Log-$\mathcal{S}$-unit Lattices using Explicit Stickelberger Generators to Solve Approx Ideal-SVP

Olivier Bernard[1,2] Andrea Lesavourey[1] Tuong-Huy Nguyen[1,3]
Adeline Roux-Langlois[1]

[1]Univ Rennes, CNRS, IRISA
olivier.bernard@normalesup.org,
{andrea.lesavourey, tuong-huy.nguyen, adeline.roux-langlois}@irisa.fr

[2]Thales, Gennevilliers

[3]DGA Maîtrise de l'Information, Bruz

Asiacrypt 2022

Taipei, 8th December 2022

Outline

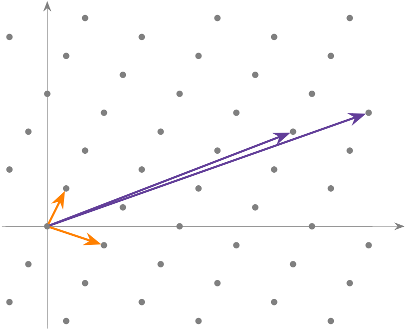
1. Cryptanalysis of Ideal-SVP
2. $\mathcal{S}$-unit attacks: Twisted-PHS
3. Towards medium dimensions

SVP and CVP in Euclidean lattices

Definition (Lattice)

A lattice L is a discrete subgroup of $\mathbb{R}^n$ (say a "$\mathbb{Z}$-vector space").

Example: $\begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}$ and $\begin{pmatrix} 13 & 5 \\ 17 & 6 \end{pmatrix}$ are two possible bases.



Shortest Vector Problem (SVP)

Given L, find the shortest $v \in L$:
$$\|v\|_2 = \lambda_1(L).$$

- NP-hard problem. [Ajt98]

Approximate SVP$_\gamma$

Given L and approximation factor γ, find $v \in L$ s.t. $\|v\|_2 \leq \gamma \cdot \lambda_1(L)$.

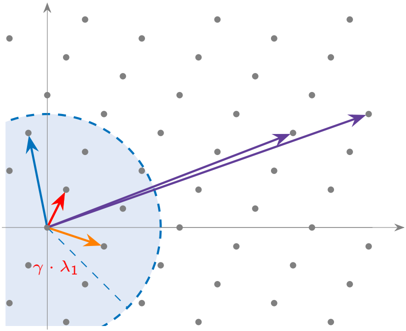
- Still hard for $\gamma = \mathrm{poly}(n)$?

SVP and CVP in Euclidean lattices

Definition (Lattice)

A lattice L is a discrete subgroup of $\mathbb{R}^n$ (say a "$\mathbb{Z}$-vector space").

Example: $\begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}$ and $\begin{pmatrix} 13 & 5 \\ 17 & 6 \end{pmatrix}$ are two possible bases.



Shortest Vector Problem (SVP)

Given L, find the shortest $v \in L$:
$\|v\|_2 = \lambda_1(L)$.

- ▶ NP-hard problem. [Ajt98]

Approximate SVP_γ

Given L and approximation factor γ,
find $v \in L$ s.t. $\|v\|_2 \leq \gamma \cdot \lambda_1(L)$.

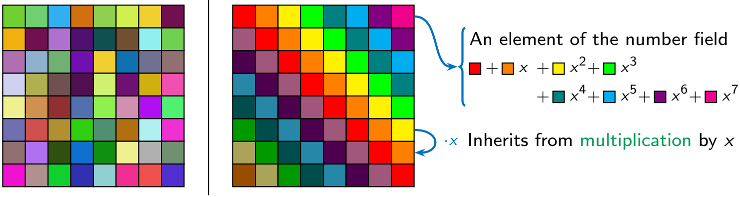
- ▶ Still hard for $\gamma = \mathrm{poly}(n)$?

Structured case: Ideal lattices

What is an ideal lattice ?

- Corresponds to an ideal in some number field

Unstructured case | **Ideal lattice** in $K = \mathbb{Q}[x]/\langle x^8 + 1\rangle$

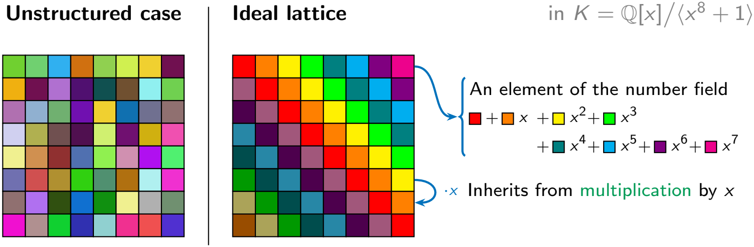


- For a long time, no algorithm for Ideal-SVP exploiting the structure.
- 2014: Quantum algorithm computing ($\mathcal{S}$-)units, class groups in polynomial time ! [EHKS14,BS16]
- Induces a long series of cryptanalysis works. [CGS14,CDPR16,CDW17/21,PHS19,BR20,this work,BL21,BEFHY22]

Structured case: Ideal lattices

What is an ideal lattice ?

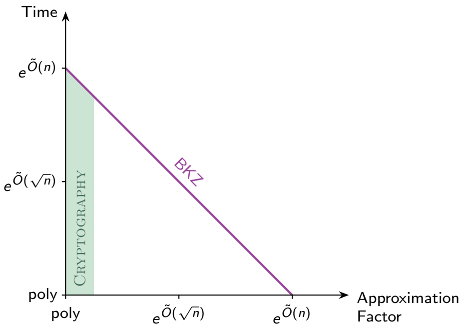
▶ Corresponds to an ideal in some number field



- For a long time, no algorithm for Ideal-SVP exploiting the structure.
- 2014: Quantum algorithm computing ($\mathcal{S}$-)units, class groups in polynomial time ! [EHKS14,BS16]
- Induces a long series of cryptanalysis works. [CGS14,CDPR16,CDW17/21,PHS19,BR20,this work,BL21,BEFHY22]

Algebraic cryptanalysis of Ideal-SVP: from Schnorr to $\mathcal{S}$-unit attacks

Picture for Ideal-SVP:

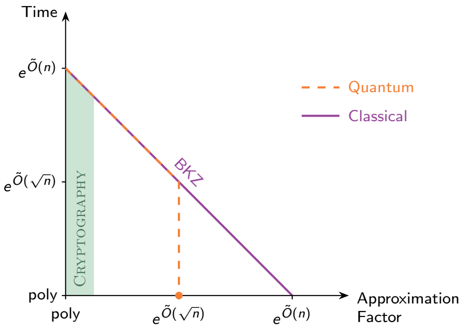


1. Schnorr's hierarchy (unstructured)
2. CDW algorithm [CDW17/21]: uses short Stickelberger relations.
3. PHS and Twisted-PHS [PHS19, BR20]: $\mathcal{S}$-unit attacks.

- How threatening are $\mathcal{S}$-unit attacks in practice ? *(Say, given a **quantum** computer)*

Algebraic cryptanalysis of Ideal-SVP: from Schnorr to $\mathcal{S}$-unit attacks

Picture for Ideal-SVP: *(cyclotomic fields)*

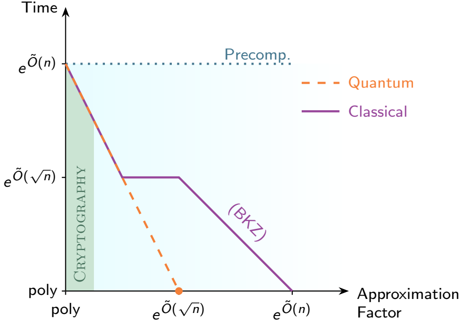


1. Schnorr's hierarchy (unstructured)
2. CDW algorithm [CDW17/21]: uses short Stickelberger relations.
3. PHS and Twisted-PHS [PHS19, BR20]: $\mathcal{S}$-unit attacks.

▶ How threatening are $\mathcal{S}$-unit attacks in practice ? *(Say, given a quantum computer)*

Algebraic cryptanalysis of Ideal-SVP: from Schnorr to $\mathcal{S}$-unit attacks

Picture for Ideal-SVP: *(cyclotomic fields)*

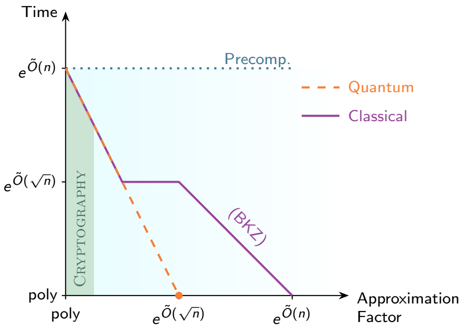


1. Schnorr's hierarchy (unstructured)
2. CDW algorithm [CDW17/21]: uses short Stickelberger relations.
3. PHS and Twisted-PHS [PHS19, BR20]: $\mathcal{S}$-unit attacks.

▶ How threatening are $\mathcal{S}$-unit attacks in practice ? *(Say, given a quantum computer)*

Algebraic cryptanalysis of Ideal-SVP: from Schnorr to $\mathcal{S}$-unit attacks

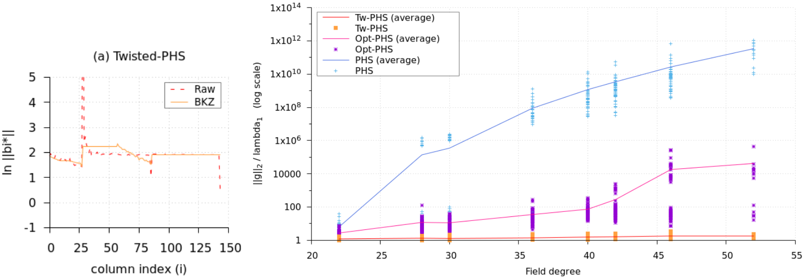
Picture for Ideal-SVP: *(cyclotomic fields)*



1. Schnorr's hierarchy (unstructured)
2. CDW algorithm [CDW17/21]: uses short Stickelberger relations.
3. PHS and Twisted-PHS [PHS19, BR20]: $\mathcal{S}$-unit attacks.

- How threatening are $\mathcal{S}$-unit attacks in practice ? *(Say, given a quantum computer)*

Phenomena observed in small dimensions [BR20]



1. Log-$\mathcal{S}$-unit (sub)lattices seem very orthogonal $(n \leq 70)$
2. Approximation Factors seem to grow very slowly $(n \leq 52)$

- **Warning!** Appearences can be very misleading in small dimensions.
  Need to gather more experimental observations before predicting things

Climbing degrees is classically HARD !!

Our work

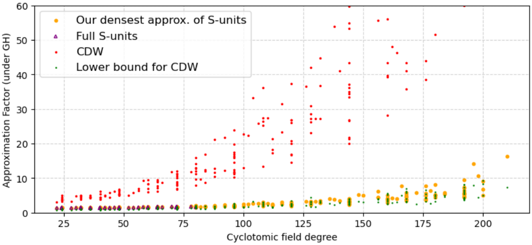
Build full-rank family of $\mathcal{S}$-units: *(cyclotomic fields, any conductor)*

Real $\mathcal{S}$-units $\bigcup$ Explicit Stickelberger generators

- Effective Formula for index in full $\mathcal{S}$-unit group, Short basis of Stickelberger ideal

Two applications:

1. Remove (almost all) quantum steps in the CDW algorithm.
   - Remove random walk, explicit PIP step
2. Simulate Twisted-PHS in medium dimensions up to 210:
   - Geometry of log-$\mathcal{S}$-unit lattices as in [BR20] *(cf. [BL21] for theory)*



$\mathcal{S}$-unit attacks principle

Let $\mathfrak{b}$ be a challenge ideal (i.e., a structured lattice).

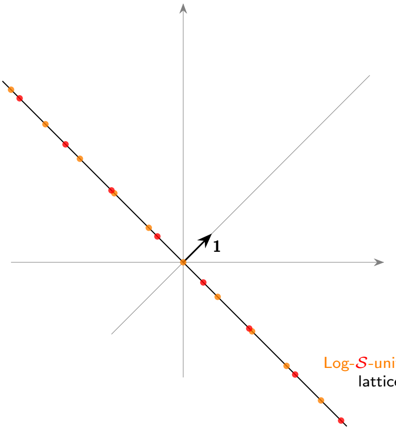
Principle:

1. Quantum (polynomial) step: decompose $\mathfrak{b}$ on a factor base $\mathcal{S}$.
   - All solutions modulo a multiplicative group, the $\mathcal{S}$-unit group.
2. Find a short solution (coset representative):
   - use some $\mathcal{S}$-logarithmic embedding $\mathrm{Log}_{\mathcal{S}}$
   - Solve an Approx-CVP instance in the log-$\mathcal{S}$-unit lattice
3. Hope that this is a short element of $\mathfrak{b}$.

Some important parameters:

- Choice of $\mathcal{S}$-logarithmic embedding *(Tw-PHS: use number-theoretic weights)*
- Choice of factor base *(Tw-PHS: maximize density)*
- Approx-CVP oracle *(Tw-PHS: randomized Babai's Nearest Plane)*

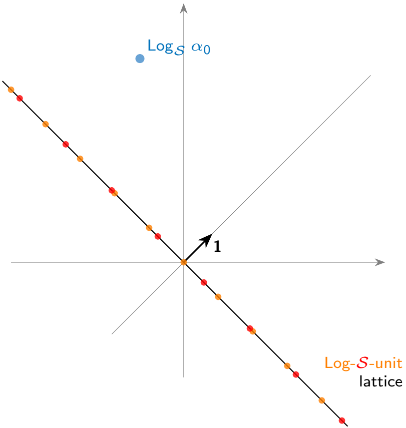
Artistic (?) view of an $\mathcal{S}$-unit attack (Twisted-PHS)



Let $\mathfrak{b}$ a challenge ideal.

1. Quantum decomposition output
   Apply $\mathrm{Log}_{\mathcal{S}}$
2. Short coset representative ?
3. Hope this is short in $\mathfrak{b}$.

Artistic (?) view of an $\mathcal{S}$-unit attack (Twisted-PHS)

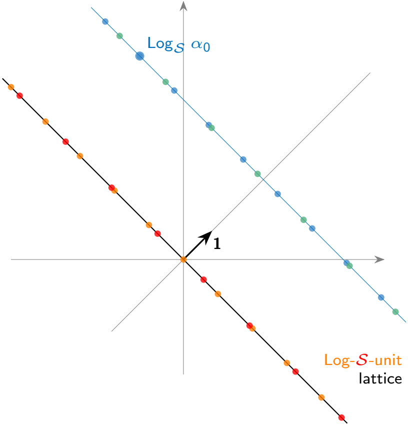


Let $\mathfrak{b}$ a challenge ideal.

1. Quantum decomposition output
   Apply $\mathrm{Log}_{\mathcal{S}}$
2. Short coset representative ?
3. Hope this is short in $\mathfrak{b}$.

$$\langle \alpha_0 \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{v}$$

Artistic (?) view of an $\mathcal{S}$-unit attack (Twisted-PHS)

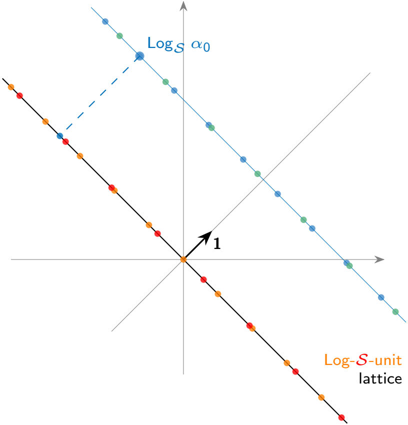


Let $\mathfrak{b}$ a challenge ideal.

1. Quantum decomposition output
   Apply Log$_\mathcal{S}$
2. Short coset representative ?
3. Hope this is short in $\mathfrak{b}$.

$$\langle \alpha_0 \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{v}$$

Artistic (?) view of an $\mathcal{S}$-unit attack (Twisted-PHS)

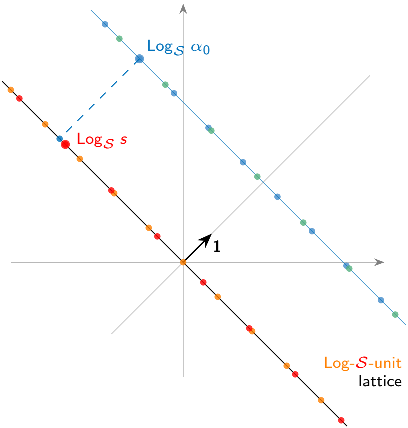


Let $\mathfrak{b}$ a challenge ideal.

1. Quantum decomposition output
   Apply $\mathrm{Log}_{\mathcal{S}}$
2. Short coset representative ?
3. Hope this is short in $\mathfrak{b}$.

$$\langle \alpha_0 \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{v}$$

Artistic (?) view of an $\mathcal{S}$-unit attack (Twisted-PHS)



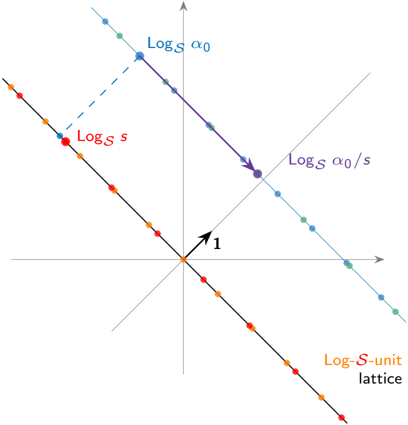
Let $\mathfrak{b}$ a challenge ideal.

1. Quantum decomposition output
   Apply $\mathrm{Log}_{\mathcal{S}}$
2. Short coset representative ?
3. Hope this is short in $\mathfrak{b}$.

$$\langle \alpha_0 \rangle = \mathfrak{b} \cdot \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{v}$$

$$\langle s \rangle = \prod_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}^{w}$$

Artistic (?) view of an $\mathcal{S}$-unit attack (Twisted-PHS)



Let $\mathfrak{b}$ a challenge ideal.

1. Quantum decomposition output
   Apply $\mathrm{Log}_{\mathcal{S}}$
2. Short coset representative ?
3. Hope this is short in $\mathfrak{b}$.

$$\begin{aligned} \langle \alpha_0 \rangle &= \mathfrak{b} \cdot \textstyle\prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{v} \\ \langle s \rangle &= \textstyle\prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{w} \\ \hline \langle \alpha_0/s \rangle &= \mathfrak{b} \cdot \textstyle\prod_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}^{v-w} \end{aligned}$$

A full-rank family of independent $\mathcal{S}$-units

Let $K_m = \mathbb{Q}(\zeta_m)$ be the mth cyclotomic field *($m \not\equiv 2 \mod 4$)*

Family of full-rank independent $\mathcal{S}$-units: *($\mathcal{S}$ set of prime ideals above d split primes)*

1. Circular units
2. Real $\mathcal{S}$-units (dim. n/2) of norm > 1
3. Explicit Stickelberger generators

- This is how we break the $n \leq 80$ barrier to reach $n = 210$!

Theorem (Stickelberger $\mathcal{S}$-units index formula (informal))

These form a maximal set of independent $\mathcal{S}$-units, generating a subgroup of index:

$$h_m^+ \cdot (h_m^-)^{d-1} \cdot 2^b \cdot \left(2^{\frac{\varphi(m)}{2}-1} \cdot 2^a\right)^d, \quad \text{for explicitly defined } a, b.$$

A full-rank family of independent $\mathcal{S}$-units

Let $K_m = \mathbb{Q}(\zeta_m)$ be the mth cyclotomic field *($m \not\equiv 2 \mod 4$)*

Family of full-rank independent $\mathcal{S}$-units: *($\mathcal{S}$ set of prime ideals above d split primes)*

1. Circular units
2. Real $\mathcal{S}$-units (dim. n/2) of norm > 1
3. Explicit Stickelberger generators

- This is how we break the $n \leq 80$ barrier to reach $n = 210$!

Theorem (Stickelberger $\mathcal{S}$-units index formula (informal))

These form a maximal set of independent $\mathcal{S}$-units, generating a subgroup of index:

$$h_m^+ \cdot (h_m^-)^{d-1} \cdot 2^b \cdot \left(2^{\frac{\varphi(m)}{2}-1} \cdot 2^a\right)^d, \quad \textit{for explicitly defined } a, b.$$

- Huge index: use 2-saturation to remove powers of 2, ...
  Use short Stickelberger basis to unlock high dimensions in practice [BK21]

Stickelberger ideal

Let $K_m = \mathbb{Q}(\zeta_m)$ be the mth cyclotomic field, $(m \not\equiv 2 \mod 4)$
$G_m = \mathrm{Gal}(K_m/\mathbb{Q}) = \left\{\sigma_s : \zeta_m \mapsto \zeta_m^s;\ (s, m) = 1\right\}$.

Definition (Stickelberger ideal)

Let $\mathcal{S}'_m$ be generated by $\{\theta_m(a);\ 0 < a < m\} \cup \{\frac{1}{2}N_m\}$, for:

$$\theta_m(a) = \sum_{s \in (\mathbb{Z}/m\mathbb{Z})^\times} \left\{-\frac{as}{m}\right\} \cdot \sigma_s^{-1} \qquad \in \mathbb{Q}[G_m],$$

and $N_m = \sum_{\sigma \in G_m} \sigma$. The Stickelberger ideal is $\mathcal{S}_m = \mathcal{S}'_m \cap \mathbb{Z}[G_m]$.

- Don't look too hard at the definition.
- The Stickelberger ideal gives free relations in the class group.
- The proof is explicit! but coefficients grow FAST. [Was97, pf. Th. 6.10, p.99])

Short Stickelberger basis

Short: $\beta = \sum_\sigma \varepsilon_\sigma \sigma \in \mathbb{Z}[G_m]$, with $\varepsilon_\sigma \in \{0,1\}$.

Theorem (A family of short Stickelberger elements [BK21, Pr. 3.1])

Let a, b st. $m \nmid a$, $m \nmid b$, $m \nmid (a+b)$. Then:

$$\theta_{a,b} = \theta_m(a) + \theta_m(b) - \theta_m(a+b)$$

is short; moreover $\|\theta_{a,b}\|_2 = \sqrt{\varphi(m)/2}$.

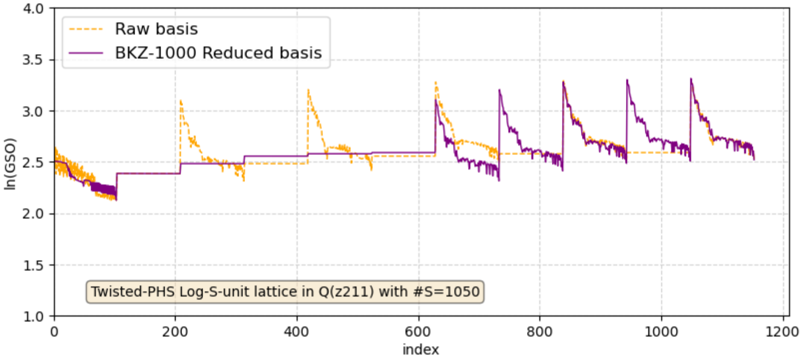
- From these we can extract a short basis for any m. [BK21, Th. 3.6]
- Express corresponding generators by Jacobi sums. [BK21, §5]
  - Efficient computation, directly in $\mathbb{Q}[\zeta_m]$.

Geometric characteristics

Orthogonality of log-$\mathcal{S}$-unit lattices:

- across all cyclotomic fields of degree ≤ 210 *(even in largest dimensions)*
- for all choices of factor base $\mathcal{S}$, any sublattice *(saturated or not)*

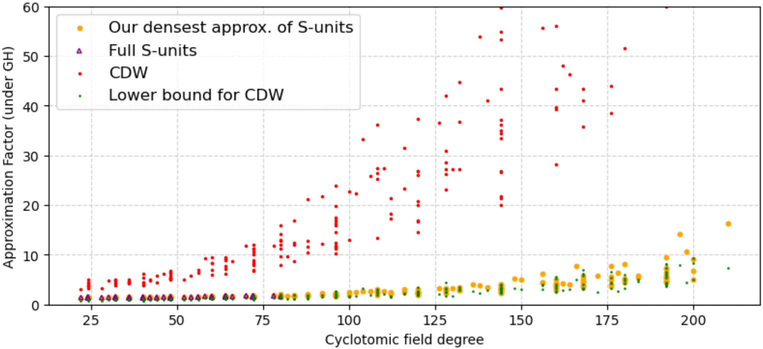
▶ This is a very general geometric phenomenon *(see also [BL21])*



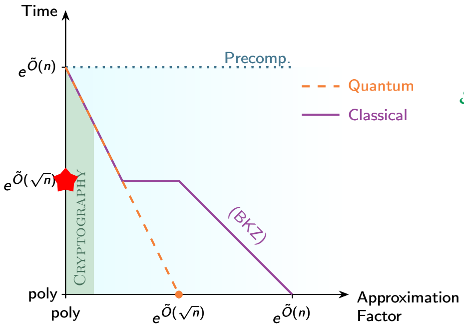
Approximation factor upper bound

Upper bound on performance of $\mathcal{S}$-unit attacks: (beyond degree 100)

- Shows no catastrophic impact of $\mathcal{S}$-unit attacks, neither reassuring
- Comparable to the volumetric lower bound of CDW
- Strong correlation between AF and density.



A recent conjecture by Bernstein & al.



$\mathcal{S}$-unit attacks: (continued)

1. PHS and Twisted-PHS [PHS19, BR20]
2. The conjecture [BERSV21]: use subexponential factor bases, enumeration-based CVP.

Some issues:

- No formal paper, but some code / description online.
- Experimental evidence so far limited to $\mathbb{Q}(\zeta_p)$ for $p \leq 43$.

Perspectives

On-going work:

1. Densify log-$\mathcal{S}$-unit sublattices: verify evolution of AF for several orbits
   - ▶ Saturation for all factors of h_m^- ($p \leq 2^{93}$)
2. Build a practical simulator of $\mathcal{S}$-unit attacks
   - Use extended data to reliably support finer heuristics and estimations.
   - Explain the strong connection between final AF and density.

▶ In particular, both allow to evaluate further previous conjecture.

Questions ?

Thank you!