Some Easy Instances of Ideal-SVP and Implications on the Partial Vandermonde Knapsack Problem

Katharina Boudgoust[1] Erell Gachon[2] Alice Pellet-Mary[2,3]

[1]Aarhus University

[2]Université de Bordeaux

[3]CNRS

Séminaire CARAMBA 20 October 2022, Nancy, France

Frozen Lake of the Shortest Vector Problem

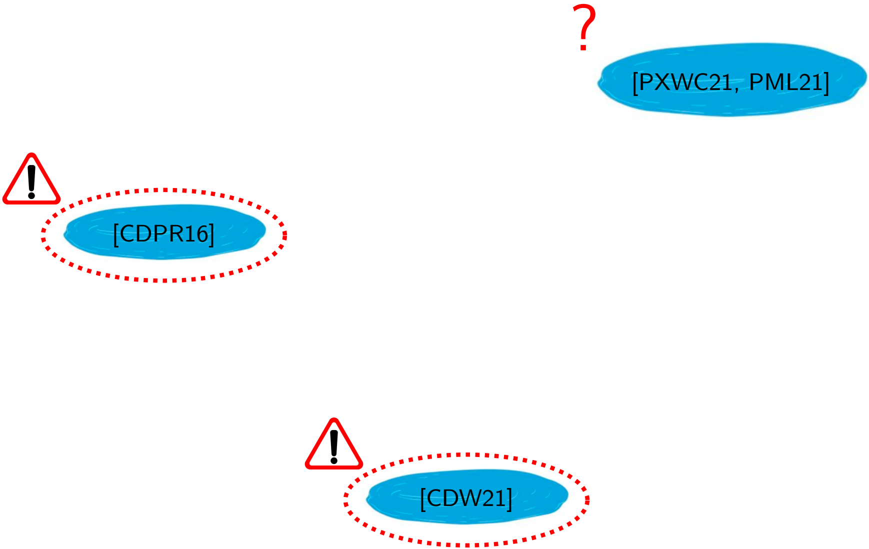
Frozen Lake of the Shortest Vector Problem Over Ideals

[PXWC21, PML21]

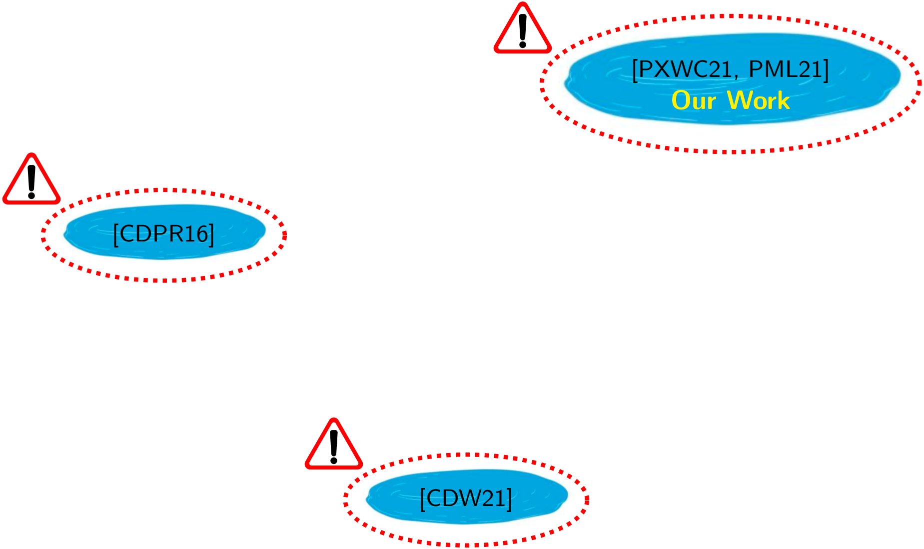
[CDPR16]

[CDW21]

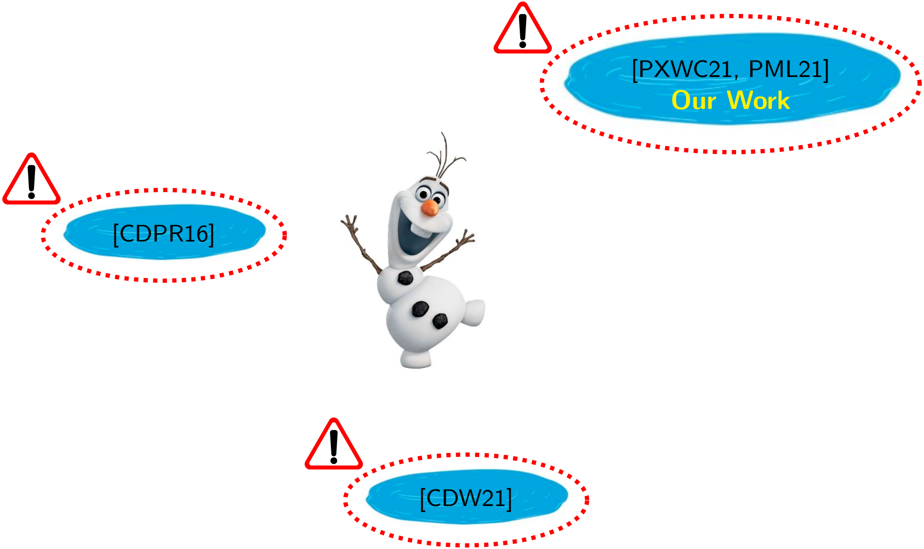
Frozen Lake of the Shortest Vector Problem Over Ideals



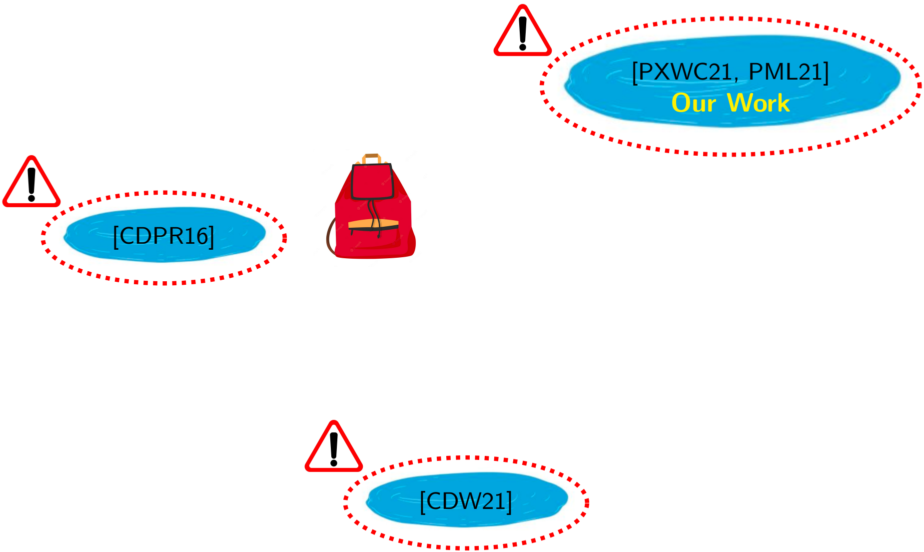
Frozen Lake of the Shortest Vector Problem Over Ideals



Frozen Lake of the Shortest Vector Problem Over Ideals

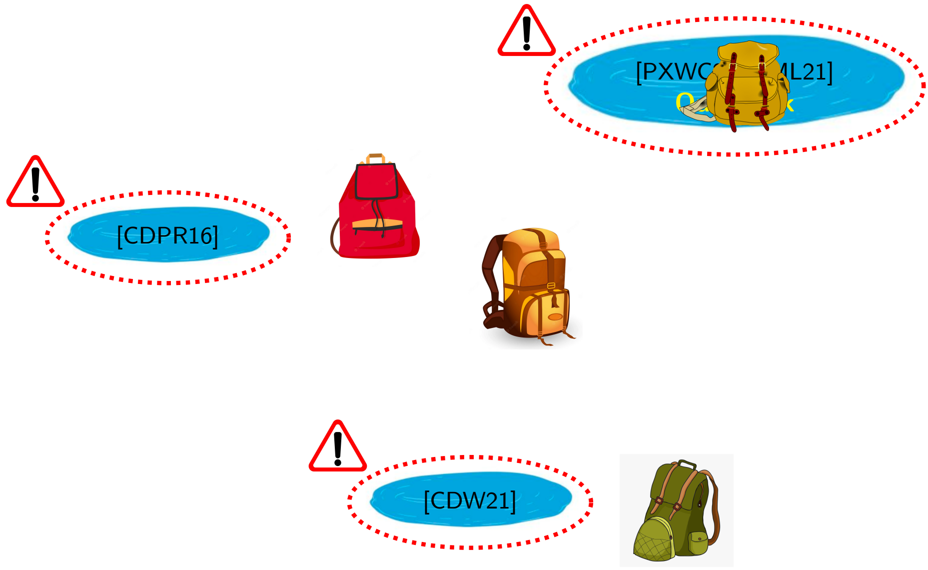


Where To Put Partial Vandermonde Knapsack?



Where To Put Partial Vandermonde Knapsack?

Where To Put Partial Vandermonde Knapsack?



1. Some Easy Instances of Ideal-SVP

2. Implications on Partial Vandermonde Knapsack

3. Implications to Cryptography

Lattices

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

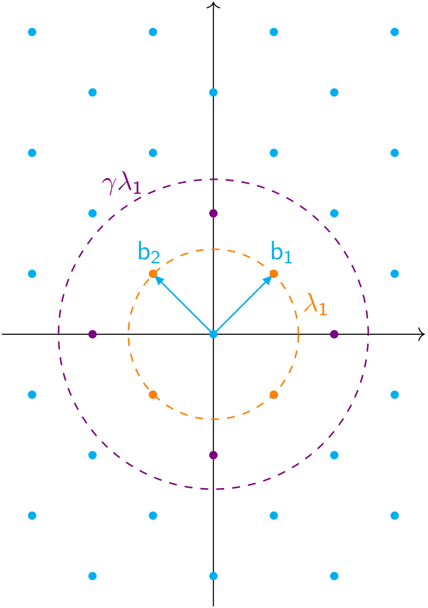
$$\Lambda(\mathrm{B}) = \left\{ \sum_{j=1}^{d} z_j \mathrm{b}_j : z_j \in \mathbb{Z} \right\}.$$

The **minimum** of Λ is

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

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

Conjecture:
There is no polynomial-time algorithm that solves SVP_γ for γ polynomial in d.



Module and Ideal Lattices

Number field K of degree d with O_K its ring of integers
Canonical embedding $\sigma\colon K \to \mathbb{R}^d$

Number Theory		Geometry
$M \subset (O_K)^r$ module of rank r	$\to$	$\sigma(M) \subset \mathbb{R}^{d \cdot r}$ module lattice
$I \subset O_K$ ideal $(r = 1)$	$\to$	$\sigma(I) \subset \mathbb{R}^d$ ideal lattice

Mod-SVP$_\gamma$ is SVP$_\gamma$ restricted to module lattices
Id-SVP$_\gamma$ is SVP$_\gamma$ restricted to ideal lattices

hardness assumption
of practical
lattice-based cryptography

Question

Is Mod-SVP and/or Id-SVP easier than SVP on all Euclidean lattices?

This paper: focus on Id-SVP for **specific** ideals

Polynomial-Time Solver for Specific Id-SVP$_\gamma$

Work	Type	Field	Ideal	Approx. γ
[CDPR16]	quantum	cyclotomic	principal (Gaussian generator)	all
[CDW21]	quantum	cyclotomic	all	$\geq 2^{\sqrt{d}}$
[PXWC21]	classic	Galois	A : prime, symmetries	$\sqrt{d}$
[PML21]	classic	Galois	B : all*, symmetries	complex**
This work	classic	all	C : all*, symmetries	$\geq 2\sqrt{d}$

- A $\cup$ B + poly-$\gamma \subsetneq$ C (easy PV-Knap is only in C)
- Membership in C can be easily checked (not true for B + poly-γ)
- all*: all ideals whose prime factors are not ramified (all but finitely many)
- complex**: depends on prime decomposition and norm of the ideal

Main Result

Let K be a number field of degree d with automorphism group $\mathrm{Aut}_{\mathbb{Q}}(K)$.
For an ideal I, we define $n_I = |\{\tau \in \mathrm{Aut}_{\mathbb{Q}}(K) \colon \tau(I) = I\}| \in [1, d]$.

Theorem

Let I be an ideal in K whose prime factors are not ramified. There is a classical algorithm that solves Id-SVP$_\gamma$ in the ideal lattice I in time roughly

$$\exp\left(\frac{d}{n_I \cdot \log \gamma}\right).$$

- if $n_I = 1$, then exponential-time algorithm (as for general (ideal) lattices)
- if n_I a fraction of d, then polynomial-time algorithm (many symmetries)
- n_I easy to compute (given a basis of I and a description of $\mathrm{Aut}_{\mathbb{Q}}(K)$)

Technical Details

Let K be a number field of degree d with automorphism group $\mathrm{Aut}_{\mathbb{Q}}(K)$.
For an ideal I, define its

- decomposition group $H_I := \{\tau \in \mathrm{Aut}_{\mathbb{Q}}(K) \colon \tau(I) = I\}$ ($n_I = |H_I|$)
- decomposition field $K_I := \{x \in K \colon \tau(x) = x, \forall \tau \in H_I\}$ (fixed field of H_I)

Lemma

Let I be an ideal in K whose prime factors are not ramified. Then it holds that

$$I = (I \cap K_I) \cdot O_K.$$

Intuitively:

- Short vectors of I are also contained in $I \cap K_I$
- The larger H_I $\Rightarrow$ the smaller K_I $\Rightarrow$ the easier it is to find short vectors

Implications on the Partial Vandermonde Knapsack Problem

Partial Vandermonde Knapsack (Partial Fourier Recovery)

- Number field K of degree d with O_K its ring of integers
- Prime q such that $qO_K = \prod_{j=1}^{d} \mathfrak{p}_j$, where $\mathfrak{p}_j$ is prime ideal of norm q
- For $\Omega \subseteq \{1, \ldots, d\}$, define $I_\Omega := \prod_{j \in \Omega} \mathfrak{p}_j$

Definition (PV-Knap$_\psi$)

Given I_Ω as above and let ψ be a distribution over O_K sampling short ring elements. Given $t = e \bmod I_\Omega$, for $e \leftarrow \psi$, the partial Vandermonde knapsack problem asks to find $e \in \mathrm{supp}(\psi)$.

Choice of Ω:

- [HPS$^+$14, HS15, DHSS20] don't specify how to choose Ω (and fix it)
- [LZA18, BSS22] sample Ω uniformly at random

Concrete Example

- $K = \mathbb{Q}[x]/\langle x^2+1\rangle$ and $O_K = \mathbb{Z}[x]/\langle x^2+1\rangle$, i.e., $d = 2$
- $q = 17$
- $x^2 + 1 = (x-4)(x-13) \in \mathbb{Z}_q$
- primitive roots are 4 and 13
- $qO_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ with $\mathfrak{p}_1 = \langle q, x-4\rangle$ and $\mathfrak{p}_2 = \langle q, x-13\rangle$
- Take $\Omega = \{1\}$, i.e., $I_\Omega = \mathfrak{p}_1$
- $\psi = \mathit{Unif}(\{ax+b \colon a, b \in \{-1,0,1\}\})$
- For $e \leftarrow \psi$ it yields $e \bmod I_\Omega = e(4) \bmod q$

Modulo I_Ω equals evaluating at the corresponding primitive roots modulo q

PV Knap as Ideal Lattice Problem

Number field K of degree d and canonical embedding $\sigma \colon K \to \mathbb{R}^d$

Definition (Id-BDD$_\delta$)

Let I be an ideal in O_K. Given $t \in \mathbb{R}^d$ such that $t = v + e$, with $v \in \sigma(I)$ and

$$\|e\| \leq \delta,$$

the **approximate bounded distance decoding** problem over **ideal lattices** (Id-BDD$_\delta$) asks to find e (or v).

Assume that ψ is δ-bounded distribution over O_K

Instance of PV-Knap$_\psi$ $\Rightarrow$ instance of Id-BDD$_\delta$ for the ideal I_Ω with

$$t = e \bmod I_\Omega = v + e,$$

where $v \in \sigma(I_\Omega)$ and $\|e\| \leq \delta$.

Missing Puzzle Piece

Lemma (Simplified)

Let I be an ideal of K. There is an efficient reduction from Id-BDD$_\delta$ in I to Id-SVP$_\gamma$ in I', where δ and γ are quite close.

- Simplified a lot
- Standard techniques
- K power-of-two cyclotomic: $\delta > 2\gamma$
- I' has symmetries $\Leftrightarrow$ I has symmetries
- Fore more details: ia.cr/2022/709

Bad Choices of Ω

Idea: If we can solve Id-SVP on I_Ω, we can solve PV-Knap on I_Ω

Question: When does I_Ω have many symmetries?

Strategy: Construct **specific** I_Ω that is fixed by many automorphisms of K

Bad Choices of Ω

Idea: If we can solve Id-SVP on I_Ω, we can solve PV-Knap on I_Ω
Question: When does I_Ω have many symmetries?
Strategy: Construct **specific** I_Ω that is fixed by many automorphisms of K

- Fix one prime ideal $\mathfrak{p}$ of the factorization of $qO_K = \prod_{i=1}^{d} \mathfrak{p}_i$
- Let H be a subgroup of $Aut_{\mathbb{Q}}(K)$
- It defines $\Omega_H \subseteq \{1, \ldots, d\}$ such that $\{\tau(\mathfrak{p})\colon \tau \in H\} = \{\mathfrak{p}_i\colon i \in \Omega_H\}$

Hence, the ideal

$$I_{\Omega_H} = \prod_{i \in \Omega_H} \mathfrak{p}_i = \prod_{\tau \in H} \tau(\mathfrak{p})$$

is fixed by H.

Example: For K power-of-two cyclotomic of degree d, it exists H of size $d/2$.

Experimental Results

- Scenario 1: **worst-case** Ω
  - Ω chosen such that I_Ω stable by many automorphisms
  - Parameter sets from the literature [HPS$^+$14, LZA18]
  - Solve PV-Knap in few minutes, even seconds
- Scenario 2: **average-case** Ω
  - Ω chosen uniformly at random
  - Only distinguishing attacks
  - Strategy: forget some indices in the set Ω
  - Trade-off: problem gets harder, but we might gain symmetries
  - With non-negligible probability lattice dimension is reduced by factor 2
  - 128-bit security claimed by [LZA18] drops to 87-bit security (against distinguishing attacks)

Implications to Cryptography

Guidelines for using Id-SVP$_\gamma$ in Cryptography

1. Check if rank can be increased from 1 to 2 (aka rely on Mod-SVP$_\gamma$ instead)
2. If not, use random ideals sampled from a distribution that is supported by worst-to-average case reductions [Gen09, dBDPW20]
3. If not, avoid known 'bad' ideals, i.e.,
   - principal ideal with Gaussian generator in cyclotomic fields [CDPR16]
   - ideals fixed by some non-trivial automorphism of the field [**this work**]
4. In any case, do not rely on the hardness of Id-SVP$_\gamma$ for $\gamma \geq 2^{\sqrt{d}}$, where d is the degree of the number field (if it is cyclotomic) [CDW21]

Implications to PV-Knap-Based Cryptography

- Our results lead to
  - secret key recovery attacks against PASS Sign [HPS+14, LZA18]
  - secret key recovery attacks against PASS Encrypt [HS15, BSS22]
  - forgery attacks against (candidate) aggregate signature MMSA(TK) [DHSS20]

  only for specific design choices of Ω

- For random Ω, the attack lattice dimension is decreased by a factor 2

- Can be mitigated by increasing the parameters

Implications to Lattice-Based Cryptography

- Our algorithm solves **specific** instances of Id-SVP
- Having many symmetries is a **strong** requirement
- No implications to the hardness of structured problems such as Ring-SIS or Ring-LWE, as they are based on **worst-case** hardness of Id-SVP
- Reductions are only proven in one direction
- No implications to the hardness of Module-LWE (Dilithium, Kyber)

Implications to Lattice-Based Cryptography

- Our algorithm solves **specific** instances of Id-SVP
- Having many symmetries is a **strong** requirement
- No implications to the hardness of structured problems such as Ring-SIS or Ring-LWE, as they are based on **worst-case** hardness of Id-SVP
- Reductions are only proven in one direction
- No implications to the hardness of Module-LWE (Dilithium, Kyber)

Thank you.

Olivier Bernard, Andrea Lesavourey, Tuong-Huy Nguyen, and Adeline Roux-Langlois.
Log-s-unit lattices using explicit stickelberger generators to solve approx ideal-svp.
IACR Cryptol. ePrint Arch., page 1384, 2021.

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

Katharina Boudgoust, Amin Sakzad, and Ron Steinfeld.
Vandermonde meets regev: Public key encryption schemes based on partial vandermonde problems, 2022.
Accepted at Designs, Codes and Cryptography.

Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev.
Recovering short generators of principal ideals in cyclotomic rings.
In *EUROCRYPT (2)*, volume 9666 of *Lecture Notes in Computer Science*, pages 559–585. Springer, 2016.

Ronald Cramer, Léo Ducas, and Benjamin Wesolowski.
Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time.

J. ACM, 68(2):8:1–8:26, 2021.

Koen de Boer, Léo Ducas, Alice Pellet-Mary, and Benjamin Wesolowski.
Random self-reducibility of ideal-svp via arakelov random walks.
In *CRYPTO (2)*, volume 12171 of *Lecture Notes in Computer Science*, pages 243–273. Springer, 2020.

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

Craig Gentry.
Fully homomorphic encryption using ideal lattices.
In *STOC*, pages 169–178. ACM, 2009.

Jeffrey Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William Whyte.
Practical signatures from the partial fourier recovery problem.
In *ACNS*, volume 8479 of *Lecture Notes in Computer Science*, pages 476–493. Springer, 2014.

Jeffrey Hoffstein and Joseph H. Silverman.
Pass-encrypt: a public key cryptosystem based on partial evaluation of polynomials.

Des. Codes Cryptogr., 77(2-3):541–552, 2015.

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

Alice Pellet-Mary, Guillaume Hanrot, and Damien Stehlé.
Approx-svp in ideal lattices with pre-processing.
In *EUROCRYPT (2)*, volume 11477 of *Lecture Notes in Computer Science*, pages 685–716. Springer, 2019.

Christian Porter, Andrew Mendelsohn, and Cong Ling.
Subfield algorithms for ideal- and module-svp based on the decomposition group.
IACR Cryptol. ePrint Arch., page 600, 2021.

Yanbin Pan, Jun Xu, Nick Wadleigh, and Qi Cheng.
On the ideal shortest vector problem over random rational primes.
In *EUROCRYPT (1)*, volume 12696 of *Lecture Notes in Computer Science*, pages 559–583. Springer, 2021.