Wagner's Algorithm Provably Runs in Subexponential Time for SIS^∞

Léo Ducas[1,2] Lynn Engelberts[1,3] Johanna Loyer[4]

[1]CWI [2]Leiden University [3]QuSoft [4]Inria Saclay

Introduction

- June 2024: NIST standardizes Dilithium
  Its security relies on the SIS^∞ problem

Short Integer Solution in infinity norm ($\mathrm{SIS}^\infty_{n,m,q,\beta}$)

Let be $n, m, q \in \mathbb{N}$ and $\beta > 0$. Given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a **non-zero** vector $\mathbf{x} \in \mathbb{Z}^m$ such that

- $\mathbf{Ax} = \mathbf{0} \bmod q$ (Parity-check matrix)
- $\|\mathbf{x}\|_\infty \leq \beta$

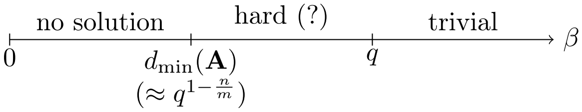
Introduction

- June 2024: NIST standardizes Dilithium
  Its security relies on the SIS^∞ problem

Short Integer Solution in infinity norm ($\mathrm{SIS}^\infty_{n,m,q,\beta}$)

Let be $n, m, q \in \mathbb{N}$ and $\beta > 0$. Given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, find a **non-zero** vector $\mathbf{x} \in \mathbb{Z}^m$ such that

- $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$ (Parity-check matrix)
- $\|\mathbf{x}\|_\infty \leq \beta$



Introduction: Lattices

Lattice-based cryptography

Lattice

Given a basis $\mathbf{B} := (\mathbf{b}_1, \ldots, \mathbf{b}_k) \in \mathbb{R}^{d \times k}$, the *lattice* associated to $\mathbf{B}$ is the set of all integer linear combinations of the basis vectors $\mathbf{b}_i$, i.e.,

$$\mathcal{L}(\mathbf{B}) := \left\{ \sum_{i=1}^{k} z_i \mathbf{b}_i : z_i \in \mathbb{Z} \right\} \subseteq \mathbb{R}^d.$$

$\mathcal{L}$ is said 'full-rank' if $d = k$.

Introduction: Lattices

$\mathrm{SIS}^{\infty}_{n,m,q,\beta}$ matrix $\mathbf{A}$

Given $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a **non-zero** vector $\mathbf{x} \in \mathbb{Z}^m$ such that

- $\mathbf{A}\mathbf{x} = \mathbf{0} \mod q$
- $\|\mathbf{x}\|_\infty \leq \beta$

Introduction: Lattices

$\mathrm{SIS}^{\infty}_{n,m,q,\beta}$ matrix $\mathbf{A}$

Given $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a **non-zero** vector $\mathbf{x} \in \mathbb{Z}^m$ such that

- $\mathbf{A}\mathbf{x} = \mathbf{0} \mod q$
- $\|\mathbf{x}\|_\infty \leq \beta$

$$\iff$$

β-SVP^{∞} in the lattice $\Lambda_q^{\perp}(\mathbf{A})$

Given $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a **non-zero** vector $\mathbf{x} \in \mathbb{Z}^m$ such that

- $\mathbf{x} \in \Lambda_q^{\perp}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{0} \bmod q\}$
- $\|\mathbf{x}\|_\infty \leq \beta$

Introduction: Lattices

$\mathrm{SIS}^{\infty}_{n,m,q,\beta}$ matrix $\mathbf{A}$

Given $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a **non-zero** vector $\mathbf{x} \in \mathbb{Z}^m$ such that

- $\mathbf{A}\mathbf{x} = \mathbf{0} \mod q$
- $\|\mathbf{x}\|_\infty \leq \beta$

$$\Longleftrightarrow$$

β-SVP^{∞} in the lattice $\Lambda_q^{\perp}(\mathbf{A})$

Given $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a **non-zero** vector $\mathbf{x} \in \mathbb{Z}^m$ such that

- $\mathbf{x} \in \Lambda_q^{\perp}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{0} \bmod q\}$
- $\|\mathbf{x}\|_\infty \leq \beta$

For simplicity, consider $\mathbf{A} = [\mathbf{A}'|\mathbf{I}_n]$ with $\mathbf{A}' \in \mathbb{Z}_q^{n\times(m-n)}$

$$\text{The basis } \mathbf{B} := \begin{pmatrix} 0 & \mathbf{I}_{m-n} \\ q\mathbf{I}_n & -\mathbf{A}' \end{pmatrix} \text{ generates } \mathcal{L}(\mathbf{B}) = \mathbf{B}\mathbb{Z}^m = \Lambda_q^{\perp}(\mathbf{A}).$$

Motivation of this work

$$\underset{\text{(LWE)}}{\textbf{BKW}} = \underset{\text{(SIS)}}{\textbf{Wagner}} + \textbf{Dual distinguishing}$$

Motivation of this work

BKW = Wagner + Dual distinguishing

(LWE) (SIS)

Motivation

- Algorithms to solve LWE are variants of [BKW03]
- [KF15] claimed to solve LWE with ternary secret in subexponential time
- [HKM18] found an issue in their proof for certain regimes ($m = \Theta(n)$)

Motivation of this work

$$\textbf{BKW} = \textbf{Wagner} + \textbf{Dual distinguishing}$$

(LWE) (SIS)

Motivation

- Algorithms to solve LWE are variants of [BKW03]
- [KF15] claimed to solve LWE with ternary secret in subexponential time
- [HKM18] found an issue in their proof for certain regimes ($m = \Theta(n)$)

Questions

- Is there a provable variant of Wagner to solve SIS^∞ in subexponential time?
- Can we fix [KF15] for LWE?
- Does it threaten Dilithium?

Motivation of this work

$$\textbf{BKW} = \textbf{Wagner} + \textbf{Dual distinguishing}$$

(LWE) (SIS)

Motivation

- Algorithms to solve LWE are variants of [BKW03]
- [KF15] claimed to solve LWE with ternary secret in subexponential time
- [HKM18] found an issue in their proof for certain regimes ($m = \Theta(n)$)

Questions

• Is there a provable variant of Wagner to solve SIS^∞ in subexponential time?	Yes for $\beta = \frac{q}{\mathrm{polylog}(n)}$
• Can we fix [KF15] for LWE?	Maybe?
• Does it threaten Dilithium?	No

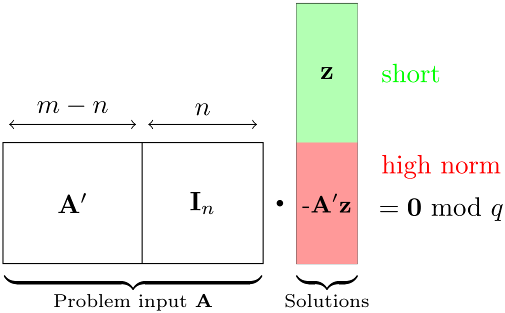
Outline

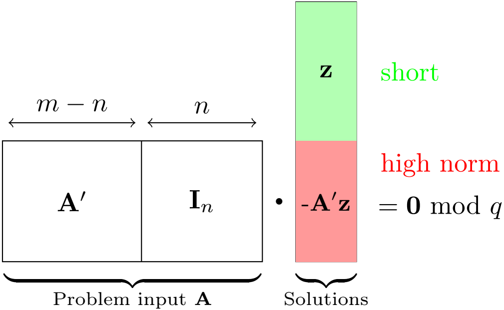
1. Wagner-style algorithms to solve SIS^∞
2. A provable algorithm for SIS^∞
3. Implications for cryptographic problems

Outline

1. Wagner-style algorithms to solve SIS^∞
2. A provable algorithm for SIS^∞
3. Implications for cryptographic problems

$$\underbrace{\left[\begin{array}{c|c} \overset{\longleftarrow\; m-n \;\longrightarrow}{\mathbf{A}'} & \overset{\longleftarrow\; n \;\longrightarrow}{\mathbf{I}_n} \end{array}\right]}_{\text{Problem input } \mathbf{A}} \bullet \underbrace{\left[\begin{array}{c} \mathbf{z} \\ \hline \text{-}\mathbf{A}'\mathbf{z} \end{array}\right]}_{\text{Solutions}} = \mathbf{0} \bmod q$$

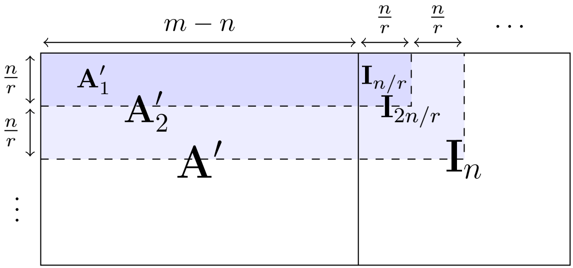

$m - n$
n
$\mathbf{A}'$
$\mathbf{I}_n$
$\bullet$
$\mathbf{z}$
short
-$\mathbf{A}'\mathbf{z}$
high norm
$= \mathbf{0} \bmod q$
Problem input $\mathbf{A}$
Solutions



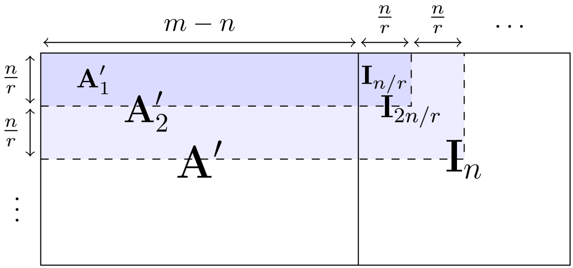
Wagner's algorithm [Wag02]

Input: list L
Output: elements in L that sum up to $\mathbf{0}$

Wagner's algorithm for SIS



Wagner's algorithm for SIS



Wagner step in [BKW03]

Input: $\mathbf{A} = [\mathbf{A}' \mid \mathbf{I}_n] \in \mathbb{Z}_q^{n\times m}$
Output: List of vectors $\mathbf{x} \in \mathbb{Z}_q^m$ such that $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \leq 2^r \leq \beta$

Divide $\mathbf{A}$ into submatrices $\mathbf{A}_i = [\mathbf{A}'_i|\mathbf{I}]$
Initialize a list L_0 with vectors from $\mathcal{U}(\{-1,0,1\}^{m-n})$
for $i = 1, \ldots, r$ **do**
  $L_i :=$ **LiftAndCombine**$(L_{i-1}, \mathbf{A}_i)$ $\triangleright\ \forall \mathbf{x} \in L_i, \mathbf{A}_i\mathbf{x} = \mathbf{0} \bmod q$
return L_r

Wagner's algorithm for SIS

LiftAndCombine

In: List L_{i-1} of vectors $\mathbf{x} \in \mathbb{Z}_q^{(i-1)n/r}$ s.t. $\mathbf{A}_{i-1}\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \leq 2^{i-1}$

Out: List L_i of vectors $\mathbf{x} \in \mathbb{Z}_q^{in/r}$ such that $\mathbf{A}_i\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \leq 2^i$

$$L_{i-1} \ni \boxed{\mathbf{x}}$$

Wagner's algorithm for SIS

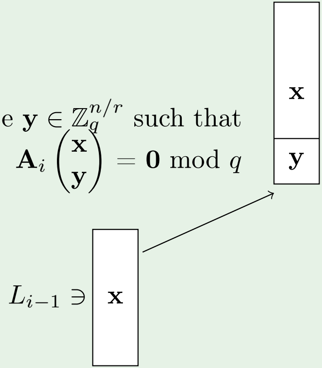
LiftAndCombine

In: List L_{i-1} of vectors $\mathbf{x} \in \mathbb{Z}_q^{(i-1)n/r}$ s.t. $\mathbf{A}_{i-1}\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \leq 2^{i-1}$

Out: List L_i of vectors $\mathbf{x} \in \mathbb{Z}_q^{in/r}$ such that $\mathbf{A}_i\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \leq 2^{i}$

Lift: Compute $\mathbf{y} \in \mathbb{Z}_q^{n/r}$ such that

$$\mathbf{A}_i \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = \mathbf{0} \bmod q$$



Wagner's algorithm for SIS

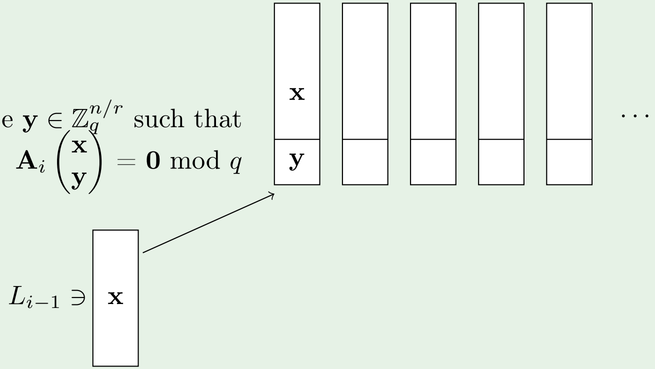
LiftAndCombine

In: List L_{i-1} of vectors $\mathbf{x} \in \mathbb{Z}_q^{(i-1)n/r}$ s.t. $\mathbf{A}_{i-1}\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \leq 2^{i-1}$

Out: List L_i of vectors $\mathbf{x} \in \mathbb{Z}_q^{in/r}$ such that $\mathbf{A}_i\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \leq 2^i$

Lift: Compute $\mathbf{y} \in \mathbb{Z}_q^{n/r}$ such that

$$\mathbf{A}_i \begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix} = \mathbf{0} \bmod q$$

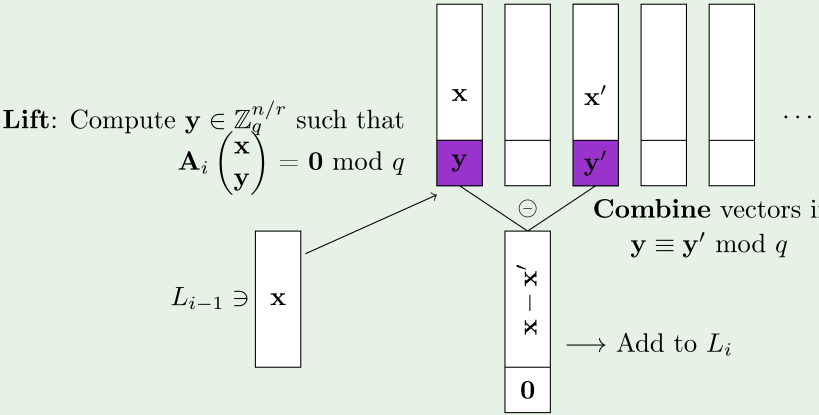


Wagner's algorithm for SIS

LiftAndCombine

In: List L_{i-1} of vectors $\mathbf{x} \in \mathbb{Z}_q^{(i-1)n/r}$ s.t. $\mathbf{A}_{i-1}\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \le 2^{i-1}$

Out: List L_i of vectors $\mathbf{x} \in \mathbb{Z}_q^{in/r}$ such that $\mathbf{A}_i\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \le 2^i$

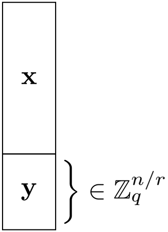


Wagner's algorithm for SIS

Wagner step in [BKW03]

Input: $\mathbf{A} = [\mathbf{A}' \mid \mathbf{I}_n] \in \mathbb{Z}_q^{n\times m}$
Output: List of vectors $\mathbf{x} \in \mathbb{Z}_q^m$ such that $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$

Divide $\mathbf{A}$ into submatrices $\mathbf{A}_i = [\mathbf{A}'_i | \mathbf{I}]$
Initialize a list L_0 with vectors from $\mathcal{U}(\{-1,0,1\}^{m-n})$
for $i = 1, \ldots, r$ **do**
  $L_i :=$ **LiftAndCombine**$(L_{i-1}, \mathbf{A}_i)$ $\triangleright\ \forall \mathbf{x} \in L_i, \mathbf{A}_i\mathbf{x} = \mathbf{0} \bmod q$
return L_r

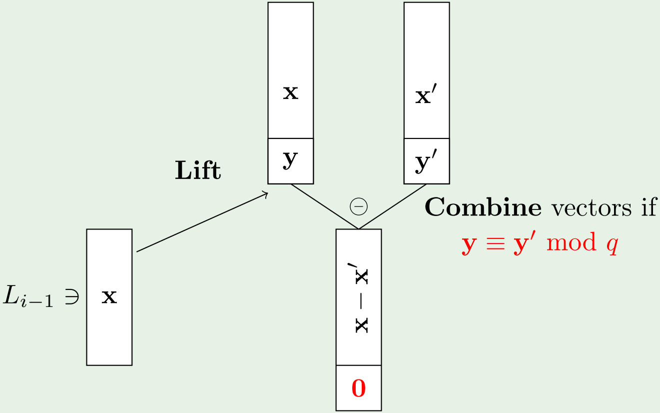


Time complexity: $O(r \cdot q^{n/r})$

Lazy-modulus switching

LiftAndCombine with lazy-mod switching [AFFP14]

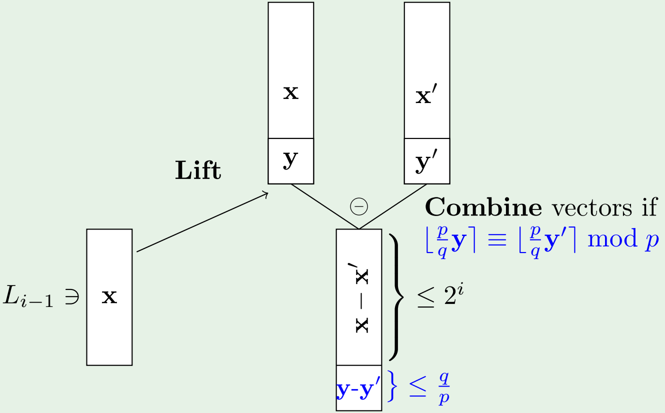
Input: List L_{i-1} of vectors $\mathbf{x}$ such that $\mathbf{A}_{i-1}\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \leq 2^{i-1}$
Output: List L_i of vectors $\mathbf{x}$ such that $\mathbf{A}_i\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \leq 2^i$



Lazy-modulus switching

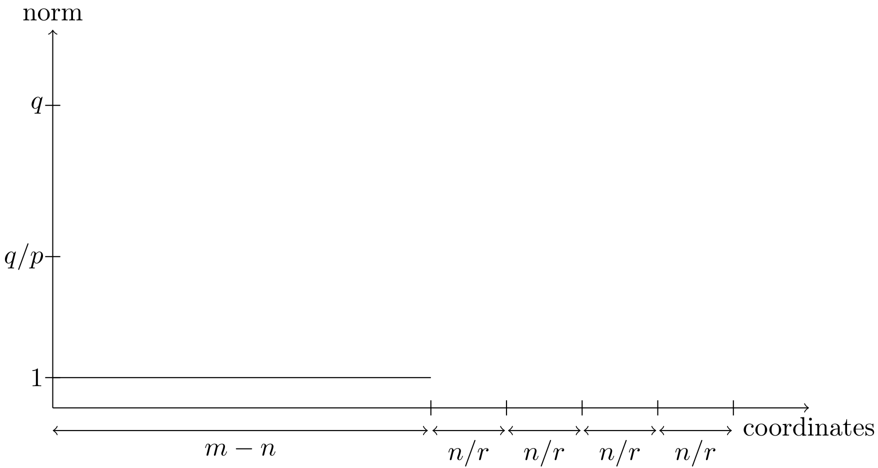
LiftAndCombine with lazy-mod switching [AFFP14]

Input: List L_{i-1} of vectors $\mathbf{x}$ such that $\mathbf{A}_{i-1}\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \leq 2^{i-1}$
Output: List L_i of vectors $\mathbf{x}$ such that $\mathbf{A}_i\mathbf{x} = \mathbf{0} \bmod q$ and $\|\mathbf{x}\|_\infty \leq 2^{i}$

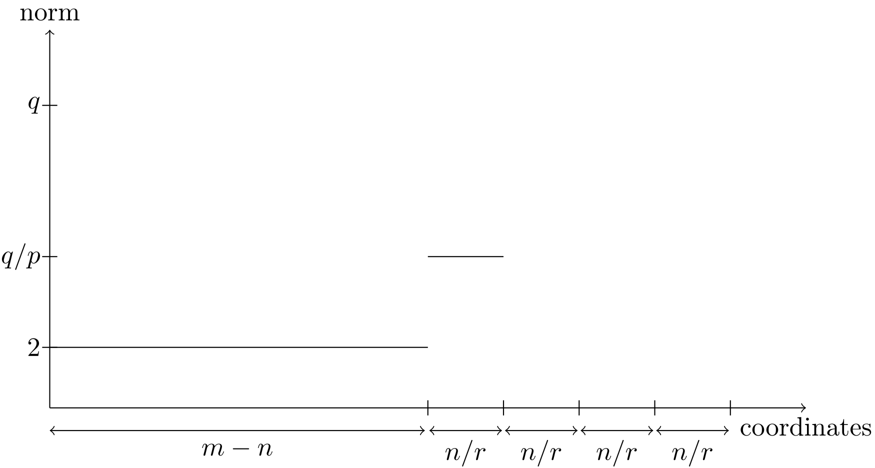


Time complexity: $O(r \cdot p^{n/r})$

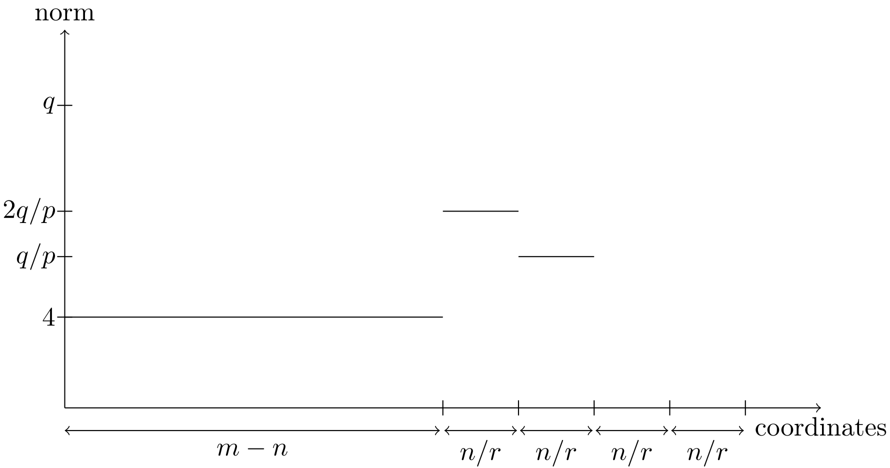
Bounds on the components of $\mathbf{x} \in L_0$ (Algorithm [AFFP14])



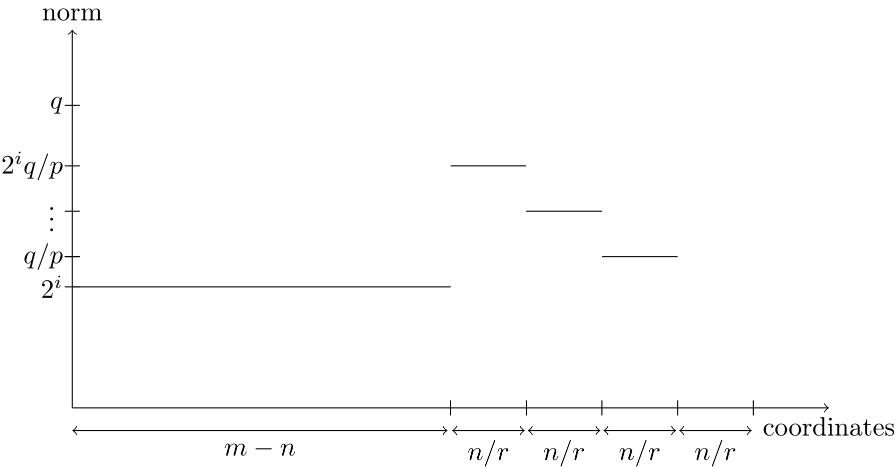
Bounds on the components of $\mathbf{x} \in L_1$ (Algorithm [AFFP14])



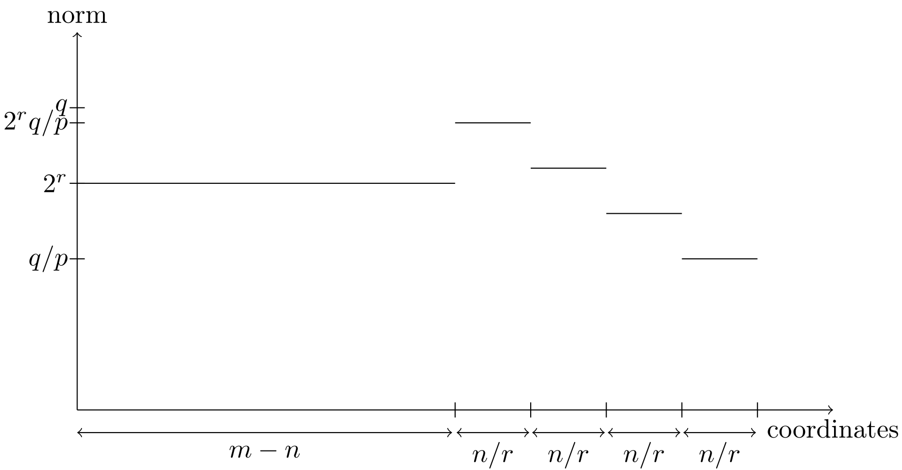
Bounds on the components of $\mathbf{x} \in L_2$ (Algorithm [AFFP14])



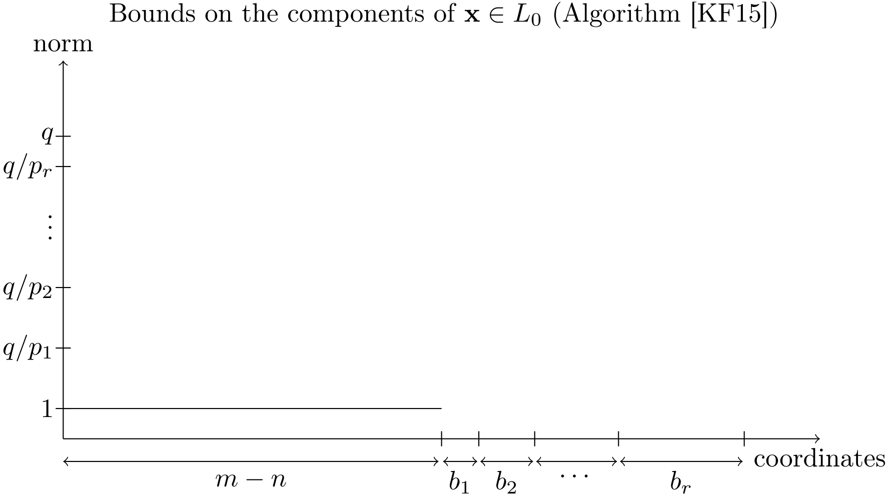
Bounds on the components of $\mathbf{x} \in L_i$ (Algorithm [AFFP14])



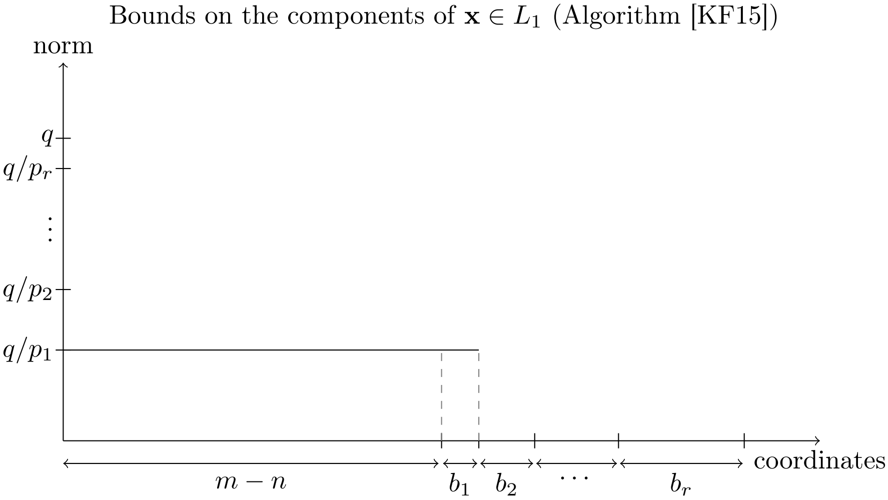
Bounds on the components of $\mathbf{x} \in L_r$ (Algorithm [AFFP14])



Kirchner-Fouque algorithm

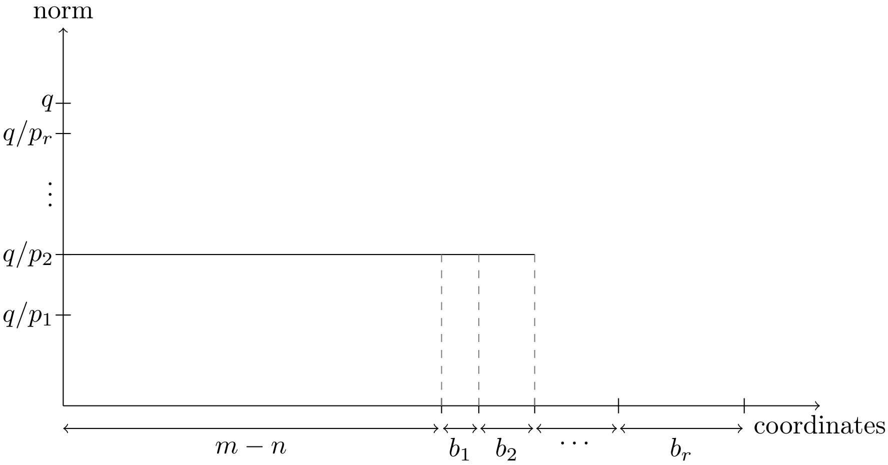


Kirchner-Fouque algorithm



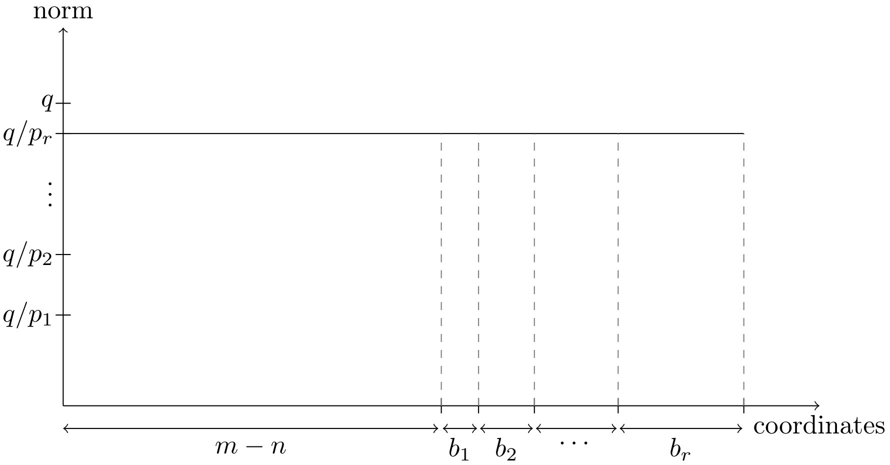
Kirchner-Fouque algorithm

Bounds on the components of $\mathbf{x} \in L_2$ (Algorithm [KF15])



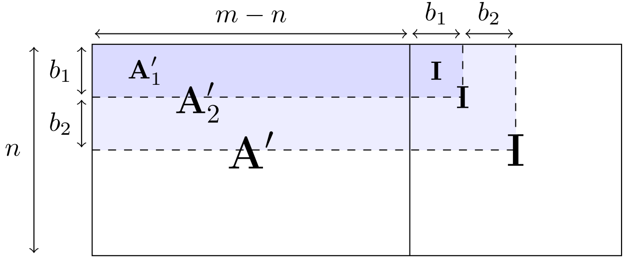
Kirchner-Fouque algorithm

Bounds on the components of $\mathbf{x} \in L_r$ (Algorithm [KF15])



Kirchner-Fouque algorithm

Time complexity: $O(r \cdot |L_i|)$

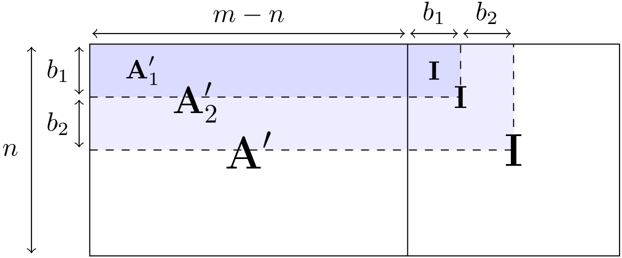


Parameter selection for target norm $\beta = \frac{q}{f}$ for some $f > 1$:

- Number of iterations r
- Moduli p_i
- Block sizes b_i
- List size $|L_i| = p_i^{b_i}$

Kirchner-Fouque algorithm

Time complexity: $O(r \cdot |L_i|)$



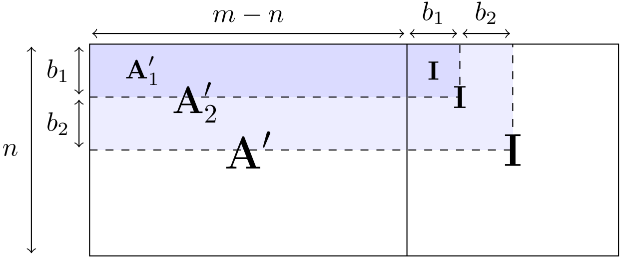
Parameter selection for target norm $\beta = \frac{q}{f}$ for some $f > 1$:

- Number of iterations $r = \log_2 \beta - 1$
- Moduli $p_i = q/2^i$
- Block sizes $b_i = \frac{\ln N}{\ln p_i}$ so that $N = |L_i| = p_i^{b_i}$
- List size $|L_i| = N$ such that it ensures

$$n = \sum_{i=1}^{r} b_i$$

Kirchner-Fouque algorithm

Time complexity: $O(r \cdot |L_i|)$



Parameter selection for target norm $\beta = \frac{q}{f}$ for some $f > 1$:

- Number of iterations $r = \log_2 \beta - 1$
- Moduli $p_i = q/2^i$
- Block sizes $b_i = \frac{\ln N}{\ln p_i}$ so that $N = |L_i| = p_i^{b_i}$
- List size $|L_i| = N$ such that it ensures

$$n = \sum_{i=1}^{r} b_i \leq \int_1^{r+1} b_x \mathrm{d}x \leq \log_2(N) \cdot (\ln\ln q - \ln\ln f)$$

Kirchner-Fouque algorithm

Kirchner-Fouque [KF15] (only their Wagner step)

For $n, m, q \in \mathbb{N}$ and $f > 1$, $\beta := \frac{q}{f}$, we are given a SIS instance $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. There exists an algorithm that returns a vector $\mathbf{x} \in \mathbb{Z}_q^m$ such that

- $\mathbf{A}\mathbf{x} = \mathbf{0} \bmod q$
- $\|\mathbf{x}\|_\infty \leq \beta = \frac{q}{f}$

in time

$$r \cdot N = \mathrm{poly}(n, \log q) \cdot 2^{\frac{n}{\ln\ln(q) - \ln\ln(f)}}$$

Kirchner-Fouque algorithm

Kirchner-Fouque [KF15] (only their Wagner step)

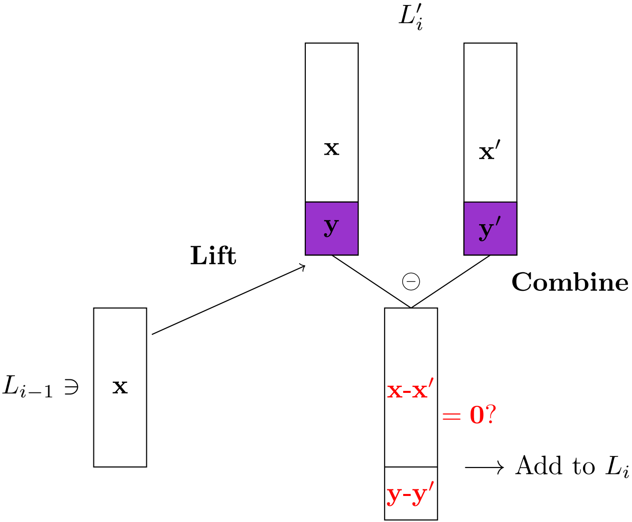
For $n, m, q \in \mathbb{N}$ and $f > 1$, $\beta := \frac{q}{f}$, we are given a SIS instance $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. There exists an algorithm that returns a vector $\mathbf{x} \in \mathbb{Z}_q^m$ such that

- $\mathbf{Ax} = \mathbf{0} \bmod q$
- $\|\mathbf{x}\|_\infty \leq \beta = \frac{q}{f}$

in time

$$r \cdot N = \mathrm{poly}(n, \log q) \cdot 2^{\frac{n}{\ln\ln(q) - \ln\ln(f)}}$$

Is $\mathbf{x}$ non-zero?


L'_i
$\mathbf{x}$
$\mathbf{x}'$
$\mathbf{y}$
$\mathbf{y}'$
Lift
$\ominus$
Combine
$L_{i-1} \ni$
$\mathbf{x}$
$\mathbf{x}$-$\mathbf{x}'$
$= \mathbf{0}?$
$\longrightarrow$ Add to L_i
$\mathbf{y}$-$\mathbf{y}'$

Distributions of the lists?

$$\begin{tikzcd} & L_1' \arrow[d] \\ L_0 \arrow[ur] & L_1 \end{tikzcd}$$

$\mathcal{U}^N(\{-1,0,1\}^{m-n})$

Distributions of the lists?

$$|\{-1, 0, 1\}^{m-n}| \gg |\mathbb{Z}_q^{b_1}|$$

$$\begin{tikzcd} & L_1' \arrow[d] \\ L_0 \arrow[ur] & L_1 \end{tikzcd}$$

$$\mathcal{U}^N(\{-1, 0, 1\}^{m-n}) \qquad \neq \{\mathbf{0}\}$$

Distributions of the lists?

$$\begin{tikzcd}
 & {|\{-1,0,1\}^{m-n}| \gg |\mathbb{Z}_q^{b_1}|} & & & \\
 & L'_1 \arrow[d] & L'_2 \arrow[d] & \cdots & L'_r \arrow[d] \\
L_0 \arrow[ur] & L_1 \arrow[ur] & L_2 \arrow[ur] & \cdots \arrow[ur] & L_r \\
\mathcal{U}^N(\{-1,0,1\}^{m-n}) & \neq \{\mathbf{0}\} & ? & & ???
\end{tikzcd}$$

Outline

1. Wagner-style algorithms to solve SIS^∞
2. A provable algorithm for SIS^∞
3. Implications for cryptographic problems

$\mathrm{SIS}^{\infty}_{n,m,q,\beta}$ matrix $\mathbf{A}$

Given $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a non-zero vector $\mathbf{x} \in \mathbb{Z}_q^m$ such that

- $\mathbf{A}\mathbf{x} = \mathbf{0} \mod q$
- $\|\mathbf{x}\|_\infty \leq \beta$

$$\Longleftrightarrow$$

β-SVP^{∞} in the lattice $\Lambda_q^{\perp}(\mathbf{A})$

Given $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a non-zero vector $\mathbf{x} \in \mathbb{Z}_q^m$ such that

- $\mathbf{x} \in \Lambda_q^{\perp}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{0} \bmod q\}$
- $\|\mathbf{x}\|_\infty \leq \beta$

$$\Lambda_i := \Lambda_q^\perp(\mathbf{A}_i) = \{\mathbf{x} \in \mathbb{Z}^{m-n+n_i} : \mathbf{A}_i\mathbf{x} = \mathbf{0} \bmod q\} = \mathcal{L}(\mathbf{B}_i)$$

$$\Lambda'_i := \mathcal{L}(\mathbf{B}'_i), \text{ with } \mathbf{B}'_i := \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{I}_{m-n} \\ \mathbf{0} & q\mathbf{I}_{n_{i-1}} & \boxed{\text{-}\mathbf{A}'_i} \\ \frac{q}{p_i}\mathbf{I}_{b_i} & \mathbf{0} & \end{pmatrix} =: \mathbf{B}_{i-1}$$

$$\Lambda_i := \Lambda_q^{\perp}(\mathbf{A}_i) = \{\mathbf{x} \in \mathbb{Z}^{m-n+n_i} : \mathbf{A}_i\mathbf{x} = \mathbf{0} \bmod q\} = \mathcal{L}(\mathbf{B}_i)$$

$$\Lambda_i' := \mathcal{L}(\mathbf{B}_i'), \text{ with } \mathbf{B}_i' := \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{I}_{m-n} \\ \mathbf{0} & q\mathbf{I}_{n_{i-1}} & \\ \frac{q}{p_i}\mathbf{I}_{b_i} & \mathbf{0} & \boxed{-\mathbf{A}_i'} \end{pmatrix} =: \mathbf{B}_{i-1}$$

$$\mathbb{Z}^{m-n} = \Lambda_0 \twoheadleftarrow \Lambda_1 \twoheadleftarrow \Lambda_2 \twoheadleftarrow \cdots \twoheadleftarrow \Lambda_r = \Lambda_q^{\perp}(\mathbf{A})$$

$$\Lambda_i := \Lambda_q^{\perp}(\mathbf{A}_i) = \{\mathbf{x} \in \mathbb{Z}^{m-n+n_i} : \mathbf{A}_i\mathbf{x} = \mathbf{0} \bmod q\} = \mathcal{L}(\mathbf{B}_i)$$

$$\Lambda_i' := \mathcal{L}(\mathbf{B}_i'), \text{ with } \mathbf{B}_i' := \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{I}_{m-n} \\ \mathbf{0} & q\mathbf{I}_{n_{i-1}} & \boxed{\text{-}\mathbf{A}_i'} \\ \frac{q}{p_i}\mathbf{I}_{b_i} & \mathbf{0} & \end{pmatrix} =: \mathbf{B}_{i-1}$$

$$\begin{tikzcd}
 & \Lambda_1' \arrow[dl, two heads] \arrow[d, phantom, "\cup\!\mid"] & \Lambda_2' \arrow[dl, two heads] \arrow[d, phantom, "\cup\!\mid"] & \cdots \arrow[dl, two heads] & \Lambda_r' \arrow[dl, two heads] \arrow[d, phantom, "\cup\!\mid"] \\
\mathbb{Z}^{m-n} = \Lambda_0 & \Lambda_1 \arrow[l, two heads] & \Lambda_2 \arrow[l, two heads] & \cdots \arrow[l, two heads] & \Lambda_r = \Lambda_q^{\perp}(\mathbf{A}) \arrow[l, two heads]
\end{tikzcd}$$

$$\Lambda_i := \Lambda_q^{\perp}(\mathbf{A}_i) = \{\mathbf{x} \in \mathbb{Z}^{m-n+n_i} : \mathbf{A}_i \mathbf{x} = \mathbf{0} \bmod q\} = \mathcal{L}(\mathbf{B}_i)$$

$$\Lambda'_i := \mathcal{L}(\mathbf{B}'_i), \text{ with } \mathbf{B}'_i := \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{I}_{m-n} \\ \mathbf{0} & q\mathbf{I}_{n_{i-1}} & \\ \frac{q}{p_i}\mathbf{I}_{b_i} & \mathbf{0} & \boxed{\text{-}\mathbf{A}'_i} \end{pmatrix} =: \mathbf{B}_{i-1}$$

$$\begin{tikzcd}
 & \Lambda'_1 \arrow[dl, two heads] \arrow[d, phantom, sloped, "\supseteq"] & \Lambda'_2 \arrow[dl, two heads] \arrow[d, phantom, sloped, "\supseteq"] & \cdots \arrow[dl, two heads] & \Lambda'_r \arrow[dl, two heads] \arrow[d, phantom, sloped, "\supseteq"] \\
\mathbb{Z}^{m-n} = \Lambda_0 & \Lambda_1 \arrow[l, two heads] & \Lambda_2 \arrow[l, two heads] & \cdots \arrow[l, two heads] & \Lambda_r = \Lambda_q^{\perp}(\mathbf{A}) \arrow[l, two heads]
\end{tikzcd}$$

Discrete Gaussian distribution

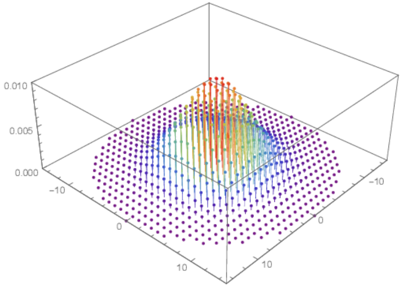
For any $s > 0$ and $\mathbf{x} \in \mathbb{R}^n$, the Gaussian function is $\rho_s(\mathbf{x}) := e^{-\pi(\|\mathbf{x}\|_2/s)^2}$.

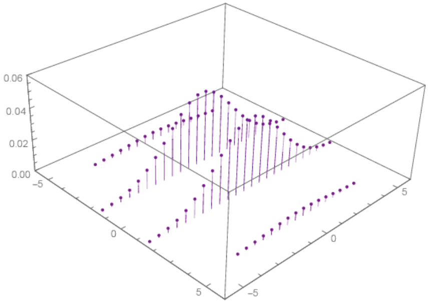
$$\rho_s(\mathcal{L}) := \sum_{\mathbf{x}\in\mathcal{L}} \rho_s(\mathbf{x})$$

Discrete Gaussian distribution

For a full-rank lattice $\mathcal{L}$ and any $s > 0$, the discrete Gaussian distribution $D_{\mathcal{L},s}$ is defined by

$$\Pr_{X\sim D_{\mathcal{L},s}}[X = \mathbf{x}] = \frac{\rho_s(\mathbf{x})}{\rho_s(\mathcal{L})}.$$





Discrete Gaussian distribution

Convolution lemma

Let be a lattice $\mathcal{L} \subseteq \mathbb{R}^n$, $\varepsilon > 0$ and $s \geq \eta_\varepsilon(\mathcal{L})$. For $X_1, X_2 \sim D_{\mathcal{L},s}$,

$$X_1 - X_2 \sim_{3\varepsilon} D_{\mathcal{L},\sqrt{2}s}.$$

Smoothing parameter: $\eta_\varepsilon(\mathcal{L}) := \inf\{s > 0 : \rho_{1/s}(\mathcal{L}^* \backslash \{\mathbf{0}\}) \leq \varepsilon\}$.

Lower bound on s for $D_{\mathcal{L},s}$ to 'behave like' a continuous Gaussian distribution.

Wagner as a Gaussian sampler

Wagner-style algorithm for SIS$^\infty$ [our algorithm]

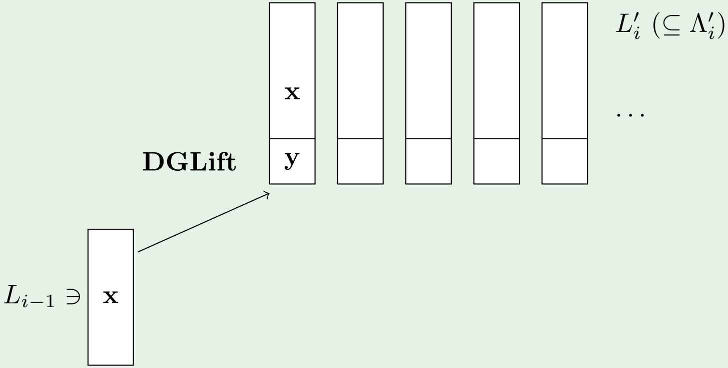
Input: $\mathbf{A} = [\mathbf{A}' \mid \mathbf{I}_n] \in \mathbb{Z}_q^{n \times m}$
Output: List of vectors $\mathbf{x} \in \Lambda_q^\perp(\mathbf{A})$

Define sequences of lattices Λ_i, Λ_i' for $i = 0, \ldots, r$
Set s_0 such that all the $s_i := \sqrt{2}^i s_0$ satisfy the smoothness conditions
Initialize a list L_0 with vectors following D_{Λ_0, s_0}
for $i = 1, \ldots, r$ **do**
    $L_i :=$ **LiftAndCombine**(L_{i-1}, Λ_i) $\triangleright \forall \mathbf{x} \in L_i, \mathbf{x} \sim_\varepsilon D_{\Lambda_i, s_i}$
return L_r

Wagner as a Gaussian sampler

LiftAndCombine [our algorithm]

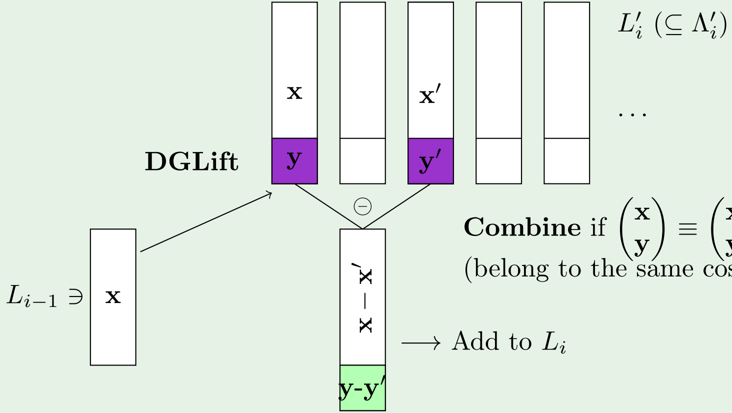
Input: List L_{i-1} of vectors $\mathbf{x} \sim D_{\Lambda_{i-1}, s_{i-1}}$
Output: List L_i of vectors $\mathbf{x} \sim D_{\Lambda_i, s_i}$



Wagner as a Gaussian sampler

LiftAndCombine [our algorithm]

Input: List L_{i-1} of vectors $\mathbf{x} \sim D_{\Lambda_{i-1}, s_{i-1}}$
Output: List L_i of vectors $\mathbf{x} \sim D_{\Lambda_i, s_i}$



Combine if $\begin{pmatrix}\mathbf{x}\\\mathbf{y}\end{pmatrix} \equiv \begin{pmatrix}\mathbf{x}'\\\mathbf{y}'\end{pmatrix} \bmod \Lambda_i$
(belong to the same coset of Λ'_i/Λ_i)

Outline

Implications for SIS

Main theorem: Solving SIS$^\infty$ in provable subexponential time

- $n \in \mathbb{N}$
- $m = n + \omega(n/\log\log n) \in \mathbb{N}$
- $q = \mathrm{poly}(n)$ prime such that $q^{1-n/m} \geq 6$
- $0 \leq \varepsilon \leq \frac{1}{mq^2}$
- $f > 1$ such that $\frac{q}{f} \geq \sqrt{\ln(1/\varepsilon)}$
- $\beta := \frac{q}{f}\sqrt{\ln m}$

Implications for SIS

Main theorem: Solving SIS^∞ in provable subexponential time

- $n \in \mathbb{N}$
- $m = n + \omega(n/\log\log n) \in \mathbb{N}$
- $q = \mathrm{poly}(n)$ prime such that $q^{1-n/m} \geq 6$
- $0 \leq \varepsilon \leq \frac{1}{mq^2}$
- $f > 1$ such that $\frac{q}{f} \geq \sqrt{\ln(1/\varepsilon)}$
- $\beta := \frac{q}{f}\sqrt{\ln m}$

There exists an algorithm that solves $\mathrm{SIS}^\infty_{n,m,q,\beta}$ in expected time

$$T = \mathrm{poly}(n, \ln(1/\varepsilon)) \cdot 2^{\frac{n/2}{\ln\ln q - \ln\left(\ln f + \frac{1}{2}\ln\ln\frac{1}{\varepsilon}\right) - O(1)}} = 2^{O\left(\frac{n}{\ln\ln n}\right)}$$

with success probability $1 - 2^{-\tilde{\Omega}(n)}$.

Implications for ternary-LWE

Definition: Decision-LWE (Learning With Errors)

Let $\mathbf{s} \sim \mathcal{U}(\mathbb{Z}_q^n)$ and χ be a probability distribution on $\mathbb{Z}$. Decide whether given pairs $(\mathbf{a}, c) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ are sampled according to

- the uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$; or
- the LWE distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$, that samples $c = \langle \mathbf{a}, \mathbf{s} \rangle + e$ with $e \sim \chi$.

Implications for ternary-LWE

Definition: Decision-LWE (Learning With Errors)

Let $\mathbf{s} \sim \mathcal{U}(\mathbb{Z}_q^n)$ and χ be a probability distribution on $\mathbb{Z}$. Decide whether given pairs $(\mathbf{a}, c) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ are sampled according to

- the uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$; or
- the LWE distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$, that samples $c = \langle \mathbf{a}, \mathbf{s} \rangle + e$ with $e \sim \chi$.

Distinguisher [AR05]: sums together subexponentially many solutions to SIS.
It forces to take $\varepsilon = e^{-\tilde{\Omega}(n)}$...

Implications for ternary-LWE

Definition: Decision-LWE (Learning With Errors)

Let $\mathbf{s} \sim \mathcal{U}(\mathbb{Z}_q^n)$ and χ be a probability distribution on $\mathbb{Z}$. Decide whether given pairs $(\mathbf{a}, c) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ are sampled according to

- the uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$; or
- the LWE distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$, that samples $c = \langle \mathbf{a}, \mathbf{s} \rangle + e$ with $e \sim \chi$.

Distinguisher [AR05]: sums together subexponentially many solutions to SIS. It forces to take $\varepsilon = e^{-\tilde{\Omega}(n)}$... that makes the runtime for $q = \mathrm{poly}(n)$

$$T = 2^{\frac{n}{\ln \ln q - \ln(\ln f + \frac{1}{2} \ln \boldsymbol{n}) - O(1)}} = 2^{n/O(1)}$$

Work in progress: Choose a sequence of lattices with smaller smoothing parameters (than $\frac{q}{p_i}\mathbb{Z}^{b_i}$)

Implications for Dilithium

In practice, attacks run faster than the proven version.
$\rightarrow$ Perform a heuristic time estimation

Implications for Dilithium

In practice, attacks run faster than the proven version.
$\rightarrow$ Perform a heuristic time estimation

NIST level	n	m	q	β	$\log_2(\text{Time})$
2 (**128**)	$256 \cdot 4$	$256 \cdot 9$	8380417	350209	**270**
3 (**192**)	$256 \cdot 6$	$256 \cdot 12$	8380417	724481	**344**
5 (**256**)	$256 \cdot 8$	$256 \cdot 16$	8380417	769537	**451**

Implications for Dilithium

In practice, attacks run faster than the proven version.
$\rightarrow$ Perform a heuristic time estimation

NIST level	n	m	q	β	$\log_2(\text{Time})$
2 (**128**)	$256 \cdot 4$	$256 \cdot 9$	8380417	350209	**270**
3 (**192**)	$256 \cdot 6$	$256 \cdot 12$	8380417	724481	**344**
5 (**256**)	$256 \cdot 8$	$256 \cdot 16$	8380417	769537	**451**

This attack does not seem to threaten Dilithium

Conclusion

- A *provable* algorithm for SIS^∞ in subexponential time $2^{O\left(\frac{n}{\ln \ln n}\right)}$
- Leads for getting a similar result for LWE
- Dilithium is not broken!

Conclusion

- A *provable* algorithm for SIS^∞ in subexponential time $2^{O\left(\frac{n}{\ln \ln n}\right)}$
- Leads for getting a similar result for LWE
- Dilithium is not broken!

Take-away

× Don't focus too much on coordinates of vectors, roundings, parity-check matrices...

✓ Explicit the mathematical structures underlying the problem

Thank you for your attention!

References

[AFFP14] Martin R Albrecht et al. "Lazy modulus switching for the BKW algorithm on LWE." In: *PKC*. 2014.

[AR05] Dorit Aharonov and Oded Regev. "Lattice problems in NP $\cap$ coNP." In: *ACM* (2005).

[BKW03] Avrim Blum, Adam Kalai, and Hal Wasserman. "Noise-tolerant learning, the parity problem, and the statistical query model." In: *ACM* (2003).

[HKM18] Gottfried Herold, Elena Kirshanova, and Alexander May. "On the asymptotic complexity of solving LWE." In: *Designs, Codes and Cryptography* (2018).

[KF15] Paul Kirchner and Pierre-Alain Fouque. "An improved BKW algorithm for LWE with applications to cryptography and lattices." In: *CRYPTO*. 2015.