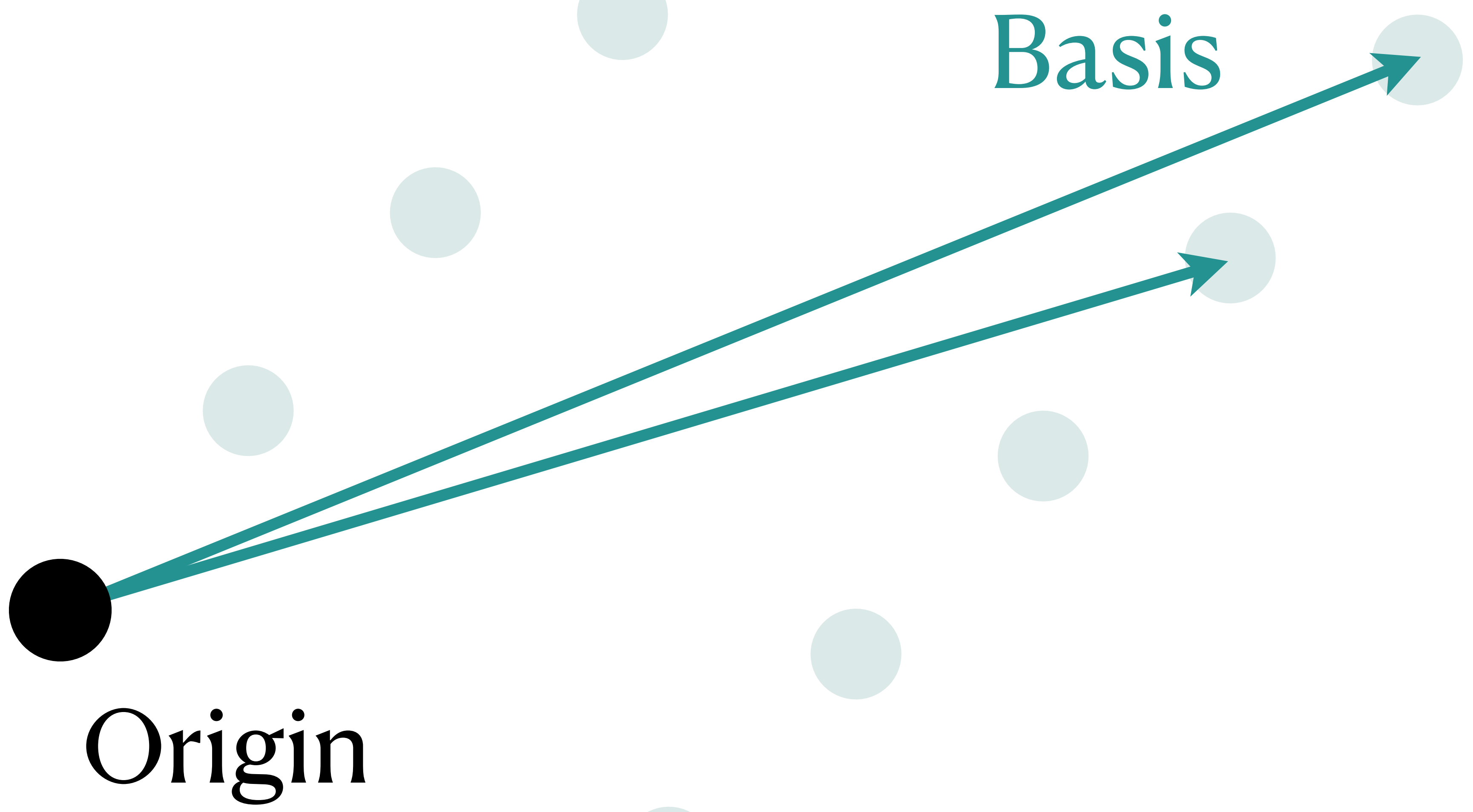
Ideal-SVP is hard for small-norm uniform prime ideals

Joël Felderhoff, Alice Pellet-Mary, Damien Stehlé, Benjamin Wesolowski

Benjamin Wesolowski, CNRS and ENS de Lyon – TCC 2023, December 2, 2023, Taipei, Taiwan

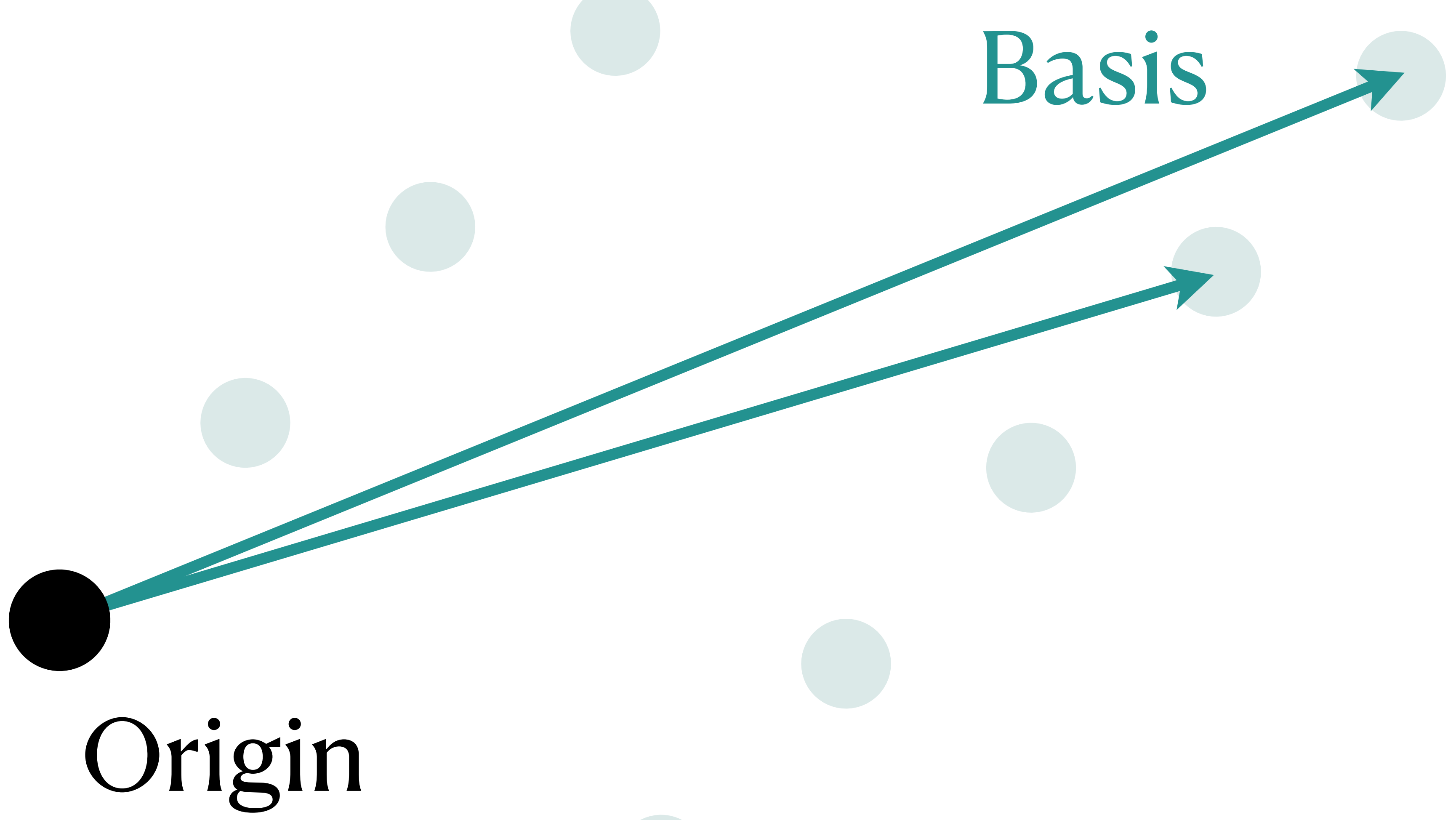
Ideal-SVP

- Any basis $(b_1, \ldots, b_n)$ of a vector space describes a lattice $L = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n$



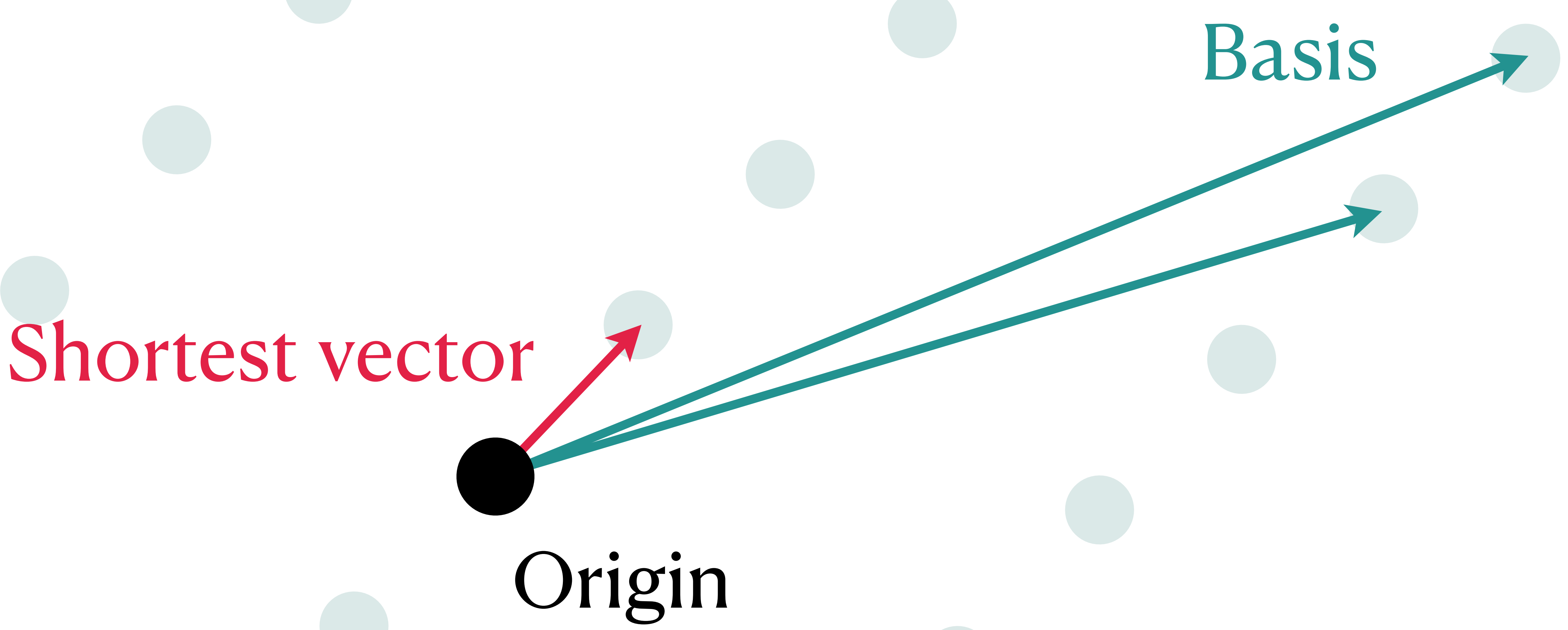
Ideal-SVP

- Any basis $(b_1, \ldots, b_n)$ of a vector space describes a lattice $L = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n$



Ideal-SVP

- Any basis $(b_1, \ldots, b_n)$ of a vector space describes a lattice $L = \mathbb{Z}b_1 + \ldots + \mathbb{Z}b_n$
- **SVP**: find the non-zero point in L closest to the origin (up to approx. factor…)



Ideal-SVP

- Some lattices have "something extra"...
- $K = \mathbb{Q}[X] / (X^n + 1)$ is a **field**, and a $\mathbb{Q}$**-vector space** of dimension $n = 2^r$
- $\mathcal{O} = \mathbb{Z}[X] / (X^n + 1)$ is a lattice in K... and a **subring**!
- An **ideal lattice** is a lattice $\mathfrak{a} \subset K$ such that $\mathcal{O}\mathfrak{a} \subset \mathfrak{a}$

Ideal-SVP

- Some lattices have "something extra"...
- $K = \mathbb{Q}[X] \,/\, (X^n + 1)$ is a **field**, and a $\mathbb{Q}$**-vector space** of dimension $n = 2^r$
- $\mathcal{O} = \mathbb{Z}[X] \,/\, (X^n + 1)$ is a lattice in K... and a **subring**!
- An **ideal lattice** is a lattice $\mathfrak{a} \subset K$ such that $\mathcal{O}\mathfrak{a} \subset \mathfrak{a}$
- An ideal lattice is **integral** if $\mathfrak{a} \subset \mathcal{O}$

Ideal-SVP

- Some lattices have "something extra"...
- $K = \mathbb{Q}[X] / (X^n + 1)$ is a **field**, and a $\mathbb{Q}$**-vector space** of dimension $n = 2^r$
- $\mathcal{O} = \mathbb{Z}[X] / (X^n + 1)$ is a lattice in K... and a **subring**!
- An **ideal lattice** is a lattice $\mathfrak{a} \subset K$ such that $\mathcal{O}\mathfrak{a} \subset \mathfrak{a}$
- An ideal lattice is **integral** if $\mathfrak{a} \subset \mathcal{O}$
- An integral ideal is **prime** if it is not a product of other integral ideals

Ideal-SVP

- Some lattices have "something extra"...
- $K = \mathbb{Q}[X] / (X^n + 1)$ is a **field**, and a $\mathbb{Q}$**-vector space** of dimension $n = 2^r$
- $\mathcal{O} = \mathbb{Z}[X] / (X^n + 1)$ is a lattice in K... and a **subring**!
- An **ideal lattice** is a lattice $\mathfrak{a} \subset K$ such that $\mathcal{O}\mathfrak{a} \subset \mathfrak{a}$
- An ideal lattice is **integral** if $\mathfrak{a} \subset \mathcal{O}$
- An integral ideal is **prime** if it is not a product of other integral ideals
- Any ideal lattice is of the form $\mathfrak{a} = \prod \mathfrak{p}_i^{e_i}$ where $\mathfrak{p}_i \subset \mathcal{O}$ is prime and $e_i \in \mathbb{Z}$

Ideal-SVP

- Ideal lattices are **important**:
    - Led to the first *fully homomorphic encryption* scheme [Gentry09]
    - Simplest case of *module lattices*, used in real world (KYBER, DILITHIUM)

Ideal-SVP

- Ideal lattices are **important**:
    - Led to the first *fully homomorphic encryption* scheme [Gentry09]
    - Simplest case of *module lattices*, used in real world (KYBER, DILITHIUM)
- Ideal lattices are **special**: is SVP as hard?
    - There are specific algorithms for SVP in ideal lattices
    - Ideal-SVP still considered hard, but one can reach better approximation factors than SVP in generic lattices

Average-case Ideal-SVP

Is Ideal-SVP hard on average?

Average-case Ideal-SVP

Is Ideal-SVP hard on average?

- **We want random self-reducibility**: if Ideal-SVP can be solved for random instances, then Ideal-SVP can be solved for any instance...

Average-case Ideal-SVP

Is Ideal-SVP hard on average?

For what distribution?

- **We want random self-reducibility**: if Ideal-SVP can be solved for random instances, then Ideal-SVP can be solved for any instance...

Average-case Ideal-SVP

- Previous work, random self-reducibility for two distributions:

Average-case Ideal-SVP

- Previous work, random self-reducibility for two distributions: $\mathfrak{p}^{-1}$-Ideal-SVP
    - [Gentry09] **Inverse of uniformly random prime ideal** of small norm
        - Non-integral… works for [Gentry09]'s purpose

Average-case Ideal-SVP

- Previous work, random self-reducibility for two distributions: p^{-1}-Ideal-SVP
    - [Gentry09] **Inverse of uniformly random prime ideal** of small norm
        - Non-integral… works for [Gentry09]'s purpose
    - [BDPW20] **Uniform ideals for the Haar measure** of large norm

Haar-Ideal-SVP

        - Geometrically canonical, rich theory! but large norms…

Average-case Ideal-SVP

- Previous work, random self-reducibility for two distributions:

P^{-1}-Ideal-SVP

  - [Gentry09] **Inverse of uniformly random prime ideal** of small norm
    - Non-integral… works for [Gentry09]'s purpose
  - [BDPW20] **Uniform ideals for the Haar measure** of large norm
    - Geometrically canonical, rich theory! but large norms…

Haar-Ideal-SVP

- This work: **uniformly random prime ideal** of small norm

P-Ideal-SVP

  - *Integral*, unlike [Gentry09], and *small*, unlike [BDPW20]
  - Composes with NTRU reductions! Links NTRU to worst-case Ideal-SVP

Method

Worst-case Ideal-SVP $\overset{\text{[Gentry09]}}{\leq}$ P^{-1}-Ideal-SVP $\overset{\text{New}}{\leq}$ P-Ideal-SVP

Method

Worst-case Ideal-SVP $\overset{\text{[Gentry09]}}{\leq}$ $\mathfrak{p}^{-1}$-Ideal-SVP $\overset{\text{New}}{\leq}$ $\mathfrak{p}$-Ideal-SVP

poly-time given a factoring oracle

P^{-1}-Ideal-SVP reduces to P-Ideal-SVP

- **Input:** an ideal $\mathfrak{a} = \mathfrak{p}^{-1}$ with $\mathfrak{p}$ uniform prime of bounded norm
- **Output:** $x \in \mathfrak{a}$ small

P^{-1}-Ideal-SVP reduces to P-Ideal-SVP

- **Input:** an ideal $\mathfrak{a} = \mathfrak{p}^{-1}$ with $\mathfrak{p}$ uniform prime of bounded norm
- **Output:** $x \in \mathfrak{a}$ small

1. Let $s_{\mathfrak{p}} \in \mathfrak{p}$ small (solve P-Ideal-SVP for $\mathfrak{p}$, *uniform prime of bounded norm*);
2. Let $(\mathfrak{b}, y) \leftarrow \texttt{SampleIdeal}(\mathfrak{p}, s_{\mathfrak{p}})$

   ➡ $\mathfrak{b}$ is a uniform integral ideal of bounded norm, and $y \in (\mathfrak{b}\mathfrak{p})^{-1}$ is small
3. If $\mathfrak{b}$ is not prime, **abort**;
4. Let $s_{\mathfrak{b}} \in \mathfrak{b}$ small (solve P-Ideal-SVP for $\mathfrak{b}$, *uniform prime of bounded norm*);
5. Return $s_{\mathfrak{b}} \cdot y \in \mathfrak{b} \cdot (\mathfrak{b}\mathfrak{p})^{-1} = \mathfrak{p}^{-1}$

P^{-1}-Ideal-SVP reduces to P-Ideal-SVP

- **Input:** an ideal $\mathfrak{a} = \mathfrak{p}^{-1}$ with $\mathfrak{p}$ uniform prime of bounded norm
- **Output:** $x \in \mathfrak{a}$ small

1. Let $s_{\mathfrak{p}} \in \mathfrak{p}$ small (solve P-Ideal-SVP for $\mathfrak{p}$, *uniform prime of bounded norm*);
2. Let $(\mathfrak{b}, y) \leftarrow \texttt{SampleIdeal}(\mathfrak{p}, s_{\mathfrak{p}})$ Need factoring oracle

   ➡ $\mathfrak{b}$ is a uniform integral ideal of bounded norm, and $y \in (\mathfrak{b}\mathfrak{p})^{-1}$ is small
3. If $\mathfrak{b}$ is not prime, **abort**;
4. Let $s_{\mathfrak{b}} \in \mathfrak{b}$ small (solve P-Ideal-SVP for $\mathfrak{b}$, *uniform prime of bounded norm*);
5. Return $s_{\mathfrak{b}} \cdot y \in \mathfrak{b} \cdot (\mathfrak{b}\mathfrak{p})^{-1} = \mathfrak{p}^{-1}$

P^{-1}-Ideal-SVP reduces to P-Ideal-SVP

- **Input:** an ideal $\mathfrak{a} = \mathfrak{p}^{-1}$ with $\mathfrak{p}$ uniform prime of bounded norm
- **Output:** $x \in \mathfrak{a}$ small

1. Let $s_{\mathfrak{p}} \in \mathfrak{p}$ small (solve P-Ideal-SVP for $\mathfrak{p}$, *uniform prime of bounded norm*);
2. Let $(\mathfrak{b}, y) \leftarrow \texttt{SampleIdeal}(\mathfrak{p}, s_{\mathfrak{p}})$ Need factoring oracle

   ➡ $\mathfrak{b}$ is a uniform integral ideal of bounded norm, and $y \in (\mathfrak{b}\mathfrak{p})^{-1}$ is small
3. If $\mathfrak{b}$ is not prime, **abort**; success proba = density of primes
4. Let $s_{\mathfrak{b}} \in \mathfrak{b}$ small (solve P-Ideal-SVP for $\mathfrak{b}$, *uniform prime of bounded norm*);
5. Return $s_{\mathfrak{b}} \cdot y \in \mathfrak{b} \cdot (\mathfrak{b}\mathfrak{p})^{-1} = \mathfrak{p}^{-1}$

P^{-1}-Ideal-SVP reduces to P-Ideal-SVP

- **Input:** an ideal $\mathfrak{a} = \mathfrak{p}^{-1}$ with $\mathfrak{p}$ uniform prime of bounded norm
- **Output:** $x \in \mathfrak{a}$ small

1. Let $s_{\mathfrak{p}} \in \mathfrak{p}$ small (solve P-Ideal-SVP for $\mathfrak{p}$, *uniform prime of bounded norm*);
2. Let $(\mathfrak{b}, y) \leftarrow \texttt{SampleIdeal}(\mathfrak{p}, s_{\mathfrak{p}})$ Need factoring oracle

   ➡ $\mathfrak{b}$ is a uniform integral ideal of bounded norm, and $y \in (\mathfrak{b}\mathfrak{p})^{-1}$ is small
3. If $\mathfrak{b}$ is not prime, **abort**; success proba = density of primes
4. Let $s_{\mathfrak{b}} \in \mathfrak{b}$ small (solve P-Ideal-SVP for $\mathfrak{b}$, *uniform prime of bounded norm*);
5. Return $s_{\mathfrak{b}} \cdot y \in \mathfrak{b} \cdot (\mathfrak{b}\mathfrak{p})^{-1} = \mathfrak{p}^{-1}$ $s_{\mathfrak{b}}$ small and y small so $s_{\mathfrak{b}} \cdot y$ small

Application to NTRU

- [PS21] gives a Karp reduction from Ideal-SVP to **NTRU** [HPS96]

Application to NTRU

- [PS21] gives a Karp reduction from Ideal-SVP to **NTRU** [HPS96]
- New NTRU distribution $D^{\mathbf{NTRU}}$: sample uniform small prime $\mathfrak{p}$, and create NTRU instance (and trapdoor) via the [PS21] reduction

Application to NTRU

- [PS21] gives a Karp reduction from Ideal-SVP to **NTRU** [HPS96]
- New NTRU distribution $D^{\mathbf{NTRU}}$: sample uniform small prime $\mathfrak{p}$, and create NTRU instance (and trapdoor) via the [PS21] reduction

NTRU for D^{NTRU} $\overset{\text{[PS21]}}{\geq}$ $\mathfrak{p}$-Ideal-SVP $\overset{\text{New}}{\geq}$ Worst-case Ideal-SVP

Application to NTRU

- [PS21] gives a Karp reduction from Ideal-SVP to **NTRU** [HPS96]
- New NTRU distribution $D^{\mathbf{NTRU}}$: sample uniform small prime $\mathfrak{p}$, and create NTRU instance (and trapdoor) via the [PS21] reduction

$$\text{NTRU for } D^{\text{NTRU}} \overset{\text{[PS21]}}{\geq} \mathfrak{p}\text{-Ideal-SVP} \overset{\text{New}}{\geq} \text{Worst-case Ideal-SVP}$$

- First distribution over NTRU instances with a polynomial modulus whose hardness is supported by a worst-case lattice problem
- Caveat: sampling $D^{\mathbf{NTRU}}$ needs factoring oracle