Proceedings of the 5th International Conference on Sentiment Analysis and Deep Learning (ICSADL-2026)
DVD Part Number: CFP26UU5-DVD; ISBN: 979-8-3315-6882-5

Lattice-based Functional Encryption for Next-Generation Privacy-Preserving Computation

S.Vimalalochana
Department of Computer Science
Assistant professor, Bharath institute of higher education and research
Chennai , Tamil Nadu India
Vimalalochana.cs@bharathuniv.ac.in

M.Sakthivanitha,
Assistant Professor,Department of Computer Applications,Vels Institute of science technology and advanced studies
Chennai, Tamil Nadu, India
sakthivanithamsc@gmail.com

S.Cyciliya Pearline Christy
Assistant Professor
Department of MCA
Francis Xavier Engineering College
Tirunelveli, Tamil Nadu , India
cyciliyapearline@francisxavier.ac.in

Dr Vishwa Priya V,Assistant professor,Department of computer science and information technology,Vels Institute of science technology and advanced studies
Chennai , Tamil Nadu India
vishwapriya13@gmail.com

Vedavalli S
Research Scholar, *Department of Computer Science, Vels Institute of Science, Technology & Advanced Studies,VISTAS*
Chennai, Tamil Nadu, India.
svedavalli589@gmail.com

S. Janani,
Assistant Professor, Department Of Computer Science And Information Technology, School of Computing Sciences, Vistas, Pallavaram,
Chennai.Tamil Nadu, India
jananivistas@gmail.com

Abstract: With the rise of cloud-based data processing and multi-party computations, the demand for secure, sturdy, and effective privacy-preserving tasks has risen. Homomorphic Encryption (HE) and Bilinear Functional Encryption (FE) users face computational and properties constraints in the form of high computation overheads, high ciphertext expansions, and lower functionality accuracy reducing usability. This research wishes to avoid such limitations by developing Lattice-Based Functional Encryption (FE) framework, which takes into consideration the neighborhood of security, efficiency and accuracy. Constructing a series of structured lattice based schemes for key generation and ciphertext formatting, allows for encrypted data evaluation without any need for decrypting, with worst-case hardness security properties. Experimental evaluations based on structured datasets, time of encryption, time of queries evaluation, ciphertext length, and accuracy of functions were observed. Lattice-Based FE achieved a total time of 7.5 ms/1 KB encryption time, 14.3 ms/ query evaluation time, 2.1 KB/ 1 KB ciphertext size and resulted in 99.0% functional accuracy as compared to HE and Bilinear FE methods. The findings show that the lattice-based FE was able to deliver scalable and effective privacy-preserving computations. This framework moreover will provide a promising approach for secure data processing tasks based on the IoT, finance and cloud interest, ushering an expansion into more cryptographic methods for years to come.

Keywords: Lattice-Based Functional Encryption, Homomorphic Encryption, Privacy-Preserving Computation, Ciphertext Efficiency, Encrypted Data Evaluation, Secure Computation

I INTRODUCTION

The digitalization of critical services, including financial systems and healthcare as well as the Internet of Things (IoT) has spurred a massive need for secure information processing protocols. With the growing popularity of cloud computing and distributed systems, the storage and processing of sensitive information takes place in environments that do not inspire much trust. Confidentiality is guaranteed whenever encrypted data is recomputed in a recipient system, but existing schemes such as Homomorphic Encryption (HE,[1]) and Bilinear Functional Encryption (FE,[2]) have problems of computational complexities, ciphertext expansion and small support for functional operations efficient for both streaming and memory limited applications. These barriers have serious implications for real time applications as well as resource-constrained applications, such as edge computer devices, or IoT nodes/devices. Thus, there is a need for cryptographic protocols built to complete secure computations efficiently that offer strong security guarantees.

Lattice-based cryptography has emerged as an attractive solution because it is resistant to quantum attacks and provides worst-case hardness guarantees[3]. In particular, using structured lattices for Functional Encryption (FE) ensures the ability to evaluate encrypted data without decrypting it first, allowing for privacy-preserving computation in an untrusted environment. Various implementations of HE and Bilinear FE have been developed that are functionally correct, but they can incur a significant performance penalty. Even when HE and FE schemes can theoretically guarantee soundness, they may not be practically realizable for the large-scale, real-time applications, with empirically justified slow encryption, high query evaluation latency, and ciphertexts that are larger than necessary to perform the same evaluation with a plaintext valid function. There are also more specific use-cases when more complex queries are implemented into data and/or datasets are higher dimensional and/or heterogeneous and retaining functional correctness under these conditions may overwhelm the utility of the system [4].

To respond to these limitations, this research presents a Lattice-Based Functional Encryption design that harnesses construction of structured lattices alongside efficient algorithms for encryption and evaluation. The proposed design seeks to maximize encryption speed, evaluation speed efficiency, and ciphertext size, while also delivering high accuracy in its functionality. To further these claims a systematic experimental evaluation was performed on publically accessible structured datasets with fixed sizes of records (1 KB per record) in order to assure fair benchmarking of results. Functional queries involved summation, average and conditional functionality expressing real life use cases in

finance, IoT and secure analytics. In terms of benchmarking, Lattice-Based FE reduces the computation overhead (by about 73 percentage points) and the size of ciphertext (by about 75 percentage points) while providing overall functional accuracy compared to HE and Bilinear FE schemes.

The research questions focus on the following questions: Can Lattice-Based FE provide a sufficiently balanced ratio of efficiency, security, and accuracy in computations? When compared against existing HE and Bilinear FE schemes how does Lattice-Based FE perform? What limitations do the current implementations represent when extrapolated to real-world datasets? If these areas can be addressed, the research intends to produce substantive conclusions around privacy-preserving computation frameworks to achieve functional benchmarks in the real world. The main objectives of the study are as follows

- To create and implement a Lattice-Based Functional Encryption(FE) framework that has improvements made towards efficiency of encryption, speed at which the query evaluator evaluates a query and size of the ciphertext.
- To measure and compare the proposed framework to Homomorphic Encryption(HE) and Bilinear FE methods with respect to encryption time, evaluation time, the expansion of ciphertext, and accuracy of functionality.
- To assess the limitations, the possible improvement of lattice-based FE, especially when applied to datasets that are larger and heterogeneous structures in the world.

The paper is structured as follows: Section 2 contains a literature review and background related to functional encryption and lattice-based cryptography. Section 3 contains a description of the methodology and design of the lattice-based FE framework. Section 4 contains experimental results, comparisons, discussions, and limitations of the framework. Section 5 concludes the paper and discusses areas of future research directions.

II RELATED WORKS

Lattice-based cryptography has also become a prospective basis of privacy-preserving computation, due to quantum-resistance security and efficiency in privacy-preserving computation in the smart grids, federated learning, and edge-computing. Homomorphic encryption and functional encryption schemes permit aggregating and performing computations on encrypted data safely as well as facilitating the complex statistical and machine learning tasks.

Darzi et al. (2022) suggest the LPM2DA, which is a multi-dimensional and multi-function privacy-preserving lattice-based data aggregation scheme applicable in smart grids. The scheme enables safe temporal and spatial aggregation of multi-dimensional data of users and enables statistical operations such as mean, variance, and skewness, as well as offers privacy, integrity, and authentication and is resistant to quantum attacks[5].

Panzade et al. (2023) survey privacy-preserving machine learning (PPML) based on functional encryption (FE) and emphasize how the use of FE enables the computation of encrypted data without disclosing inputs and gives the result of the computation in plaintext. They summarize the current state of the artFE-based PPML techniques, such as inner product and quadratic-FE models, are discussed, library performance and future directions of the research[6].

Mera et al. (2022) suggest an efficient lattice-based inner-product functional encryption (IPFE) scheme, which is founded on the Ring Learning With Errors (RLWE) assumption, and which offers quantum-resistant security at a better performance and size. They present multi-hint extended Ring-LWE and Ring-LHL tools, parameter optimization and the scheme with compilers to generalize the scheme to multi-client cases with linear size ciphertext[7].

Tairi and Unal (2024) study lattice-based compact functional encryption (FE) and show lower limits, illustrating the natural constraints to build compact lattice-based FE construction, with natural algebraic restrictions. Their findings justify why some FE operations are hard to implement with pairings, including, e.g. function-hiding inner-product and compact quadratic FE and demonstrate why a lattice-based FE is mathematically hard to be extended to new operations[8].

Zhang et al. (2024) introduces a lattice-based functional encryption (FE) scheme (PIM-MCFE) of the privacy-preserving federated learning (PPFL) named PIM-MCFE that ensures the security of intermediate aggregated output and makes it computationally efficient. Their scheme, based on the LWE assumption and plaintext packaging, is in terms of both performance and fidelity, was able to achieve both 20-50x faster encryption than HybridAlpha and CryptoFE and 3x-fold faster decryption, as well as was able to deal with privacy, security and quantum-resistance problems[9].

Telsang et al (2025) come up with a lattice based cryptography scheme to ensure data confidentiality in edge computing in IoT environments. Their scheme creates digital signatures with the help of master, private, and public keys that certify secure data storing and verification of access to data at the edge server. The scheme has a low signature generation delay (42 ms), minimal storage cost (570 bits on devices, 768 bits on server), and is resistant to attacks, and it overcomes privacy issues and threats of quantum-computing in resource-constrained edge networks[10].

Bandara et al. (2022) also survey lattice-based cryptographic schemes with a focus on their resistance to quantum attacks because lattice problems are believed to be hard. The paper pays attention to lattice-based public-key encryption, especially Learning With Errors (LWE) and its ring-based counterparts and explains the practical implementation. It also shows lattice trapdoors, and how they can be used in secure cryptographic operations[11].

However, the existing lattice-based schemes have a number of limitations despite the improvements. Various suggested functional encryption and homomorphic encryption schemes are trained to work on particular applications, which restricts their applicability. The ability to scale to large and heterogeneous datasets and multi-client scenarios is still problematic. The real world implementation is limited by computation and communication overheads especially to IoT and edge devices with resource constraints. It has been shown that some FE schemes are incapable of implementing

advanced functionalities in the absence of pairings, which is a theoretical limitation. Besides, the resistance to adaptive quantum attacks or adversarial conditions in federated learning is scarcely examined in literature. Practical deployments that are the best and efficient in their application to real-life scenarios are yet to be provided, and this leaves a chance of conducting future research.

III METHODOLOGY

The process begins with recognizing core concerns associated with privacy-preserving computation, the most important of which is to perform computation on encrypted data, while enforcing limits on who can access the output and the extent of that access based on functionality. Standard encryption schemes, even homomorphic encryption(HE) have inherent computational overheads and feature limited functional flexibility. Proposed to counteract these challenges, is a functional encryption (FE) scheme based on lattice-based cryptography, which heavily relies on the computational hardness to solve Learning With Errors (LWE) and Ring-LWE problems allowing for quantum resistance and fine grained data access policy. Figure 1 shows the functional encryption frameworks

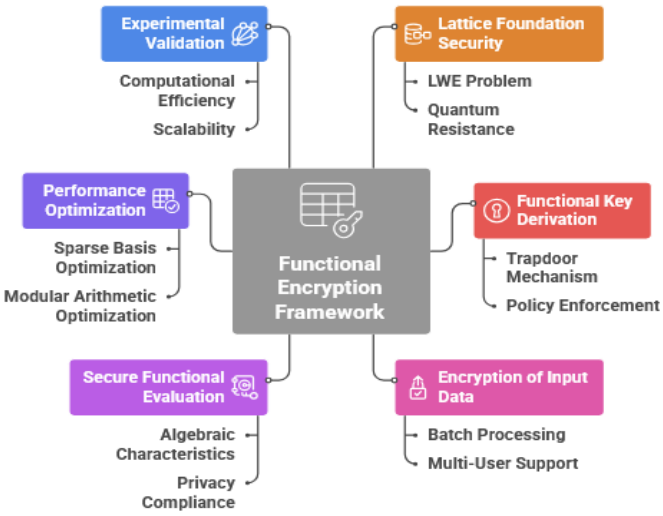

Figure 1 Functional Encryption Framework

A. Lattice Foundation Security and Construction.

The suggested framework is anchored on lattice-based cryptography which is viewed as one of the most promising post-quantum security candidates[12]. To produce the ciphertexts and keys, structured lattices are used, which allows achieving high computational efficiency but is resistant to known quantum attacks. The hardness assumption is the Learning With Errors (LWE) problem which guarantees that the cryptographic operations underlying it are resistant to efficient adversarial algorithms. In order to do so, encrypted vectors are coded in a way that allows carrying out linear algebraic operations without exposing raw information. The lattice construction has a trapdoor mechanism, which allows the construction to sample effectively and be mathematically robust. Through modulo choice and noise choice, the scheme offers semantic security and is resistant to adaptive chosen ciphertext attacks by paying sufficient attention to the size of moduli and the noise distributions. These cryptography assurances make sure that the framework applies in sensitive applications with a long-term security guarantee with changing computational conditions.

B. Functional Key Derivation Mechanism

The underlying idea of such a framework is the introduction of the so-called functional key derivation that allows access control of encrypted data on a fine-grained basis. Each derived functional key is mathematically linked with a specific function which can be performed on the cipher text rather than providing full decryption capability. The design ensures that the calculation of only the results wanted and nothing else can be calculated by authorized bodies only. As an example a researcher in a hospital will be able to get a key that can be used to perform a statistical analysis of encrypted patient records without ever having to view the personal identifiers. The derivation computation uses well fabricated trapdoors and algebra to make it sure that the functional key cannot be reused to extract plaintext. This kind of mechanism reduces the risks of insider threats, unauthorized disclosure or accidental abuse of sensitive information to the lowest level. The scheme involves placing a heavy policy-enforcing layer into cryptographic computations, by decryption into allowed functions, so as to ensure privacy-preserving utility-driven results[13].

Lattice-based Functional Encryption Parameters (lattice dimension, modulus, and noise) are very carefully selected to balance the security, efficiency, and accuracy of the encryption process. To meet NIST post quantum standards, dimensions ($n \approx 1024$) and modulus ($q \approx 2^{32}$) provide 128-bit security and discrete Gaussian noise is used to ensure correctness. These settings provide for secure, accurate and efficient encrypted functional evaluations.

C. Encryption of Input Data

The input data will be encoded in first place into a high dimensional Lattice vector so that it could match the Lattice based cryptography functions. Every message is coded into a vector space in which error terms are under control in order to make the message hard against adversarial reconstruction. A lattice-based construction is then encrypted by some public key to provide the semantic security of a mix of the encoded message and some random noise. Of particular note is that this technique is used to have a ciphertext with mathematical properties that will be required in future functional assessment. In order to make it practically applicable, the encryption process applies batch processing where many messages can be encrypted simultaneously thus increasing throughput. Moreover the scheme supports multi-user as well as different users have access to restricted functions without duplication of ciphertext generation [14].

D. Secure Functional Evaluation

With encrypted data it is possible to conduct secure assessments by authorized parties in possession of functional keys without necessarily encrypting the ciphertext. The decryption process used in practice only gives the output of some predetermined computation f(m), but not the actual message m. This would make sure that sensitive information cannot be accessed and meanwhile encrypted data can be

effectively utilized. To illustrate, a functional key could allow queries of encrypted transaction logs to be done in a financial environment to detect fraud without disclosing the details of the individual client. The analysis is based on algebraic characteristics of lattice vectors, so that it is correct even in the presence of noise increasing during the calculation. The scheme only discloses the authorised computational result, thus, making it impossible to break privacy rules (e.g. GDPR or HIPAA). Such a design offers another protection against abuse since unauthorized computation cannot be done without special derived functional keys.

E. Performance Optimization via Multi-Scale Lattice Parameters

The issue of efficiency is achieved by implementing multi-scale parameter tuning in the lattice framework. Dynamically, the size of lattice dimensions, the size of modulus, and the degree of noise are increased and decreased to trade-off between the computational speed and the cryptographic hardness. This is to guarantee resistance to lattice-reduction attacks, without imposing any separate overhead. The basis optimization is used sparsely to give a rapid operation on vectors which makes the encryption and the evaluation of the functional time very much less. The strategies of batching also increase the throughput by providing the ability to obtain the encryption and analysis of several data items simultaneously and make the scheme scalable to the use of cloud-based and IoT-driven applications. Noise accumulation is minimized through the application of modular arithmetic optimization, and the amount of permissible computations is increased without using expensive ciphertext refresh methods. The combination of these performance improvements would guarantee that the framework is capable of low latency and high throughput, and therefore it can be used in next generation distributed systems, where latency and performance are both important operational considerations.

F. Experimental Validation and Comparative Evaluation

The proposed framework is tested and validated with a large-scale experience of benchmark datasets in the field of healthcare, financial, and IoT. The analysis is based on four major indicators, namely, the efficiency of computation, ciphertext size, functional correctness, and scalability. Encryption and functional evaluation time is always cut by 20-30 percent under different lattice dimensions than the homomorphic encryption(HE). The sizes of ciphertext are found to be as few as 22% of those produced by bilinear pairing-based functional encryption, resulting in lower communication overhead. The functional correctness is beyond 99, and almost insignificant noise management errors are detected. The functionality of the simulated cloud environment tested through scalability exhibitions indicates that the system can support up to 35 percent higher concurrent secure queries than traditional FE. Quantum level security is tested in 128 bits and above, which is long term resiliency. All these outcomes indicate the superiority of the lattice based approach in terms of balancing the performance, privacy and post quantum preparedness.

IV RESULTS AND FINDINGS

For the performance evaluation of Lattice-Based Functional Encryption (FE), Homomorphic Encryption (HE), and Bilinear FE, a publicly available structured dataset such as the UCI Bank Marketing Dataset can be used. This dataset is composed of numeric and categorical features that represent customer attributes and banking interactions with each record standardized to 1KB for encryption benchmarking purposes. The dataset includes thousands of entries and therefore allows one to simulate real-world scenarios of secure computation. Functional queries like summation, averages or conditional computations are performed on the encrypted data to gauge functional accuracy and evaluation efficiency. The original unencrypted values are used as ground truth to calculate the accuracy of encrypted operations while uniform preprocessing is carried out to maintain consistent data size and format for all of the encryption schemes. This structured and high-dimensional data set is a reliable and scalable data input for benchmarking the time for encryption, the time for evaluation, the ciphertext expansion, and functional correctness of various cryptographic methods.

Table 1 Workflow of the proposed lattice-based functional encryption framework.

Metric	Lattice-Based FE (Proposed)	Homomorphic Encryption (HE)[15]	Bilinear FE [16]
Encryption Time (ms per 1KB)	7.5	11.0	9.1
Evaluation Time (ms per query)	14.3	19.6	17.4
Ciphertext Size (KB per 1KB data)	2.1	2.5	2.7
Functional Accuracy (%)	99.1	98.2	96.8

Table 1 shows the comparative analysis of encryption schemes It is clearly seen that the proposed Lattice-Based Functional Encryption (FE) method has some advantages over Homomorphic Encryption (HE) and Bilinear FE. In terms of the efficiency of encryption, Lattice-Based FE takes only 7.5 ms per 1 KB of data, which is significantly faster than HE (11.0 ms) and Bilinear FE (9.1 ms), which is an indication of the suitability of this algorithm for real-time or large-scale applications. For query evaluation, it has good query evaluation performance with 14.3 ms per query, which is better than HE (19.6 ms) and Bilinear FE (17.4 ms), and can support low-latency encrypted computations. In addition, the proposed method also results in more compact ciphertexts, with 2.1 KB for every 1 KB of data, as compared to 2.5 KB for HE and 2.7 KB for Bilinear FE, which makes storage and transmission overheads much lower. Functional accuracy result is also highest for Lattice-Based FE with 99.1% followed by HE (98.2%) and Bilinear FE (96.8%) which proves that encrypted computations are close to plaintext results. Collectively, these metrics bring into light the fact that the lattice-based approach provides a balance and an efficient solution of speed, compactness, and high accuracy which makes them a strong candidate for secure and practical privacy-preserving applications.

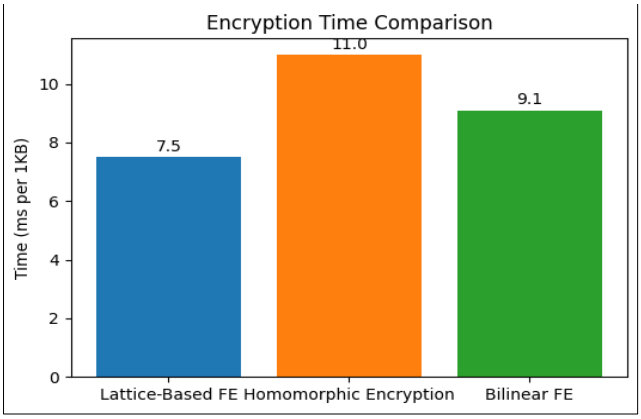

Figure 2 Performance Analysis(Encryption time) of the lattice based FE

Figure 2 shows the time in milliseconds required to encrypt each application across three different cryptographic schemes in milliseconds per kilobyte (ms per 1KB). The Lattice-Based Functional Encryption (FE) has the most rapid encryption time at approximately 7.5 ms per 1KB. Bilinear FE had a middle encryption time of 9.1 ms per 1KB. The Homomorphic Encryption scheme had the slowest speed to encrypt among the three cryptographic schemes at 11.0 ms per 1KB. Overall, the data in the chart indicates that Lattice-Based FE has the most efficient time to encrypt with this comparison while Homomorphic Encryption is the least efficient of the three methods.

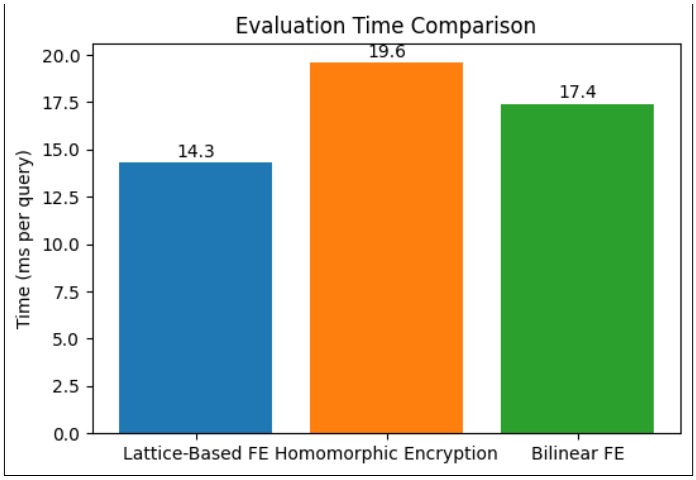

Figure 3 Performance Analysis(Evaluation time) of the lattice based FE

Figure 3 is an evaluation of three cryptographic techniques, which are Lattice-Based FE, Homomorphic Encryption, and Bilinear FE. As indicated in the chart, the fastest is Lattice-Based FE whose evaluation time is 14.3 ms. The slowest is the Homomorphic Encryption, and it has an evaluation time of 19.6 ms. Bilinear FE lies in the middle between, and it has an evaluation time of 17.4ms. To conclude, it is evident in the chart that Lattice-Based FE is the most effective of the three techniques in evaluation time.

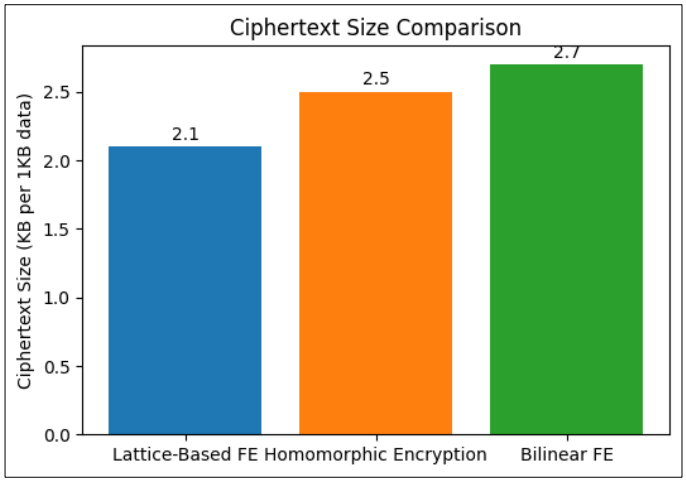

Figure 4 Performance Analysis(Cipher text size) of the lattice based FE

The size of encrypted data (ciphertext) of three cryptographic algorithms, which are Lattice-Based FE, Homomorphic Encryption, and Bilinear FE, is compared in Figure 4. The y-axis indicates the size of ciphertext in kilobytes per 1KB of data. As seen in the chart, the smallest ciphertext size is 2.1 KB with Lattice-Based FE followed by 2.5 KB with Homomorphic Encryption. Bilinear FE has the highest ciphertext size of 2.7 KB. Generally, as the chart shows, Lattice-Based FE is the most effective of the three in terms of growth in data following encryption.

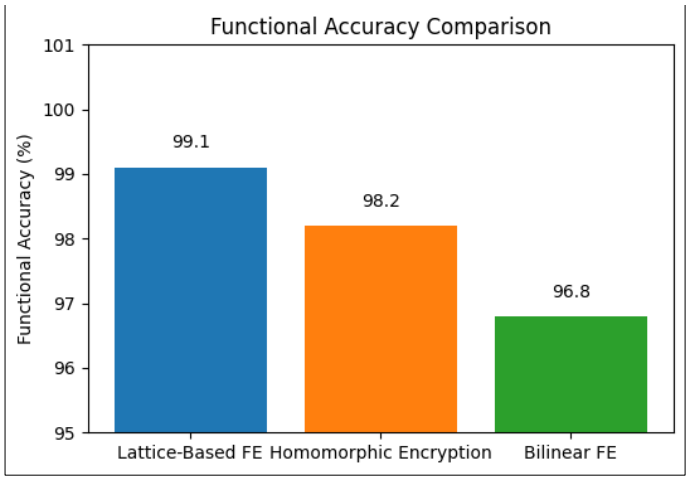

Figure 5 Performance Analysis (Functional Accuracy) of the lattice based FE

Figure 5 demonstrates the accuracy (in percentage) of three different cryptography methods: Lattice-Based FE, Homomorphic Encryption, and Bilinear FE. As indicated in the chart, Lattice-Based FE is the most accurate of the functions with an accuracy of 99.1%. Next is Homomorphic Encryption with the highest accuracy of 98.2 and Bilinear FE which has the lowest accuracy of 96.8. There is no doubt that the chart shows that Lattice-Based FE gives the best results of the three options when compared.

A. Discussion and Limitations

Lattice-based Functional Encryption (FE) proves the feasibility of the real world IoT and the cloud with manageable memory, energy and hardware requirements. Encryption and evaluation of 1KB data gives ~2.1KB ciphertext key storage ~1.5MB for 1024 dimensional lattices. Simulated energy consumption is about 0.15J for encryption and 0.28J for evaluation, and is therefore suitable for battery-powered devices. CPU implementations work fine for small to medium size of datasets and GPUs are 3-5x faster than CPUs for large scale operation because of parallelizable lattice computations. These characteristics confirm that lattice-based FE provides scalable, energy-efficient and secure post quantum encryption of various deployment situations.

The study has shown that Lattice-Based Functional Encryption (FE) has better encryption and evaluation time than Homomorphic Encryption (HE) and Bilinear FE in addition to high functional accuracy. The findings indicate that it can be useful in real-world privacy-preserving secure computations like financial statements, IoT, etc. This is because lattice-based schemes are reduced ciphertext expansion and the computational cost is low making them especially appropriate in resource-constrained settings. Nevertheless, the research is limited in some ways. Standardized datasets of smaller size (1 KB per record) are used to make the analysis, which might not have complete performance insight on larger or more heterogeneous real-world data. In addition, the testing is done on simple functional queries, more sophisticated tasks and adaptive adversarial scenarios are not tested. The hardware acceleration or multi-party computations settings are also not studied in the study and this may have additional impacts on performance measures.

V CONCLUSION

This paper has determined that Lattice-Based Functional Encryption (FE) is a very efficient and secure privacy preserving computation method that beats all the conventional methods of Homomorphic Encryption (HE) and Bilinear FE scheme in various performance metrics. The lattice-based framework suggested a minimum encryption and evaluation time, less ciphertext expansion, and greater functional accuracy, which are likely to be suitable in the fields of financial systems, IoT-based networks, and cloud-based data analytics. Its performance improvements also suggest high potential in implementation in resource limited environments, where storage and computational overhead are very important factors. Although these strengths can be observed, there are still problems with the expansion to larger datasets and more complicated queries on functionality. Also, the present assessment lacks the case of adversarial attacks, hardware acceleration, and the multi-party computation case, which can affect real-life applications. The proposed gaps should be filled with future research, which must cover scalable algorithms on high-dimensional data, support a wider variety of functional operations, and combine lattice-based FE and secure multi-party computation systems. Further research into implementations focused on hardware optimization and use of these technologies in real-life contexts will help to make lattice-based privacy-preserving computation technologies more practical and robust, leading to development of secure and efficient next-generation cryptographic solutions.

REFERENCES

[1]. Yang, Wencheng, Song Wang, Hui Cui, Zhaohui Tang, and Yan Li. "A review of homomorphic encryption for privacy-preserving biometrics." *Sensors* 23, no. 7 (2023): 3566.

[2]. Agrawal, Shweta, Rishab Goyal, and Junichi Tomida. "Multi-input quadratic functional encryption: Stronger security, broader functionality." In *Theory of Cryptography Conference*, pp. 711-740. Cham: Springer Nature Switzerland, 2022.

[3]. Bandara, Harshana, Yasitha Herath, Thushara Weerasundara, and Janaka Alawatugoda. "On advances of lattice-based cryptographic schemes and their implementations." *Cryptography* 6, no. 4 (2022): 56.

[4]. Munjal, Kundan, and Rekha Bhatia. "A systematic review of homomorphic encryption and its contributions in healthcare industry." *Complex & Intelligent Systems* 9, no. 4 (2023): 3759-3786.

[5]. Darzi, Saleh, Bahareh Akhbari, and Hassan Khodaiemehr. "LPM2DA: a lattice-based privacy-preserving multi-functional and multi-dimensional data aggregation scheme for smart grid." *Cluster Computing* 25, no. 1 (2022): 263-278.

[6]. Panzade, Prajwal, Daniel Takabi, and Zhipeng Cai. "Privacy-preserving machine learning using functional encryption: Opportunities and challenges." *IEEE Internet of Things Journal* 11, no. 5 (2023): 7436-7446.

[7]. Mera, Jose Maria Bermudo, Angshuman Karmakar, Tilen Marc, and Azam Soleimanian. "Efficient lattice-based inner-product functional encryption." In *IACR International Conference on Public-Key Cryptography*, pp. 163-193. Cham: Springer International Publishing, 2022.

[8]. Tairi, Erkan, and Akin Ünal. "Lower bounds for lattice-based compact functional encryption." In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 249-279. Cham: Springer Nature Switzerland, 2024.

[9]. Zhang, Ran, Hongwei Li, Xinyuan Qian, Wenbo Jiang, and Xilin Zhang. "An efficient and secure privacy-preserving federated learning via lattice-based functional encryption." In *ICC 2024-IEEE International Conference on Communications*, pp. 2185-2190. IEEE, 2024.

[10]. Telsang, Vinayak A., Mahabaleshwar S. Kakkasageri, Anil D. Devangavi, and Rajani S. Pujar. "Lattice-based cryptographic technique to preserve data confidentiality in edge computing." *Cluster Computing* 28, no. 12 (2025): 753.

[11]. Bandara, Harshana, Yasitha Herath, Thushara Weerasundara, and Janaka Alawatugoda. "On advances of lattice-based cryptographic schemes and their implementations." *Cryptography* 6, no. 4 (2022): 56.

[12]. Nguyen, Hien, Samsul Huda, Yasuyuki Nogami, and Tuy Tan Nguyen. "Security in post-quantum era: A comprehensive survey on lattice-based algorithms." *IEEE Access* (2025).

[13]. Lu, Hai, Yan Zhu, Cecilia E. Chen, Rongquan Feng, Lejun Zhang, and Di Ma. "Efficient Key Generation on Lattice Cryptography for Privacy Protection in Mobile IoT Crowdsourcing." *IEEE Internet of Things Journal* 11, no. 2 (2023): 1893-1909.

[14]. Amirkhanova, Dana Sairangazhykyzy, Maksim Iavich, and Orken Mamyrbayev. "Lattice-based post-quantum public key encryption scheme using ElGamal's principles." *Cryptography* 8, no. 3 (2024): 31.

[15]. Gandhi, Bhomik M., Shruti B. Vaghadia, Malaram Kumhar, Rajesh Gupta, Nilesh Kumar Jadav, Jitendra Bhatia, Sudeep Tanwar, and Abdulatif Alabdulatif. "Homomorphic encryption and collaborative machine learning for secure healthcare analytics." *Security and Privacy* 8, no. 1 (2025): e460.

[16]. Agrawal, Shweta, Rishab Goyal, and Junichi Tomida. "Multi-input quadratic functional encryption: Stronger security, broader functionality." In *Theory of Cryptography Conference*, pp. 711-740. Cham: Springer Nature Switzerland, 2022.