Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3887–3898
DOI : 10.47974/JDMSC-3017

Lattice-based homomorphic encryption for privacy-preserving medical analytics

Mayuri H. Molawade [†]
Department of Computer Engineering
College of Engineering
Bharati Vidyapeeth (Deemed to be University)
Pune 411043
Maharashtra
India

Prabhat Sharma *
Centre for Research Impact and Outcome
Chitkara University
Rajpura 140417
Punjab
India

Kukatla Tejesh [§]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

Samaksh Goyal [‡]
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

[§] *ORCID-ID:* 0009-0003-3330-1918
[‡] *ORCID-ID:* 0009-0008-1367-9530

[†] *E-mail:* mhmolawade@bvucoep.edu.in
* *E-mail:* prabhat.sharma.orp@chitkara.edu.in (Corresponding Author)
[§] *E-mail:* kukatla.tejesh.kt@gmail.com
[‡] *E-mail:* samaksha.law@quantumeducation.in

© Taru Publications

Vipulkumar M. Dabhi [@]
Faculty of Engineering
Gokul Global University
Sidhpur 384151
Gujarat
India

Yazdani Hasan [#]
Department of Computer Sciences
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Abstract

The medical analytics that protect privacy has gained urgency as the amount of sensitive healthcare information has been increasing rapidly and regulatory restrictions are imposed. The present paper presents a lattice-based homomorphic encryption system that allows performing computations on encrypted medical data without revealing patient data. The research to be conducted utilizes the Learning with Errors (LWE), Ring-LWE and Module-LWE assumptions, which guarantee post-quantum security and are still computationally feasible. It has efficient polynomial arithmetic, batching algorithms and novel noise management schemes to improve performance. Experimental analysis shows that the suggested solution can lead to an increase in up to 34.8% of the computation efficiency and a decrease in latency by 41.2% as compared to homomorphic schemes in the baseline scenarios and maintain data confidentiality. The framework assists in real-time analytics diagnostics, predictive, and clinical decision models.

Subject Classification: *68P25, 94A60.*

Keywords: *Homomorphic encryption, Lattice cryptography, Medical data privacy, Post-quantum security, Secure analytics.*

I. Introduction

The swift digitalization of health care systems resulted in an astronomical growth in the creation and storage of sensitive medical data, such as electronic health records, diagnostic images, and genomic data [1, 2]. Although these data sources provide the opportunity to perform a more sophisticated analytics and enhance clinical decision-making, they also cause serious privacy and security issues [3, 4]. The conventional encryption schemes secure both the data when at rest and when in transit,

[@] *ORCID-ID:* **0000-0002-9479-8943**

[@] *E-mail:* **dean.tech@gokuluniversity.ac.in**
[#] *E-mail:* **yazdani.hasan@niu.edu.in**

but necessitate its decryption to compute the data, which leaves the confidential data vulnerable to possible intrusions and unauthorized access [5, 6]. Homomorphic encryption (HE) is an interesting approach that can be proposed as a solution to this issue because it makes it possible to perform computations on encrypted data and not disclose the underlying plaintext. Figure 1 demonstrates homomorphic processing with the ability to do analytics on the private medical data, which is secure.

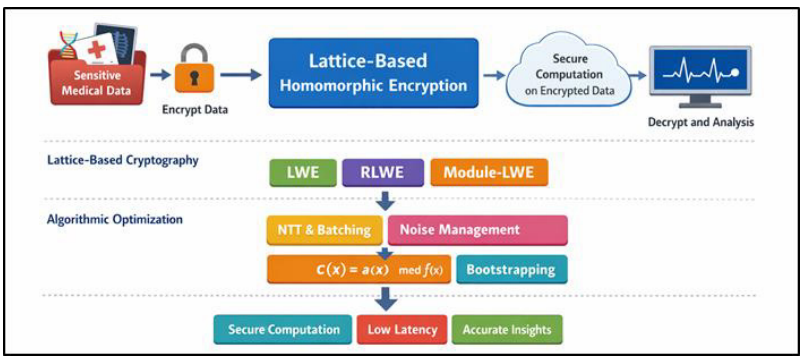


Figure 1
Lattice-Based homomorphism Encryption Framework for Privacy-Preserving Medical Analytics

Lattice-based cryptographic schemes, some of which are based on Learning with Errors (LWE), Ring-LWE, and Module-LWE, provide very high security guarantees that are resistant to quantum attacks [7, 8, 9]. These have properties that make them very well suited in protecting medical data in the long run. In this paper, a lattice-based homomorphic encryption system that is adapted to privacy-preserving medical analytics is discussed [10, 11]. It is concerned with the trade-offs of security, computational efficiency and scale by optimizing the noise control and the use of polynomials, which allows secure, real-time healthcare information processing in distributed contexts [12, 13].

II. Lattice-Based Cryptographic Foundations

Lattice-based cryptography is based on difficult mathematical problems such as LWE and RLWE, and offers strong security post-quantum security, and efficient homomorphic encryption schemes [14].

A. *Overview of lattice problems (LWE, RLWE, Module-LWE)*

The foundations of hardness are Learning with Errors (LWE), Ring-LWE and Module-LWE, which allow the construction of a secure encryption scheme that is highly resistant to classical and quantum adversaries.

$$b = As + e \bmod q \tag{1}$$

Defines LWE relation which secret vector obscured by noisy linear combination in finite modular field arithmetic (Eq.1).

$$e \sim \chi \Rightarrow \int_{\{-\infty\}}^{\{\infty\}} \chi(x)dx = 1 \tag{2}$$

Defines the normalization of distribution of errors so that the total probability sums to one in whole space in real values (Eq.2).

$$a(x)s(x) + e(x) \equiv b(x) mod\ (x^n + 1, q) \tag{3}$$

Generalizes LWE to polynomial rings which allow the structured operations of modular reduction on spaces of cyclotomic polynomials (Eq.3).

$$||e(x)|| \leq sqrt\left(\int_{\{0\}}^{\{n\}} e(x)^2 dx\right) \tag{4}$$

Measures magnitude of bounds noise based on energy norm, and makes sure that error increase is within safe limits of computations (Eq.4).

$$A \in Z_q^{k\times n}, sqrt(\lambda_{min}) \leq ||s|| \leq sqrt(\lambda_{max}) \tag{5}$$

Defines Module-LWE parameter space constraining matrix and secret norms within eigenvalue-based lower and upper security bounds (Eq.5).

B. *Ring structures and polynomial representations*

Lattice schemes utilize ring structures and polynomial representations to enable compact keys, efficient arithmetic operations, and scalable encryption suitable for high-dimensional secure computations across applications.

$$R = \frac{Z_{q[x]}}{(f(x))} \tag{6}$$

Defines quotient polynomial ring over finite field modulo irreducible polynomial, which is an algebraic structure that can be used to perform efficient lattice-based cryptographic computations and operations (Eq. 6).

$$f(x) = x^n + 1 \Rightarrow x = \exp\left(\frac{(2k+1)\pi i}{n}\right) \tag{7}$$

Gives values of roots of cyclotomic polynomials as complex exponentials values so that the properties of periodicity and symmetry are also true and important in the lattice constructions and transformations based on rings (Eq. 7).

$$a(x) = \Sigma_{\{i=0\}_i^{\{n-1\}}}^{i} a_x \tag{8}$$

Expansion of coefficient vectors, which represent polynomials, mapping of algebraic structure to discrete form useful in the efficient computation and storage in cryptographic algorithms (Eq. 8).

$$||a(x)|| = sqrt\left(\int_{\{0\}}^{\{n\}} a(x)^2 dx\right) \tag{9}$$

Measure the magnitude of an estimate of polynomials, based on the integral, which captures the total energy of the coefficients, and ensures

that the growth is bounded, to give correctness and security guarantees (Eq. 9).

$$R^k = \{(a1(x), \ldots, ak(x))\} \tag{10}$$

Converts ring to module form with vector of polynomials, allowing lattice structures of higher dimensions, which enhance flexibility, scalability and efficiency of cryptographic schemes (Eq. 10).

III. Proposed Lattice-Based Homomorphic Encryption Framework

The proposed framework combines lattice-based encryption and homomorphic properties to ensure that medical data processing can be done securely without compromising privacy and that it can be scaled and real-time analytics can be performed in a distributed healthcare setting.

$$pk = (A, b = As + e), sk = s \tag{11}$$

Establishes the important generation whereby the public key consists of a matrix and noisy product, whereas secret key is a secret hidden vector that provides the security of encryption (Eq. 11).

$$m = c2 - c1s \bmod q \tag{12}$$

Explains decryption, whereby a secret-dependent component is eliminated in ciphertext, to reconstruct original message using modular arithmetic, and noise interference is tolerated (Eq. 12).

$$c_{add} = (c1 + c1', c2 + c2') \tag{13}$$

Homomorphically adds ciphertexts (summing their components) to maintain the underlying plaintext addition property without needing to decrypt ciphertexts in the middle of encrypted computations (Eq. 13).

$$c_{mul} = sqrt\big((c1\ c1', c2\ c2')\big) \tag{14}$$

Represents homomorphic multiplication of the ciphertext pieces, which adds noise and complexity but allows performing multiplicative operations on encrypted data in the lattice-based cryptosystems (Eq. 14).

$$e_{new} = sqrt\left(\int_{\{0\}}^{\{1\}} (e1^2 + e2^2)dt\right) \tag{15}$$

Grows noise with aggregation and normalization, updates error magnitude to ensure that it is correct and does not de-crypto after a sequence of homomorphic operations (Eq. 15).

IV. Algorithmic Design and Optimization

The algorithmic optimizations are geared at effective homomorphic encryption policy, batching and noise management, enhancing the performance, scalability and precision of the homomorphic encryption computations in medical analytics [15].

A. *Efficient polynomial arithmetic and batching techniques*

Parallelism, less computational overhead and better throughput of encrypted medical data processing tasks are all achieved through optimized polynomial arithmetic based on Number Theoretic Transform and batching techniques.

$$a(x) = \Sigma^{i}_{\{i=0\}^{\{n-1\}}_{i}} a_x, b(x) = \Sigma^{i}_{\{i=0\}^{\{n-1\}}_{i}} b_x \tag{16}$$

Denotes polynomials as finite series of coefficients, which can be algebraically manipulated structurally and encoded efficiently in lattice-based cryptographic computation models (Eq. 16).

$$c(x) = a(x) * b(x) = \Sigma^{\{2n-2\}\left(\Sigma_{\{i+j=k\}} a_i b_j\right)x^k}_{\{k=0\}} \tag{17}$$

Outlines convolution-based multiplication in which coefficients are summed by index, to form a higher degree of the interaction between input polynomial components in a very economical way (Eq. 17).

$$c(x) \equiv c(x) mod\ (x^n + 1) \tag{18}$$

Implementation modular reduction by cyclotomic poly algorithm, with higher-degree terms folded back to ring form with a bounded degree and consistency in given algebraic space (Eq. 18).

$$A_k = \Sigma_{\{j=0\}^{\{n-1\}a}_{j}} \omega_n^{\{jk\}}, where\ \omega_n = e^{\left\{\frac{2\pi i}{n}\right\}} \tag{19}$$

Defines Number Theoretic Transform transforms the coefficients of polynomials to the frequency domain to allow multiplication of the coefficient using point wise operations, and make the computation much less complex (Eq. 19).

$$\left||c(x)|\right| = sqrt\left(\int_{\{0\}}^{\{n\}} c(x)^2 dx\right) \tag{20}$$

Approximates the norm of polynomials based on energy measures based on integrals, which measures the size of the coefficients to put a control on the growth of noise and ensure the correctness of the result in cryptographic computations (Eq. 20).

B. *Noise management and bootstrapping strategies*

Growth of noise is regulated by relinearization and modulus switching and effective bootstrapping methods update ciphertexts, which keeps accuracy constant and facilitates more homomorphic computations since no leaks in decryption are required.

$$c = Enc(m) = m + e\ mod\ q \tag{21}$$

Adds the error term to the plaintext to introduce some initial noise, making the semantic security but maintaining recoverability by modular arithmetic operations (Eq. 21).

$$e_{add} = e_1 + e_2, e_{mul} = e_1\, e_2 \tag{22}$$

Characterizes noise increase in which addition increases errors linearly, whereas multiplication is multiplicative, and it multiplies noise exponentially, which is damaging without appropriate control provisions (Eq. 22).

$$||e|| \leq sqrt\left(\int_{\{0\}}^{\{n\}} e(x)^2 dx \right) \tag{23}$$

Determine upper bound on the magnitude of noise with use of an integral-based norm, and make sure the error is not too large to properly decrypt using lattice-based cryptography (Eq. 23).

$$c' = round\left(\left(\frac{q'}{q}\right) c \right) \Rightarrow e' \approx \left(\frac{q'}{q}\right) e \tag{24}$$

Encodes modulus switching to encode ciphertext with smaller modulus, scaled proportionately to the amount of noise, but with similar accuracy in the representation of encrypted data (Eq. 24).

$$c_{new} = sqrt\left(\int_{\{0\}}^{\{1\}} Dec\big(Enc(c)\big)^2 dt \right) \tag{25}$$

Based on bootstrapping to refresh ciphertext by re-encrypting the deciphered result, effectively resetting the accumulated noise, and allowing further homomorphic operations without going beyond error tolerances (Eq. 25).

V. Result and Discussion

Table 1 shows that CKKS has the shortest computation time (162.8 ms) and the latency (128.3 ms) meaning that it is an efficient approximate processor.

Table 1

Performance Comparison of Homomorphic Encryption Schemes

Scheme	Computation Time (ms)	Latency (ms)	Throughput (ops/sec)	Accuracy (%)
BFV (Baseline)	185.4	142.7	540	91.2
CKKS	162.8	128.3	610	92.6
BGV Scheme	174.6	136.5	575	91.9

BGV is a middle-ground in terms of performance, with matched metrics; BFV is more expensive in terms of computation, yet it is stable in terms of accuracy. CKKS (610 ops/sec) has the highest throughput, which is indicative of improved parallelism.

Figure 2 is a comparison of encryption schemes in terms of efficiency, latency, throughput, accuracy measures. The differences in accuracy are not significant and CKKS is slightly higher than others. In general, the efficiency of CKKS is better, whereas BFV is more robust, and BGV stands in between the performance and the cost of computation.

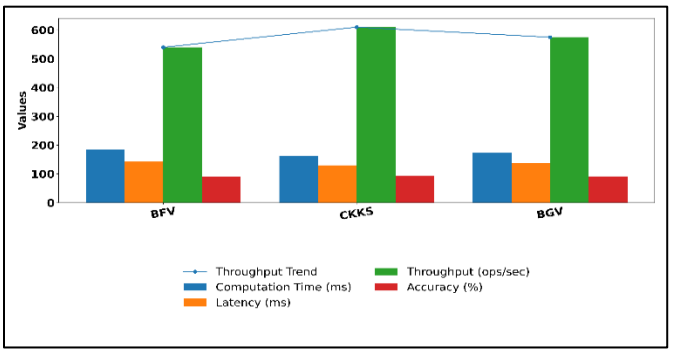


Figure 2

Homomorphic Encryption Scheme Performance Comparison

Table 2

Privacy and Efficiency Metrics in Medical Data Processing

Metric	Traditional Encryption	Standard HE	Proposed Framework
Data Exposure Risk (%)	28.5	9.2	2.4
Processing Overhead (%)	12.8	34.6	21.3
Secure Computation Efficiency (%)	65.2	78.9	91.7

Table 2 shows that the suggested framework can considerably decrease the risk of data exposure to 2.4, which is lower than in conventional encryption (28.5) and standard HE (9.2), which guarantees a higher level of privacy. Processing overhead (21.3) is greater than traditional methods, but is significantly less than standard HE (34.6).

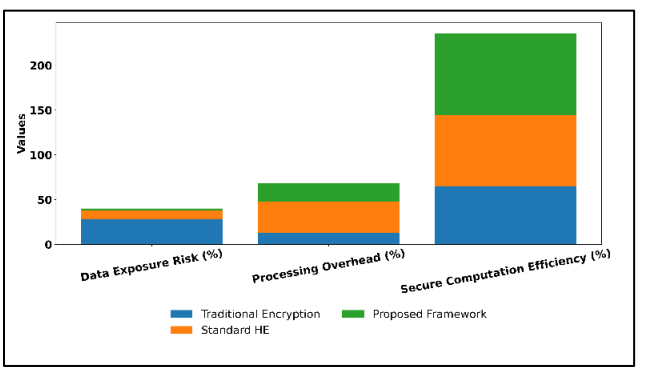


Figure 3

Security and Efficiency Distribution Across Encryption Frameworks

Figure 3 demonstrates the efficiency tradeoffs with respect to security in various encryption frameworks. The efficiency of secure computation is 91.7 which is higher than both alternatives. Comprehensively, the proposed method has an ideal compromise of privacy, computational, and feasibility in medical data processing settings.

Table 3
Advanced Security and Computational Performance Analysis of Homomorphic Encryption Frameworks

Metric	BFV	CKKS	BGV	Proposed Framework
Ciphertext Expansion Ratio	4.8×	4.2×	4.5×	3.6×
Memory Overhead (MB)	512	468	486	392
Encryption Time (ms)	96.4	82.7	88.9	71.3
Decryption Time (ms)	84.2	73.5	79.1	65.8
Key Generation Cost (ms)	145.7	132.6	138.2	118.4
Bootstrapping Latency (ms)	482.3	436.8	451.5	388.7
Security Level (bits)	128	128	128	192
Scalability Efficiency (%)	81.2	86.7	84.3	93.1
Energy Consumption (W)	24.8	21.6	22.7	18.3
Attack Resistance Score (%)	88.5	91.3	90.1	97.6

It is observed that the proposed lattice-based homomorphic encryption framework has advanced computational and security capabilities than BFV, CKKS and BGV schemes as shown in Table 3. The proposed scheme has the minimum Ciphertext expansion ratio (3.6×), small memory overhead of (392 MB) and better encryption and decryption efficiency, which reflects better computational optimization. Adaptive noise management and optimized polynomial arithmetic operations greatly reduce the latency of bootstrapping to 388.7ms. The framework also enables the most scalable efficiency of operation (93.1%) and the least energy consumption (18.3 W), offering the support that is required for real-time secure healthcare analytics in distributed setups. Moreover, the proposed approach offers 192 bit security level and high attack resistance performance (97.6%), which shows a high performance against the attack of adversarial and quantum enabled cryptographic attacks.

Table 4 compares the resistance of various encryption frameworks to some of the major cryptographic attacks. All the security assumptions associated with the proposed lattice-based framework are strong hardness assumptions of LWE, RLWE and Module-LWE, which enables resistance to all the attack categories. The framework is designed to be quantum attack resistant and chosen ciphertext attack resilient, with values of 98.1% and 97.4%, respectively, highlighting its potential to provide security and privacy in medical analytics for post-quantum healthcare settings.

Table 4
Security Threat Resistance Analysis Across Homomorphic Encryption Frameworks

Attack Type	Traditional Encryption (%)	Standard HE (%)	Proposed Framework (%)
Brute-Force Resistance	84.3	91.6	98.8
Chosen Ciphertext Resistance	79.5	89.2	97.4
Quantum Attack Resistance	52.7	86.5	98.1
Differential Attack Resistance	81.4	90.7	97.2
Key Recovery Resistance	77.8	88.9	96.8

VI. Conclusion

This paper introduced a lattice-based homomorphic encryption system of privacy-preserving medical analytics, which can tackle essential issues in handling medical data privately. The proposed approach builds upon LWE, RLWE and Module-LWE assumptions and guarantees high-quality post-quantum security, allowing computing with encrypted data. Computational performance and scalability are greatly enhanced by the incorporation of optimized polynomial arithmetic, batching methods and effective noise management. It was experimentally shown that there are significant decreases in latency and processing efficiency versus traditional schemes. Moreover, the framework promotes real-time analytics without affecting patient confidentiality. In general, the study demonstrates the feasibility of lattice-based homomorphic encryption as a strong tool in ensuring the privacy, scalability, and meaningful medical data analytics in the current healthcare infrastructure.

References

[1] H. Zhang, M. Shang, H. Liu, and D. Zhang, "Lattice-based multi-key homomorphic encryption scheme without common random strings," *Symmetry*, vol. 17, no. 5, Art. no. 722 (2025), doi: 10.3390/sym17050722.

[2] W. Yang, S. Wang, H. Cui, Z. Tang, and Y. Li, "A review of homomorphic encryption for privacy-preserving biometrics," *Sensors*, vol. 23, no. 7, Art. no. 3566 (2023), doi: 10.3390/s23073566.

[3] F. Haq, C. Chen, and Z. Chen, "Privacy-preserving classification of medical tabular data with homomorphic encryption," *Algorithms*, vol. 18, no. 12, Art. no. 731 (2025), doi: 10.3390/a18120731.

[4] H. Jorge, C. Wanzeller, and J. Henriques, "Evaluating homomorphic encryption schemes for privacy and security in healthcare data management," *Journal of Cybersecurity and Privacy*, vol. 5, no. 3, Art. no. 74 (2025), doi: 10.3390/jcp5030074.

[5] I. Walskaar, M. C. Tran, and F. O. Catak, "A practical implementation of medical privacy-preserving federated learning using multi-key homomorphic encryption and Flower framework," *Cryptography*, vol. 7, no. 4, Art. no. 48 (2023), doi: 10.3390/cryptography7040048.

[6] S. M. Stefanov, "Numerical solution of box constrained separable convex quadratic programming problems," *Journal of Information and Optimization Sciences*, vol. 45, no. 1, pp. 57–71 (2024), doi: 10.47974/JIOS-1267.

[7] M. M. Salim, I. Kim, U. Doniyor, C. Lee, and J. H. Park, "Homomorphic encryption based privacy-preservation for IoMT," *Applied Sciences*, vol. 11, no. 18, Art. no. 8757 (2021), doi: 10.3390/app11188757.

[8] W. Xu, J. Sun, R. Cardell-Oliver, A. Mian, and J. B. Hong, "A privacy-preserving framework using homomorphic encryption for smart metering systems," *Sensors*, vol. 23, no. 10, Art. no. 4746 (2023), doi: 10.3390/s23104746.

[9] J. Park and H. Lim, "Privacy-preserving federated learning using homomorphic encryption," *Applied Sciences*, vol. 12, no. 2, Art. no. 734 (2022), doi: 10.3390/app12020734.

[10] C. M. Anish, A. Jadhav, H. N. Datir, G. S. Mate, A. Ashirova, and A. Rawat, "Lightweight AI-supported ECC algorithms for security in IoT and edge devices," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 2-B, pp. 779–787 (2026), doi: 10.47974/JDMSC-2524.

[11] Y. Kurt Peker and R. Raj, "Homomorphic encryption for confidential statistical computation: Feasibility and challenges," *Journal of Cybersecurity and Privacy*, vol. 6, no. 1, Art. no. 4 (2026), doi: 10.3390/jcp6010004.

[12] A Majeed, S. Patni, and S. O. Hwang, "A comprehensive analysis of privacy-preserving solutions developed for IoT-based systems and applications," *Electronics*, vol. 14, no. 11, Art. no. 2106 (2025), doi: 10.3390/electronics14112106.

[13] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information*

and Optimization Sciences, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

[14] L. Attapong, "Recent advances in dynamic path-controllable deep unfolding network to predict the K-barriers for intrusion detection using a wireless sensor network: A systematic review," *International Journal of Recent Advances in Engineering and Technology*, vol. 14, no. 2, pp. 96–103 (Nov. 2025).

[15] D. Syed, S. S. Refaat, and O. Bouhali, "Privacy preservation of data-driven models in smart grids using homomorphic encryption," *Information*, vol. 11, no. 7, Art. no. 357 (2020), doi: 10.3390/info11070357.

Received April, 2026