

How Far Are We from Breaking Lattice-Based Cryptography?

An Analysis via Short Integer Solution and the Extrapolated Dihedral Coset Problem

Weiqliang Wen, C² team, Télécom Paris

Context

Lattice-based cryptography, including the NIST standards [FIPS203, FIPS204], relies on the hardness of lattice problems such as the *Short Integer Solution* (SIS) problem [Ajt96]. An SIS instance is a random matrix $\mathbf{A} = (\mathbf{a}_1 | \dots | \mathbf{a}_m) \in \mathbb{Z}_q^{n \times m}$ with m columns for integers n, m, q . The goal is to find a nonzero $\mathbf{x} \in \mathbb{Z}^m$ with $\|\mathbf{x}\|_\infty \leq 1$ and $\mathbf{A}\mathbf{x} \equiv \mathbf{0} \pmod{q}$. As given by Micciancio and Peikert [MP13], SIS is as hard as worst-case lattice problems for up to $m \approx q^2/n^c$ (that is polynomial in n) for any constant $c > 0$ columns. From quantum perspective, the *Dihedral Coset Problem* (DCP) plays a similar role: Regev [Reg04] reduced worst-case lattice problems to DCP with any polynomially many samples, and Brakerski et al. [BKSW18] extended this connection to the *Extrapolated DCP* (EDCP). A DCP sample is of form $\frac{1}{\sqrt{2}}(|0\rangle|x\rangle + |1\rangle|x+s\rangle)$, where $s \in \mathbb{Z}_{q^n}$ is a fixed secret and $x \in \mathbb{Z}_{q^n}$ is uniformly random. An EDCP sample has the same form $\frac{1}{\sqrt{2}}(|0\rangle|\mathbf{x}\rangle + |1\rangle|\mathbf{x}+\mathbf{s}\rangle)$, with $\mathbf{x}, \mathbf{s} \in \mathbb{Z}_q^n$. Given m samples, the goal is to recover the secret. Concretely, an efficient (E)DCP algorithm with polynomial (in n) samples would break lattice-based cryptography. For *power-of-two* moduli, there are quasi-polynomial time attacks on both SIS [CLZ22, App. A] and EDCP [BJK+25] when there are quasi-polynomial available columns/samples. Interestingly, both algorithms share a similar recursion structure. Later, Chailloux and Hermouet [CH26] confirm this similarity: plugging a randomness-recoverable variant of Regev’s solver into their reduction from EDCP to Inhomogeneous SIS (ISIS) gives the same result for solving EDCP by [BJK+25].

Very recently, Ding et al. [DGJT26] improves the Regev–CLZ recursion by *two-bit lifting*. This reduces the number of columns from $O(N^d)$ to $O(N^{\lceil d/2 \rceil})$. A natural question follows: *does the EDCP side admit an analogous two-bit algorithm*, halving the exponent in the sample complexity of [BJK+25] and moving closer to the regime that matters for cryptography?

Objectives

1. Understand the Regev–CLZ recursion for SIS [CLZ22] and its quantum counterpart for EDCP [BJK+25].
2. Re-derive [BJK+25] from Regev’s recursion through [CH26].
3. Try to realize the two-bit lifting for EDCP by instantiating the framework in [CH26].

Deliverables

1. Implementations of Regev–CLZ and two-bit lifting with experiments.
2. If it works, a two-bit lifting algorithm for EDCP.

Practical information

Regular meetings will be organized to make progress. If you are interested, send an email to weiqliang.wen@telecom-paris.fr.

References

- [Ajt96] M. Ajtai. Generating hard instances of lattice problems. STOC 1996.
- [BJK+25] S. Bai, H. Jangir, E. Kirshanova, T. Ngo, W. Youmans. A quasi-polynomial time algorithm for the extrapolated dihedral coset problem over power-of-two moduli. CRYPTO 2025.
- [BKSW18] Z. Brakerski, E. Kirshanova, D. Stehlé, W. Wen. Learning with errors and extrapolated dihedral cosets. PKC 2018.
- [CCH+26] L. Chen, Y. Chen, Z. Huang, N. Sun, T. Yang, Y. Zhang. Fiat–Shamir for bounded-depth adversaries. ITC 2026.
- [CH26] A. Chailloux, P. Hermouet. On the quantum equivalence between S[LWE] and ISIS. CRYPTO 2026.
- [CLZ22] Y. Chen, Q. Liu, M. Zhandry. Quantum algorithms for variants of average-case lattice problems via filtering. EUROCRYPT 2022.
- [DGJT26] R. Ding, X. Gong, H. Jiang, L. Tang. Two-bit lifting for ternary SIS: polynomial-time collision attacks on LtHash. IACR ePrint 2026/2083.
- [FIPS203] NIST. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. 2024.
- [FIPS204] NIST. FIPS 204: Module-Lattice-Based Digital Signature Standard. 2024.
- [Kup05] G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM J. Comput. 35(1), 2005.
- [MP13] D. Micciancio, C. Peikert. Hardness of SIS and LWE with small parameters. CRYPTO 2013.
- [Reg04] O. Regev. Quantum computation and lattice problems. SIAM J. Comput. 33(3), 2004.