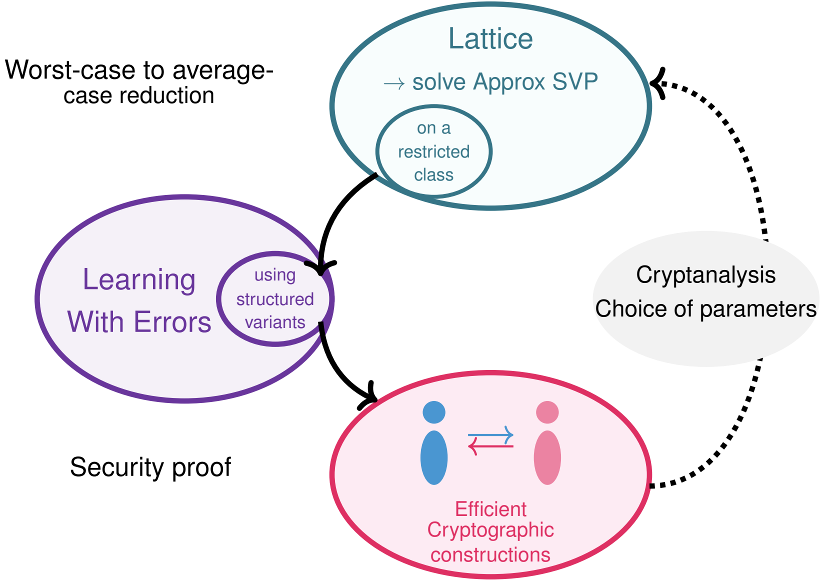
Using LWE to build constructions



Using LWE to build constructions in practice



Using LWE to build constructions in practice

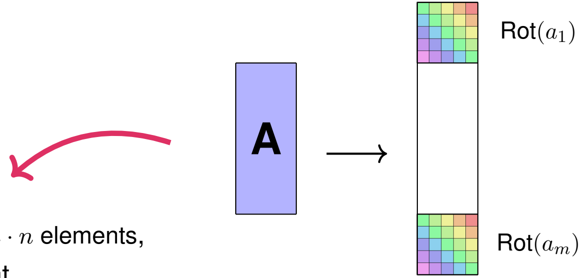


From SIS/LWE to structured variants

Problem: constructions based on LWE enjoy a nice guaranty of security but are too costly in practice.

$\rightarrow$ replace $\mathbb{Z}^n$ by a Ring, for example $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ $(n = 2^k)$.

- Ring variants since 2006:



- Structured **A** $\in \mathbb{Z}_q^{m \cdot n \times n}$ represented by $m \cdot n$ elements,
- Product with matrix/vector more efficient,
- Hardness of Ring-SIS, [Lyubashevsky and Micciancio 06] and [Peikert and Rosen 06]
- Hardness of Ring-LWE [Lyubashevsky, Peikert and Regev 10].

Idea: replace $\mathbb{Z}^n$ by $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$

where $n = 2^k$ then the polynomial $x^n + 1$ is irreducible.
Elements of this ring are polynomials of degree less than n.

R is a **cyclotomic ring.** R is also the ring of integer $\mathcal{O}_K$ of an number field K:

- $K = \mathbb{Q}[x]/\langle x^n + 1\rangle$: K is a cyclotomic field,
- $R = \mathbb{Z}[x]/\langle \phi_m(x)\rangle$ where ϕ_m is the mth cyclotomic polynomial of degree $n = \varphi(m)$. Its roots are the mth roots of unity $\zeta_m^j \in \mathbb{C}$, with $\zeta_m = e^{\frac{2i\pi}{m}}$. (For $m = 2^{k+1}$, we have $\phi_m(x) = x^n + 1$.)
- Canonical embedding: $\sigma_K : \alpha \in K \mapsto ((\sigma(\alpha))_\sigma = (\alpha(\zeta_m^j))_j$.

Idea: replace $\mathbb{Z}^n$ by $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$

R is isomorph to $\mathbb{Z}^n$

Let $a \in R$, we have $a(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$,
the isomorphism $R \to \mathbb{Z}^n$ associate

the polynomial $a \in R$ to the vector $\mathbf{a} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \in \mathbb{Z}^n$.

Idea: replace $\mathbb{Z}^n$ by $R = \mathbb{Z}[x]/\langle x^n + 1 \rangle$

Let's look at the product of two polynomials $x^n + 1$

- $a(x) = a_0 + a_1 \cdot x + \ldots + a_{n-1} \cdot x^{n-1}$
- $s(x) = s_0 + a_1 \cdot x + \ldots + a_{n-1} \cdot x^{n-1}$

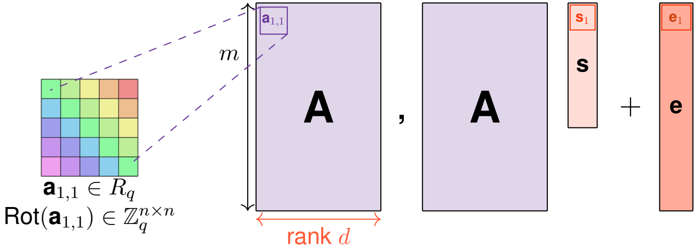
Using matrices, it gives the following block:

$$\begin{bmatrix} a_0 & -a_{n-1} & \cdots & -a_2 & -a_1 \\ a_1 & a_0 & \cdots & -a_3 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-2} & a_{n-3} & \cdots & a_0 & -a_{n-1} \\ a_{n-1} & a_{n-2} & \cdots & a_1 & a_0 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-2} \\ s_{n-1} \end{bmatrix}$$

Module LWE

Let K be a number field of degree n with R its ring of integers.
Think of K as $\mathbb{Q}[x]/(x^n+1)$ and of R as $\mathbb{Z}[x]/(x^n+1)$ for $n = 2^k$.

Replace $\mathbb{Z}$ by R, and $\mathbb{Z}_q$ by $R_q = R/qR$.



- $\mathbf{A} \leftarrow U(R_q^{m\times d})$,
- $\mathbf{s} \leftarrow U(R_q^d)$,
- $e \in R^m$ small compared to q.

Special case $d = 1$
is Ring-LWE

Module SIS and LWE

$R = \mathbb{Z}[x]/\langle x^n + 1 \rangle$ and $R_q = R/qR$.

Module-SIS$_{q,m,\beta}$
Given $\mathbf{a}_1, \ldots, \mathbf{a}_m \in R_q^d$ independent and uniform, find $z_1, \ldots, z_m \in R$ such that $\sum_{i=1}^m \mathbf{a}_i \cdot z_i = 0 \bmod q$ and $0 < \|\mathbf{z}\| \leq \beta$.

Let $\alpha > 0$ and $\mathbf{s} \in (R_q)^d$, the distribution $A^{(M)}_{\mathbf{s}, D_{R,\alpha q}}$ is:

- $\mathbf{a} \in (R_q)^d$ uniform,
- e sampled from $D_{R,\alpha q}$,

Outputs: $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$.

Module-LWE$_{q,\nu_\alpha}$
Let $\mathbf{s} \in (R_q)^d$ uniform, distinguish between an arbitrary number of samples from $A^{(M)}_{\mathbf{s}, D_{R,\alpha q}}$ or the same number from $U((R_q)^d \times R_q)$.

Ideals and modules

$R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ and $R_q = R/qR$.

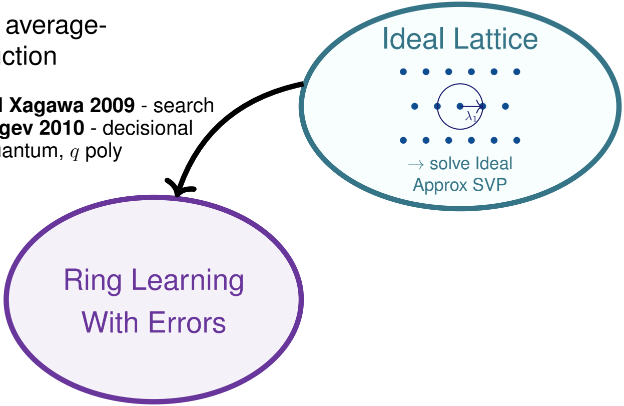
- An ideal I of R is an additive subgroup of R closed under multiplication by every elements of R.
- As R is isomorph to $\mathbb{Z}^n$, any ideal $I \in R$ defines an integer lattice $\Lambda(\mathbf{B})$ where $\mathbf{B} = \{g \bmod x^n + 1 : g \in I\}$.

- A subset $M \subseteq K^d$ is an R-module if it is closed under addition and multiplication by elements of R.
- A finite-type R-module: $M \subseteq R^d : \sum_{i=1}^{D} R \cdot \mathbf{b}_i$, $(\mathbf{b}_i) \in R^d$,
- $M = \sum_{i=1}^{d} I_i \cdot \mathbf{b}_i$ where I_i are ideals of R and $(I_i, \mathbf{b}_i)$ is a pseudo-basis of M.
- As ideals, any module defines an integer module lattice.

Hardness of Ring Learning With Errors problem

Worst-case to average-case reduction

- **Stehlé, Steinfeld, Tanaka and Xagawa 2009** - search
- **Lyubashevsky, Peikert, Regev 2010** - decisional reduction both quantum, q poly



Self reductions

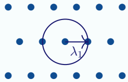
- **Applebaum, Cash, Peikert, Sahai 2009** - same error and secret

Hardness of Module Learning With Errors problem

Worst-case to average-case reduction

- **Langlois Stehlé 2015** - quantum, q poly
- Folklore: adapting **Peikert 2009** gives classical reduction but q exp and only search variant
- **Boudgoust, Jeudy, Roux-Langlois, Wen 2021** classical, q poly, decisional, linear rank

Module Lattice



$\rightarrow$ solve Module Approx SVP

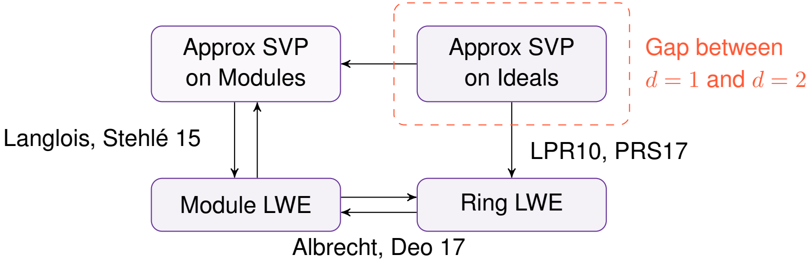
Module Learning With Errors

Self reductions

- **Applebaum, Cash, Peikert, Sahai 2009** - same error and secret
- **Boudgoust, Jeudy, Roux-Langlois, Wen 2022**: short error and secret distributions

Module or Rings?

- Hardness of the problem



Module or Rings?

- Choice of parameters
  - Example of Ring $R_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$
  - Constraints on parameters $n = 2^k$, $q = 1 \bmod 2n$ ...
- An example of parameter set:
  - $n = 512 \Rightarrow$ 60 bits of security,
  - $n = 1024 \Rightarrow$ 140 bits of security,
  - $(n = 256, d = 3)$ gives $nd = 768$ which is ”in between”.
- Module LWE allows more flexibility.

NIST competition

From 2017 to 2024, NIST competition to develop new standards on post-quantum cryptography

2022 first results: **3 over 4 new standards** are lattice-based

- Kyber - encryption scheme based on Module-LWE,
- Dilithium - signature scheme based on Module SIS and LWE,
- Falcon - signature scheme based on NTRU and Ring-SIS.

Encryption scheme based on Ring-LWE

[Lyubashevsky, Peikert, Regev 2011]

KeyGen : The secret key is a small $s \in R$
The public key is $(a, b) = (a, b = a \cdot s + e) \in R_q^2$,
with $a \leftarrow U(R_q)$ and a small $e \in R$.

Enc : Given $m \in \{0, 1\}^n$, a message is a polynomial in R with coordinates in $\{0, 1\}$. Sample small r, e_1, e_2 in R and output

$$(a \cdot r + e_1, b \cdot r + e_2 + \lfloor q/2 \rfloor \cdot m) \in R_q \times R_q.$$

Dec : Given $(u, v) \in R_q \times R_q$, compute

$$v - u \cdot s = (r \cdot e - s \cdot e_1 + e_2) + b\lfloor q/2 \rfloor \cdot m$$

For each coordinate of m, the plaintext is 0 if the result is closer from 0 than $\lfloor q/2 \rfloor$, and 1 otherwise.

Kyber

[Avanzi, Bos, Ducas, Kiltz, Lepoint, Lyubashevsky, Schanck, Schwabe, Seiler, Stehle]

- Kyber relies on Module-LWE,
- Use $R_q = \mathbb{Z}_q[x]/\langle x^{256}+1\rangle$ with $q = 7681$.

- The small elements follow a binomial distribution B_η:
  For some positive integer η, sample $\{(ai, bi)\}_{i=1}^{\eta} \leftarrow (\{0,1\}^2)^\eta$ and output $\sum_{i=1}^{\eta}(a_i - b_i)$.

- The uniform public key is generated given a $seed$ and a function PARSE,
- Multiplication operations uses NTT - Number Theoretic Transform - which is a variant of the FFT in rings,
- Size of ciphertext is compressed by keeping only high order bits.

Performances

Current timings (ECDH)
Public key around 32 bytes
Efficiency comparable in terms of cycles.

Kyber-512

Sizes (in bytes)		Haswell cycles (ref)		Haswell cycles (avx2)	
sk:	1632	gen:	122684	gen:	33856
pk:	800	enc:	154524	enc:	45200
ct:	768	dec:	187960	dec:	34572

Kyber-768

Sizes (in bytes)		Haswell cycles (ref)		Haswell cycles (avx2)	
sk:	2400	gen:	199408	gen:	52732
pk:	1184	enc:	235260	enc:	67624
ct:	1088	dec:	274900	dec:	53156

Kyber-1024

Sizes (in bytes)		Haswell cycles (ref)		Haswell cycles (avx2)	
sk:	3168	gen:	307148	gen:	73544
pk:	1568	enc:	346648	enc:	97324
ct:	1568	dec:	396584	dec:	79128

Choice of parameters

- Parameters used by Kyber:
  - $n = 256$ and $d = 2, 3, 4$ giving three levels of security: $512, 768, 1024$,
  - $q = 7681$

Choice of parameters

- Parameters used by Kyber:
  - $n = 256$ and $d = 2, 3, 4$ giving three levels of security: $512, 768, 1024$,
  - $q = 7681$

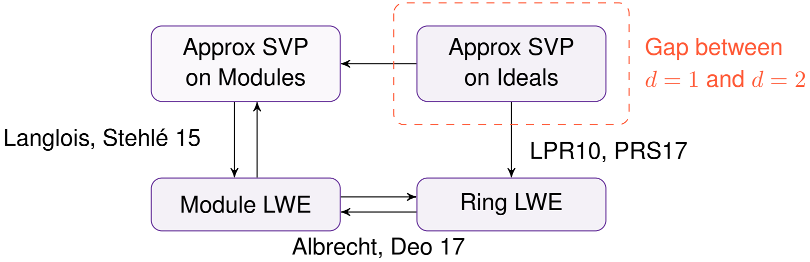
- How do they choose the parameters?
  - By considering the LWE instance with dimension nd,
  - and the ”lattice estimator” [Albrecht, Player, Scott 2015],

Choice of parameters

- Parameters used by Kyber:
  - $n = 256$ and $d = 2, 3, 4$ giving three levels of security: $512, 768, 1024$,
  - $q = 7681$
- How do they choose the parameters?
  - By considering the LWE instance with dimension nd,
  - and the ”lattice estimator” [Albrecht, Player, Scott 2015],
- There is no consideration of the structure!
  - Why?
  - Because we don’t know how...

Approx Ideal SVP seems to be the easiest

- Hardness of the problem



Solving Approx Ideal SVP[1]

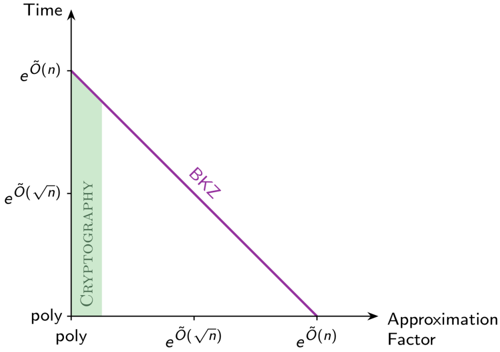
- For a long time, no algorithm manages to exploit the structure of Ideal SVP.

- 2014: Quantum algorithm computing ($\mathcal{S}$-)units, class groups in polynomial time!
  [EHKS14,BS16]

- Followed by a long series of cryptanalysis works.
  [CGS14,CDPR16,CDW17/21,PHS19,BR20,BLNR22,BL21,BEFHY22]

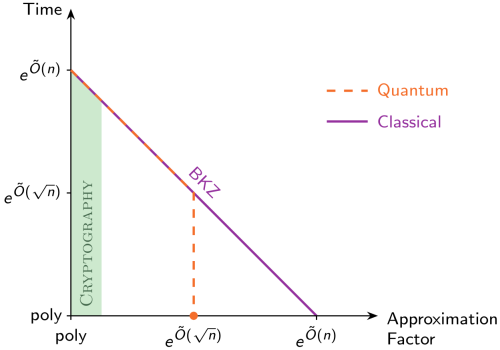
[1] Thanks to Olivier Bernard and Andrea Lesavourey for part of the slides (particularly to Olivier for the `tikz` picture!)

Algebraic cryptanalysis of Ideal-SVP



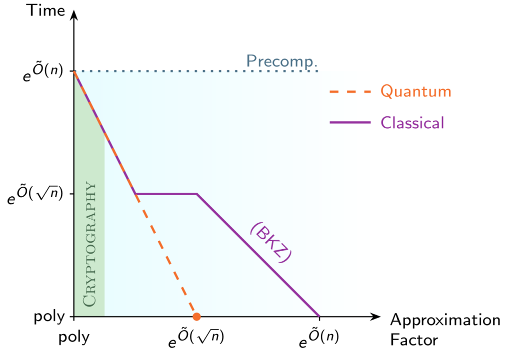
1. Schnorr's hierarchy (*unstructured*)

Algebraic cryptanalysis of Ideal-SVP



1. Schnorr's hierarchy (*unstructured*)
2. CDW algorithm [Cramer, Ducas, Wesolowski 17/21]: uses short *Stickelberger* relations.

Algebraic cryptanalysis of Ideal-SVP



1. Schnorr's hierarchy (*unstructured*)
2. CDW algorithm [Cramer, Ducas, Wesolowski 17/21]: uses short *Stickelberger* relations.
3. PHS and Twisted-PHS [Pellet-Mary, Hanrot, Stehlé 19, Bernard, Roux-Langlois 20, Bernard, Lesavouvey, Nguyen, Roux-Langlois 22]: *$\mathcal{S}$-unit attacks*.

Solving Approx Ideal SVP

Consider an intermediate problem.

Short Generator Principal ideal Problem (SG-PIP):
Given a principal ideal $I = (g)$ such that g is short, retrieve g.

[2] $\text{Log}_K : x \mapsto (\ln|\sigma_1(x)|, \ldots, \ln|\sigma_n(x)|)$

Solving Approx Ideal SVP

Consider an intermediate problem.

Short Generator Principal ideal Problem (SG-PIP):
Given a principal ideal $I = (g)$ such that g is short, retrieve g.

1. Find a generator $h = gu$ of I ($u \in \mathcal{O}_K^\times$)
   Can be done in polynomial time with a quantum computer

2. Find g given h.
   Use the Log-embedding[2] and the Log-unit lattice $\mathrm{Log}(\mathcal{O}_K^\times)$

[2] $\mathrm{Log}_K : x \mapsto (\ln|\sigma_1(x)|, \ldots, \ln|\sigma_n(x)|)$

Solving Approx Ideal SVP

Consider an intermediate problem.

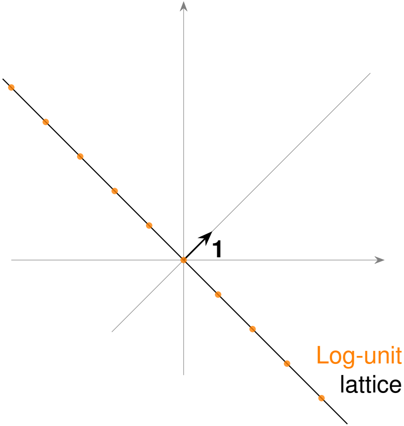
Short Generator Principal ideal Problem (SG-PIP):
Given a principal ideal $I = (g)$ such that g is short, retrieve g.

1. Find a generator $h = gu$ of I ($u \in \mathcal{O}_K^\times$)
   Can be done in polynomial time with a quantum computer
2. Find g given h.
   Use the Log-embedding[2] and the Log-unit lattice $\mathrm{Log}(\mathcal{O}_K^\times)$

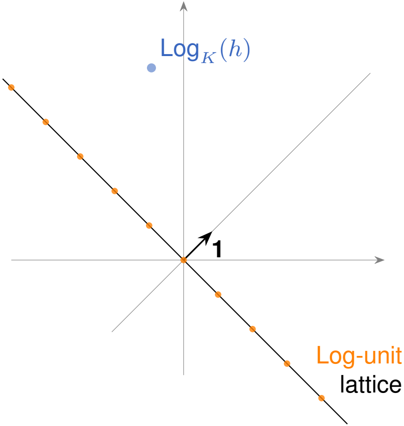
- [Cramer, Ducas, Peikert, Regev 2016] quantum polynomial-time or classical $2^{n^{2/3+\epsilon}}$-time algorithm to solve SG-PIP over cyclotomic fields.

[2] $\mathrm{Log}_K : x \mapsto (\ln|\sigma_1(x)|, \ldots, \ln|\sigma_n(x)|)$

View of the algorithm



View of the algorithm

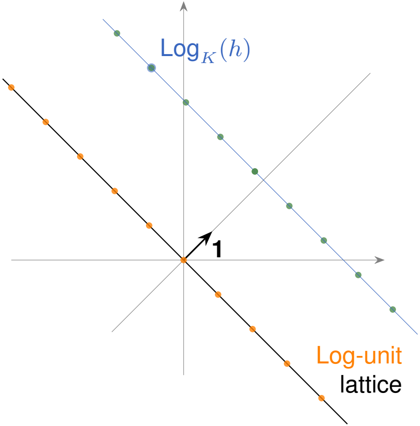


Let I be a challenge ideal.

1. Quantum decomposition
   Apply Log_K
   $\mathrm{Log}_K(h) = \mathrm{Log}_K(g) + \mathrm{Log}_K(u) \in \mathrm{Log}_K(g) + \mathrm{Log}_K(\mathcal{O}_K^\times)$

$$h = g \cdot u$$

View of the algorithm



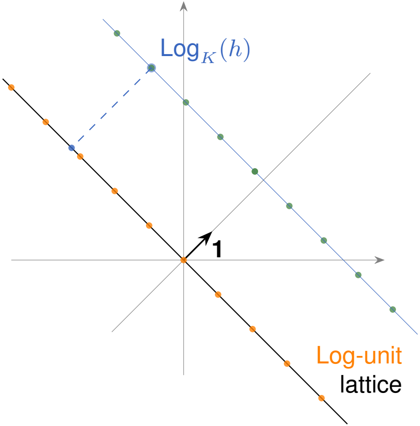
Let I be a challenge ideal.

1. Quantum decomposition
   Apply Log_K
   $\mathrm{Log}_K(h) = \mathrm{Log}_K(g) + \mathrm{Log}_K(u) \in \mathrm{Log}_K(g) + \mathrm{Log}_K(\mathcal{O}_K^\times)$

2. *Short* coset representative ?

$$h = g \cdot u$$

View of the algorithm

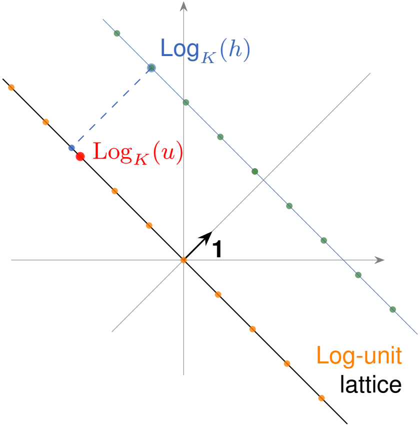


Let I be a challenge ideal.

1. Quantum decomposition
   Apply Log_K
   $\mathrm{Log}_K(h) = \mathrm{Log}_K(g) + \mathrm{Log}_K(u) \in \mathrm{Log}_K(g) + \mathrm{Log}_K(\mathcal{O}_K^\times)$
2. *Short* coset representative ?

$$h = g \cdot u$$

View of the algorithm



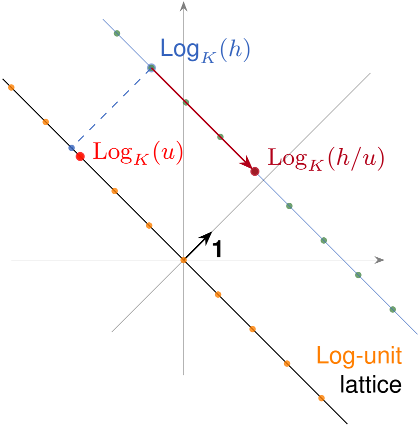
Let I be a challenge ideal.

1. Quantum decomposition
   Apply *Log*$_K$
   $\mathrm{Log}_K(h) = \mathrm{Log}_K(g) + \mathrm{Log}_K(u) \in \mathrm{Log}_K(g) + \mathrm{Log}_K(\mathcal{O}_K^\times)$

2. *Short* coset representative ?

$$h = g \cdot u$$

View of the algorithm



Let I be a challenge ideal.

1. Quantum decomposition
   Apply Log_K
   $\mathrm{Log}_K(h) = \mathrm{Log}_K(g) + \mathrm{Log}_K(u) \in \mathrm{Log}_K(g) + \mathrm{Log}_K(\mathcal{O}_K^\times)$

2. *Short* coset representative ?

3. Hope this is *short* in I.

$$h = g \cdot u$$

$$(h/u) = g$$

SVP of general ideals

Consider K a number field, I an ideal and S a set of prime ideals.

1. Compute a S-generator of I, i.e. h s.t. $(h) = I \prod_{\mathfrak{p}\in S} \mathfrak{p}^{v_\mathfrak{p}}$
2. Reduce h

Two variants for step 2.

1. First reduce $\prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}}$; then find a generator with the Log-embedding.
   $\rightarrow$ [Cramer, Ducas, Wesolowski 2017] cyclotomic fields, subexponential approximation factor

2. Use the Log-S-embedding[3] to reduce everything.
   $\rightarrow$ [Pellet-Mary, Hanrot, Stehlé 2019] all number fields, exponential preprocessing, subexponential approximation factor
   $\rightarrow$ [Bernard, Roux-Langlois 2020] other def. of $\mathrm{Log}_{K,S}$, same asymptotic results, **good results in practice for cyclotomics up to dimensions 70.**

[3] $\mathrm{Log}_{K,S} : x \mapsto (\ln|\sigma_1(x)|, \ldots, \ln|\sigma_n(x)|, -v_{\mathfrak{p}_1}(x)\ln(N(\mathfrak{p}_1)), \ldots, -v_{\mathfrak{p}_r}(x)\ln(N(\mathfrak{p}_r)))$

Bernard, Lesavourey, Nguyen, Roux-Langlois (2022)

Can we extend these good results to higher dimensions ?

Two major obstructions for experiments:

- Decomposition $(h) = I \cdot \prod_{\mathfrak{p}\in S} \mathfrak{p}^{v_\mathfrak{p}}$
- Group of S-units $(s) = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{e_\mathfrak{p}}$

Bernard, Lesavourey, Nguyen, Roux-Langlois (2022)

GREYC
Electronics and Computer Science Laboratory

Can we extend these good results to higher dimensions ?

Two major obstructions for experiments:

- Decomposition $(h) = I \cdot \prod_{\mathfrak{p} \in S} \mathfrak{p}^{v_\mathfrak{p}}$
- Group of S-units $(s) = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{e_\mathfrak{p}}$

Use new results of Bernard and Kučera (2021) on Stickelberger ideal

- Obtain explicit short basis of S_m
- It is constructive: the associated generators can be computed efficiently
- Free family of short S-units

Bernard, Lesavourey, Nguyen, Roux-Langlois (2022)

GREYC
Electronics and Computer Science Laboratory

Can we extend these good results to higher dimensions ?

Two major obstructions for experiments:

- Decomposition $(h) = I \cdot \prod_{\mathfrak{p} \in S} \mathfrak{p}^{v_{\mathfrak{p}}}$
- Group of S-units $(s) = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{e_{\mathfrak{p}}}$

Use new results of Bernard and Kučera (2021) on Stickelberger ideal

- Obtain explicit short basis of S_m
- It is constructive: the associated generators can be computed efficiently
- Free family of short S-units

Allows us to approximate $\mathrm{Log}(\mathcal{O}_{K,S}^{\times})$ with a full-rank sublattice

- Cyclotomic units
- Explicit Stickelberger generators
- Real $S \cap K_m^{+}$-units $\rightarrow$ only part sub-exponential; dimension $n/2$
- 2-saturation to reduce the index

Experimental results[4]

Cyclotomic fields with almost all conductors, up to dimension 210.

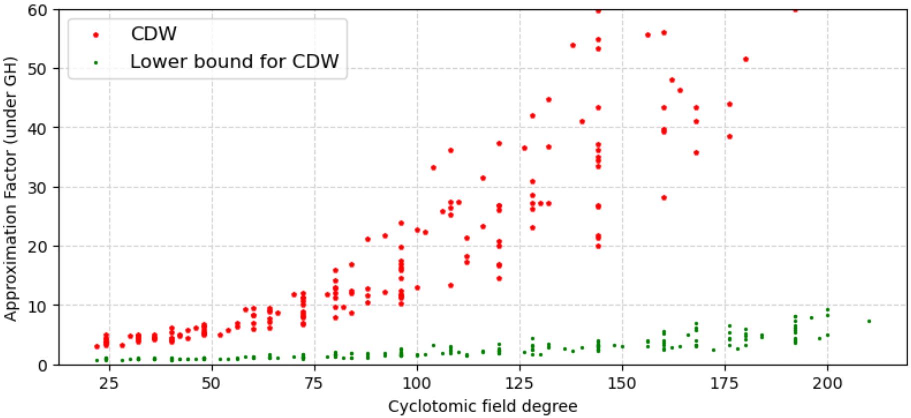
Simulated targets in the Log-space

[4] Code available at https://github.com/ob3rnard/Tw-Sti.

Experimental results[4]

Cyclotomic fields with almost all conductors, up to dimension 210.

Simulated targets in the Log-space

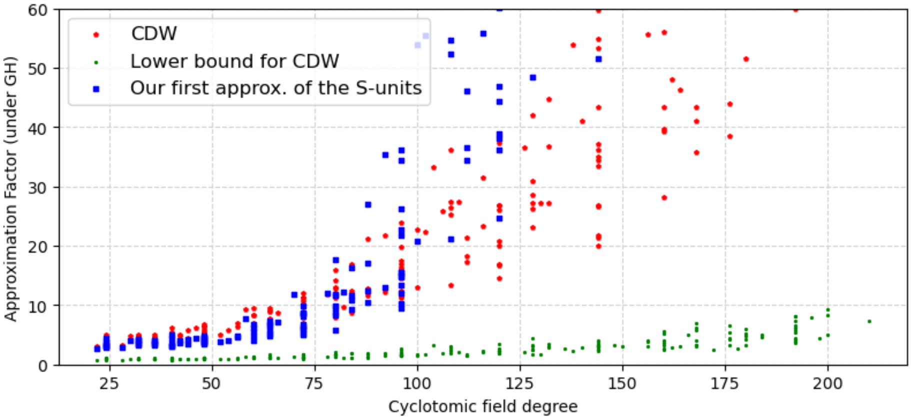


[4] Code available at `https://github.com/ob3rnard/Tw-Sti`.

Experimental results[4]

Cyclotomic fields with almost all conductors, up to dimension 210.

Simulated targets in the Log-space

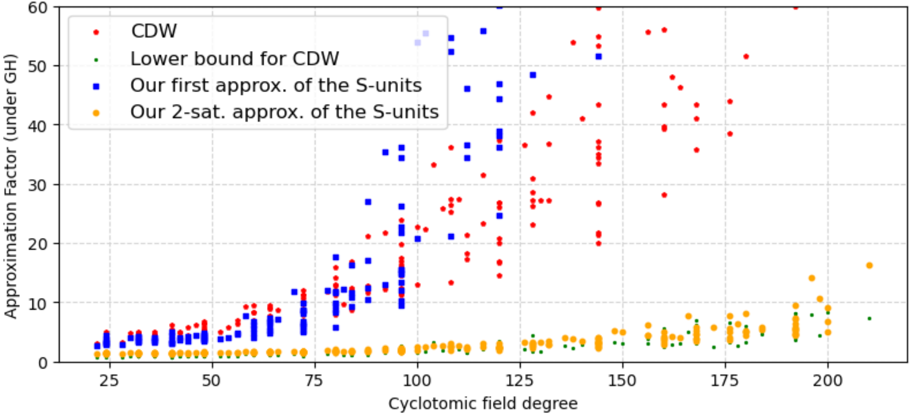


[4] Code available at https://github.com/ob3rnard/Tw-Sti.

Experimental results[4]

Cyclotomic fields with almost all conductors, up to dimension 210.

Simulated targets in the Log-space

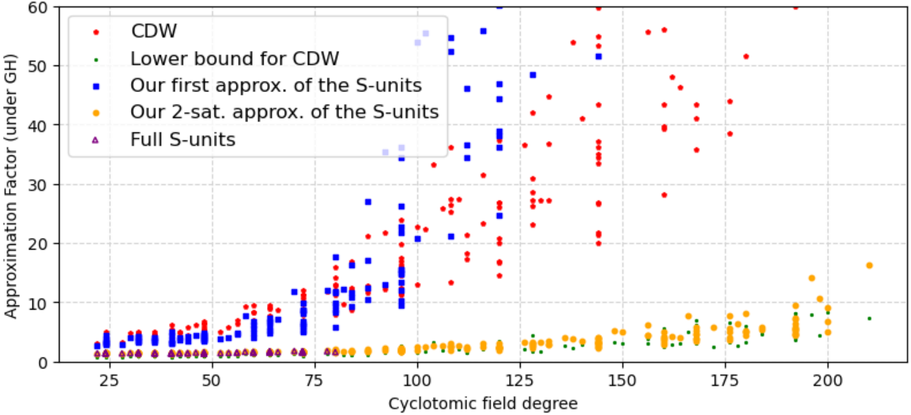


[4] Code available at `https://github.com/ob3rnard/Tw-Sti`.

Experimental results[4]

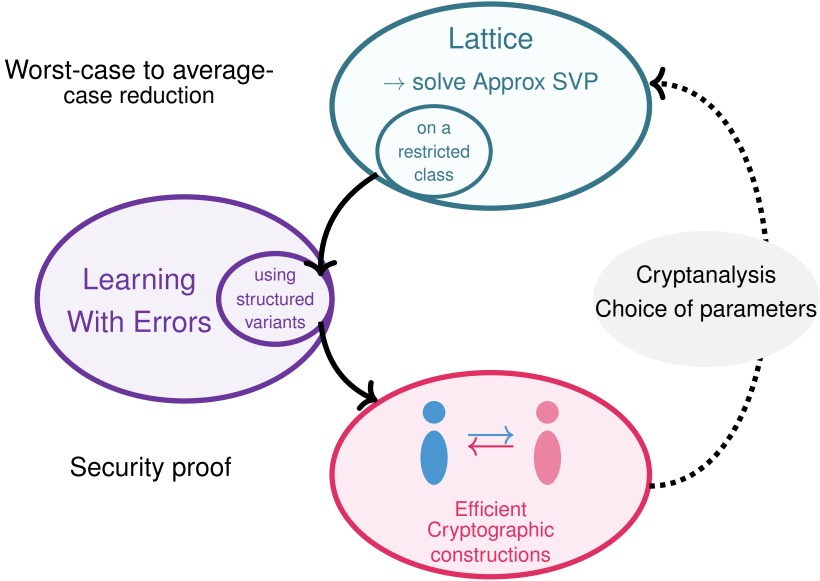
Cyclotomic fields with almost all conductors, up to dimension 210.

Simulated targets in the Log-space



[4]Code available at https://github.com/ob3rnard/Tw-Sti.

Using LWE to build constructions in practice



Conclusion

- Lattice-based cryptography allows to build efficient constructions such as encryption or signature schemes with a security based on the hardness of difficult algorithmic problems on lattices.

- Three schemes (Kyber, Dilithium and Falcon) will be standardise by the NIST, together with a hash-based signature.
  Two of them are based on Module-LWE.

- Approx Ideal SVP seems to be the easier problem to try to solve $\rightarrow$ the results of recent attacks does not impact the security of lattice-based constructions.