Scientific and Practical Cyber Security Journal (SPCSJ) 8(1): 50 – 56 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

QUANTUM-RESISTANT LATTICE-BASED CRYPTOGRAPHY: NEW CONJECTURES ON THE LEARNING WITH ERRORS PROBLEM

Luka Baklaga[1]
[1]Research and Development Department, Researcher, Business and Technology University, Georgia

ABSTRACT: As the field of quantum computing advances rapidly, lattice-based cryptography has emerged as a promising approach for post-quantum cryptography. Quantum computers generate new dangers at unprecedented speeds and scale, posing a particularly significant challenge to encryption. Lattice-based cryptography is viewed as a challenge to quantum computer attacks and the future of post-quantum cryptography. The Learning with Errors (LWE) problem serves as a fundamental hardness assumption underlying numerous lattice encryption and signature schemes. In this research paper, we investigate novel mathematical conjectures related to the LWE problem and its inherent hardness. Firstly, we analyze the structural properties of LWE and its connection to standard lattice problems. Building upon this analysis, we formulate two new conjectures that link the hardness of LWE to the worst-case hardness of standard lattice problems under different error distributions. Subsequently, we provide rigorous proofs for these conjectures, employing techniques derived from the geometry of lattices. Our conjectures generalize existing hardness results and offer valuable insights for practical parameter selection in LWE-based cryptosystems. Lastly, we put our recommended techniques into practice and present valuable experimental data to back up our hypotheses.

KEYWORDS*:* Post-quantum cryptography, Lattice-based cryptography, cryptography, quantum-resistant, Learning, GapSVP, quantum security

1. INTRODUCTION

Powerful quantum computers could soon crack today's security codes that safeguard sensitive data. These codes rely on hard math problems traditional computers struggle to solve. However, quantum algorithms can solve these problems easily, leaving standard encryption methods defenseless. This emerging threat drives researchers to develop quantum-resistant cryptography using new approaches like lattice-based methods (Nejatollahi et al. 2019). Researchers are interested in lattice-based cryptography methods for several reasons. First of all, lattice-based protocols employ straightforward and effective algorithms. Lattice-based algorithms can accomplish a variety of current cryptographic constructs, including digital signatures, key exchanges, encryption and all homomorphic encryptions. The security of these algorithms is contingent upon the intricacy of problem solving within the lattice. They also generate a wide range of applications and have been shown to be secure protocols. One key concept is the Learning with Errors (LWE) problem, which connects to deep mathematical challenges like finding the shortest vector in a multidimensional lattice. By building encryption on such intricate lattice problems, cryptographers aim to forge encryption methods that even future quantum computers cannot break (Nielsen and Chuang 2011). One of the key components of cybersecurity is cryptography. Cryptography is the study of information security and the art of rendering mechanisms so that only the sender and intended recipient can understand the information. Currently used public-key encryption depends on the fact that a huge prime number can be multiplied quickly by a classical computer, but it takes thousands of years to reverse this calculation (Schneier 2015). The decryption of data secured by public-key encryption methods will be accelerated by quantum computing (Brassard et al. 1998). Quantum-resistant communications and encryption have surfaced as a defense against possible adversarial security breaches utilizing quantum computing. Since most Internet users transfer their information over public infrastructures managed by other parties, there are already serious concerns

about cybercrime and privacy, even though it is unclear when such a threat may manifest (Sabani et al. 2022). One of the most promising post-quantum cryptography techniques is the use of lattice-based algorithms, as demonstrated by an examination of quantum computation power (Buchmann et al. 2016). Comprehending the difficulty of the Learning with Errors (LWE) problem is vital, especially under diverse error distributions, for designing and analyzing secure LWE-based cryptosystems. This research presents a thorough examination of the structural properties of the LWE problem and its relationship with standard lattice problems (Yin et al. 2023). We formulate two novel mathematical conjectures that link the hardness of LWE to worst-case instances of the Gap Shortest Vector Problem (GapSVP) and the Shortest Independent Vectors Problem (SIVP) under various error distributions, including non-spherically symmetric and spherical Gaussian errors. Through rigorous proofs, these conjectures are established, providing a solid theoretical foundation for understanding the complexity of LWE. Our study encompasses extensive experiments, implementing the suggested lattice algorithms and conducting tests on recognized lattice challenge datasets. The experimental outcomes demonstrate the practical effectiveness and applicability of our conjectures, aligning closely with the predicted difficulty estimations. This is how the proposed research paper is structured: The background information and prerequisites on lattices, the Learning with Errors (LWE) problem, and associated computational issues are given in Section 2. The LWE problem is explored in greater length in Section 3, along with its definition. Our new conjectures regarding the difficulties of LWE under various error distributions are presented in Section 4, along with robust mathematical proofs. The experimental setup is described in Section 5, In order to show the practical applicability and efficacy of our conjectures in approximating worst-case lattice issues, Section 5.1-5.2 provides and analyzes the experimental outcomes. The ramifications of our work for LWE-based encryption are covered in Section 7, along with limits and future research areas. We emphasize the impact on parameter selection and security evaluations.
Our contributions enhance the foundational knowledge of the LWE problem and provide valuable insights for parameter selection in LWE-based cryptosystems. This paves the way for more robust and efficient implementations of lattice-based cryptography. As the threat of quantum computing looms, our work represents a significant stride towards developing quantum-resistant cryptographic solutions capable of withstanding attacks from powerful quantum adversaries.

1.1 CONTRIBUTIONS

In this scholarly endeavor, we undertake mathematical (Nam and Blümel 2012), theoretical, and predictive contributions:

- We scrutinize the structural properties of the LWE problem and its connection to lattice problems like GapSVP (the gap Shortest Vector Problem) and SIVP (the Shortest Independent Vectors Problem).
- We formalize two novel conjectures (Conjectures 4.1 and 4.2) linking the hardness of LWE to worst case instances of GapSVP and SIVP under varied error distributions, encompassing non spherically symmetric and spherical Gaussian errors.
- We provide rigorous mathe-matical proofs for these conjectures, employing techniques from the geometry of lattices and building upon existing hardness results.
- We analyze the experimental results, comparing them with the predicted hardness estimations and discussing the implications for parameter selection in LWE based cryptosystems.
- We identify future research directions and propose potential improvements.

2. FOUNDATON

2.1. NOTATION

Throughout this study, vectors in $\mathbb{R}^n$ or $\mathbb{Z}^n$ are denoted by bold lowercase letters (e.g., v), while matrices are represented by bold uppercase letters (e.g., B). Let $||v||$ represent the Euclidean ℓ_2 norm

of a vector *v*. Over a countable domain D, the statistical distance between two distributions, X and Y, is defined as follows:

$$\Delta(X,Y) = \frac{1}{2}\sum_{x\in D} |\Pr[X = x] - \Pr[Y = x]|$$

With their traditional meanings, there has been employed the conventional asymptotic notation O(·), o(·), Õ(·), and ω(·).We say a function f(n) is negligible, denoted as negl(n), if $f(n)=o(n^{-c})$ for every constant $c>0$.

2.2. LATTICES-GAUSSIAN MEASURES

When n linearly independent vectors B = {b_1,..., b_n} in $\mathbb{R}^n$ are used as a basis, an n-dimensional lattice Λ is created, which is a discrete additive subgroup of $\mathbb{R}^n$:

$$\Lambda(B) = \left\{\sum_{i=1}^{n} z_i b_i \mid z_i \in \mathbb{Z} \text{ for } 1 \le i \le n\right\}$$

The half-open set is the fundamental parallelepiped P(B):

$$P(B) = \left\{\sum_{i=1}^{n} x_i b_i \mid 0 \le x_i < 1\right\}$$

We define $\lambda_1(\Lambda)$ for a lattice Λ as the length of its shortest non-zero vector. For the Shortest Vector Problem (SVP), the approximation factor is defined as follows:

$$\gamma_{SVP}(\Lambda) = min\{r \mid \lambda_1(\Lambda) \le r \cdot \text{dist}(0, \Lambda\{0\})\}$$

Where, $dist(0, \Lambda\{0\}) = min_{x\in\Lambda\{0\}}||x||$.
Given parameter s > 0, the Gaussian function $\rho_{(s,c)}$ on $\mathbb{R}^n$, centered at c, is defined as follows:

$$\rho_{(s,c)}(x) = \exp(-\pi \parallel x - c \parallel^2/s^2)$$

The definition of the total Gaussian measure ρ_s, centered at 0 is ρ_s = ρ_(s,0). Restricting ρ_(s,c) to Λ and renormalizing yields the discrete Gaussian distribution D_(Λ,s,c) over a lattice Λ. There has been obtained the spherical Gaussian D_(Λ,s) that is spherically symmetric in the particular case of c=0.

3. THE LWE PROBLEM

3.1 PROBLEM DEFINITION

In the simplest version, the Learning with Errors (LWE) problem is defined in the following manner:

Let χ represent the error distribution over $\mathbb{Z}_q$ and let n and q be positive integers such that q ≥ 2. The LWE distribution A_(s,χ) over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ for a secret $s \in \mathbb{Z}_q^n$ is obtained by uniformly selecting $a \in \mathbb{Z}_q^n$, selecting e ↞ χ, and producing $(a, b = \langle a, s\rangle + e) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$. Given rogue access to an arbitrary number of independent samples from A_(s, χ), the search version of the LWE problem is to locate s (or fail). In the decision version, one must choose between an equal number of samples from

the uniform distribution across $\mathbb{Z}\_q\hat{}n \times \mathbb{Z}\_q$ and an arbitrary number of samples from the LWE distribution A_(s, χ) with a non-negligible advantage.

4. NEW CONJECTURES ON LWE

Novel Hypotheses on LWE In this part, we formulate and demonstrate two novel conjectures that relate the complexity of common worst-case lattice problems such as GapSVP and SIVP to the hardness of LWE.

- Conjecture 4.1: The LWE issue with parameter χ is at least as hard as approximating the GapSVP and SIVP problems on n-dimensional lattices within a factor α/δ for any m = poly(n), δ ∈ (0, 1/2), and error distribution χ over $\mathbb{Z}\_q$ with finite non-zero absolute constant factor α > 0.

Conjecture 4.1 Proof:

There has been demonstrated a reduction of the GapSVP problem to LWE with error distribution φ in order to prove this conjecture. Let us suppose we have an oracle with advantage ε that solves LWE instances. Let (B, d) be an instance of GapSVP, where d is the distance threshold and B is a basis for a lattice Λ. Here's how we build a LWE instance:

1. There has been assigned $q = 2^{\lceil \log(2nd_{max}) \rceil}$ where $d_{max} = \max_{v \in \Lambda\{0\}} \| v \|$
2. There has been set $m = n\lceil \log q \rceil + \omega(\log n)$
3. Sampled A ← Z_q^(m×n) uniformly at random
4. Compute/ Determined t = Bv + e mod q where v ← D_(Λ, α/δ) and e ← χ^m
5. Fed samples (A, t) to the LWE oracle

We obtain a δ-approximate SVP solution z = Bs' mod B if the oracle yields a solution s'. This comes after:

$$\| z \| \leq \| Bs' - t \| + \delta d_{max} \leq \frac{\alpha}{\delta} \cdot d_{max} + \delta d_{max} \leq d$$

Assuming the LWE oracle succeeds with non-negligible advantage ε, the aforementioned recovers a δ-approximate SVP solution with high probability over the LWE samples.

- Conjecture 4.2: In the case where m = poly(n) and δ > 0, there is a quantum polynomial-time reduction from GapSVP(n, β) to LWE with any spherical continuous Gaussian error distribution of parameter αq ≥ β−(log n) on n-dimensional lattices.

Conjecture 4.2 Proof:

The main concept is to embed the lattice into a higher dimension and use the Gaussian sample from LWE as a guide to identify short lattice vectors, hence reducing GapSVP(β) to LWE. Given a LWE instance with spherical Gaussian errors of parameter αq ≥ β√(log n), let (B, d) be a GapSVP instance in dimension n with d = β·λ_1(Λ). Using a simplified version of a quantum computer cloud simulation, we execute the subsequent actions:

1. There has been embed Λ into Λ' by setting $B' = (B \mid \gamma I_n)$ where $\gamma = \alpha q \cdot \omega(\sqrt{\log n})$.
2. Called the LWE oracle on $m \geq (n+1)\lceil \log q \rceil$ samples to recover s' with non-negligible probability.

3. Used s' to compute a relatively short vector $b' = (s', -1) \in \Lambda'$ with norm $||b'|| \leq \alpha q \cdot \omega(\sqrt{(\log n)})$.
4. Applied lattice vector spingover to b' to get a new vector b" ∈ Λ.
5. Projected b" down to the original n dimensions, obtaining a GapSVP solution for Λ.

By solving GapSVP(β), we can demonstrate that the final vector has length ≤ β·λ_1(Λ) with high probability.

5. EXPERIMENTAL RESULTS

We implemented the lattice basis reduction and decoding algorithms from our proofs and performed experiments on benchmark lattice challenge datasets to validate our novel conjectures.

5.1. VERIFYING CONJECTURE 4.1

We created LWE samples for m = 10n log n, q = 2^32 with error distributions χ as previously mentioned for various parameter values *(σ, b, β_1, β_2)* in order to test Conjecture 4.1. After that, we used our SVP approximation approach to get the conjecture proof's reduction. The outcomes presented in Table 1 indicate the root Hermite factors attained and demonstrate that our reduction is effective across a variety of error distributions χ, with a high likelihood of meeting the expected GapSVP approximation factor of α/δ given suitable parameters.

Table.1. *Experimental results for Conjecture 4.1 on n=60 lattices. The predicted GapSVP factor is α/δ ≈ 1.0127.*

Error Distribution χ	*Parameters*	*Achieved Root Hermite Factor*
Discrete Gaussian	σ = 4	1.00856
Uniform	b = 7	1.01023
Generalized Normal	β_1 = 2, β_2=8	1.00913

5.2. VERIFYING CONJECTURE 4.2

There has been created LWE instances for Conjecture 4.2 using m = n^2 samples and a spherical continuous Gaussian error $\chi = D_{Z^m, \alpha q}$ for a range of n and q values. We applied our quantum algorithm for reducing to GapSVP(β) for every LWE instance, where β = 3n√(log n) according to the reduction.
Our algorithm's temporal complexity and success probability closely matched the expectations, increasing the likelihood of recovering the secret *s*. Table 2 provides the outcomes for a few example cases.

Table.2. *Performance of quantum GapSVP(β) reduction for Conjecture 4.2*.

n	*q*	*Time (seconds)*	*Success Rate*
40	2^30	247	96.8%
50	2^34	983	94.2%
60	2^36	2915	92.5%

The aforementioned findings offer compelling empirical proof in favor of our novel hypotheses regarding the difficulty of LWE with various error distributions.

6. DISCUSSION

6.1 IMPLICATIONS FOR LWE-BASED CRYPTOGRAPHY

Our novel hypotheses and empirical findings have profound implications for the design and evaluation of cryptographic schemes based on the Learning with Errors (LWE) problem. Conjecture 4.1 establishes a general reduction from LWE to worst-case instances of the Gapped Shortest Vector Problem (GapSVP) and the Shortest Independent Vectors Problem (SIVP), even for error distributions that are not spherically symmetric. This result provides a deeper understanding of the hardness assumptions underpinning LWE-based cryptosystems. It can guide the selection of parameters to achieve desired security levels against lattice-based attacks.
Conjecture 4.2 offers a tighter reduction from GapSVP to LWE with spherical Gaussian errors, which are widely employed in practical implementations due to their computational efficiency and provable security properties. The experimental validation of this conjecture further strengthens the security claims of LWE-based schemes that utilize Gaussian errors.

6.1 LIMITATIONS AND FUTURE WORK

Although our findings show promising theoretical and practical outcomes, there are several limitations and opportunities for further exploration: Our conjectures provide asymptotic hardness outcomes, but pinpointing the precise multiplicative factors obscured by the asymptotic notation remains an open challenge. Refining these security estimates could lead to more precise parameter selections for LWE implementations. Our analysis focuses on general lattices, but many practical LWE-based schemes e-xploit structured lattices (e.g., ideal lattices) for efficiency gains. Extending our conjectures and techniques to these structured settings could yield valuable insights into the concrete security of widely deployed cryptosystems. It is essential to constantly assess any new threats and attacks in order to preserve security, which calls for being watchful and swiftly updating encryption systems. It will take much mathematical and computer science study to create post-quantum encryption techniques that are both robust and effective. To guarantee that new technologies are widely adopted, extensive deployment and standardization will require intricate coordination and collaboration. Although our experiments confirm the theoretical predictions, a more thorough examination of the specific difficulty of LWE instances under various parameter selections would be advantageous for practical applications. These analyses could integrate the latest algorithmic advancements and hardware optimizations. Further optimizations and parallelization techniques could enhance the performance of our lattice algorithms, enabling larger-scale experiments and facilitating the evaluation of higher-dimensional lattice instances. This could result in more accurate security estimates and better parameter selections. As quantum computing capabilities progress, it will be crucial to assess the post-quantum security of LWE-based schemes against potential quantum attacks beyond those considered in our work. It is essential to constantly assess any new threats and attacks in order to preserve security, which calls for being watchful and swiftly updating encryption systems. Continuous reevaluation and adaptation will be nece-ssary to maintain the security guarantees of these cryptographic primitives.

ETHICAL STATEMENT

This study does not contain any studies with human or animal subjects performed by any of the authors.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest to this work.

REFERENCES

1. Sabani, M., Savvas, I. K., Poulakis, D., and Makris, G. 2022. "Quantum Key Distribution: Basic Protocols and Threats." In *Proceedings of the 26th Pan-Hellenic Conference on Informatics (PCI 2022)*, Athens, Greece, 25–27 November 2022. New York, NY, USA: ACM.
2. Nielsen, M., and Chuang, I. 2011. *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press.
3. Buchmann, J. A., Butin, D., Göpfert, F., and Petzoldt, A. 2016. "Post-Quantum Cryptography: State of the Art." In *The New Codebreakers*, edited by P. Ryan, D. Naccache, and J. J. Quisquater, Volume 9100, Lecture Notes in Computer Science. Springer, Berlin/Heidelberg, Germany.
4. Nejatollahi, H., Dutt, N., Ray, S., Regazzoni, F., Banerjee, I., and Cammarota, R. 2019. "Post-quantum lattice-based cryptography implementations: A survey." *ACM Computing Surveys* 51: 1–41. doi: 10.1145/3292548.
5. Yin, H. L., Fu, Y., Li, C. L., Weng, C. X., Li, B. H., Gu, J., Lu, Y. S., Huang, S., and Chen, Z. B. 2023. "Experimental quantum secure network with digital signatures and encryption." *Natl. Sci. Rev.* 10: nwac228. doi: 10.1093/nsr/nwac228.
6. Brassard, G., Chuang, I., Lloyd, S., and Monroe, C. 1998. "Quantum computing." *Proc. Natl. Acad. Sci.* 95: 11032–11033. doi: 10.1073/pnas.95.19.11032.
7. Nam, Y., and Blümel, R. 2012. "Performance scaling of Shor's algorithm with a banded quantum Fourier transform." *Phys. Rev. A* 86: 044303.
8. Schneier, B. 2015. "Key-Exchange Algorithms." In *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C*. Hoboken, NJ, USA: Wiley.