Overview of attacks on ideal lattices

Alice Pellet-Mary

CNRS and Université de Bordeaux

talk at ANSSI

Outline of the talk

1. First definitions

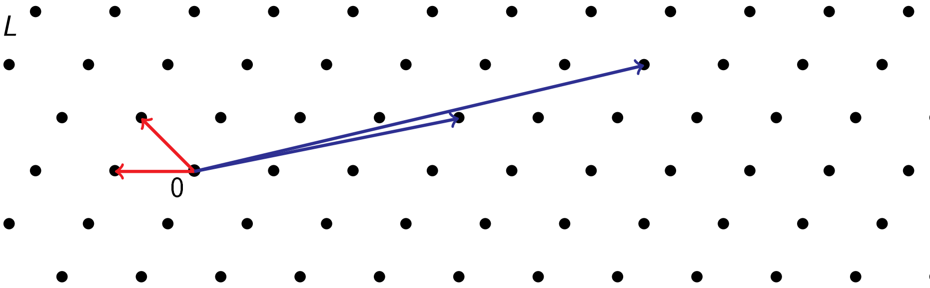
2. Context

3. State-of-the-art for ideal-SVP

4. Techniques

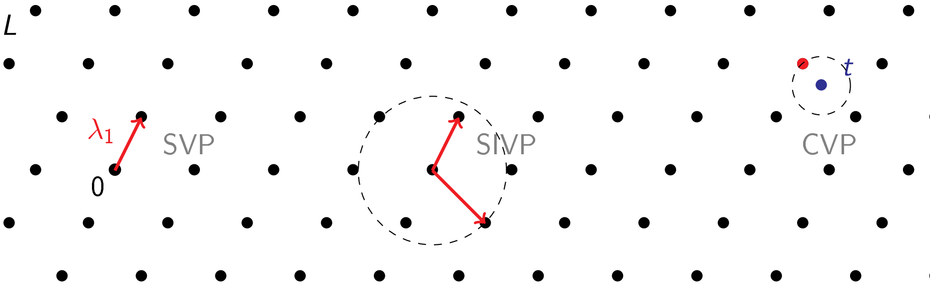
First definitions

Lattices



- $L = \{Bx \mid x \in \mathbb{Z}^n\}$ is a lattice
- $B \in \mathrm{GL}_n(\mathbb{R})$ is a basis
- n is the dimension of L

Algorithmic problems

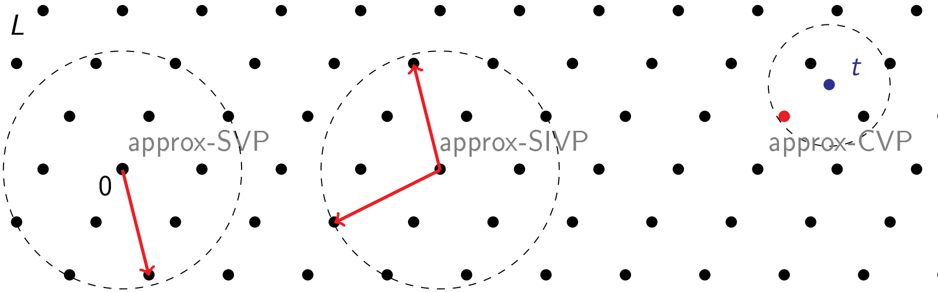


SVP
shortest vector problem

SIVP
shortest independent vector problem

CVP
closest vector problem

Algorithmic problems

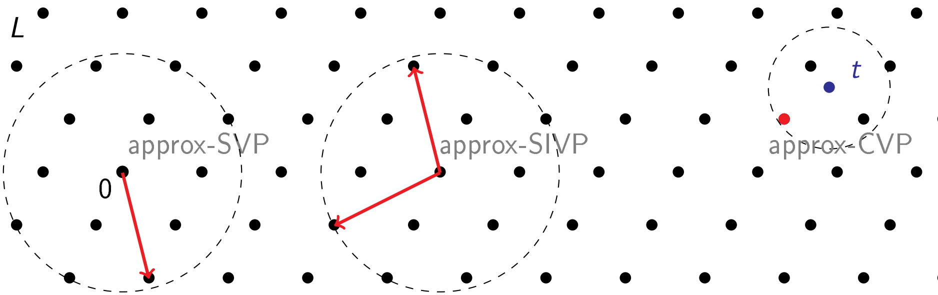


approx-SVP
shortest vector problem

approx-SIVP
shortest independent vector problem

approx-CVP
closest vector problem

Algorithmic problems



approx-SVP
shortest vector problem

approx-SIVP
shortest independent vector problem

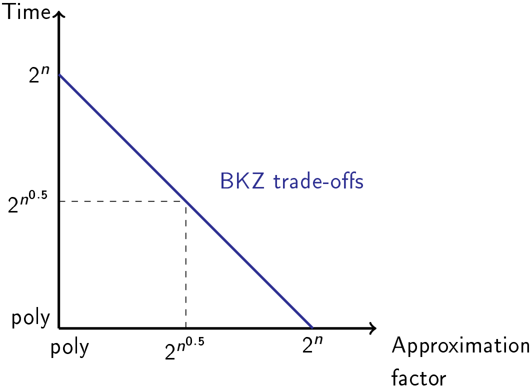
approx-CVP
closest vector problem

Supposedly hard to solve when n is large (input: a bad basis of L)

- even with a quantum computer
- even with a small approximation factor ($\mathrm{poly}(n)$)

Hardness of SVP and CVP

Best Time/Approximation trade-off for SVP, CVP (even quantumly):
BKZ algorithm [Sch87,SE94]

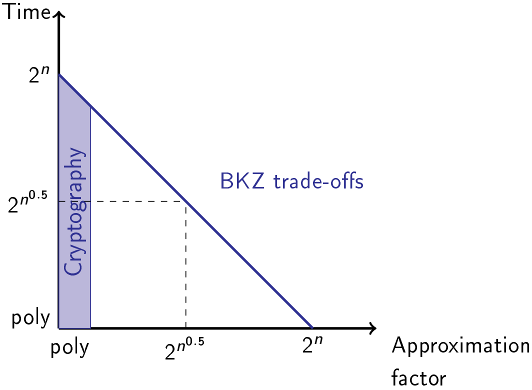


[Sch87] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. TCS.

[SE94] C.-P. Schnorr and M. Euchner. Lattice basis reduction: improved practical algorithms and solving subset sum problems. Mathematical programming.

Hardness of SVP and CVP

Best Time/Approximation trade-off for SVP, CVP (even quantumly):
BKZ algorithm [Sch87,SE94]



[Sch87] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. TCS.

[SE94] C.-P. Schnorr and M. Euchner. Lattice basis reduction: improved practical algorithms and solving subset sum problems. Mathematical programming.

Structured lattices

$$M_a = \begin{pmatrix} a_1 & -a_n & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \vdots & \ddots & \ddots & \vdots \\ a_n & a_{n-1} & \dots & a_1 \end{pmatrix}$$

basis of a special case of
ideal lattice

Structured lattices

$$M_a = \begin{pmatrix} a_1 & -a_n & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \vdots & \ddots & \ddots & \vdots \\ a_n & a_{n-1} & \cdots & a_1 \end{pmatrix}$$

basis of a special case of
ideal lattice

$$\begin{array}{ccc} n & \begin{pmatrix} M_{a_{11}} & M_{a_{12}} & \cdots & M_{a_{1m}} \\ M_{a_{21}} & M_{a_{22}} & \cdots & M_{a_{2m}} \\ \vdots & \vdots & \ddots & \vdots \\ M_{a_{m1}} & M_{a_{m2}} & \cdots & M_{a_{mm}} \end{pmatrix} & nm \end{array}$$

basis of a special case of
module lattice
of rank m

Structured lattices

$$M_a = \begin{pmatrix} a_1 & -a_n & \cdots & -a_2 \\ a_2 & a_1 & \cdots & -a_3 \\ \vdots & \ddots & \ddots & \vdots \\ a_n & a_{n-1} & \cdots & a_1 \end{pmatrix}$$

basis of a special case of
ideal lattice

n

$$\begin{pmatrix} M_{a_{11}} & M_{a_{12}} & \cdots & M_{a_{1m}} \\ M_{a_{21}} & M_{a_{22}} & \cdots & M_{a_{2m}} \\ \vdots & \vdots & \ddots & \vdots \\ M_{a_{m1}} & M_{a_{m2}} & \cdots & M_{a_{mm}} \end{pmatrix}$$

nm

basis of a special case of
module lattice
of rank m

ideal-SVP = SVP restricted to ideal lattices
module-SVP = SVP restricted to module lattices
$\Rightarrow$ hardness of these restricted problems much less understood than SVP

Context

Standard lattice-based problems

LWE

- post-quantum
- equivalent to worst-case SIVP in unstructured lattice
- not super efficient

Standard lattice-based problems

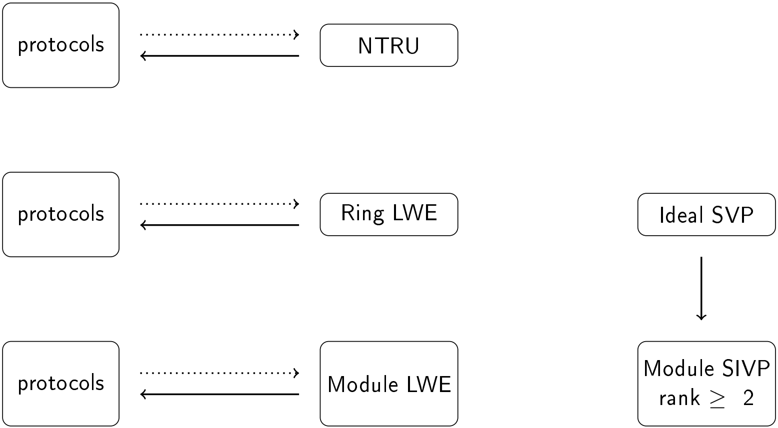
LWE

- post-quantum
- equivalent to worst-case SIVP in unstructured lattice
- not super efficient

RLWE / Module-LWE / NTRU

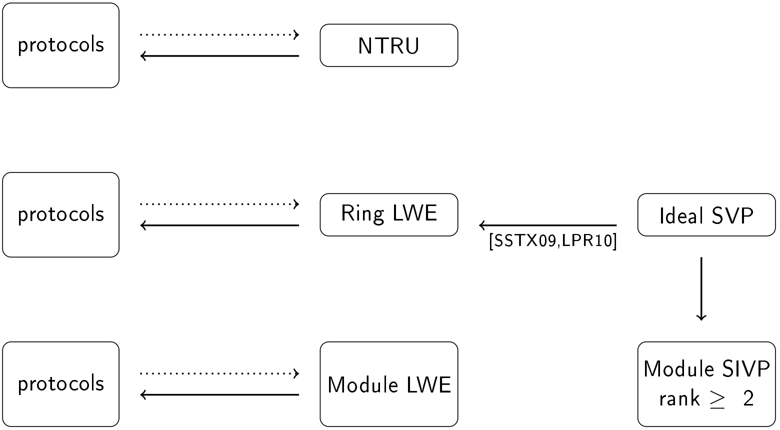
- post-quantum
- efficient
- how do they compare to structured lattice problems?

Reductions



⚠ Arrows may not all compose (different parameters) ⚠

Reductions

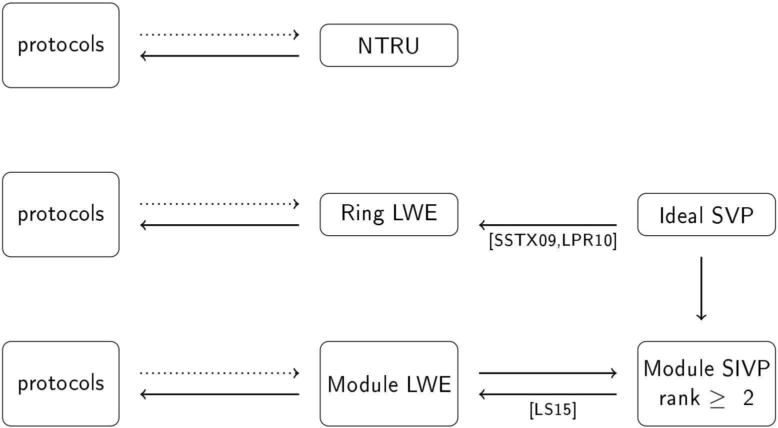


⚠ Arrows may not all compose (different parameters) ⚠

[SSTX09] Stehlé, Steinfeld, Tanaka, Xagawa. Efficient public key encryption based on ideal lattices. Asiacrypt.

[SSTX09] Lyubashevsky, Peikert, Regev. On ideal lattices and learning with errors over rings. Eurocrypt.

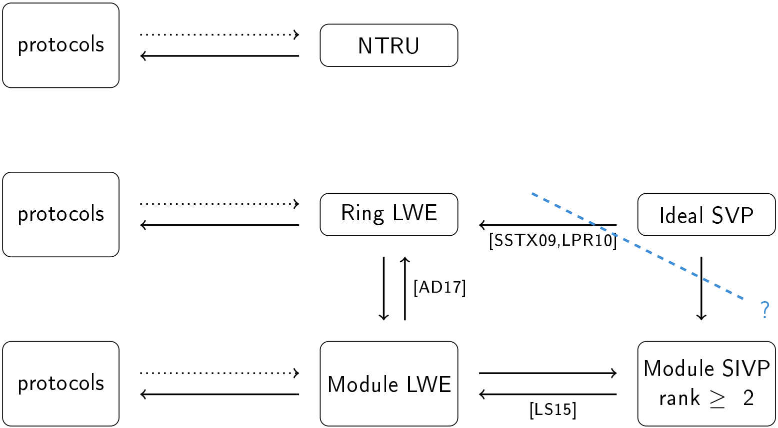
Reductions



⚠ Arrows may not all compose (different parameters) ⚠

[LS15] Langlois, Stehlé. Worst-case to average-case reductions for module lattices. DCC.

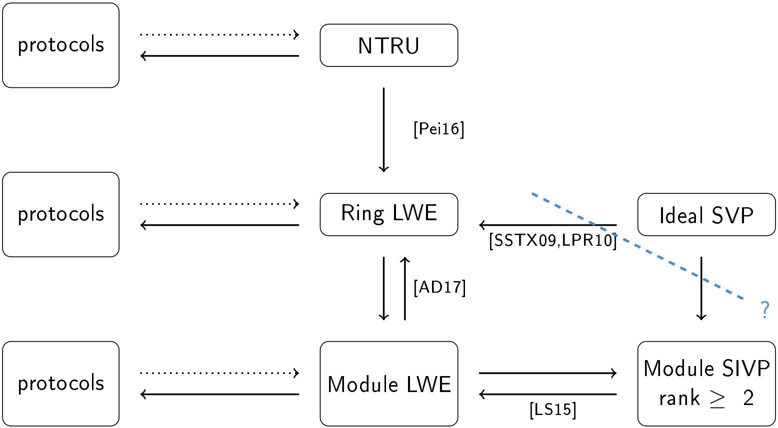
Reductions



⚠ Arrows may not all compose (different parameters) ⚠

[AD17] Albrecht, Deo. Large modulus ring-LWE ≥ module-LWE. Asiacrypt.

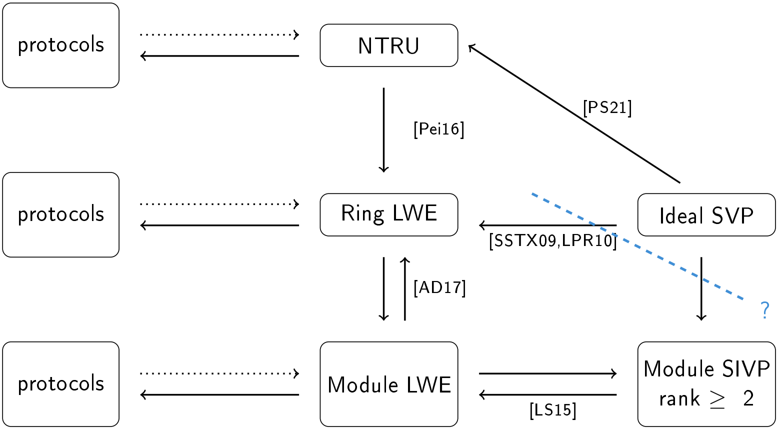
Reductions



⚠ Arrows may not all compose (different parameters) ⚠

[Pei16] Peikert. A decade of lattice cryptography. Foundations and Trends in TCS.

Reductions



⚠ Arrows may not all compose (different parameters) ⚠

[PS21] Pellet-Mary, Stehlé. On the hardness of the NTRU problem. Asiacrypt.

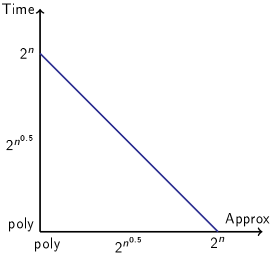
Summing up

breaking ideal-SVP $\not\Rightarrow$ breaking RLWE / module-LWE / NTRU

- as long as the attack does not generalize to rank ≥ 2, we are safe
- belief that there is a gap between rank 1 (ideals) and rank ≥ 2

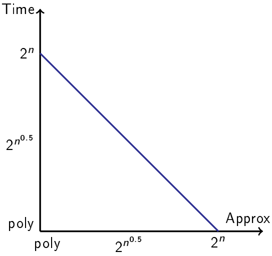
State-of-the-art for ideal-SVP

How easy is ideal-SVP compared to SVP?

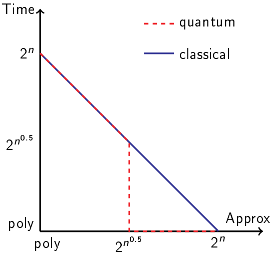


Unstructured lattices

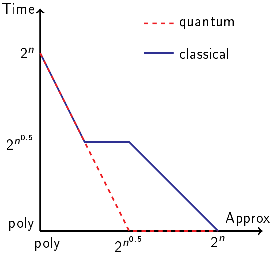
How easy is ideal-SVP compared to SVP?



Unstructured lattices



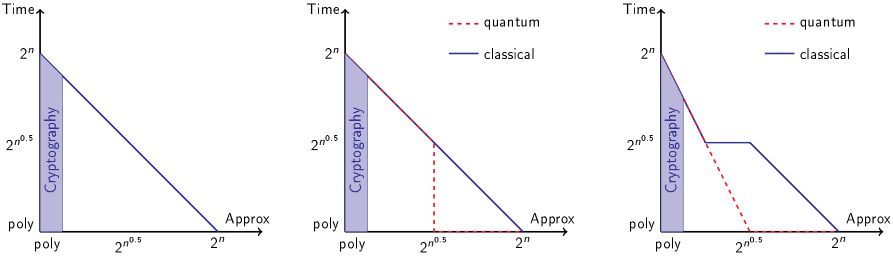
ideals lattices [CDW17]
(in cyclotomic fields)



ideals lattices [PHS19,BR20]
(with $2^{O(n)}$ pre-processing)

[CDW17] Cramer, Ducas, Wesolowski. Short stickelberger class relations and application to ideal-SVP. Eurocrypt.
[PHS19] Pellet-Mary, Hanrot, Stehlé. Approx-SVP in ideal lattices with pre-processing. Eurocrypt.
[BR20] Bernard, Roux-Langlois. Twisted-PHS: using the product formula to solve approx-SVP in ideal lattices. AC.

How easy is ideal-SVP compared to SVP?



Unstructured lattices

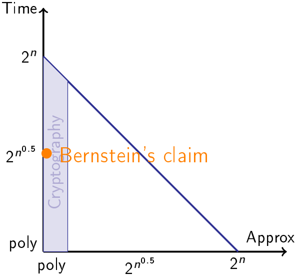
ideals lattices [CDW17]
(in cyclotomic fields)

ideals lattices [PHS19,BR20]
(with $2^{O(n)}$ pre-processing)

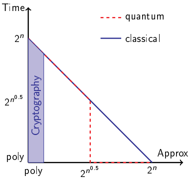
- almost no impact for crypto size params
- no reduction from RLWE to ideal-SVP

[CDW17] Cramer, Ducas, Wesolowski. Short stickelberger class relations and application to ideal-SVP. Eurocrypt.
[PHS19] Pellet-Mary, Hanrot, Stehlé. Approx-SVP in ideal lattices with pre-processing. Eurocrypt.
[BR20] Bernard, Roux-Langlois. Twisted-PHS: using the product formula to solve approx-SVP in ideal lattices. AC.

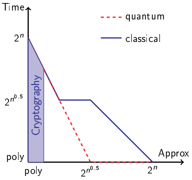
Bernstein's claim



Ideal lattices
(power-of-two cyclotomic)

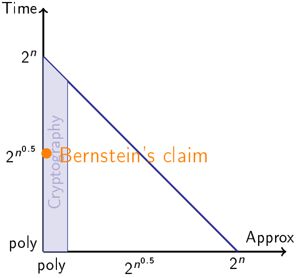


ideals lattices [CDW17]
(in cyclotomic fields)



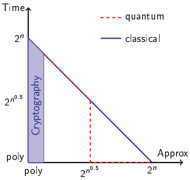
ideals lattices [PHS19,BR20]
(with $2^{O(n)}$ pre-processing)

Bernstein's claim

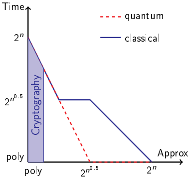


Ideal lattices
(power-of-two cyclotomic)

- This is in the crypto regime
  (but still ideal-SVP $\not\to$ RLWE)

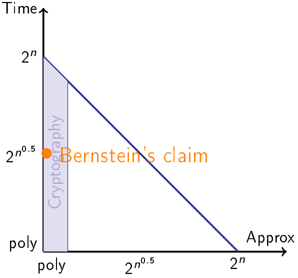


ideals lattices [CDW17]
(in cyclotomic fields)



ideals lattices [PHS19,BR20]
(with $2^{O(n)}$ pre-processing)

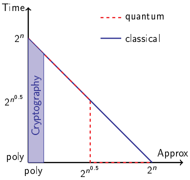
Bernstein's claim



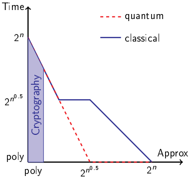
Ideal lattices
(power-of-two cyclotomic)

- This is in the crypto regime
  (but still ideal-SVP $\not\to$ RLWE)

⚠ So far, no argument to support this claim



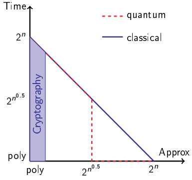
ideals lattices [CDW17]
(in cyclotomic fields)



ideals lattices [PHS19,BR20]
(with $2^{O(n)}$ pre-processing)

Concrete impact

When does [CDW17] starts out-performing BKZ?

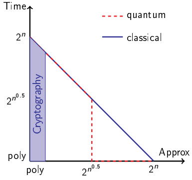


ideals lattices [CDW17]
(in cyclotomic fields)

Concrete impact

When does [CDW17] starts out-performing BKZ?

- For reasonable run-time (a few core-days):
  - dim $\gtrsim 5\,000$
- For NIST's weakest security requirement:
  - dim $\gtrsim 17\,000$

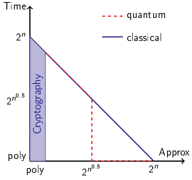


ideals lattices [CDW17]
(in cyclotomic fields)

Concrete impact

When does [CDW17] starts out-performing BKZ?

- For reasonable run-time (a few core-days):
  - dim $\gtrsim 5\,000$
- For NIST's weakest security requirement:
  - dim $\gtrsim 17\,000$
- Dimension of NIST candidates:
  - dim ≈ 500 or $1\,000$



ideals lattices [CDW17]
(in cyclotomic fields)

Techniques

Math background

Notation

$K = \mathbb{Q}[X]/(X^n + 1)$, with $n = 2^k$ (or any cyclotomic field)

$O_K = \mathbb{Z}[X]/(X^n + 1)$

Math background

Notation

$K = \mathbb{Q}[X]/(X^n + 1)$, with $n = 2^k$ (or any cyclotomic field)

$O_K = \mathbb{Z}[X]/(X^n + 1)$

- Units: $O_K^\times = \{a \in O_K \mid \exists b \in O_K, ab = 1\}$

Math background

Notation

$K = \mathbb{Q}[X]/(X^n + 1)$, with $n = 2^k$ (or any cyclotomic field)

$O_K = \mathbb{Z}[X]/(X^n + 1)$

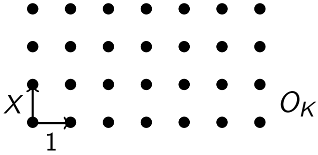
- Units: $O_K^\times = \{a \in O_K \mid \exists b \in O_K, ab = 1\}$
- Principal ideals: $\langle g \rangle = \{gr \mid r \in O_K\}$
  - g is a generator of $\langle g \rangle$
  - $\{$ generators of $\langle g \rangle$ $\} = \{gu \mid u \in O_K^\times\}$

Why is $\langle g \rangle$ a lattice?

O_K is a lattice

$$O_K = \mathbb{Z}[X]/(X^n+1) \rightarrow \mathbb{R}^n$$

$$r(X) = \sum_{i=0}^{n-1} r_i X^i \mapsto (r_0, r_1, \ldots, r_{n-1})$$

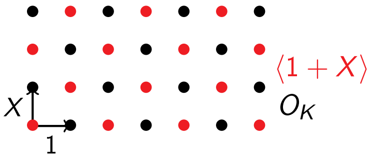


Why is $\langle g \rangle$ a lattice?

O_K is a lattice

$$O_K = \mathbb{Z}[X]/(X^n+1) \;\to\; \mathbb{R}^n$$
$$r(X) = \sum_{i=0}^{n-1} r_i X^i \;\mapsto\; (r_0, r_1, \ldots, r_{n-1})$$

$$\begin{cases} \langle g \rangle \subseteq O_K \simeq \mathbb{Z}^n \\ \text{stable by '+' and '−'} \end{cases} \Rightarrow \text{ideal lattice}$$



Why is $\langle g \rangle$ a lattice?

O_K is a lattice

$$\begin{aligned} O_K = \mathbb{Z}[X]/(X^n+1) \; &\to \; \mathbb{R}^n \\ r(X) = \sum_{i=0}^{n-1} r_i X^i \; &\mapsto \; (r_0, r_1, \ldots, r_{n-1}) \end{aligned}$$

$$\begin{cases} \langle g \rangle \subseteq O_K \simeq \mathbb{Z}^n \\ \text{stable by '+' and '−'} \end{cases} \Rightarrow \text{ideal lattice}$$

Basis: $g, gX, gX^2, \ldots, gX^{n-1}$

Why is $\langle g \rangle$ a lattice?

O_K is a lattice

$$O_K = \mathbb{Z}[X]/(X^n+1) \rightarrow \mathbb{R}^n$$
$$r(X) = \sum_{i=0}^{n-1} r_i X^i \mapsto (r_0, r_1, \ldots, r_{n-1})$$

$$\begin{cases} \langle g \rangle \subseteq O_K \simeq \mathbb{Z}^n \\ \text{stable by '+' and '−'} \end{cases} \Rightarrow \text{ideal lattice}$$

Basis: $g, gX, gX^2, \ldots, gX^{n-1}$

$$\text{i.e.,} \quad \begin{pmatrix} g_0 & & & \\ g_1 & & & \\ \vdots & & & \\ g_{n-1} & & & \end{pmatrix}$$

Why is $\langle g \rangle$ a lattice?

O_K is a lattice

$$O_K = \mathbb{Z}[X]/(X^n+1) \;\to\; \mathbb{R}^n$$
$$r(X) = \sum_{i=0}^{n-1} r_i X^i \;\mapsto\; (r_0, r_1, \dots, r_{n-1})$$

$$\begin{cases} \langle g \rangle \subseteq O_K \simeq \mathbb{Z}^n \\ \text{stable by '$+$' and '$-$'} \end{cases} \quad \Rightarrow \quad \text{ideal lattice}$$

Basis: $g, gX, gX^2, \dots, gX^{n-1}$

$$\text{i.e.,} \quad \begin{pmatrix} g_0 & -g_{n-1} & & \\ g_1 & g_0 & & \\ \vdots & \vdots & & \\ g_{n-1} & g_{n-2} & & \end{pmatrix}$$

Why is $\langle g \rangle$ a lattice?

O_K is a lattice

$$O_K = \mathbb{Z}[X]/(X^n+1) \;\to\; \mathbb{R}^n$$
$$r(X) = \sum_{i=0}^{n-1} r_i X^i \;\mapsto\; (r_0, r_1, \dots, r_{n-1})$$

$$\begin{cases} \langle g \rangle \subseteq O_K \simeq \mathbb{Z}^n \\ \text{stable by `}+\text{' and `}-\text{'} \end{cases} \Rightarrow \text{ ideal lattice}$$

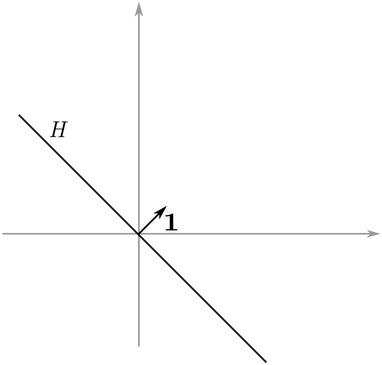
Basis: $g, gX, gX^2, \dots, gX^{n-1}$

$$\text{i.e., } \begin{pmatrix} g_0 & -g_{n-1} & \cdots & -g_1 \\ g_1 & g_0 & \cdots & -g_2 \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-1} & g_{n-2} & \cdots & g_0 \end{pmatrix}$$

The Log space

Log : $O_K \to \mathbb{R}^n$ (take the log of every coordinate)

Let $1 = (1, \cdots, 1)$ and $H = 1^{\perp}$.



The Log space

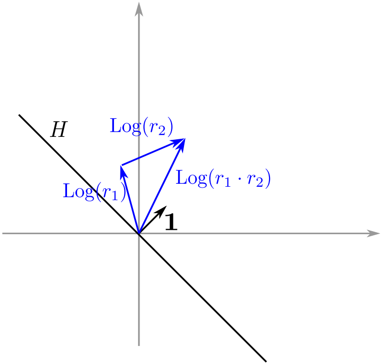
Log : $O_K \to \mathbb{R}^n$ (take the log of every coordinate)

Let $\mathbf{1} = (1, \cdots, 1)$ and $H = \mathbf{1}^\perp$.

Properties ($r \in O_K$)

$\operatorname{Log} r = h + a \cdot \mathbf{1}$, with $h \in H$

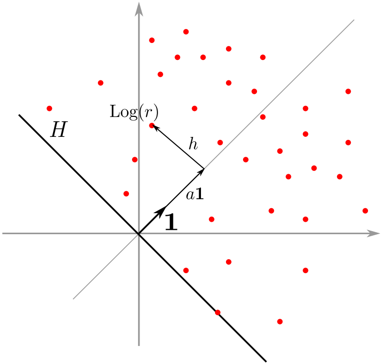
- $\operatorname{Log}(r_1 \cdot r_2) = \operatorname{Log}(r_1) + \operatorname{Log}(r_2)$



The Log space

Log : $O_K \to \mathbb{R}^n$ (take the log of every coordinate)

Let $\mathbf{1} = (1, \cdots, 1)$ and $H = \mathbf{1}^{\perp}$.



Properties ($r \in O_K$)

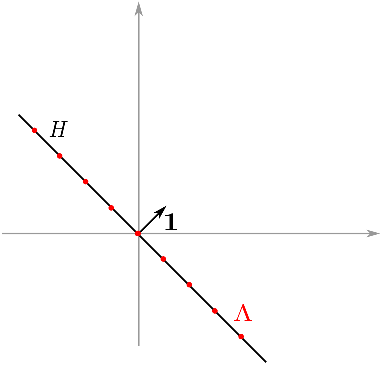
Log $r = h + a \cdot \mathbf{1}$, with $h \in H$

- $\text{Log}(r_1 \cdot r_2) = \text{Log}(r_1) + \text{Log}(r_2)$
- $a \geq 0$

The Log space

Log : $O_K \to \mathbb{R}^n$ (take the log of every coordinate)

Let $\mathbf{1} = (1, \cdots, 1)$ and $H = \mathbf{1}^\perp$.



Properties ($r \in O_K$)

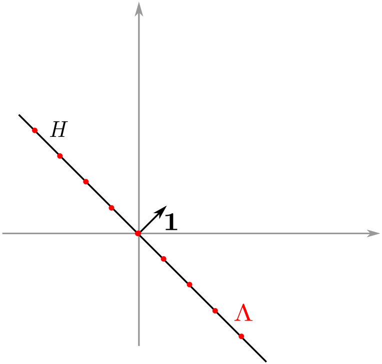
Log $r = h + a \cdot \mathbf{1}$, with $h \in H$

- $\mathrm{Log}(r_1 \cdot r_2) = \mathrm{Log}(r_1) + \mathrm{Log}(r_2)$
- $a \geq 0$
- $a = 0$ iff r is a unit

The Log space

$\mathrm{Log} : O_K \to \mathbb{R}^n$ (take the log of every coordinate)

Let $1 = (1, \cdots, 1)$ and $H = 1^{\perp}$.



Properties ($r \in O_K$)

$\mathrm{Log}\, r = h + a \cdot 1$, with $h \in H$

- $\mathrm{Log}(r_1 \cdot r_2) = \mathrm{Log}(r_1) + \mathrm{Log}(r_2)$
- $a \geq 0$
- $a = 0$ iff r is a unit

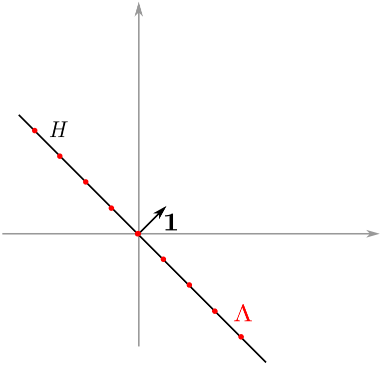
The Log unit lattice

$\Lambda := \mathrm{Log}(O_K^{\times})$ is a lattice in H.

The Log space

Log : $O_K \to \mathbb{R}^n$ (take the log of every coordinate)

Let $\mathbf{1} = (1, \cdots, 1)$ and $H = \mathbf{1}^\perp$.



Properties ($r \in O_K$)

$\operatorname{Log} r = h + a \cdot \mathbf{1}$, with $h \in H$

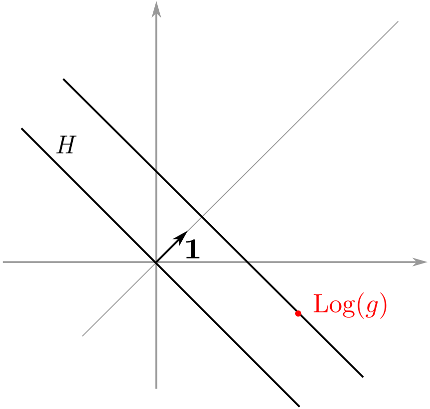
- $\operatorname{Log}(r_1 \cdot r_2) = \operatorname{Log}(r_1) + \operatorname{Log}(r_2)$
- $a \geq 0$
- $a = 0$ iff r is a unit
- $\|r\| \simeq \exp(\|\operatorname{Log} r\|_\infty)$

The Log unit lattice

$\Lambda := \operatorname{Log}(O_K^\times)$ is a lattice in H.

The basic algorithm [CGS14,CDPR16]

What does $\mathrm{Log}\langle g\rangle$ look like?

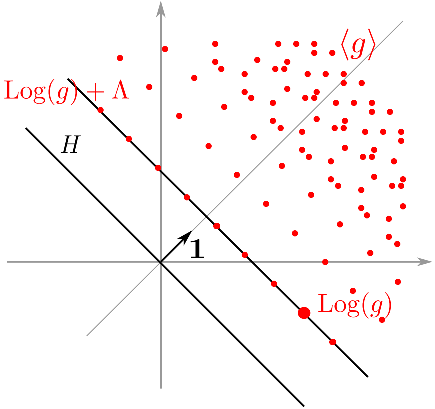


[CGS14]: Campbell, Groves, and Shepherd. Soliloquy: a cautionary tale.

[CDPR16] Cramer, Ducas, Peikert and Regev. Recovering short generators of principal ideals in cyclotomic rings. EC.

The basic algorithm [CGS14,CDPR16]

What does $\mathrm{Log}\langle g\rangle$ look like?

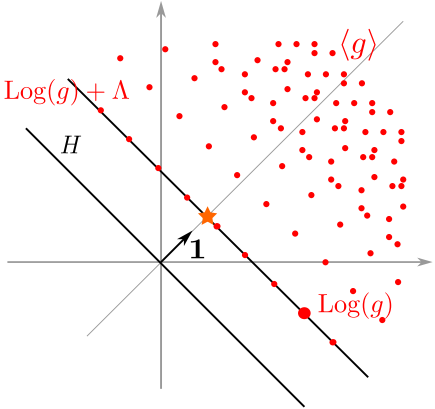


[CGS14]: Campbell, Groves, and Shepherd. Soliloquy: a cautionary tale.

[CDPR16] Cramer, Ducas, Peikert and Regev. Recovering short generators of principal ideals in cyclotomic rings. EC.

The basic algorithm [CGS14,CDPR16]

What does $\mathrm{Log}\langle g\rangle$ look like?

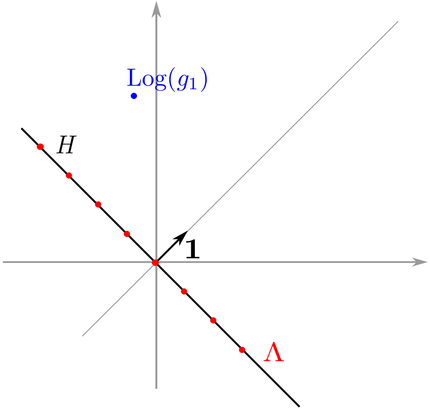


[CGS14]: Campbell, Groves, and Shepherd. Soliloquy: a cautionary tale.

[CDPR16] Cramer, Ducas, Peikert and Regev. Recovering short generators of principal ideals in cyclotomic rings. EC.

The basic algorithm [CGS14,CDPR16]

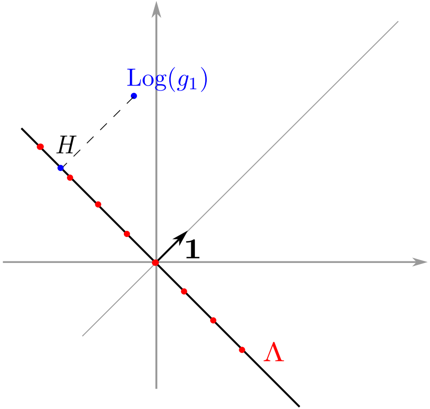
- Find a generator g_1 of $\langle g \rangle$.
  - [BS16]: quantum poly time



[BS16]: Biasse, Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

The basic algorithm [CGS14,CDPR16]

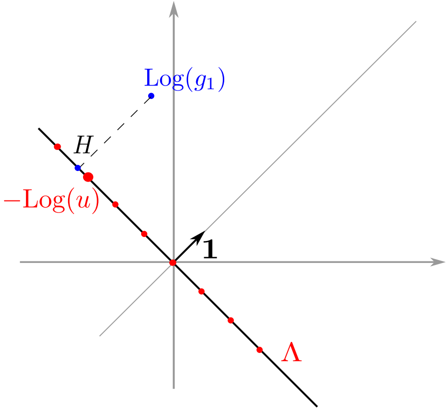
- Find a generator g_1 of $\langle g \rangle$.
  - [BS16]: quantum poly time



[BS16]: Biasse, Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

The basic algorithm [CGS14,CDPR16]

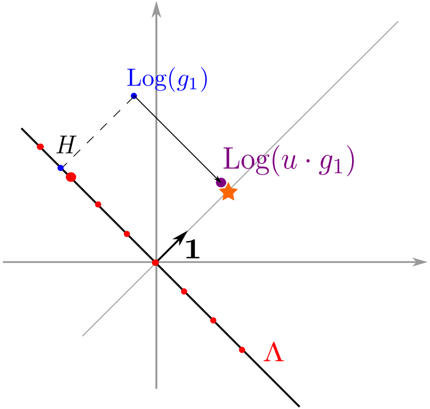
- Find a generator g_1 of $\langle g \rangle$.
  - [BS16]: quantum poly time
- Solve CVP in Λ



[BS16]: Biasse, Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

The basic algorithm [CGS14,CDPR16]

- Find a generator g_1 of $\langle g \rangle$.
  - [BS16]: quantum poly time
- Solve CVP in Λ

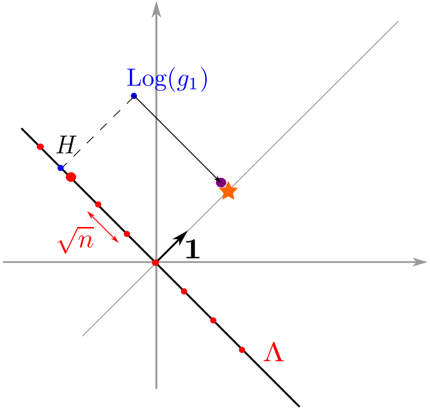


[BS16]: Biasse, Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

The basic algorithm [CGS14,CDPR16]

- Find a generator g_1 of $\langle g \rangle$.
  - [BS16]: quantum poly time
- Solve CVP in Λ
  - Good basis of Λ (cyclotomic field)

    $\Rightarrow$ CVP in poly time
    $\Rightarrow \|h\| \leq \widetilde{O}(\sqrt{n})$



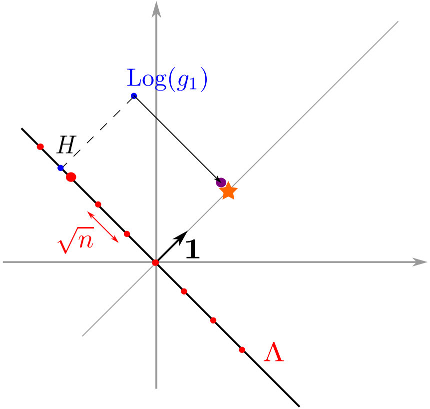
[BS16]: Biasse, Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

The basic algorithm [CGS14,CDPR16]

- Find a generator g_1 of $\langle g \rangle$.
  - [BS16]: quantum poly time
- Solve CVP in Λ
  - Good basis of Λ (cyclotomic field)

    $\Rightarrow$ CVP in poly time
    $\Rightarrow \|h\| \leq \widetilde{O}(\sqrt{n})$

$$\boxed{\|ug_1\| \leq 2^{\widetilde{O}(\sqrt{n})} \cdot \lambda_1}$$



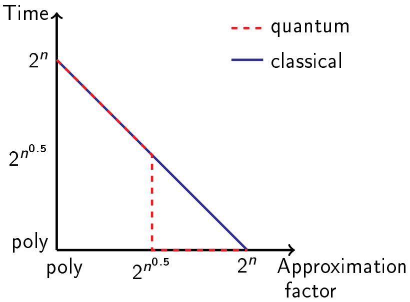
[BS16]: Biasse, Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

The basic algorithm [CGS14,CDPR16]

- Find a generator g_1 of $\langle g \rangle$.
  - [BS16]: quantum poly time
- Solve CVP in Λ
  - Good basis of Λ
    (cyclotomic field)

    $\Rightarrow$ CVP in poly time
    $\Rightarrow \|h\| \leq \widetilde{O}(\sqrt{n})$

$$\boxed{\|ug_1\| \leq 2^{\widetilde{O}(\sqrt{n})} \cdot \lambda_1}$$



- Heuristic
- Cyclotomic fields

[BS16]: Biasse, Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

More evolved algorithms: using S-units

Idea: replace units by S-units

More evolved algorithms: using S-units

Idea: replace units by S-units

+ covering radius of Log-S-unit lattice = $O(1)$ (instead of $O(\sqrt{n})$)
  - can reach approximation factor $\mathrm{poly}(n)$ (instead of $2^{O(\sqrt{n})}$)

More evolved algorithms: using S-units

Idea: replace units by S-units

+ covering radius of Log-S-unit lattice $= O(1)$ (instead of $O(\sqrt{n})$)
  - can reach approximation factor $\mathrm{poly}(n)$ (instead of $2^{O(\sqrt{n})}$)

− we don't know a good basis of the Log-S-unit lattice
  - need to pre-compute it (time $2^{O(n)}$)
  - even with the best basis possible,
    we can only solve CVP with approx $O(\sqrt{n})$ in poly time
    $\Rightarrow$ still $2^{O(\sqrt{n})}$ approx-SVP in poly time

Conclusion

Attacks on module lattices

Not much:

- BKZ algorithm for modules [MS20]
  - does not outperform BKZ, but the algo uses only modules (no unstructured lattices)

[MS20] Mukherjee and Stephens-Davidowitz. Lattice reduction for modules, or how to reduce module-SVP to module-SVP. Crypto.

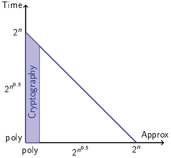
Attacks on module lattices

Not much:

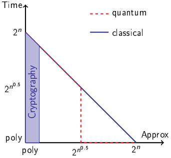
- BKZ algorithm for modules [MS20]
  - does not outperform BKZ, but the algo uses only modules (no unstructured lattices)
- Algorithm for SVP in rank-2 modules [LPSW19]
  - Needs an oracle solving CVP in a fixed lattice of dimension n^2

[LPSW19] Lee, Pellet-Mary, Stehlé, Wallet. An LLL algorithm for module lattices. Asiacrypt.

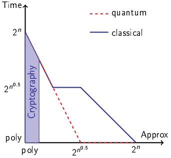
Conclusion



Unstructured lattices
and module lattices



ideals lattices [CDW17]
(in cyclotomic fields)

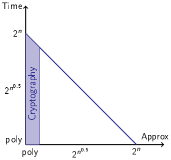


ideals lattices [PHS19,BR20]
(with $2^{O(n)}$ pre-processing)

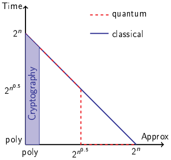
Missing ingredients to have an impact on crypto:

[1] https://pqcrypto2021.kr/download/program/3.1_PQC.pdf

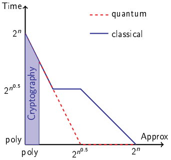
Conclusion



Unstructured lattices
and module lattices



ideals lattices [CDW17]
(in cyclotomic fields)



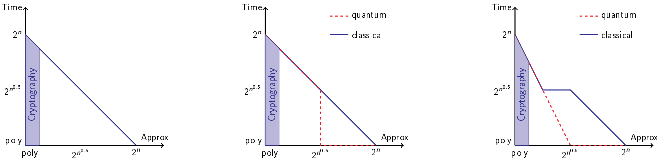
ideals lattices [PHS19,BR20]
(with $2^{O(n)}$ pre-processing)

Missing ingredients to have an impact on crypto:

- Attacks on modules of rank ≥ 2 (not ideals)

[1] https://pqcrypto2021.kr/download/program/3.1_PQC.pdf

Conclusion



Unstructured lattices and module lattices

ideals lattices [CDW17] (in cyclotomic fields)

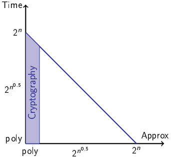
ideals lattices [PHS19,BR20] (with $2^{O(n)}$ pre-processing)

Missing ingredients to have an impact on crypto:

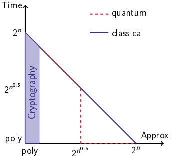
- Attacks on modules of rank ≥ 2 (not ideals)
- Attacks for small approximation factors

[1] https://pqcrypto2021.kr/download/program/3.1_PQC.pdf

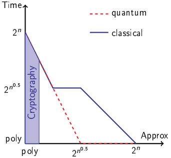
Conclusion



Unstructured lattices
and module lattices



ideals lattices [CDW17]
(in cyclotomic fields)



ideals lattices [PHS19,BR20]
(with $2^{O(n)}$ pre-processing)

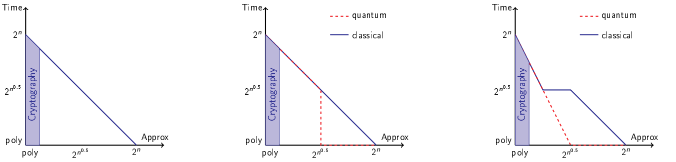
Missing ingredients to have an impact on crypto:

- Attacks on modules of rank ≥ 2 (not ideals)
- Attacks for small approximation factors

To learn more: Damien Stehlé's invited talk at PQCrypto 2021[1]

[1] https://pqcrypto2021.kr/download/program/3.1_PQC.pdf

Conclusion



Unstructured lattices and module lattices

ideals lattices [CDW17] (in cyclotomic fields)

ideals lattices [PHS19,BR20] (with $2^{O(n)}$ pre-processing)

Missing ingredients to have an impact on crypto:

- Attacks on modules of rank ≥ 2 (not ideals)
- Attacks for small approximation factors

To learn more: Damien Stehlé's invited talk at PQCrypto 2021[1]

Thank you

[1] https://pqcrypto2021.kr/download/program/3.1_PQC.pdf