Some attacks on algebraic lattice problems

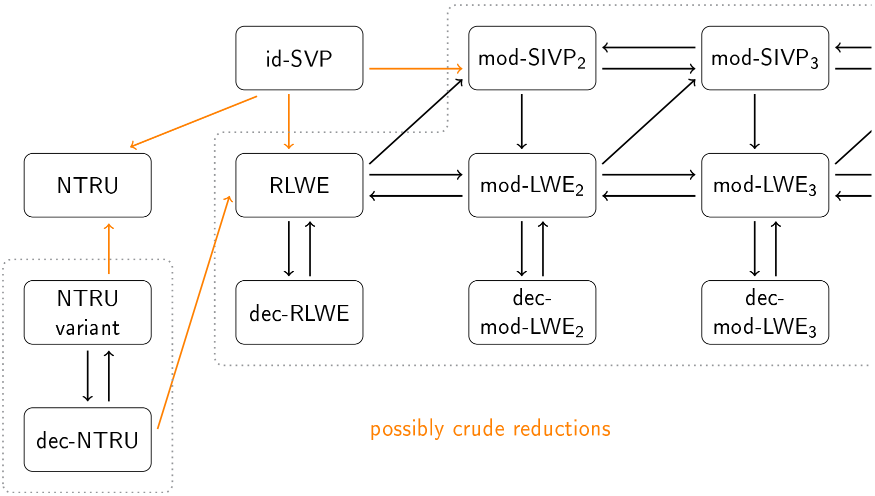
Alice Pellet--Mary

CNRS and university of Bordeaux, France

Fundations and applications of lattice-based cryptography workshop

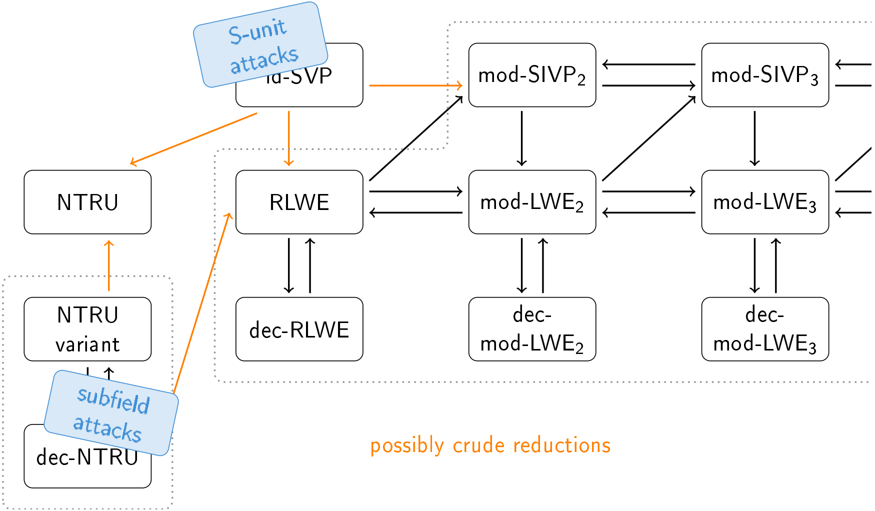
25-28 July 2022, Edinburgh

Two algebraic attacks



⚠ Arrows may not all compose (different parameters) ⚠

Two algebraic attacks



⚠ Arrows may not all compose (different parameters) ⚠

Outline of the talk

1. S-unit attacks on id-SVP

2. subfield attacks on dec-NTRU

Attacks on id-SVP

Brief history:

- using units [CGS14,CDPR16] $\rightsquigarrow$ cyclotomics, only principal ideals

[CGS14] Campbell, Groves, and Shepherd. Soliloquy: A cautionary tale. ETSI 2nd Quantum-Safe Crypto Workshop
[CDPR16] Cramer, Ducas, Peikert, and Regev. Recovering Short Generators of Principal Ideals in Cyclotomic Rings. Eurocrypt.

Attacks on id-SVP

Brief history:

- using units [CGS14,CDPR16] $\rightsquigarrow$ cyclotomics, only principal ideals
- using Stickelberger's relations [CDW17] $\rightsquigarrow$ cyclotomics, all ideals

[CDW17] Cramer, Ducas, Wesolowski. Short stickelberger class relations and application to ideal-SVP. Eurocrypt.

Attacks on id-SVP

Brief history:

- using units [CGS14,CDPR16] $\rightsquigarrow$ cyclotomics, only principal ideals
- using Stickelberger's relations [CDW17] $\rightsquigarrow$ cyclotomics, all ideals
- using S-units [PHS19,BR20] $\rightsquigarrow$ all ideals, different trade-offs

[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.

Attacks on id-SVP

Brief history:

- using units [CGS14,CDPR16] $\rightsquigarrow$ cyclotomics, only principal ideals
- using Stickelberger's relations [CDW17] $\rightsquigarrow$ cyclotomics, all ideals
- using S-units [PHS19,BR20] $\rightsquigarrow$ all ideals, different trade-offs

---

[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.

Attacks on id-SVP

Brief history:

- using units [CGS14,CDPR16] $\rightsquigarrow$ cyclotomics, only principal ideals
- using Stickelberger's relations [CDW17] $\rightsquigarrow$ cyclotomics, all ideals
- using S-units [PHS19,BR20] $\rightsquigarrow$ all ideals, different trade-offs

Motivations:

- that's the simplest case of mod-SIVP$_k$
- for the moment that's all we manage to do

[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.

Attacks on id-SVP

Brief history:

- using units [CGS14,CDPR16] $\rightsquigarrow$ cyclotomics, only principal ideals
- using Stickelberger's relations [CDW17] $\rightsquigarrow$ cyclotomics, all ideals
- using S-units [PHS19,BR20] $\rightsquigarrow$ all ideals, different trade-offs

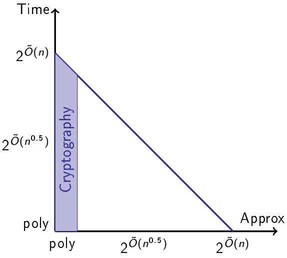
Motivations:

- that's the simplest case of mod-SIVP$_k$
- for the moment that's all we manage to do
- can also break some exotic cryptographic primitives/assumptions

[PHS19] Pellet-Mary, Hanrot, Stehlé. Approx-SVP in ideal lattices with pre-processing. Eurocrypt.

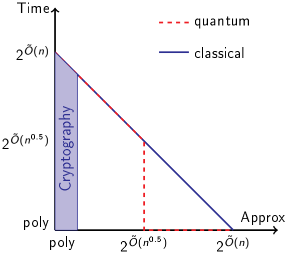
[BR20] Bernard, Roux-Langlois. Twisted-PHS: using the product formula to solve approx-SVP in ideal lattices. AC.

id-SVP vs SVP



SVP and mod-SVP$_k$

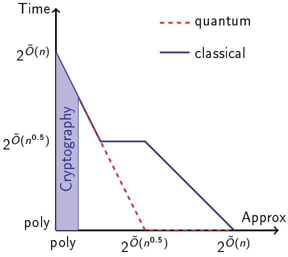
$(k \geq 2)$



id-SVP [CDW21]

(in cyclotomic fields)

units + Stickelberger



id-SVP [PHS19]

(with $2^{O(n)}$ pre-processing)

S-units

[CDW21] Cramer, Ducas, Wesolowski. Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time. Journal of the ACM.

[PHS19] Pellet-Mary, Hanrot, Stehlé. Approx-SVP in ideal lattices with pre-processing. Eurocrypt.

Number theoretical reminders

From now on:

- $K = \mathbb{Q}[X]/(X^d + 1)$ $\quad (d = 2^\ell)$
- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d + 1)$

Number theoretical reminders

From now on:

- $K = \mathbb{Q}[X]/(X^d + 1) \quad (d = 2^\ell)$
- $\mathcal{O}_K = \mathbb{Z}[X]/(X^d + 1)$

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 $\langle g \rangle$ $\} = \{gu \,|\, u \in O_K^\times\}$

Dimension of ideal lattices: $n = d$

The Log function

$$\begin{aligned} \mathrm{Log} : K &\to \mathbb{R}^d \\ y &\mapsto (\log|y(\alpha_1)|, \cdots, \log|y(\alpha_d)|) \end{aligned}$$

The Log function

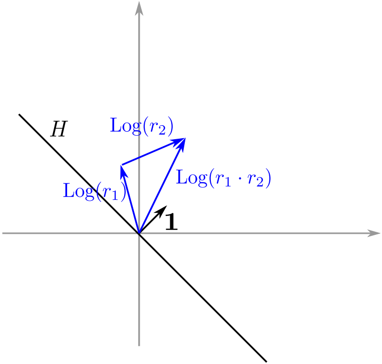
$$\text{Log} : K \to \mathbb{R}^d$$
$$y \mapsto (\log|y(\alpha_1)|, \cdots, \log|y(\alpha_d)|)$$

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

Properties ($r \in O_K$)

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

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



The Log function

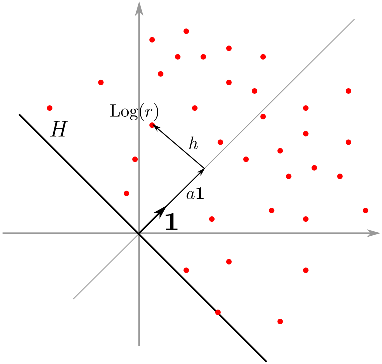
$$\begin{aligned}\text{Log} : K &\to \mathbb{R}^d \\ y &\mapsto (\log|y(\alpha_1)|, \cdots, \log|y(\alpha_d)|)\end{aligned}$$

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

Properties ($r \in O_K$)

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

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



The Log function

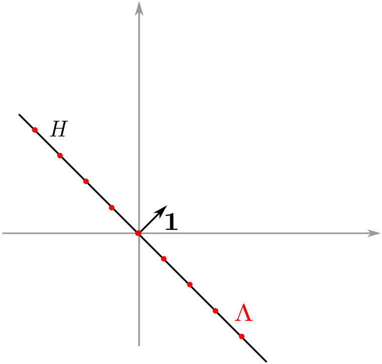
$$\text{Log}: K \to \mathbb{R}^d$$
$$y \mapsto (\log|y(\alpha_1)|, \cdots, \log|y(\alpha_d)|)$$

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

Properties ($r \in O_K$)

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

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



The Log function

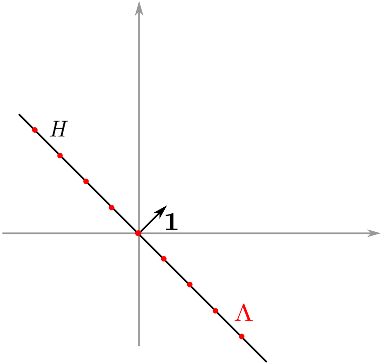
$$\mathrm{Log} : K \to \mathbb{R}^d$$
$$y \mapsto (\log|y(\alpha_1)|, \cdots, \log|y(\alpha_d)|)$$

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

Properties ($r \in O_K$)

$\mathrm{Log}\, r = h + a \cdot \mathbf{1}$, 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-unit lattice: $\Lambda := \mathrm{Log}(O_K^\times)$ is a lattice in H.

The Log function

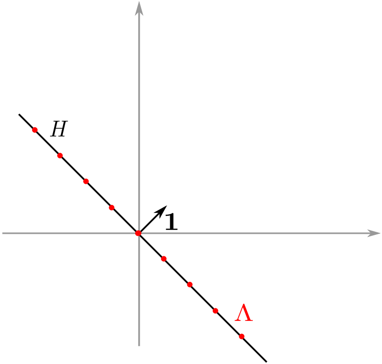
$$\text{Log} : K \to \mathbb{R}^d$$
$$y \mapsto (\log|y(\alpha_1)|, \cdots, \log|y(\alpha_d)|)$$

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

Properties ($r \in O_K$)

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

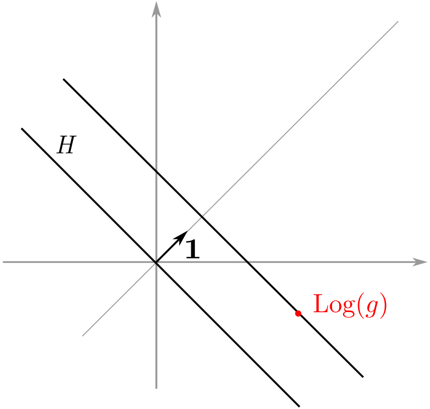
- $\text{Log}(r_1 \cdot r_2) = \text{Log}(r_1) + \text{Log}(r_2)$
- $a \geq 0$
- $a = 0$ iff r is a unit
- $\|r\| \simeq \exp(\|\text{Log}\, r\|_\infty)$



The Log-unit lattice: $\Lambda := \text{Log}(O_K^\times)$ is a lattice in H.

Solving id-SVP using units [CGS14,CDPR16]

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

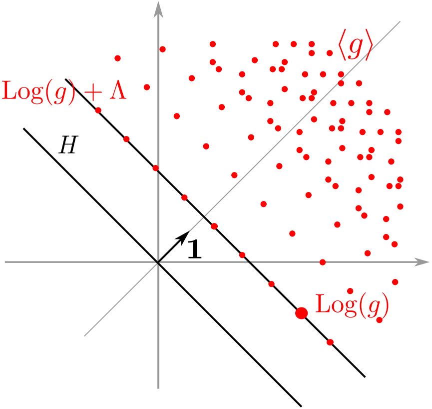


[CGS14]: Campbell, Groves, and Shepherd. Soliloquy: a cautionary tale.

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

Solving id-SVP using units [CGS14,CDPR16]

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

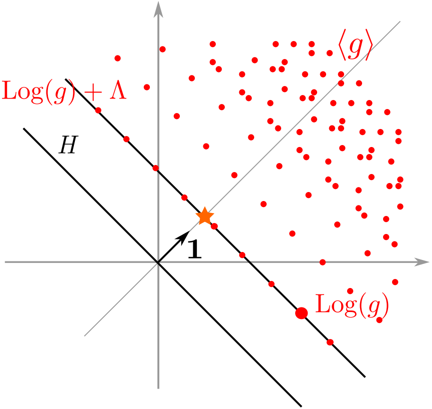


[CGS14]: Campbell, Groves, and Shepherd. Soliloquy: a cautionary tale.

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

Solving id-SVP using units [CGS14,CDPR16]

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

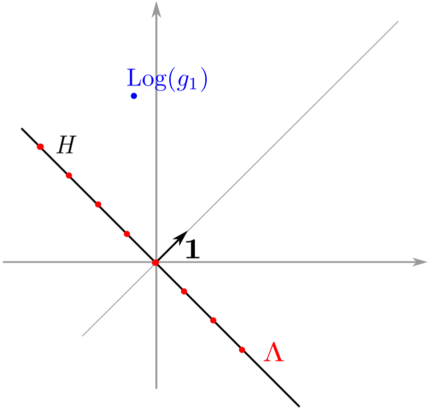


[CGS14]: Campbell, Groves, and Shepherd. Soliloquy: a cautionary tale.

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

Solving id-SVP using units [CGS14,CDPR16]

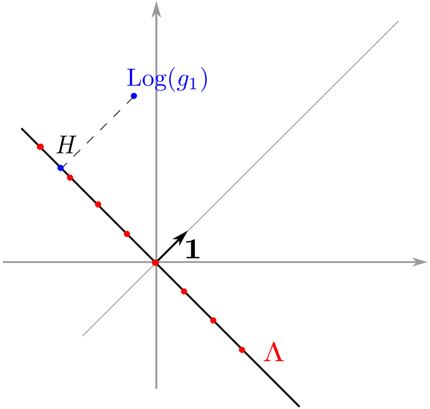
- Find a generator g_1 of $\langle g \rangle$.
  - [BS16]: quantum poly time



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

Solving id-SVP using units [CGS14,CDPR16]

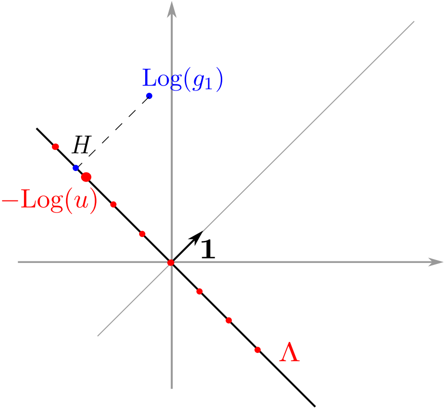
- Find a generator g_1 of $\langle g \rangle$.
  - [BS16]: quantum poly time



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

Solving id-SVP using units [CGS14,CDPR16]

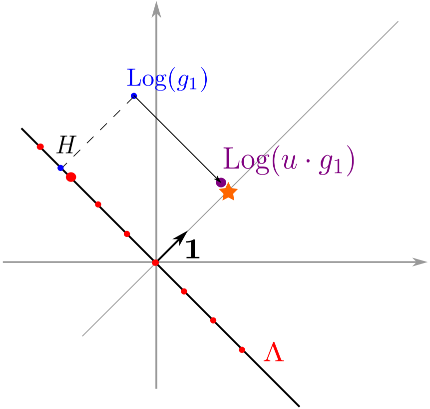
- Find a generator g_1 of $\langle g \rangle$.
  - [BS16]: quantum poly time
- Solve CVP in Λ



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

Solving id-SVP using units [CGS14,CDPR16]

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

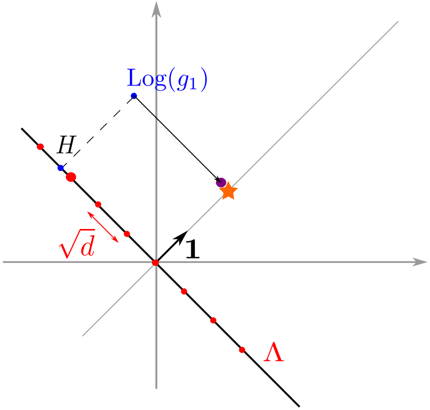


[BS16]: Biasse, Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

Solving id-SVP using units [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
    $\Rightarrow \|h\| \leq \widetilde{O}(\sqrt{d})$



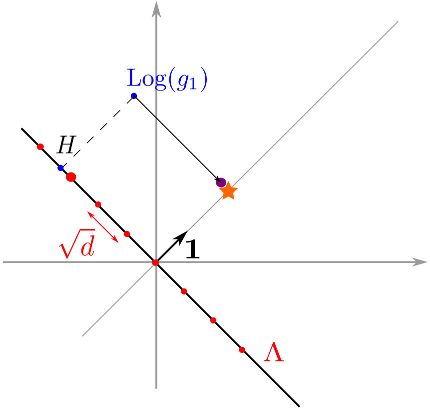
[BS16]: Biasse, Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

Solving id-SVP using units [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
    $\Rightarrow \|h\| \leq \widetilde{O}(\sqrt{d})$

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



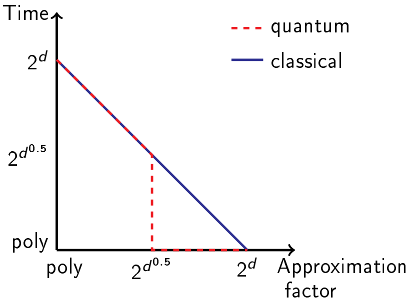
[BS16]: Biasse, Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. SODA.

Solving id-SVP using units [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
    $\Rightarrow \|h\| \leq \widetilde{O}(\sqrt{d})$

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



- 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.

Limitations

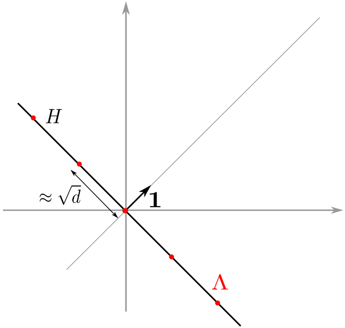
- only principal ideals $\rightsquigarrow$ solved using Stickelberger's relations

Limitations

- only principal ideals $\rightsquigarrow$ solved using Stickelberger's relations
- approximation factor $\exp(\sqrt{d})$
  - cannot do better if we only use units

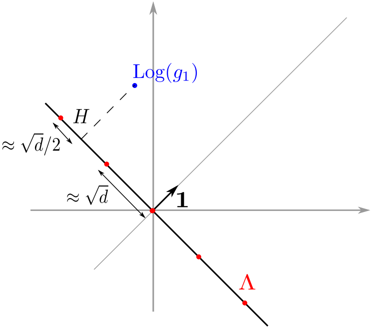
Limitations

- only principal ideals $\rightsquigarrow$ solved using Stickelberger's relations
- approximation factor $\exp(\sqrt{d})$
  - cannot do better if we only use units



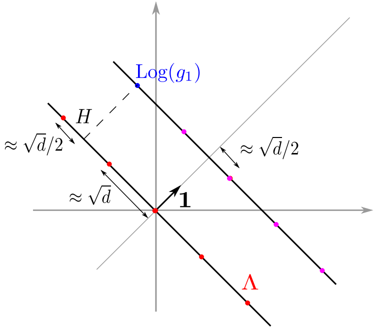
Limitations

- only principal ideals ⇝ solved using Stickelberger's relations
- approximation factor $\exp(\sqrt{d})$
  - cannot do better if we only use units



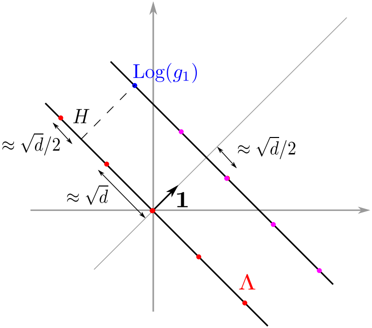
Limitations

- only principal ideals ⇝ solved using Stickelberger's relations
- approximation factor $\exp(\sqrt{d})$
  - cannot do better if we only use units



Limitations

- only principal ideals ⇝ solved using Stickelberger's relations
- approximation factor $\exp(\sqrt{d})$
  - cannot do better if we only use units



The covering radius of Λ is $\approx \sqrt{d}$

Generalize the algorithm: using S-units

Idea: replace units by S-units

Generalize the algorithm: using S-units

Idea: replace units by S-units

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

Generalize the algorithm: using S-units

Idea: replace units by S-units

\+ covering radius of Log-S-unit lattice $= O(1)$ (instead of $O(\sqrt{d})$)

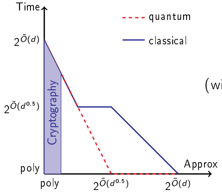
- can reach approximation factor $\mathrm{poly}(d)$ (instead of $2^{O(\sqrt{d})}$)

− we don't know a good basis of the Log-S-unit lattice

- need to pre-compute it (time $2^{O(d)}$)
- even with the best basis possible,
  we can only solve CVP with approx $O(\sqrt{d})$ in poly time
  $\Rightarrow$ still $2^{O(\sqrt{d})}$ approx-SVP in poly time

Generalize the algorithm: using S-units

Idea: replace units by S-units



(with $2^{O(d)}$ pre-processing)

\+ covering radius of Log-S-unit lattice $= O(1)$ (instead of $O(\sqrt{d})$)

- can reach approximation factor $\mathrm{poly}(d)$ (instead of $2^{O(\sqrt{d})}$)

– we don't know a good basis of the Log-S-unit lattice

- need to pre-compute it (time $2^{O(d)}$)
- even with the best basis possible,
  we can only solve CVP with approx $O(\sqrt{d})$ in poly time
  $\Rightarrow$ still $2^{O(\sqrt{d})}$ approx-SVP in poly time

Estimating the actual performance

How will these algorithms perform in practice for crypto relevant fields?

Estimating the actual performance

How will these algorithms perform in practice for crypto relevant fields?

[DPW19]: Answers the question for [CDW21] algorithm (units+Stickelberger)

- [CDW21] beats BKZ-80 for fields of degree $\gtrsim 2,000$
- [CDW21] beats BKZ-300 for fields of degree $\gtrsim 16,000$

[DPW19] Ducas, Plançon, Wesolowski. On the shortness of vectors to be found by the ideal-SVP quantum algorithm. Crypto.

Estimating the actual performance

How will these algorithms perform in practice for crypto relevant fields?

[DPW19]: Answers the question for [CDW21] algorithm (units+Stickelberger)

- [CDW21] beats BKZ-80 for fields of degree $\gtrsim 2,000$
- [CDW21] beats BKZ-300 for fields of degree $\gtrsim 16,000$

[BR19,BLNR21]: first experimental results for S-units

[BLNR21] Bernard, Lesavourey, Nguyen, Roux-Langlois. Log-S-unit lattices using Explicit Stickelberger Generators to solve Approx Ideal-SVP. EPrint.

Estimating the actual performance

How will these algorithms perform in practice for crypto relevant fields?

[DPW19]: Answers the question for [CDW21] algorithm (units+Stickelberger)

- [CDW21] beats BKZ-80 for fields of degree $\gtrsim 2,000$
- [CDW21] beats BKZ-300 for fields of degree $\gtrsim 16,000$

[BR19,BLNR21]: first experimental results for S-units

- main limitation so far: computation of the S-units
  - [BR19] computes S-units up to degree 70
  - [BLNR21] computes a sublattice of the S-units up to degree 210

[BLNR21] Bernard, Lesavourey, Nguyen, Roux-Langlois. Log-S-unit lattices using Explicit Stickelberger Generators to solve Approx Ideal-SVP. EPrint.

Estimating the actual performance

How will these algorithms perform in practice for crypto relevant fields?

[DPW19]: Answers the question for [CDW21] algorithm (units+Stickelberger)

- [CDW21] beats BKZ-80 for fields of degree $\gtrsim 2,000$
- [CDW21] beats BKZ-300 for fields of degree $\gtrsim 16,000$

[BR19,BLNR21]: first experimental results for S-units

- main limitation so far: computation of the S-units
  - [BR19] computes S-units up to degree 70
  - [BLNR21] computes a sublattice of the S-units up to degree 210
- no CVP with pre-processing so far (BKZ then Babai nearest plane)

[BLNR21] Bernard, Lesavourey, Nguyen, Roux-Langlois. Log-S-unit lattices using Explicit Stickelberger Generators to solve Approx Ideal-SVP. EPrint.

Outline of the talk

1. S-unit attacks on id-SVP
2. subfield attacks on dec-NTRU

Reminder: NTRU [HPS98]

dec-NTRU

Parameters: $q \geq B > 1$ and ψ distribution over $\mathcal{O}_K$ outputting elements $\leq B$

Objective: distinguish between h as above and u, where

- u is uniform in $\mathcal{O}_K/(q\mathcal{O}_K)$
- $f, g \leftarrow \psi$ conditioned on g invertible modulo q
- $h = f \cdot g^{-1} \bmod q$

[HPS98] Hoffstein, Pipher, and Silverman. NTRU: a ring based public key cryptosystem. ANTS.

Attacks on dec-NTRU

Brief history:

- subfield attacks [ABD16,CJL16]
  - solves dec-NTRU in time $\approx \exp\left(\frac{d \cdot \log B}{(\log q)^2}\right)$
    $\rightsquigarrow$ e.g., for $B = O(1)$, poly time attack when $q \gtrsim 2^{\sqrt{d}}$

[ABD16] Albrecht, Bai, and Ducas. A subfield lattice attack on overstretched NTRU assumptions. Crypto.

[CJL16] Cheon, Jeong, and Lee. An algorithm for NTRU problems. LMS J Comput Math.

Attacks on dec-NTRU

Brief history:

- subfield attacks [ABD16,CJL16]
  - solves dec-NTRU in time $\approx \exp\left(\frac{d \cdot \log B}{(\log q)^2}\right)$
    $\rightsquigarrow$ e.g., for $B = O(1)$, poly time attack when $q \gtrsim 2^{\sqrt{d}}$
  - requires (many) subfields

[ABD16] Albrecht, Bai, and Ducas. A subfield lattice attack on overstretched NTRU assumptions. Crypto.

[CJL16] Cheon, Jeong, and Lee. An algorithm for NTRU problems. LMS J Comput Math.

Attacks on dec-NTRU

Brief history:

- subfield attacks [ABD16,CJL16]
  - solves dec-NTRU in time $\approx \exp\left(\frac{d \cdot \log B}{(\log q)^2}\right)$
    $\rightsquigarrow$ e.g., for $B = O(1)$, poly time attack when $q \gtrsim 2^{\sqrt{d}}$
  - requires (many) subfields
- Kirchner-Fouque attack [KF17]
  - solves dec-NTRU in time $\approx \exp\left(\frac{d \cdot \log B}{(\log q)^2}\right)$
  - works in any number field
    (only plain lattice reduction, no algebraic tools)

[KF17] Kirchner and Fouque. Revisiting lattice attacks on overstretched NTRU parameters. Eurocrypt

Attacks on dec-NTRU

Brief history:

- subfield attacks [ABD16,CJL16]
  - solves dec-NTRU in time $\approx \exp\left(\frac{d \cdot \log B}{(\log q)^2}\right)$
    $\rightsquigarrow$ e.g., for $B = O(1)$, poly time attack when $q \gtrsim 2^{\sqrt{d}}$
  - requires (many) subfields

- Kirchner-Fouque attack [KF17]
  - solves dec-NTRU in time $\approx \exp\left(\frac{d \cdot \log B}{(\log q)^2}\right)$
  - works in any number field
    (only plain lattice reduction, no algebraic tools)

[KF17] Kirchner and Fouque. Revisiting lattice attacks on overstretched NTRU parameters. Eurocrypt

Attacks on dec-NTRU

Brief history:

- subfield attacks [ABD16,CJL16]
  - solves dec-NTRU in time $\approx \exp\left(\frac{d \cdot \log B}{(\log q)^2}\right)$
    $\rightsquigarrow$ e.g., for $B = O(1)$, poly time attack when $q \gtrsim 2^{\sqrt{d}}$
  - requires (many) subfields
- Kirchner-Fouque attack [KF17]
  - solves dec-NTRU in time $\approx \exp\left(\frac{d \cdot \log B}{(\log q)^2}\right)$
  - works in any number field
    (only plain lattice reduction, no algebraic tools)

Impact: few schemes use such large q's, but some of them did
(e.g., some FHE schemes or multilinear maps)

[KF17] Kirchner and Fouque. Revisiting lattice attacks on overstretched NTRU parameters. Eurocrypt

Subfields

$$\begin{tikzcd} K \arrow[d, dash, "n_1"] \\ L \arrow[d, dash, "n_2"] \\ \mathbb{Q} \end{tikzcd}$$

Meaning:

- K contains L, which contains $\mathbb{Q}$

Subfields

$$\begin{tikzcd} K \arrow[d, dash, "n_1"] \\ L \arrow[d, dash, "n_2"] \\ \mathbb{Q} \end{tikzcd}$$

Meaning:

- K contains L, which contains $\mathbb{Q}$
- K is a L-vector space of degree $[K : L] = n_1$
- L is a $\mathbb{Q}$-vector space of degree $[L : \mathbb{Q}] = n_2$

Subfields

$$\begin{array}{c} K \\ \Big| \; {\scriptstyle n_1} \\ L \\ \Big| \; {\scriptstyle n_2} \\ \mathbb{Q} \end{array}$$

Meaning:

- K contains L, which contains $\mathbb{Q}$
- K is a L-vector space of degree $[K : L] = n_1$
- L is a $\mathbb{Q}$-vector space of degree $[L : \mathbb{Q}] = n_2$

  $\Rightarrow$ K is a $\mathbb{Q}$-vector space of degree $n_1 \cdot n_2$

Subfields

$$\begin{array}{c} K \\ \big| \; n_1 \\ L \\ \big| \; n_2 \\ \mathbb{Q} \end{array}$$

Meaning:

- K contains L, which contains $\mathbb{Q}$
- K is a L-vector space of degree $[K : L] = n_1$
- L is a $\mathbb{Q}$-vector space of degree $[L : \mathbb{Q}] = n_2$

$\Rightarrow$ K is a $\mathbb{Q}$-vector space of degree $n_1 \cdot n_2$

Example:

$$\begin{array}{c} \vdots \\ \big| \; 2 \\ \mathbb{Q}[X]/(X^4+1) \\ \big| \; 2 \\ \mathbb{Q}[X]/(X^2+1) \\ \big| \; 2 \\ \mathbb{Q} \end{array}$$

Automorphisms and subfields

In this slide $K = \mathbb{Q}[X]/(X^d + 1)$
(or any Galois field)

Automorphisms: $\exists\, \sigma_1, \cdots, \sigma_d$ automorphisms of K

Automorphisms and subfields

In this slide $K = \mathbb{Q}[X]/(X^d + 1)$
(or any Galois field)

Automorphisms: $\exists\, \sigma_1, \cdots, \sigma_d$ automorphisms of K

Properties:

- if $f \in \mathcal{O}_K$ then $\sigma_i(f) \in \mathcal{O}_K$
- $\|\sigma(f)\| = \|\sigma(\sigma_i(f))\|$, for all $f \in K$

Automorphisms and subfields

In this slide $K = \mathbb{Q}[X]/(X^d + 1)$
(or any Galois field)

Automorphisms: $\exists\, \sigma_1, \cdots, \sigma_d$ automorphisms of K

Properties:

- if $f \in \mathcal{O}_K$ then $\sigma_i(f) \in \mathcal{O}_K$
- $\|\sigma(f)\| = \|\sigma(\sigma_i(f))\|$, for all $f \in K$

Subfields: If L subfield of K, there exist $S_L \subseteq \{1, \cdots, d\}$ s.t.

- $|S_L| = [K : L] - 1$
- for all $f \in K$,

$$\mathcal{N}_{K/L}(f) := f \cdot \prod_{i \in S_L} \sigma_i(f) \in L$$

A subfield attack on dec-NTRU [ABD16]

Objective: distinguish between

- $h = f/g \bmod q$ with $\|f\|, \|g\| \leq B$
- h uniform mod q

Attack: runs in time $\approx \exp\left(\frac{d \cdot \log B}{(\log q)^2}\right)$

On the board

[ABD16] Albrecht, Bai, and Ducas. A subfield lattice attack on overstretched NTRU assumptions. Crypto.

Other algorithms using subfields

$$\begin{array}{ll} K & X \\ \big| \; n_1 & \\ L & \\ \big| \; n_2 & \\ \mathbb{Q} & \end{array}$$

Main idea:

Other algorithms using subfields

$$\begin{array}{cc} K & X \\ \big|\, n_1 & \downarrow \\ L & X' \\ \big|\, n_2 & \\ \mathbb{Q} & \end{array}$$

Main idea:

- transform instance X in K into instance X' in L

Other algorithms using subfields

$$\begin{tikzcd}[row sep=small]
K \arrow[d, dash, "n_1"] & X \arrow[d] & \\
L \arrow[d, dash, "n_2"] & X' & s' \\
\mathbb{Q} & &
\end{tikzcd}$$

Main idea:

- transform instance X in K into instance X' in L
- solve X' in L (smaller lattice problems)

Other algorithms using subfields

$$\begin{array}{lcc} K & X & s \\ \big|\; n_1 & \downarrow & \uparrow \\ L & X' & s' \\ \big|\; n_2 & & \\ \mathbb{Q} & & \end{array}$$

Main idea:

- transform instance X in K into instance X' in L
- solve X' in L (smaller lattice problems)
- move the solution back to X in K

Other algorithms using subfields

$$\begin{array}{cccc} K & X & s \\ \big| \, {\scriptstyle n_1} & \downarrow & \uparrow \\ L & X' & s' \\ \big| \, {\scriptstyle n_2} & & \\ \mathbb{Q} & & \end{array}$$

Main idea:

- transform instance X in K into instance X' in L
- solve X' in L (smaller lattice problems)
- move the solution back to X in K

Can be used for:

- computing S-units [BFHP22]

[BFHP22] Biasse, Fieker, Hofmann, and Page. Norm relations and computational problems in number fields. Journal of the London Mathematical Society.

Other algorithms using subfields

$$\begin{array}{ccc} K & X & s \\ \Big|\, n_1 & \downarrow & \uparrow \\ L & X' & s' \\ \Big|\, n_2 & & \\ \mathbb{Q} & & \end{array}$$

Main idea:

- transform instance X in K into instance X' in L
- solve X' in L (smaller lattice problems)
- move the solution back to X in K

Can be used for:

- computing S-units [BFHP22]
- solving id-SVP in some very specific ideals [PXWC21,BGP22]

[PXWC21] Pan, Xu, Wadleigh, and Cheng. On the ideal shortest vector problem over random rational primes. Eurocrypt.

[BGP22] Boudgoust, Gachon, and Pellet-Mary. Some Easy Instances of Ideal-SVP and Implications on the Partial Vandermonde Knapsack Problem. Crypto.

Other algorithms using subfields

$$
\begin{array}{lcc}
K & X & s \\
\big| \; n_1 & \downarrow & \uparrow \\
L & X' & s' \\
\big| \; n_2 & & \\
\mathbb{Q} & &
\end{array}
$$

Main idea:

- transform instance X in K into instance X' in L
- solve X' in L (smaller lattice problems)
- move the solution back to X in K

Can be used for:

- computing S-units [BFHP22]
- solving id-SVP in some very specific ideals [PXWC21,BGP22]
- ...?

[PXWC21] Pan, Xu, Wadleigh, and Cheng. On the ideal shortest vector problem over random rational primes. Eurocrypt.

[BGP22] Boudgoust, Gachon, and Pellet-Mary. Some Easy Instances of Ideal-SVP and Implications on the Partial Vandermonde Knapsack Problem. Crypto.

Conclusion

Two algebraic attacks:

- on id-SVP when $\gamma \geq 2^{\sqrt{d}}$
  (or smaller γ's with pre-processing)
- on NTRU when q is large

Conclusion

Two algebraic attacks:

- on id-SVP when $\gamma \geq 2^{\sqrt{d}}$
  (or smaller γ's with pre-processing)
- on NTRU when q is large

One of my favorite open problems:

Can we transfer a problem instance to another number field?
(e.g., id-SVP over $K \to$ id-SVP over K')

$\rightsquigarrow$ would allow to move from a field without subfields to a field with many subfields

Conclusion

Two algebraic attacks:

- on id-SVP when $\gamma \geq 2^{\sqrt{d}}$
  (or smaller γ's with pre-processing)
- on NTRU when q is large

One of my favorite open problems:

Can we transfer a problem instance to another number field?
(e.g., id-SVP over $K \to$ id-SVP over K')

$\rightsquigarrow$ would allow to move from a field without subfields to a field with many subfields

Thank you