SpacSec'2026 · International Conference on Cyber Warfare, Security & Space Computing

Analysis of the Application of the Lenstra–Lenstra–Lovász Algorithm in Lattice Cryptosystems

Efficiency of lattice basis reduction and its practical role in modern post-quantum cryptosystems

Korobeynikov A.G.
— SPbF IZMIRAN, St. Petersburg, Russia

LLL BKZ CVP PQC SVP

spacsec.itmo.ru

Agenda

01 **Motivation & Quantum Threat**
Shor’s algorithm and the need for post-quantum cryptography

02 **Lattice Cryptography & NIST PQC**
SVP, CVP and selected standards (ML-KEM, ML-DSA)

03 **LLL Algorithm Fundamentals**
Gram–Schmidt, Lovász condition, polynomial-time reduction

04 **Comparison: LLL · BKZ · Seysen**
Speed vs. quality trade-offs in lattice reduction

05 **Noise Robustness Experiments**
Empirical analysis of Hermite factor and Seysen measure

06 **Conclusions & Recommendations**
Parameter choices and practical security implications

MOTIVATION

The Quantum Threat to Modern Cryptography

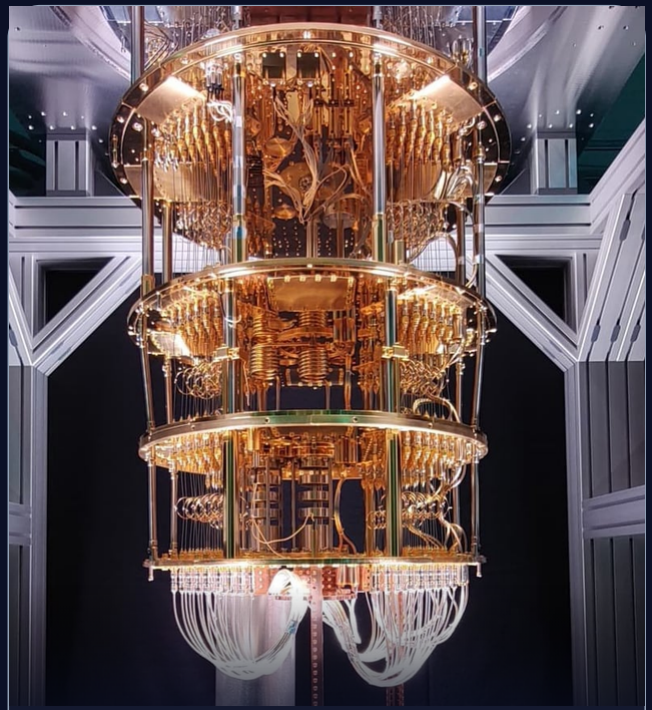
01 Shor's algorithm (1994) factors integer N in polynomial time in $\log N$ and solves the discrete logarithm problem — on a quantum computer

02 Consequently RSA, ElGamal, Diffie–Hellman are guaranteed NOT post-quantum; 2003 — Shor adapted to discrete logs on elliptic curves (ECC affected too)

03 Best classical algorithms (even probabilistic) need only subexponential operations — margin is thin

04 The response: global PQC research and NIST standardization project (2024–2025 completion) driving new standards

⚡ **RSA-2048** → broken in polynomial time by Shor



Quantum computing: from theory to engineering reality

BACKGROUND

Lattice Cryptography and the Dual Role of LLL

Why lattices?

- SVP (Shortest Vector Problem) and CVP (Closest Vector Problem) are NP-hard and believed intractable for quantum computers
- NIST PQC standardization selected three algorithms, all lattice-based: `ML-KEM` (key encapsulation, confidentiality) and `ML-DSA` (digital signatures)

Why now?

PQC shifted LLL from purely academic interest (factoring polynomials, 1982) to a fundamental component determining the security of the digital world

1982 · purely academic ⟶ `security of the digital world`

The dual role of LLL

Cryptanalysis tool

ROLE 01

- `LLL` and `BKZ` are the primary methods cryptanalysts use to attack lattice schemes; attack efficiency depends on basis quality
- Parameters (e.g. 128-bit security) are chosen so LLL/BKZ attacks require prohibitive resources

Design foundation

ROLE 02

New schemes still rely on LLL-type reduction principles:

`lattice attribute-based encryption`

`homomorphic public polynomial encryption`

`anamorphic encryption`

BACKGROUND

LLL Beyond Cryptography

Number Theory

Finding integer relations among real numbers; discovering Ramanujan-type series; enumerating perfect lattices.

Algebra & Polynomials

Factoring polynomials over $\mathbb{Z}$; solving monogeneity problems for number fields.

Signal Processing & ML

Ideas related to lattice reduction appear in dictionary learning and certain linear-system solvers.

Privacy & Homomorphic Encryption

Error management and correctness maintenance in lattice-based FHE schemes.

MATHEMATICAL MODEL

Lattice, Basis and Gram–Schmidt Orthogonalization

01 · LATTICE

$$L = \{ \sum a_i b_i : a_i \in \mathbb{Z} \}$$

Discrete additive group in $\mathbb{R}^n$ generated by linearly independent vectors $b_1, \ldots, b_n$

02 · BASIS MATRIX

$$B = [b_1, \ldots, b_n] \in \mathbb{R}^{n \times n} \text{ (full rank)}$$

03 · GRAM–SCHMIDT

$$b^*_i = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b^*_j$$

$$\mu_{i,j} = \langle b_i, b^*_j \rangle / \|b^*_j\|^2$$

Coefficients $\mu_{i,j}$ and GS lengths $\|b^*_i\|$ are the decision variables inside LLL

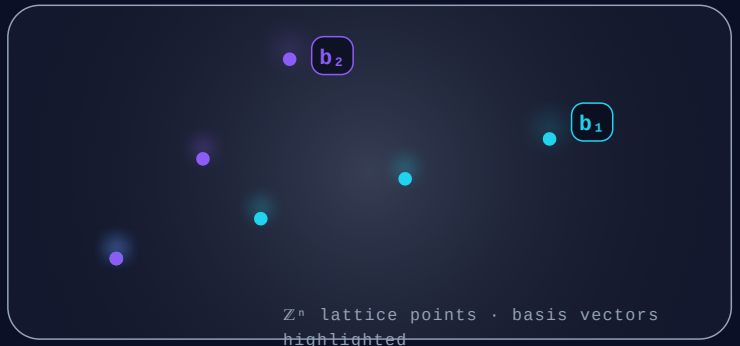
Security foundation

Hardness of SVP / CVP underpins lattice cryptosystems — several underlying problems are NP-hard

Advantages: simple implementation, path to fully homomorphic encryption

Why GS matters

GS is equivalent to QR decomposition $B = QR$; the triangular factor R is directly tied to $\mu_{i,j}$ — this is where perturbation analysis starts



CORE MECHANISM

LLL: Reduction Driven by the Lovász Condition

$$\delta \cdot \|b^*_k\|_2 \leq \|b^*_{k+1}\|_2 + \mu^2_{k+1,k} \cdot \|b^*_k\|_2$$

δ — Lovász coefficient, ¼ < δ < 1

01

Check

At every step **k** the Lovász condition is verified for adjacent basis vectors.

02

Swap

If violated, vectors b_{k-1} and b_k are swapped and the process repeats.

03

Reduce

Once all adjacent pairs satisfy the condition, a size-reduction step minimizes $\mu_{i,j}$.

Polynomial time

Complexity of the reduction

$y = 2^{(n-1)/2}$

Exponential approximation accuracy of the found basis

1982

Lenstra–Lenstra–Lovász, factoring polynomials with rational coefficients — original purpose

✦ Finds ‘short enough’ basis vectors — exactly what lattice security estimates need.

COMPARATIVE ANALYSIS

Reduction Algorithms: LLL vs BKZ vs Seysen

Criterion	LLL	BKZ	Seysen
⚑Main goal	Fast, approximately reduced basis	Better basis via SVP oracle on blocks of k vectors (partial simulation of Kannan's exact algorithm)	Minimize Σ of inverse squared GS-norms — maximize orthogonality of the whole basis
✦Complexity	Polynomial	Exponential in block size k	No exact order; faster than BKZ
⋆Result quality	Limited — approximation factor ~2d	Significantly higher than LLL	Often better than LLL, in less time than BKZ
❄Ecosystem role	Basic fast preprocessing stage	Gold standard for very good bases, but slow	Compromise alternative between speed and quality



No universally best algorithm — the choice follows **problem size, time budget and quality target**. **LLL** preprocessing accelerates **BKZ** convergence, which is exactly how classic sieving attacks start.

EXPERIMENT SETUP

Research Design: Quantifying LLL Robustness to Noise

01

Generate ensembles

Dimensions $n \in \{20, 30, 50\}$; 100 random well-balanced lattices per dimension (orthonormal matrix × diagonal × random unimodular).

02

Inject noise

Normal noise added to every element of basis matrix B; $\sigma \in [10^{-6}, 10^{-2}]$.

03

Run LLL

All parameters fixed, Lovász coefficient $\delta = 0.995$; Python software system.

04

Collect metrics

Quality: Hermite factor η (closer to 1 = better), Seysen measure μ_s (overall orthogonality); performance: time t, iteration count N_{iter}.

05

Statistical analysis

Means and boxplots of η, μ_s, t, N_{iter} as functions of σ; correlation coefficients noise ↔ metric.

Why it matters — in real attacks (e.g. side channels) input data is noisy; the experiments show which noise level still admits a successful LLL attack, and how much error the algorithm itself absorbs.

RESULTS · EXPERIMENT 1

LLL Is Robust to Random Noise

TABLE 2

n = 50 COLUMN

σ	η (n=20)	η (n=30)	η (n=50)
1.0e-06	1.260	1.480	2.143
1.0e-05	1.245	1.513	2.299
1.0e-04	1.248	1.568	2.400
1.0e-03	1.287	1.534	2.444
1.0e-02	1.241	1.544	2.146

Hermite factor η vs noise level σ — averaged over 100 lattices per dimension

Noise barely matters

For all dimensions η and μ_s depend only weakly on σ; the spread of η within one n does not exceed ±0.15.

Dimension dominates

η grows with n: 1.25 (n=20) → 1.53 (n=30) → 2.29 (n=50); μ_s grows even faster: 2.6 → 6.0 → 33.4 — consistent with theory.

Time scales polynomially

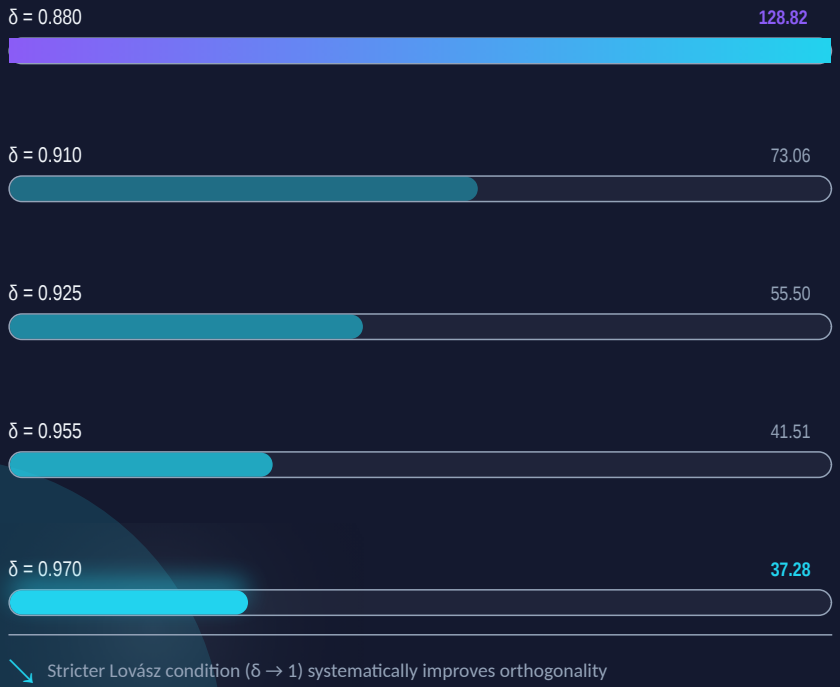
Execution time increases with dimension, empirically confirming polynomial complexity.

RESULTS · EXPERIMENT 2

Tuning the Lovász Coefficient δ

δ ∈ { 0.880 · 0.910 · 0.925 · 0.955 · 0.970 }

Seysen measure μS at n=50 vs δ



↘ Stricter Lovász condition (δ → 1) systematically improves orthogonality

◆ Quality η

for n=20/30 η varies narrowly with no clear monotonic dependence on δ (new random lattice per point); at n=50 the spread widens: η = 2.28–3.08, higher dimensions are more parameter-sensitive

◔ Time t

for n=20/30 virtually independent of δ (3–45 ms); for n=50 range 0.33–0.74 s with no clear trend — initialization overhead dominates

↗ Absolute values grow with n

lattice geometry gets harder

★ Optimal range: δ ∈ [0.92, 0.96]

— minimal μS with acceptable execution time

SPACE COMPUTING

Post-Quantum Security for Space Systems

SpacSec'2026

Satellites operate in bandwidth- and computationally constrained environments — crypto must be light

Lattice schemes `ML-KEM` and `ML-DSA` demonstrate an optimal balance between security and efficiency for exactly such settings (systematic survey, *Acta Astronautica*, 2026)

NIST standardization paid major attention to optimized software and hardware implementations — PQC is an engineering discipline, not only theory (lattice accelerators for the post-quantum era)

Unified PQC architectures combine `Dilithium + Kyber` (both lattice schemes) — understanding and optimizing the underlying LLL-class algorithms becomes even more relevant

Robustness studies matter in orbit: noisy side-channel data in attacks, parameter selection for constrained flight hardware



Constrained orbit: every byte and every FLOP counts

CONCLUSIONS

Conclusions and Recommendations

01 Dimension effect confirmed

Exponential growth of Hermite factor with n: $\eta \approx 1.25$ (n=20), 1.53 (n=30), 2.29 (n=50) — fully consistent with theory

02 Noise resistance

LLL maintains reduction quality up to $\sigma \leq 10^{-2}$ — important for cryptanalytic attacks that rely on noisy data

03 Optimal $\delta \in [0.92, 0.96]$

Minimal Seysen measure μS with acceptable execution time — recommended operating point

04 High dimensions need compensation

For $n \geq 50$ reduction quality degrades significantly; PQC designers must compensate via other security parameters

05 LLL is indispensable

Fast polynomial-time pre-processing and security estimation tool for all lattice-based PQC schemes.

> **Simply running LLL is not enough to assess PQC security** — targeted empirical studies of perturbation robustness, parameter optimization and comprehensive quality assessment, combined with modern tools such as G6K, are required for reliable and reproducible security evaluations of next-generation cryptographic schemes

SpacSec'2026 · ITMO · spacsec.itmo.ru

Thank You for Your Attention

Questions & Discussion Welcome

Korobeynikov A.G.

SPbF IZMIRAN, St. Petersburg, Russia

✉ Korobeynikov_A_G@mail.ru

LLL BKZ CVP PQC SVP

Analysis of the Application of the Lenstra–Lenstra–Lovász Algorithm in Lattice Cryptosystems