# Refined Attack on LWE with Hints: Constructing Lattice via Gaussian Elimination

Jinzheng Cao Haodong Jiang Qingfeng Cheng

Information Engineering University

CRYPTO 2025

# Outline

1. Background
   - LWE
   - LWE with Hints
   - Frameworks for LWE with Hints
2. Our Novel Framework
   - Our Novel Framework
3. Complexity Analysis
4. Experiments

# Learning with Errors, LWE

- LWE equation:

$$\mathbf{b} \equiv \mathbf{sA} + \mathbf{e} \mod q$$

small secret LWE: **s** and **e** are short vectors

- Primal attack:

$$\mathbf{B}^{\mathrm{LWE}} = \begin{bmatrix} q\mathbf{I}_m & \mathbf{0} & \mathbf{0} \\ \mathbf{A} & \mathbf{I}_n & \mathbf{0} \\ \mathbf{b} & \mathbf{0} & 1 \end{bmatrix}$$

contains short vector $[\mathbf{w}, \mathbf{s}, -1] \cdot \mathbf{B}^{\mathrm{LWE}} = [-\mathbf{e}, \mathbf{s}, -1]$

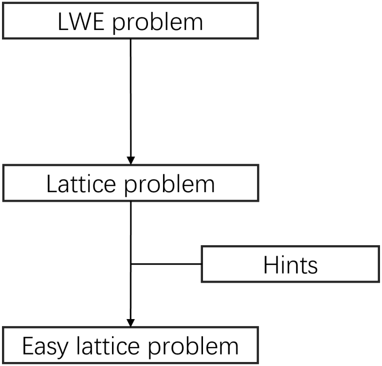
# Hints

- Summarize the side-channel information about **s**
- Modeled as inner products
  - Perfect hint: A tuple $\bar{\mathbf{v}} = (\mathbf{v}, l) \in \mathbb{Z}^n \times \mathbb{Z}$ with $< \mathbf{v}, \mathbf{s} >= l$.
  - Approximate hint: A tuple $\bar{\mathbf{v}} = (\mathbf{v}, l) \in \mathbb{Z}^n \times \mathbb{Z}$ with $< \mathbf{v}, \mathbf{s} >= l + \epsilon$.
  - Modular hint: A tuple $\bar{\mathbf{v}} = (\mathbf{v}, l, m) \in \mathbb{Z}^n \times \mathbb{Z} \times \mathbb{N}$ with $< \mathbf{v}, \mathbf{s} > \equiv l \mod m_i$.
  - Mod-$q$ hint: We call modular hint $\bar{\mathbf{v}} = (\mathbf{v}, l, m_i)$ a mod-$q$ hint if $m_i = q$.

# The DDGR20 Frameworks

First systematic framework for LWE with hints [1]

- Use hints to reconstruct the lattice
- Process each hint successively
- hard to implement with current software

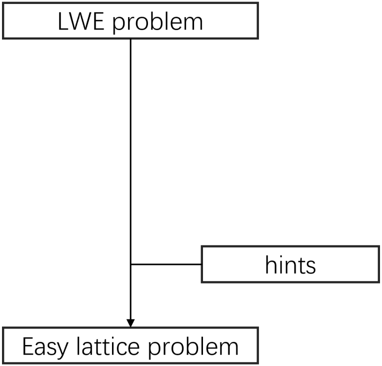



[1] Dana Dachman-Soled et al. “LWE with Side Information: Attacks and Concrete Security Estimation”. In: Advances in Cryptology – CRYPTO 2020. 2020, pp. 329-358.

# The MN23 Frameworks

Efficient framework for LWE with hints [2]

- Process all hints together
- Discuss the "too many hints" regime
- LLL-reduction

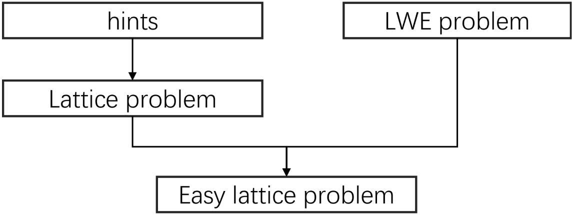



[2] Alexander May and Julian Nowakowski. “Too Many Hints – When LLL Breaks LWE”. In: Advances in Cryptology – ASIACRYPT 2023. 2023, pp. 106-137.

# New Approach for LWE with Hints

Main idea

- Hint-centric view
- New lattice construction
- Method for too many hints



# Constructing $\mathbb{Z}$-SIS Basis

Hints:

- $< \mathbf{v}, \mathbf{s} >= l$
- $\mathbb{Z}$-SIS problem: Find $\mathbf{s}$ such as $\|\mathbf{s}\| \leq \nu$ and $\mathbf{s} \cdot \mathbf{V} = \ell$

$$\mathbf{V} = \begin{bmatrix} | & & | \\ \mathbf{v}_1^T & \dots & \mathbf{v}_k^T \\ | & & | \end{bmatrix}$$

- Share secret vector with LWE

# Constructing $\mathbb{Z}$-SIS Basis

Given hint matrix $\mathbf{H}$, $\mathcal{L}(\mathbf{H})$ contains a sublattice $\mathcal{L}_{\mathbf{H},k} = \{[v_1, \ldots, v_{n+1}] \in \mathcal{L}(\mathbf{H}) : v_1 = \ldots = v_k = 0\}$

Lattice construction:

$$\mathbf{H} = \left[\begin{array}{ccc|c|c} | & & | & \mathbf{0} & 0 \\ \mathbf{v}_1^T & \ldots & \mathbf{v}_k^T & \overline{\mathbf{I}_{n-k}} & \vdots \\ | & & | & & 0 \\ \hline l_1 & \ldots & l_k & 0\ldots0 & 1 \end{array}\right] = \left[\begin{array}{c|c|c} \mathbf{V}_1 & \mathbf{0} & \mathbf{0} \\ \mathbf{V}_2 & \mathbf{I}_{n-k} & \\ \hline \ell & 0\ldots0 & 1 \end{array}\right]$$

$$[\mathbf{s}, -1] \cdot \mathbf{H} = [0^k, s_{k+1}, \ldots, s_n, -1]$$

# Constructing $\mathbb{Z}$-SIS Basis

Given hint matrix $\mathbf{H}$, $\mathcal{L}(\mathbf{H})$ contains a sublattice $\mathcal{L}_{\mathbf{H},k} = \{[v_1, \ldots, v_{n+1}] \in \mathcal{L}(\mathbf{H}) : v_1 = \ldots = v_k = 0\}$

Lattice construction:

$$\left[\begin{array}{c|c|c} \mathbf{V}_1 & \mathbf{0} & \\ \hline \mathbf{V}_2 & \mathbf{I}_{n-k} & \mathbf{0} \\ \hline \ell & 0\ldots0 & 1 \end{array}\right] \xrightarrow{\text{Gaussian}} \left[\begin{array}{c|c|c} \mathbf{V}'_k & \mathbf{J}'_1 & \\ \hline \mathbf{0} & \mathbf{J}'_2 & \mathbf{0} \\ \hline \ell & 0\ldots0 & 1 \end{array}\right] \xrightarrow{\text{reduce}}$$

$$\left[\begin{array}{c|c|c} \mathbf{V}'_k & \mathbf{J}'_1 & \\ \hline \mathbf{0} & \mathbf{J}'_2 & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{s}'' & 1 \end{array}\right] = \left[\begin{array}{c|c} \mathbf{V}'_k & \mathbf{J}'_1 \mid \mathbf{0} \\ \hline \mathbf{0} & \mathbf{B}_{\mathrm{SIS}} \end{array}\right]$$

# Constructing $\mathbb{Z}$-SIS Basis

Given hint matrix $\mathbf{H}$, $\mathcal{L}(\mathbf{H})$ contains a sublattice $\mathcal{L}_{\mathbf{H},k} = \{[v_1, \ldots, v_{n+1}] \in \mathcal{L}(\mathbf{H}) : v_1 = \ldots = v_k = 0\}$

Lattice construction:

$$\mathbf{U}_{\text{SIS}} \cdot \left[\begin{array}{c|c|c} \begin{array}{c}\mathbf{V}_1 \\ \hline \mathbf{V}_2\end{array} & \begin{array}{c}\mathbf{0} \\ \hline \mathbf{I}_{n-k}\end{array} & \mathbf{0} \\ \hline \ell & 0 \ldots 0 & 1 \end{array}\right] \rightarrow \left[\begin{array}{c|c|c} \begin{array}{c}\mathbf{V}'_k \\ \hline \mathbf{0}\end{array} & \begin{array}{c}\mathbf{J}'_1 \\ \hline \mathbf{J}'_2\end{array} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{s}'' & 1 \end{array}\right] = \left[\begin{array}{c|cc} \mathbf{V}'_k & \mathbf{J}'_1 & \mathbf{0} \\ \hline \mathbf{0} & \multicolumn{2}{c}{\mathbf{B}_{\text{SIS}}} \end{array}\right]$$

# Comparison with Other Works

Given hint matrix $\mathbf{H}$, $\mathcal{L}(\mathbf{H})$ contains a sublattice
$\mathcal{L}_{\mathbf{H},k} = \{[v_1, \ldots, v_{n+1}] \in \mathcal{L}(\mathbf{H}) : v_1 = \ldots = v_k = 0\}$

Our construction:

$$\left[\begin{array}{c|c|c} \begin{array}{c}\mathbf{V}_1 \\ \hline \mathbf{V}_2\end{array} & \begin{array}{c}\mathbf{0} \\ \hline \mathbf{I}_{n-k}\end{array} & \mathbf{0} \\ \hline \ell & 0\ldots0 & 1 \end{array}\right] \xrightarrow{\text{Gaussian}} \left[\begin{array}{c|c|c} \begin{array}{c}\mathbf{V}'_k \\ \hline \mathbf{0}\end{array} & \begin{array}{c}\mathbf{J}'_1 \\ \hline \mathbf{J}'_2\end{array} & \mathbf{0} \\ \hline \ell & 0\ldots0 & 1 \end{array}\right] \xrightarrow{\text{reduce}} \left[\begin{array}{c|cc} \mathbf{V}'_k & \mathbf{J}'_1 & \mathbf{0} \\ \hline \mathbf{0} & \multicolumn{2}{c}{\mathbf{B}_{\text{SIS}}} \end{array}\right]$$

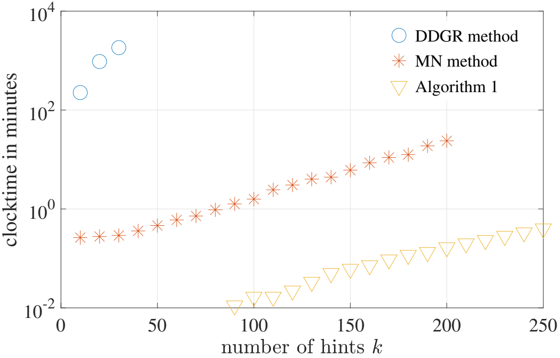
DDGR method:

- process one hint per time
- compute dual basis

MN method:

- LLL reduction
- multiply columns of $\mathbf{H}$ by $\lceil 2^{\frac{n}{2}} \cdot gh(\mathcal{L}(\mathbf{H})) \rceil$

# Comparison with Other Works




- Process multiple hints in one stroke
- LLL $\rightarrow$ Gaussian elimination
- Remove the scaling factor

# Combining $\mathbb{Z}$-SIS and LWE

- Theoretical basis: $\mathbb{Z}$-SIS and LWE have the same secret vector $\mathbf{s}$
- Main technique: reuse the transformation matrix $\mathbf{U}_{\text{SIS}}$

$$\mathbf{U}_{\text{SIS}} \cdot \left[\begin{array}{c|c|c} \begin{array}{c}\mathbf{V}_1 \\ \hline \mathbf{V}_2\end{array} & \begin{array}{c}\mathbf{0} \\ \hline \mathbf{I}_{n-k}\end{array} & \mathbf{0} \\ \hline \ell & 0 \ldots 0 & 1 \end{array}\right] \rightarrow \left[\begin{array}{c|c|c} \begin{array}{c}\mathbf{V}'_k \\ \hline \mathbf{0}\end{array} & \begin{array}{c}\mathbf{J}'_1 \\ \hline \mathbf{J}'_2\end{array} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{s}'' & 1 \end{array}\right] = \left[\begin{array}{c|c} \mathbf{V}'_k & \mathbf{J}'_1 \;\big|\; \mathbf{0} \\ \hline \mathbf{0} & \mathbf{B}_{\text{SIS}} \end{array}\right]$$

$$\mathbf{U}_{\text{SIS}} \cdot \left[\begin{array}{c|c|c|c} \begin{array}{c}\mathbf{V}_1 \\ \hline \mathbf{V}_2\end{array} & \mathbf{A} & \begin{array}{c}\mathbf{0} \\ \hline \mathbf{I}_{n-k}\end{array} & \mathbf{0} \\ \hline \ell & \mathbf{b} & 0 \ldots 0 & 1 \end{array}\right] \rightarrow \left[\begin{array}{c|c|c|c} \begin{array}{c}\mathbf{V}'_k \\ \hline \mathbf{0}\end{array} & \begin{array}{c}\mathbf{A}'_1 \\ \hline \mathbf{A}'_2\end{array} & \begin{array}{c}\mathbf{J}'_1 \\ \hline \mathbf{J}'_2\end{array} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{b}' & \mathbf{s}'' & 1 \end{array}\right] \rightarrow \mathbf{B}_1$$

# Combining $\mathbb{Z}$-SIS and LWE

- Theoretical basis: $\mathbb{Z}$-SIS and LWE have the same secret vector $\mathbf{s}$
- Main technique: reuse the transformation matrix $\mathbf{U}_{\mathrm{SIS}}$

$$\mathbf{U}_{\mathrm{SIS}} \cdot \left[\begin{array}{c|c|c} \mathbf{A} & \begin{array}{c}\mathbf{0}\\ \hline \mathbf{I}_{n-k}\end{array} & \mathbf{0} \\ \hline \mathbf{b} & 0\ldots0 & 1 \end{array}\right] \to \left[\begin{array}{c|c} \mathbf{A}' & * \\ \hline \multicolumn{2}{c}{\mathbf{B}_1} \end{array}\right]$$

New lattice basis: $\mathbf{B}_2 = \left[\begin{array}{c|c} q\mathbf{I}_m & \mathbf{0} \\ \hline \multicolumn{2}{c}{\mathbf{B}_1} \end{array}\right]$

Target vector:

$$[\mathbf{s}, -1]\cdot(\mathbf{U}_{\mathrm{SIS}})^{-1}\cdot\mathbf{U}_{\mathrm{SIS}}\cdot \left[\begin{array}{c|c|c} \mathbf{A} & \begin{array}{c}\mathbf{0}\\ \hline \mathbf{I}_{n-k}\end{array} & \mathbf{0} \\ \hline \mathbf{b} & 0\ldots0 & 1 \end{array}\right] = [-\mathbf{e} \bmod q, s_{k+1}, \ldots, s_n, -1]$$

# Complexity Analysis

Dimension decrease

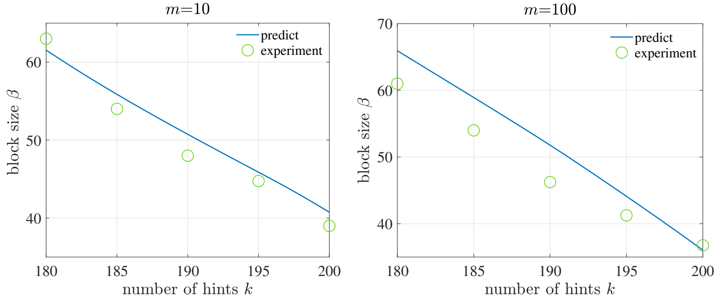
- $[-\mathbf{e} \bmod q, s_1, \ldots, s_n, -1] \to [-\mathbf{e} \bmod q, s_{k+1}, \ldots, s_n, -1]$

Volume increase

- $\det(\mathbf{B}_2) = q^m \cdot \det(\mathbf{B}_{\mathrm{SIS}})$
- $\det(\mathbf{B}_{\mathrm{SIS}}) = \frac{\det(\mathbf{H})}{\det(\mathbf{V}'_k)} = \frac{\det(\mathbf{V}_1)}{\det(\mathbf{V}'_k)}$

$$\mathbf{H} = \left[\begin{array}{c|c|c} \mathbf{V}_1 & \mathbf{0} & \\ \hline \mathbf{V}_2 & \mathbf{I}_{n-k} & \mathbf{0} \\ \hline \ell & 0 \ldots 0 & 1 \end{array}\right] \to \left[\begin{array}{c|c|c} \mathbf{V}'_k & \mathbf{J}'_1 & \mathbf{0} \\ \hline \mathbf{0} & \multicolumn{2}{c}{\mathbf{B}_{\mathrm{SIS}}} \end{array}\right]$$

# Complexity Analysis




- evaluate new lattice's dimension and volume
- predict block $\beta$ with BKZ estimator

# Too Many Hints

## $\mathbb{Z}$-SIS lattice

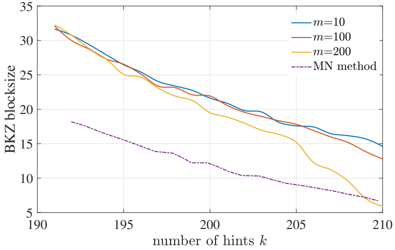
$$\text{basis: } \mathbf{H} = \left[\begin{array}{c|c|c} \mathbf{V}_1 & \mathbf{0} & \\ \hline \mathbf{V}_2 & \mathbf{I}_{n-k} & \mathbf{0} \\ \hline \ell & 0\ldots0 & 1 \end{array}\right] \to \mathbf{B}_{\text{SIS}}$$

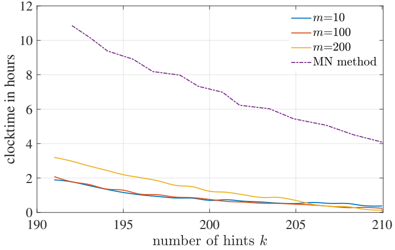
$$\text{target: } \mathbf{v}_{\text{SIS}} = [s_{k+1}, \ldots, s_n, -1]$$

- Average case: can't identify the shortness of $\mathbf{v}_{\text{SIS}}$ in $\mathcal{L}(\mathbf{B}_{\text{SIS}})$
- Too many hints case:
  - lattice $\mathcal{L}(\mathbf{B}_{\text{SIS}})$ already forms an uSVP instance
  - extract $\mathbf{v}_{\text{SIS}}$ solely from $\mathcal{L}(\mathbf{B}_{\text{SIS}})$

# Our Results

Experiments on CRYSTALS-KYBER 512 with perfect hints

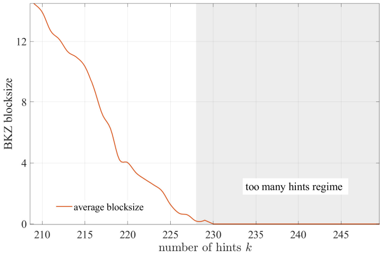


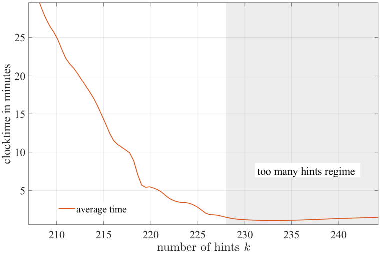




- Overall time of lattice construction and BKZ reduction
- Faster than MN method
- Fewer LWE samples already suffices to solve

# Our Results

## Too many hints




- $k < 228$: solvable by BKZ
- $k > 228$: solvable by LLL
- extend the bound for too many hints

# Summary

- Novel Framework for LWE with various kinds of hints
- Faster lattice construction based on new perspective of hints
- Discuss too many hints regime using the complexity analysis model

- Future works
  - Explore new kinds of hints in real-world side-channel attacks
  - Use the framework to analyze PQC schemes

# Thank You