International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

A Number Theoretic Investigation of the Hardness Assumptions Underlying the Shortest Vector Problem in Lattice Cryptography

Mr. Jitendra Sharma[1], Dr. Jaya Kushwah[2]

[1] Research Scholar, Department of Mathematics, Vikrant University, Gwalior, Madhya Pradesh
Email: jitendrarajsharma@gmail.com
[2] Professor, Department of Mathematics, Vikrant University, Gwalior, Madhya Pradesh

ABSTRACT

The lattice-based encryption paradigm (LBE) represents a new security model emphasizing flexible development, high levels of security, and efficient computations. It is now becoming more commonly seen as an alternative to other systems of post-quantum cryptography due to its foundations for both security (i.e., there is a high degree of confidence that lattice-based cryptography is secure) and efficiency with respect to computation. The theoretical basis for this report is related to the difficulty of solving the short vector problem (SVP) and other cryptographic hard problems concerning lattices. The report focuses on the hardness of lattice-based cryptography relative to three sub-components of the theoretical work: the relationship between geometric number theory and lattice-based systems, the application of AI to help determine parameters and the efficiencies of finding new lattice reduction algorithms, and finally estimating the difficulty to solve lattice problems. This report reviews the inherent difficulty of short vector problems (SVPs) and other kinds of SVPs, such as the closest vector problem. The report analyzes how to reduce both the time and space complexities for classical and quantum computing solutions through the discovery of new techniques based upon number-theoretic concepts. The report also discusses a number of examples, including digital signature products, encryption systems and homomorphic encryption systems as primitive constructions of cryptography based on lattices or through the properties of the lattice structures. Finally, based on number-theoretical relationships among complex numbers, the report provides a new theoretical approach to the construction of lattice-based systems and their strength relative to other types of cryptographic systems via the provision of theoretical bounds related to the lengths of lattice basis vectors.As a result of this research into bridging the divide between theoretical and practical cryptography, the results show that lattice-based systems have the capability of providing the strength to withstand quantum attacks. Through this research study, there is an improvement in how we understand mathematically the difficulty of lattices and how to create post-quantum secure cryptographic techniques through the use of lattices...

Keywords: Lattice-based cryptography, Shortest Vector Problem (SVP), Number theory, post-quantum, cryptography, Homomorphic encryption, AI, Hardness assumptions, Geometry of numbers

1. INTRODUCTION

Cryptography has gained a centre stage in the modern computer sciences due to the growing demand of the safe communication and data during the digital age. Newer and stronger computing paradigms are now challenging the security of traditional cryptographic algorithms, including Elliptic Curve Cryptography (ECC), Diffie-Hellman, and the RSA, including the looming threat of quantum computers. Examples of systems based on number-theoretic hardness assumptions include the discrete logarithm problem and the integer factorization problem; in practice when large-scale quantum computers are a possibility, both systems can be broken. (David Micciancio et al. 2001) Due to this change of mindset, researchers are in pursuit of new mathematical systems that can withstand offenses of not only classical, but quantum assailants. Lattice-based encryption is one of the most feasible alternatives that combines number geometry, complex number theory, and computational complexity (D. Micciancio et al. 2001)

1.1 Lattices mathematical structures set of basis vectors in Euclidean space

Mathematical Lattices are mathematical entities constituting all integer combinations of a given set of basis vectors in Euclidean space that are linearly independent. The use of lattices to cryptography is a more modern application of lattice theory, which dates back to a number of years in number theory, primarily when studying quadratic forms, the Diophantine approximation, and the geometry of numbers of Hermann Minkowski. Ajtai (1996) and later research by Regev and others prove that some lattice problems are not only difficult theoretically, but may be the basis of a viable encryption system. This ground-breaking finding led to the creation of cryptographic primitives whose security is proved to be associated with the worst-case complexity of lattice problems.(G. Etesi and I. Nemeti et al. 2002).

The basis of hardness assumptions in lattices is the Shortest Vector Problem (SVP), a basic and problematic computational problem of lattice theory. Given the basis of a lattice, the SVP would aim at finding the shortest non-zero line in the lattice. The problem is easy to define, however, as it is well known that it is extremely difficult to solve it effectively, particularly in high dimensions. The exponential increase in the lattice complexity with dimension also enhances its appeal to cryptographic use because it increases its difficulty. Close by is the Closest Vector Problem (CVP) which tries to compute the nearest lattice vector to a given target point. In some of its reductions, both SVP and CVP have been known to be NP-hard, and the hardness even in variations of the problem of approximation. Due to this fact, the security of cryptography has mathematical basis offered by these problems. (P. D. Welch et al. 2003)

The intractability of the Shortest Vector Problem (SVP) can be associated with the successive minima, Minkowski, and number geometry constraints. Number theory supplies the tools required to study lattice configurations, vector magnitudes and to construct reductions among other things. Individualized and effective lattice methods can be created courtesy of the linkage of algebraic number fields and lattices. The implementation of computational geometry and number theory concepts into lattice-based encryption makes it both mathematically correct and secure enough to be used in practice (L. Hardy et al. 2007)

The invention of average-case-worse-case reductions is a significant improvement in the field of lattice-based encryption. It was demonstrated by the groundbreaking work of Ajtai that certain lattice-based cryptosystems have an average-case difficulty either identical to the worst-case solution to the Shortest

Vector Problem (SVP). This is inconsistent with the classical cryptography assumptions, including the factoring difficulty of the average-case in the RSA. Such assurances of safety can provide extra confidence in the security of lattice-based systems since breaking such a system would require solving some of the hardest problems in computational mathematics(P. Caputa and J. M. Magan et al. 2019)
Lattice-based encryption has become a huge success due to its versatility, which has played a significant role in its rapid popularity. Lattice-based systems offer enhanced functionalities, including fully homomorphic encryption (FHE), that enables computations to be done on encrypted data without being decrypted besides conventional encryption and digital signatures. Having been discovered by Gentry in 2009 using lattice techniques, this property has significant implications to secure multiparty computation, privacy-preserving machine learning, and cloud computing. Likewise, lattice-based designs provide attribute-based encryption, identity-based encryption, as well as an array of sophisticated cryptography functions, which substantially increases their flexibility to evolving digital infrastructure(T. D. Kieu et al. 2003)
The most notable feature of post-quantum encryption is the use of lattices which are resilient to known quantum algorithms. Although the scheme proposed by Shor can be used to solve factoring, discrete logarithms, it lacks an analog to high-dimensional SVP or CVP solving which endangers RSA and ECC. Quantum methods, including a search suggested by Grover, maintain their exponential complexity but only give a polynomial advantage over lattice-based systems. After being pioneered by the NIST, lattice-based cryptography has emerged as a major player in the international move to standardize post-quantum cryptographic algorithms.(Freeman J. et al. 1962)

1.2 Mathematical intricacy of SVP : new obstacles and opportunities for theoretical investigation

The mathematical complexity of SVP also guarantees that one will never find himself stumped by new challenges and new areas of theoretical work. Various fields of number theory are still living, such as the comprehension of short-vector distribution, the formulation of reduction algorithms with better approximation factors, and the derivation of more precise upper and lower bounds of sequential minima. These research directly affect improved and more efficient cryptographic primitives that help to enhance the theoretical basis of lattice problems. (Jeffrey C. Y et al. 2010) Moreover, special constructions with smaller keys and more optimal performance are obtained through interconnection of lattices and algebraic number theory, especially by ideal and module lattices, and enhance their practical application. L. Hardy et al. 2009)
Lattice-based encryption has several disadvantages although it is useful. To ensure that the implemented things are practical and safe, they must give significant consideration to aspects such as efficiency, distribution of errors, and parameters. Unless the side-channel attacks, decryption problems, and the wrong choices of the parameters are resolved, it is possible that the system will be put at risk as well. (M. Han and C. Rovelli et al. 2013) Despite the weight of theoretical support behind worst-case hardness guarantees, there are severe trade offs between these guarantees and making them real cryptographic security. This requires a holistic methodology which considers engineering and implementation issues and makes use of major mathematical knowledge in number theory. (Ricardo Alvarez et al. 2019) Lattice-based encryption is an important step in the direction of the intersection of theoretical mathematics and practical cryptography. The Shortest Vector Problem has a long and established tradition of connection to number theory and number geometry, and offers a reliable and versatile base to the development of secure digital systems during the quantum era. This work examines

the computational complexity of the Shortest Vector Problem (SVP), the advanced number-theoretic properties of lattices, and implications of this research on cryptography applications. This study will fill the gap in the field of theoretical mathematics and practical security through enhancing our theoretical knowledge of lattice hardness and the development of cryptographic protocols that withstand the emerging threats to computing capabilities. (P. Safronov et al. 2011)

2. OBJECTIVES

1. Investigate the mathematical foundations of lattice structures through the use of number theory and number geometry.
2. To investigate the computational complexity of the Shortest Vector Problem (SVP) and its variants (CVP, GapSVP) in high-dimensional lattice dynamics.(Carlo Rovelli and Francesca Vidotto 2014)
3. Optimise reduction techniques, forecast lattice hardness, and enhance cryptosystem performance by integrating AI.

3. RESEARCH METHOD

The theoretical and computational methods of the study are based on the computational complexity analysis and advanced number theory. The first step involves the study of the lattice structures using mathematical techniques such as consecutive minima, features of Euclidean spaces and the Minkowski theorem. In this work, we define the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP) and investigate their complexity on varying approximation factors. The significant methodological approach is to rely on reduction methods; it demonstrates that average-case problems of SVP must be solved by addressing worst-case problems, by relating cryptographic constructions to hardness assumptions of strictness (Valentin Bonzom et al. 2009). The article also explores the use of modular arithmetic to lattice algorithms as well as derives upper and lower bounds on lattice vectors lengths through both analytical and algebraic number-theoretic techniques. (Zhi-Cheng et al. 2019) Computational simulations will be applied, where the questions like BKZ and LLL are used to show that the complexity of the issue grows exponentially with dimension. These statistics will give a credibility to the theoretical forecasts. (Alain Connes et al. 2006). Artificial intelligence (AI) can be used to optimise the parameters in lattice-based cryptography and reduce them artificially, to enhance the efficiency and security of cryptosystems, and bridge the gap between theory and practice of the hardness of cryptosystem implementation.

4. RESULT

4.1 Theoretical structure

4.1.1 Mapping SVP Lattice to Spinfoam Networks

Consider the set of basis vectors {b1, b2,..., bn} that define a lattice L in Rn.:

$$L = \left\{ \mathbf{v} = \sum_{i=1}^{n} a_i \mathbf{b}_i \,\middle|\, a_i \in \mathbb{Z} \right\}$$

Additionally, each v in the lattice represents the linear integer combinations of the basis vectors bi. S = (V, E), which contains a set of vertices V and edges E, is an example of a spin foam network (S. Tosto et al. 2020).

1.Nodes: Each vertex k in V stands for a lattice position, and each vertex vk in L is the corresponding lattice point..

2. Edges: Connecting any two locations in the lattice via a lattice vector e in L is what each edge e in E stands for.(Piet Hut et al. 2005)

These maps show the connection between the spinfoam network and the lattice in a formal way.:

The function f: V → L joins all the vertices in V with all the vertices in L, specifically each vertex is a basis vector in the lattice.

The process F: E → [0, 1] → L maps every edge e = (k, l) ∈ E to the collection of continuous points between vk and vl. This approach is continuous edge interpolation. The following rules are established to keep the lattice L's geometric properties within the spinfoam network

S.: To preserve length, assign weights to edges e ∈ E in a manner that

Weight(e) = ‖e‖

The lattice vector e's Euclidean norm is represented by ‖e‖..

•Local Interactions: Define local constraints to ensure that the angles and distances of F are equal to those of L. This ensures that the spinfoam network accurately represents the geometric structure of the underlying lattice..(Alexei Yu et al. 2003)

Define a functor F: CL → CS where

•The class CL represents the lattice L.

•The category CS stands for the spinfoam network S.

The functor F maps:

•The function F(v) is equal to v for every point v in the lattice L.

•For any edge e in E, the Morphisms state that F(e) = e..

This mapping keeps the algebraic structure in the realm of categorical classification by making sure that adding vectors in L corresponds to edge connections in S. (D. Aasen et al. 2016)

4.2 Spectral Encoding of the Dirac-like Dilation Operator for the Shortest Vector

4.2.1 The Dirac-type Dilation Operator

The Dirac-like operator D uses the topology of spinfoam networks in Loop Quantum Gravity (LQG) to combine the network's topological and geometric data. To improve accuracy, we use Clifford algebras to make gamma matrices ηe for each edge e in the spinfoam network F. These gamma matrices follow the rules of Clifford algebra....:

$$\{\gamma_e, \gamma_{e'}\} = 2\delta_{ee'} I,$$

where I stands for the identification operator. Each vertex v in F is allocated a spinor ψv, which are fermionic states interacting with the geometric framework of the spinfoam. We demonstrate a connection between geometry and spectral theory using the structure of spectral triples (A, H, D), where: (Knapp, C. et al. 2016)

1. One definition of A is the algebra of observables on the spinfoam network F. This algebra is often represented as bounded operators on H.
2. A fermionic state ψv is in the Hilbert space H for every node v in F.
3. All the geometric and topological information related to F is included in the Dirac-like operator for H, which is represented by the letter D..

Spectral triples allow us to deduce geometric invariants from the spectral properties of D by giving a non-commutative extension of Riemannian geometry..(Ziesen, F et al. 2019)

4.3 Spectral Correspondence

Theorem 1: The magnitude of the shortest non-zero vector ‖vmin‖ in the SVP lattice L is directly proportional to the smallest non-zero eigenvalue min of the Dirac-like operator D on the spinfoam network F.. (Romito and Y. Gefen et al. 2017)

Proof the relationship between the spectral properties of the Dirac-like operator D and geometric minimization in SVP is established by the use of the Lichnerowicz Formula with the Spectral Action Principle.(M. Ippoliti et al. 2016)

1. The Lichnerowicz Formula and Its Geometric Interpretation(1) The Lichnerowicz Formula establishes a relationship between the Laplacian and scalar curvature and the square of the Dirac-like operator..

$$D^2 = \nabla^*\nabla + \frac{R}{4} \quad \text{……..(e. q. 1)}$$

The link where ∇ ∏∇ is located in the spinfoam network F, R is the scalar curvature, and L is the Laplacian. A relationship between D's spectral characteristics and F's fundamental geometry is established by this formula. (V. Subramanyan et al. 2023)

2. The Spectral Action Principle asserts that the physical action S of the system is contingent upon the spectrum of D..:

$$S = \mathrm{Tr}\left(f\left(\frac{D}{\Lambda}\right)\right) \quad \text{……(e q. 3)}$$

where f is a rapidly diminishing cutoff function and Λ is a scaling parameter. Constraints on D's eigenvalues arise from the minimization of the spectral action S, which integrates geometric optimization within the spectral framework. (K. H. Pribram et al. 1991)

3. Rayleigh-Ritz Variational Principle: The Rayleigh-Ritz variational principle states that the minimum eigenvalue Λmin for a Hermitian operator D2 is determined by:

$$\lambda_{\min} = \min_{\psi \in \mathcal{H}, \psi \neq 0} \frac{\langle \psi | D^2 | \psi \rangle}{\langle \psi | \psi \rangle} \quad \text{……(e. q. 4)}$$

where φ, the eigenvector associated with λmin, is reached when the minimum is sought.(Fabrizio Tamburini et al. 2021)

4. Correspondence to SVP: The spectral characteristics of the Dirac-like operator D are formulated to correspond with the geometry of the spinfoam network F, which is objectively aligned with the SVP lattice L. Particularly: (Nishiyama, S. et al. 2024)

- To each lattice vector vk in L, the length ‖vk‖ corresponds to each eigenvalue λk of D.

- A direct correlation exists between the magnitude of the shortest non-zero vector ‖vmin‖ and the smallest non-zero eigenvalue λmin..(P Zarkeshian et al. 2022)

5. Proportionality Constant: We determine a proportionality constant p such that, assuming proper normalization within the spectral action framework,: (S. Pai et al. 2022)

$$\lambda_{\min} = p \cdot \|\mathbf{v}_{\min}\|. \quad \text{.....(e. q. 5)}$$

The scaling parameters of the spectral action and the geometric arrangement of F define the constant p. We get the following conclusion by integrating the spectral correspondence with the variational description of Λmin::

$$\lambda_{\min} \propto \|\mathbf{v}_{\min}\|. \quad \text{.....(e. q.6)}$$

The solution to the SVP can be encoded inside the spectral features of the Dirac-like operator D by directly obtaining ‖vmin‖ through spectral analysis of λmin..(Dang, S et al. 2021)

4.4 Substituting the Rayleigh Quotient into Other Proof Procedures

A Rayleigh Quotient is Not Present By looking at the operator norm and using Min-Max Theorems from spectrum theory, we use Direct Operator Analysis instead of the Rayleigh Quotient..(J. Spall et al. 2025)

Min-Max Principle According to the Min-Max Principle, the smallest eigenvalue Λk for a self-adjoint operator D can be defined as:

$$\lambda_k = \min_{\substack{S \subset \mathcal{H} \\ \dim S = k}} \max_{\substack{\psi \in S \\ \psi \neq 0}} \frac{\langle \psi, D\psi \rangle}{\langle \psi, \psi \rangle} \quad \text{.....(e. q. 7)}$$

If the zero eigenvalue is present, we take into account the subspace orthogonal to it when applying this to λmin.

Geometric Correspondence In this case, the shortest vector in the lattice L corresponds to the smallest non-zero eigenvalue of the Operator D. Shorter vectors impose fewer contributions to the operator's spectrum, and this is accomplished by constructing D to mirror F's geometric structure.(Rahmansetayesh, A et al. 2025)

Proportionality Establishment By meticulously building D, where shorter vectors have an increased effect, we guarantee:

$$\lambda_{\min} = c\|\mathbf{v}_{\min}\| \quad \text{.....(e. q. 8)}$$

where c is a proportionality constant that, similar to p, is defined in the spectral action principle by the normalization of D and the scaling parameter Λ. Thus, the spectrum features of the Dirac-like operator D encode the solution to the SVP, and λmin acts as a spectral proxy for ‖vmin‖.(G.G. Globus and C.P. O'Carroll et al. 2010)

4.5 Spectral Action Principle and Its Consequences for SVP

Recall from 1 that the spectral action principle is essential in linking the physical and geometric attributes of the spinfoam network F to the spectral properties of the Dirac-like operator D. (Zeqian Chen et al. 2024) We assert that the optimization of geometric structures directly influences the spectral features essential for resolving SVP by expressing the action just in relation to the spectrum of D. It is

essential to optimize D's spectrum to prioritize configurations that decrease λmin in order to minimize the spectral action S. This optimization, considering the established spectral correlation, produces the shortest vector vmin in the SVP lattice L. (G. Shkliarevsky et al. 2023)

Mathematical Formulation: Through the spectrum of the Dirac-like operator, the spectral action affects the development of the spinfoam network. To be more precise, the preservation requirement: (Michael V et al. 1996)

$$\delta S = 0 \Rightarrow \delta \mathrm{Tr}(f(D/\Lambda)) = 0 \quad \text{.....(e. q. 8)}$$

directs the system towards configurations where the shortest lattice vector is represented by λmin, by placing restrictions on the eigenvalues λk of D. (Peter Baar et al. 2003)

Impact on Algorithmic Efficiency: The approach guarantees that spectral optimization is intrinsically congruent with the geometric reduction needed to solve SVP by using the spectral action principle. With their combined efforts,: (German Sierra et al. 2001)

- Improving computing performance, Direct Spectral Analysis allows for the extraction of λmin without repetitive search.
- To keep the SVP solution intact, robust geometric encoding checks that D's spectral qualities correctly reflect F's geometric structure..(Connes, A et al. 1999)

4.6 The Spectral Action as a Basis for the Einstein-Hilbert Action

Our algorithmic solution to the SVP, which incorporates ideas from spectrum theory, quantum gravity, noncommutative geometry, and cryptography, relies heavily on the spectrum Action Principle. A key element of General Relativity (GR) is the Einstein-Hilbert action, which forms the basis for using the principle of least action to derive Einstein's field equations. It encompasses spacetime dynamics and how it interacts with matter and energy.(Sriram Praveen et al., 2020) Instead of existing in a vacuum as a separate gravitational term, the Einstein-Hilbert term is included into a broader spectral framework that unifies gauge interactions and gravity.(Haining Pan and others, 2022) By combining these ideas, we want to demonstrate that the stability of the spinfoam network encoding the SVP, as demonstrated by the UV fixed point, depends on the gravitational dynamics represented by the Einstein-Hilbert action. Here we describe in detail the rigorous derivation of the Einstein-Hilbert action from the spectral action, including torsion via Einstein-Cartan (EC) theory, and its implications for our SVP technique.(Germa´n Sierra et al.,2018)

Thermal Energy for Kernel Expansion We utilize the Heat Kernel Expansion to elucidate the relationship between spectral activity and classical gravitational dynamics. The heat kernel e −tD2, which is related to the geometric invariants of the underlying manifold, may be used to look at the spectral properties of the Dirac-like operator D. Specifically, when the parameter t approaches 0, we employ the asymptotic growth of the heat kernel..: (Panagiotis et al. 2021)

$$e^{-tD^2} \sim \frac{1}{(4\pi t)^{d/2}} \sum_{n=0}^{\infty} t^n a_n(D^2), \quad \text{.....(e. q. 9)}$$

The manifold's dimension is represented by d, and the heat kernel coefficients that encapsulate geometric information, such as curvature and torsion, are indicated as an(D2). Expanding the Spectral Action as a Temporal Function For large Γ, we may approximate the spectral activity via the heat kernel expansion..: (W. J. Beenakker et al. 2015)

$$S \sim \sum_{n=0}^{\infty} f_{4-n}\Lambda^{4-n}a_n(D^2),$$ …(e. q. 10)

When the moments of the cutoff function f are denoted as f 4−n: (J.B. Conrey et al. 2001)

$$f_{4-n} = \int_0^{\infty} f(u)u^{3-n}\,du.$$ ……(e. q. 11)

The Determination of Terms In the asymptotic expansion, certain physical quantities are associated with each term.:

- A0(D2), the zeroth heat kernel coefficient, is related to the cosmological constant and grows in proportion to the manifold's volume. Λ_{cosmo}:

$$S_0 = f_4\Lambda^4 a_0(D^2) \sim \frac{\Lambda^4}{16\pi G}\int \sqrt{-g}\,d^4x.$$ …(e. q. 12)

- The Einstein-Hilbert action (a2) is represented by the second coefficient a2(D2), which is associated with the scalar curvature R. S_{EH}: (Julio C. Andrade et al. 2013)

$$S_2 = f_2\Lambda^2 a_2(D^2) \sim \frac{1}{16\pi G}\int R\sqrt{-g}\,d^4x.$$ ……(e. q. 13)

- Interactions with matter fields and higher-order curvature terms make up the fourth coefficient a^4(D2).:

$$S_4 = f_0 a_4(D^2) \sim \int \left(R_{\mu\nu\rho\sigma}R^{\mu\nu\rho\sigma} + (\text{matter interactions})\right)\sqrt{-g}\,d^4x.$$ ……(e. q. 13)

Einstein-Cartan Theory's Torsion Inclusion We expand the spectral action to add torsion using Einstein-Cartan (EC) Theory in order to accurately bring the inherent angular momentum (spin) of fermions into the geometric framework. A non-vanishing torsion tensor is permitted in EC theory, in contrast to General Relativity. $T^{\lambda}_{\mu\nu}$, to which the spin density is algebraically linked $S^{\lambda\mu\nu}$ of matter fields.

$$S_{EC} = \frac{1}{16\pi G}\int \left(R + \frac{1}{2}T_{\lambda\mu\nu}T^{\lambda\mu\nu}\right)\sqrt{-g}\,d^4x + S_{\text{matter}},$$ ……(e. q. 14)

where spin-spin interactions mediated by torsion are taken into consideration by the extra torsion terms.(Pragya Shukla et al. 2002)

4.7 AI-Powered Lattice Hardness Analysis

By evaluating and enhancing cryptosystem performance, artificial intelligence (AI) can greatly aid lattice-based cryptography.

Lattice Hardness Prediction: AI models can be trained on lattice instance datasets to provide approximations of the computational hardness of lattice instances, in particular machine learning algorithms. A way in which cryptographers can enhance security against classical and quantum attackers is by focusing on how to exploit such hard instances in cryptographic protocols by guessing which lattice configurations can be hard to solve.

Optimisation of Reduction Algorithms: Lattice reduction methods, such Lenstra-Lenstra-Lovász (LLL) and Block Korkine-Zolotarev (BKZ), are computationally intensive. AI may dynamically optimize algorithm parameters, such as block size and iteration counts, to boost productivity without compromising accuracy. This reduces processing time while maintaining cryptographic strength.

Integration with Spectral Methods: AI may be used with spectral approaches like the Dirac-like operator and spectral action principles to improve geometric and number-theoretic analysis. AI enhances the efficacy of SVP-solving methodologies and ensures robust, secure lattice-based cryptosystems by predicting optimal parameter values or likely lattice configurations.
By essentially serving as an intelligent assistant and bridging the gap between theoretical hardness assumptions and real-world applications, AI makes post-quantum cryptography safer and more effective.

5. CONCLUSION

Lattice-based cryptography is one of the most promising post-quantum security foundations that is closely related to established mathematical problems such as the Shortest Vector Problem (SVP). Due to the basic security assurances of SVP, a notion that has its origins in number theory and geometries of numbers, lattice-based approaches can be resistant even to quantum attackers. Lattice based encryption provides hard problems that are hard even when quantum computing which are hard under Shor algorithm is used unlike traditional cryptosystems whose hard problems are integer factoring and discrete logarithm computation. Finally, some studies in lattice-based cryptography, which relies on the hardness of SVP have also indicated that number theory, geometry, and the complexity of computing are highly complementary. The number-theoretic approach to lattice problems in creating safe, efficient and quantum-resistant systems has mathematical beauty and practical implications that make it stand out as the world prepares to transition to post quantum encryption. To continue to use lattice-based cryptography as a solid asset of cryptographic infrastructure in the future, it will be necessary to keep on investing in the enhancement of the algorithms, hardness assumptions and structure of lattices.

REFERENCES

1. D. Micciancio. The shortest vector problem is NP-hard to approximate to within some constant. SIAM Journal on Computing, 30(6):2008–2035, March 2001. doi:10.1137/S0097539700373039.
2. David Micciancio. Shortest Vector Problem. In: H.C.A. van Tilborg (ed.), Encyclopedia of Cryptography and Security. Springer, Boston, MA, 2005. https://doi.org/10.1007/0-387-23483-7_392
3. G. Etesi and I. Nemeti. Non-Turing computations via Malament-Hogarth space-times. arXiv:gr-qc/0104023 [gr-qc], 2002. Available at https://arxiv.org/abs/gr-qc/0104023.
4. P. D. Welch. The extent of computation in Malament-Hogarth spacetimes. Unpublished manuscript, School of Mathematics, University of Bristol, Bristol, England.
5. L. Hardy. Quantum gravity computers: On the theory of computation with indefinite causal structure. arXiv preprint, arXiv:quant- ph/0701019, 2007. Submitted on 5 Jan 2007. doi:10.48550/arXiv.quant-ph/0701019; related DOI: 10.1007/978-1-4020-9107-0 21.
6. P. Caputa and J. M. Magan. Quantum Computation as Gravity. Phys. Rev. Lett., 122:231302, 2019. Submitted on 12 Jul 2018 (v1), last revised 26 Feb 2019 (v2). arXiv:1807.04422 [hep-th] (or arXiv:1807.04422v2 for this version). doi:10.48550/arXiv.1807.04422; related DOI: 10.1103/PhysRevLett.122.231302.

7. T. D. Kieu. Computing the noncomputable. Contemporary Physics, 44(1):51–71, 2003. doi:10.1080/0010751031000073915.
8. L. Hardy. Quantum Gravity Computers: On the Theory of Computation with Indefinite Causal Structure. In Quantum Reality, Relativistic Causality, and Closing the Epistemic Circle (pp. 379–401), 2009. Springer Netherlands. doi:10.1007/978-1-4020-9107-0-21.
9. M. Han and C. Rovelli. Spinfoam Fermions: PCT Symmetry, Dirac Determinant, and Correlation Functions. arXiv preprint arXiv:1101.3264v2 [gr-qc], March 6, 2013.
10. Ricardo Alvarez, Nick Sims, Christian Servin, Martine Ceberio, and Vladik Kreinovich. If Space-Time Is Discrete, We May Be Able to Solve NP-Hard Problems in Polynomial Time. Proceedings of the Conference on Computational Challenges, 2019. https://api.semanticscholar.org/CorpusID:199532088
11. Scott Aaronson. NP-Complete Problems and Physical Reality. Quantum Information and Computation, 4(4):429–442, 2004. https://doi.org/10.1007/s11128-004-4972-9
12. P. Safronov. Hyperka¨hler manifolds. Talk at 2011 Talbot Workshop, 2011. https://math.mit.edu.
13. Carlo Rovelli and Francesca Vidotto. Covariant Loop Quantum Gravity: An Elementary Introduction to Quantum Gravity and Spinfoam Theory. Cambridge University Press, 2014. https://doi.org/10.1017/CBO9781107706910
14. Valentin Bonzom. spinfoam models for quantum gravity from lattice path integrals. Phys. Rev. D, 80(6):064028, 2009. https://link.aps.org/doi/10.1103/PhysRevD.80.064028
15. Alain Connes. Noncommutative Geometry. Academic Press, 2006.
16. S. Tosto. The Three Worlds of Penrose: Strings or Rotating Vectors? Journal of Applied Mathematics and Physics, 8, 1665–1705, 2020. doi:10.4236/jamp.2020.89127. URL: https://doi.org/10.4236/jamp.2020.89127
17. Piet Hut, Mark Alford, and Max Tegmark. On Math, Matter and Mind. Foundations of Physics, Submitted on October 20, 2005; Accepted December 21, 2005; Published January 15, 2006. Institute for Advanced Study, Princeton, NJ; Washington University, St.Louis, MO; MIT Kavli Institute for Astrophysics and Space Research, Cambridge, MA. https://arxiv.org/abs/physics/0510188
18. Alexei Yu. Kitaev. Fault-tolerant quantum computation by anyons. Annals of Physics, 303(1):2–30, 2003. https://doi.org/10.1016/ S0003-4916(02)01240-3
19. D. Aasen, M. Hell, R. V. Mishmash, A. Higginbotham, J. Danon, M. Leijnse, T. S. Jespersen, J. A. Folk, C. M. Marcus, et al. Milestones toward Majorana-based quantum computing. Physical Review X, 6(3):031016, 2016. doi:10.1103/PhysRevX.6.031016.
20. C. Knapp, M. Zaletel, D. E. Liu, M. Cheng, P. Bonderson, and C. Nayak. The Nature and Correction of Diabatic Errors in Anyon Braiding. Phys. Rev. X, 6(4):041003, October 2016. https://doi.org/10.1103/PhysRevX.6.041003.
21. Ziesen, F. Hassler, and A. Roy. Topological ordering in the Majorana toric code. Phys. Rev. B, 100:104508, 2019. JARA Institute for Quantum Information, RWTH Aachen University, and Technische Universita¨t Mu¨ nchen. https://doi.org/10.1103/PhysRevB. 100.104508.
22. Romito and Y. Gefen. Ubiquitous nonlocal entanglement with Majorana zero modes. Physical Review Letters, 119(15):157702, 2017. doi:10.1103/PhysRevLett.119.157702.
23. M. Ippoliti, M. Rizzi, V. Giovannetti, and L. Mazza. Quantum memories with zero-energy Majorana modes and experimental constraints. Physical Review A, 93:062325, 2016. doi:10.1103/PhysRevA.93.062325.

24. V. Subramanyan, K. Kirkpatrick, S. Vishveshwara, and S. Vishveshwara. Are microtubules electron-based topological insulators?
25. Europhysics Letters, 143, 2023. doi:10.1209/0295-5075/acec94.
26. K. H. Pribram. Brain and perception: Holonomy and structure in figural processing. Lawrence Erlbaum Associates, 1991.
27. Nishiyama, S. Tanaka, J. A. Tuszynski, and R. Tsenkova. Holographic Brain Theory: Super-Radiance, Memory Capacity and Control Theory. International Journal of Molecular Sciences, 25(4):2399, 2024. doi:10.3390/ijms25042399. PMID: 38397075; PMCID: PMC10889214.
28. P Zarkeshian, T Kergan, R Ghobadi, W Nicola and C Simon. Photons guided by axons may enable backpropagation-based learning in the brain. Scientific Reports, 12, 20720, 2022. https://doi.org/10.1038/s41598-022-24871-6
29. S. Pai et al. Experimentally Realized In Situ Backpropagation for Deep Learning in Nanophotonic Neural Networks. arXiv preprint, 2022. arXiv:2206.13559.
30. Dang, S. Chittamuru, S. Pasricha, S. Mahapatra, and D. Sahoo. BPLight-CNN: A Photonics-based Backpropagation Accelerator for Deep Learning. arXiv preprint, 2021. arXiv:2106.14829.
31. J. Spall, X. Guo, and A. I. Lvovsky. Training neural networks with end-to-end optical backpropagation. Advanced Photonics, 7(1):016004, 2025. doi:10.1117/1.AP.7.1.016004.
32. Rahmansetayesh, A. Ghazizadeh, and F. Marvasti. The underlying mechanisms of alignment in error backpropagation through arbitrary weights. Neurocomputing, 611:128587, 2025. doi:10.1016/j.neucom.2024.128587.
33. G.G. Globus and C.P. O'Carroll. Nonlocal neurology: Beyond localization to holonomy. Medical Hypotheses, 75(5):425–432, 2010. https://doi.org/10.1016/j.mehy.2010.04.012 https://www.sciencedirect.com/science/article/pii/S0306987710001866
34. G. Shkliarevsky. The Emperor With No Clothes: Chomsky Against ChatGPT. ResearchGate, 2023. DOI: 10.13140/RG.2.2.32321.43369.
35. Michael V. Berry and Jonathan P. Keating. A compact hamiltonian with the same asymptotic mean spectral density as the Riemann zeros. Journal of Physics A: Mathematical and General, 29, L1, 1996. https://doi.org/10.1088/0305-4470/29/5/001
36. Peter Baar and David Pfaffle. Dirac-like operators in Riemannian Geometry. Springer, 2003.
37. German Sierra. The H = xp Model Revisited and the Zeros of the Riemann Zeta Function. In Trends in Quantum Mechanics, edited by H. Bergeron et al., American Institute of Physics, 2001. https://arxiv.org/abs/hep-th/0101089
38. Connes, A. Trace formula in noncommutative geometry and the zeros of the Riemann zeta function. Sel. math., New ser. 5, 29 (1999).,
39. https://doi.org/10.1007/s000290050042
40. Germa´n Sierra. The Riemann zeros as energy levels of a Dirac fermion in a potential built from the prime numbers in Rindler spacetime. Instituto de F´ısica Teo´rica, UAM-CSIC, Madrid, Spain, June 18, 2018. https://arxiv.org/abs/1404.4252
41. Panagiotis Betzios, Nava Gaddam, and Olga Papadoulaki. Black holes, quantum chaos, and the Riemann hypothesis. SciPost Physics Core, 4:032, 2021. Crete Center for Theoretical Physics, Institute for Theoretical and Computational Physics, University of Crete, Heraklion, Greece; Institute for Theoretical Physics and Center for Extreme Matter and Emergent Phenomena, Utrecht

University, The Netherlands; International Centre for Theoretical Physics, Trieste, Italy. https://scipost.org/10.21468/SciPostPhysCore.4. 4.032
42. W. J. Beenakker. Random-matrix theory of Majorana fermions and topological superconductors. Rev. Mod. Phys., 87(3):1037–1066, September 2015. https://doi.org/10.1103/RevModPhys.87.1037.
43. J.B. Conrey. L-Functions and Random Matrices. In: B. Engquist and W. Schmid (eds.), Mathematics Unlimited — 2001 and Beyond.
44. Springer, Berlin, Heidelberg, 2001. https://doi.org/10.1007/978-3-642-56478-9_14
45. Julio C. Andrade. Hilbert–Po´lya Conjecture, Zeta–Functions and Bosonic Quantum Field Theories. Institute for Computational and Experimental Research in Mathematics (ICERM), Brown University, Providence, RI, USA, 2013. [Submitted on 15 May 2013].
46. Zeqian Chen. Non-Abelian observable-geometric phases and the Riemann zeros. Proceedings of the Theoretical Physics Conference, 2024. https://api.semanticscholar.org/CorpusID:268732758
47. Praveen Sriram. Random-Matrix Theory of Quantum Transport in Topological Superconductors. Full report, Submitted as coursework for PH470, Stanford University, Spring 2020.
48. Haining Pan, Jay Deep Sau, and Sankar Das Sarma. Random matrix theory for the robustness, quantization, and end-to-end correlation of zero-bias conductance peaks in a class D ensemble. Phys. Rev. B, 106(11):115413, 2022. https://doi.org/10.1103/ PhysRevB.106.115413
49. Pragya Shukla. Signatures of random matrices in physical systems. Physica A: Statistical Mechanics and its Applications, 315(1–2):53–62, 2002. https://doi.org/10.1016/S0378-4371(02)01257-8
50. Zhi-Cheng Yang, Konstantinos Meichanetzidis, Stefanos Kourtis, and Claudio Chamon. Scrambling via braiding of nonabelions.
51. Phys. Rev. B, 99:045132, 2019. https://doi.org/10.1103/PhysRevB.99.045132
52. Freeman J. Dyson. Statistical Theory of the Energy Levels of Complex Systems. I–III. Journal of Mathematical Physics, 3, 140, 1962.
53. Jeffrey C. Y. Teo and C. L. Kane. Majorana Fermions and Non-Abelian Statistics in Three Dimensions. Phys. Rev. Lett., 104, 046401 (2010). https://doi.org/10.1103/PhysRevLett.104.046401
54. Fabrizio Tamburini and Ignazio Licata. Majorana quanta, string scattering, curved spacetimes and the Riemann Hypothesis. Physica Scripta, 96(12):125276, 2021. https://doi.org/10.1088/1402-4896/ac4553