Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/SA07.20260168
Published: August 4, 2026

Design of a Hybrid Quantum-Classical Model for Encrypted Data Multiplication to Preserve Security

Lauro Enciso Rodas and Karla Catherine Rojas Pedraza
Rector of the University
Professor in the Department of Informatics and Systems Engineering
Universidad Nacional de San Antonio Abad del Cusco
Cusco, Perú
lauro.enciso@unsaac.edu.pe, karla.rojas@unsaac.edu.pe

Abstract

This research addressed the challenge of secure multiplication over encrypted data, where information security and data integrity must be preserved. To this end, we proposed the design and validation of a hybrid quantum – classical model that multiplies encrypted polynomials, a foundational component of the Cheon–Kim–Kim-Song (CKKS) homomorphic encryption, grounded in the Ring Learning With Errors (RLWE) problem. Furthermore, the proposed solution leverages quantum convolutions by Quantum Fourier Transform (QFT), to explore quantum interference and superposition properties within the homomorphically encrypted domain. Methodologically, the model was implemented using the Qiskit framework, integrated with the Microsoft SEAL cryptographic library using the Python programming language. The results demonstrated that the product computed over homomorphically encrypted data corresponds–within a bounded and controlled error margin – to the plaintext product, thereby validating that the integration of quantum techniques into a classical cryptosystem does not compromise data security and preserves algebraic fidelity. Throughout the quantum multiplication process, the data remained unintelligible, accessible exclusively to authorized users. This constitutes a significant and scalable contribution to the development of secure data processing models within quantum environments.

Keywords
Quantum computing, CKKS homomorphic encryption, Quantum multiplication, Data security, Quantum Fourier Transform

1. Introduction
The present research proposes a hybrid quantum-classical multiplication model that integrates the CKKS homomorphic cryptosystem (Cheon et al. 2017) with quantum computing paradigms. Under this approach, the multiplication of high-degree encrypted polynomials is performed through quantum convolutions using the QFT, which applies controlled phase rotations (Nielsen and Chuang 2010). The constructive and destructive interference behavior of these rotations allows for the efficient redistribution of quantum amplitudes, maximizing the probability of obtaining the correct output upon measurement (Mahadev and Brakerski 2021). The need for this model arises because the polynomial multiplication problem is the foundation for solving other computational problems (Gao et al. 2025).

Specifically, in the polynomial convolution present in CKKS, the multiplication operation generates polynomials with exponential degree growth that exceeds the capabilities of current classical computing environments. In this context, the proposed model applies quantum paradigms solely in the convolution stage of encrypted polynomials, serving as an alternative solution to the limited availability of quantum infrastructure (Ma et al. 2022). The multiplication of encrypted polynomials using CKKS presents unique challenges due to noise growth and the associated algebraic cost (Mahadev and Brakerski 2021), raising the challenge of preserving data coherence and integrity during the process.

© IEOM Society International

The challenge consists not only of preventing information degradation or vulnerabilities to unauthorized third parties, but also of achieving functional integration between classical and quantum computing. This implies strategically allocating available resources based on the computational and mathematical demands of each stage of the homomorphic cryptosystem, as well as analyzing the impact of total cryptographic noise expansion on the modular overflow boundaries and on the preservation of the model's security level.

The application of the model involves the input of two numerical values homomorphically encrypted with CKKS. The resulting high-degree polynomials are mapped from the computational domain to the Fourier domain in order to apply the QFT, where the cumulative effect of phase rotations in the frequency domain on the polynomials allows for the execution of a circular convolution within the value of a predefined modulus.

The comparison of both quantum and classical products–with data remaining unintelligible during the operation and with an error value within pre-established margins (Lyubashevsky et al. 2013)–demonstrates homomorphic correctness. Furthermore, evaluating the model's resistance against BKZ algorithm attacks (Chen and Nguyen 2011) demonstrated a security level of 287 bits on the NIST scale.
To obtain these results, classical homomorphic encryption techniques, quantum circuit simulation, and a formal analysis of the impact of cryptographic noise expansion on modular overflow boundaries were integrated, guaranteeing the preservation of the achieved security level.

As a contribution, a secure and scalable hybrid quantum-classical model for the multiplication of homomorphically encrypted polynomials is proposed, integrating the CKKS cryptosystem with quantum paradigms.

The remainder of this paper is organized as follows: the objectives; the conceptual theoretical framework supporting the mathematical, cryptographic, and quantum foundations of the study; the applied methodology including the proposed model; the implementation results and discussion; and finally, the conclusion.

1.1 Objectives

The main objective of this research is to design a hybrid classical-quantum model for multiplying encrypted data using homomorphic cryptosystems to preserve security. To achieve this overarching goal, the specific objectives are established as follows:

- To validate the approximate homomorphic correctness in encrypted data multiplication and plaintext operations within the proposed quantum model.
- To guarantee data security and confidentiality during the execution of multiplication operations in the proposed quantum model.
- To determine the impact of cryptographic noise expansion on modular overflow boundaries and on the preservation of the proposed model's security level.

2. Literature Review

The evolution of modern cryptography requires secure paradigms capable of processing sensitive data without exposing the underlying information (Faneela et al. 2025). With the rapid advancement of quantum computing, traditional cryptographic frameworks face significant challenges, driving the development of advanced quantum homomorphic cryptography models with an efficient distribution of quantum and classical resources (Broadbent and Jeffery 2015).

The complexity of the classical polynomial multiplication problem constitutes a computational bottleneck, which becomes relevant as it serves as the basis for solving other computational problems, such as structured matrix multiplication. Gao et al. (2025) addressed this challenge by proposing a QFT-based quantum algorithm that leverages superposition and parallelism to transform coefficients into the quantum Fourier domain, thereby accelerating the polynomial convolution process.

Building upon foundational cryptographic primitives, recent studies have evaluated the feasibility and security properties of Quantum Fully Homomorphic Encryption (QFHE) and distributed architectures. Savadatti et al. (2025) analyzed fault-tolerant schemes based on Calderbank-Shor-Steane (CSS) codes and the Quantum One-Time Pad (QOTP) technique with Learning With Errors (LWE); they identified that, despite preserving data security, circuit complexity and noise mitigation introduce a substantial memory overhead. Complementing this perspective on

© IEOM Society International

distributed secure processing, Li et al. (2025) introduced a multi-party quantum homomorphic encryption scheme using quantum teleportation, allowing non-interactive circuit evaluations on encrypted states without requiring intermediate client decryption.

As a complement to the analyzed theoretical models and numerical demonstrations, hybrid architectures focused on managing logical control and encryption states have emerged. Biamonte et al. (2024) developed a hybrid classical-quantum model for secure multiplication using Quantum Homomorphic Encryption (QHE), evaluating T gates on QOTP-encrypted data through semiclassical Szegedy quantum walks. This approach implements homomorphic encryption directly on quantum states, where encryption management remains in the classical domain while quantum states evolve securely.

The reviewed theoretical foundations are as follows:

2.1 Mathematical Foundations

The research is structured upon abstract algebra concepts, incorporating formal definitions of abelian groups, rings, and the principles of modular arithmetic under the closed set Z_q (Katz and Lindell 2020). On this algebraic foundation, polynomials and their properties of degree and monicity are defined (Regev 2009), enabling the construction of the polynomial ring $R[x]$ equipped with polynomial addition and multiplication operations (Katz and Lindell 2020). This theoretical foundation sustains the security and efficiency of lattice-based cryptographic schemes; specifically, the LWE problem, which introduces random noise to disrupt the linearity of a system of linear equations (Savadatti et al. 2025), and its algebraic evolution, the Ring Learning with Errors (RLWE) problem, which translates these operations into the domain of polynomial rings (Savadatti et al. 2025).

2.2. Cryptographic Foundations

The security of the proposed model relies on the existence of homomorphisms between ciphertext rings, guaranteeing the feasibility of processing data without compromising the secret key or requiring prior decryption (Tebaa et al. 2012, Katz and Lindell 2020). Within this domain, fully homomorphic encryption (FHE) schemes have evolved from their initial theoretical conception (Rivest et al. 1978) and first viable construction (Gentry 2009) to the development of modern cryptosystems such as CKKS (Cheon et al. 2017). The latter operates as an approximate asymmetric scheme based on the hardness of the RLWE problem (Savadatti et al. 2025), employing modular reduction over the cyclotomic polynomial ring structure $R_q = \mathbb{Z}_q[x]/(x^N + 1)$ to mitigate the uncontrolled growth of polynomial coefficients (Cheon et al. 2017, Katz and Lindell 2020). The algorithmic workflow of CKKS comprises six critical phases: encoding, encryption via the injection of discrete Gaussian noise, homomorphic evaluation of additions and multiplications, rescaling for scale and noise control, decryption, and final decoding (Cheon et al. 2017). Since the homomorphic evaluation of multiplication in the encrypted domain requires computing complex polynomial convolutions, CKKS relies on the discrete linear transform (Oppenheim et al. 1997), specifically the number theoretic transform (NTT), to enhance efficiency.

2.3 Quantum Computing Foundations

Information processing using qubits in superposition within a complex Hilbert space H is the foundation of quantum computing, exploiting quantum entanglement and interference phenomena through unitary transformations that preserve the norm of the system (Nielsen and Chuang 2010). Furthermore, the QFT maps computational basis amplitudes to the Fourier domain via Hadamard gates and controlled phase rotations R_k, being distinguished by its mathematical unitarity and reversibility ($QFT^{-1} = QFT^{\dagger}$) (Nielsen and Chuang 2010). In encrypted polynomial multiplication, unitarity is indispensable to preserve the quantum state norm, guaranteeing that the scale factor Δ and the cryptographic noise injected under the RLWE scheme do not undergo distortions that would corrupt the plaintext during the change of basis. Meanwhile, mathematical reversibility ensures that, after performing linear multiplication via phase rotations in the Fourier domain, the adjoint operator $QFT^{\dagger}$ acts as a bijective, dissipation-free mapping that accurately retrieves the resulting polynomial coefficients in the computational basis through the quantum destructive interference of spurious terms. Quantum addition and multiplication in the Fourier domain are executed via controlled phase rotations that act directly on the state of the qubits. These phase rotations are mathematically grounded in Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$, where Euler's number $e \approx 2.718$ and the imaginary unit i project a continuous angular displacement $\theta_k = 2\pi/2^k$ onto the unit circle of the complex plane, altering the relative phase of the qubit without modifying its physical state probability. In quantum multiplication, obtaining the resulting phases is achieved through the binary decomposition of the multiplier, which conditionally triggers fractional rotation gates $R_k = \mathrm{diag}\left(1, e^{i\theta_k}\right)$ over an accumulator in a superposition state previously transformed by the QFT. Consequently, the product is encoded in parallel within the accumulated relative phase of the qubits, which is translated back to readable amplitudes in the

© IEOM Society International

computational basis by applying the inverse operator $QFT^{\dagger}$, leveraging constructive phase interference to reveal the correct final coefficients (Ruiz-Perez and Garcia-Escartin 2017).

In summary, although the existing literature demonstrates significant advances in quantum polynomial acceleration, multi-party quantum homomorphic frameworks, and hybrid circuit simulations, several critical challenges still persist. Specifically, current QFHE implementations suffer from high circuit complexity, severe noise accumulation, and high memory intensity. This highlights the need for an optimized hybrid model that integrates quantum structural improvements – such as the QFT – with suitable homomorphic encryption schemes to ensure secure data processing without loss of integrity and with appropriate noise management tailored to user needs.

3. Methods

The research is of an applied nature, as it uses existing foundations to propose and validate a secure quantum multiplication model. It is conducted at an explanatory level, since the model explains the invariance of the outcome of the homomorphic encrypted multiplication with respect to its plaintext counterpart. The techniques and instruments employed were simulation, algorithmic tests, and result comparison, oriented towards validating the quantum model for the secure multiplication of encrypted data. Within this context, the Microsoft SEAL library was used for encrypting and decrypting data in the classical domain; Python was used to sequentially integrate the different stages of the model; and quantum simulation in Qiskit allowed the implementation of quantum multiplication of encrypted polynomials via QFT.

3.1 Proposed Model

The hybrid quantum – classical model proposed in this research, shown in Figure 1, focuses on the CKKS approximate homomorphic cryptosystem within a classical environment.

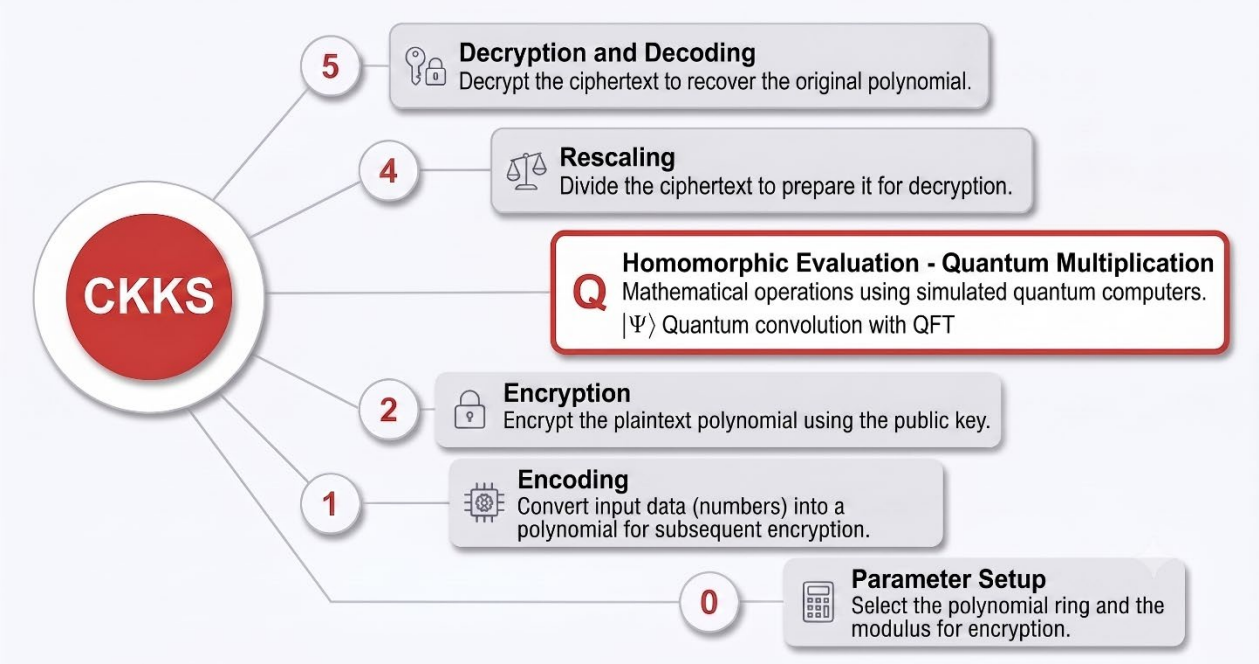


Figure 1. Quantum Model for Homomorphic Multiplication of Encrypted Data to Preserve Security

As shown in Figure 1, below, each stage of the CKKS cryptosystem and its integration with the QFT in the homomorphic evaluation stage are detailed:

© IEOM Society International

3.2 Classical Environment for Cryptogram Generation

Stages 0, 1, and 2 constitute the initial preprocessing of the CKKS cryptosystem. In this phase, cryptograms are generated and represented as high-degree polynomials, which serve as inputs for the homomorphic evaluation stage (Stage 3) of the model.

3.3 Quantum Environment for Homomorphic Evaluation via Polynomial Convolution

In the homomorphic evaluation stage (Stage 3), the encrypted polynomials transform into vectors of probability amplitudes within a quantum environment, and the convolution of the polynomials is executed via QFT. It is important to emphasize that this convolution process operates directly on the encrypted cryptograms, guaranteeing that the original information remains protected throughout the calculation process. As a result of this stage, a new polynomial encoded in quantum amplitudes is obtained, which is returned to the classical environment to retrieve the plaintext message.

3.4 Classical Environment for Post-processing and Decryption

Stages 4, 5, and 6 correspond to the final phases of CKKS. In this environment, rescaling, decryption, and decoding operations are executed, allowing for the retrieval of the product's resulting value after application of the private key (Cheon et al. 2017). The hybrid model demonstrates the integration of the QFT quantum paradigm into the classical computational environment of the CKKS cryptosystem. This integration has been made possible due to the representation of homomorphic encrypted polynomials as probability amplitude vectors of qubits processed via phase rotations within a quantum environment.

4. Data Collection

For the algorithmic testing of the model – aimed at optimizing encrypted data processing through the integration of the QFT with the CKKS approximate homomorphic cryptosystem the use of static datasets or conventional data collections was avoided. Instead, a strategy based on the generation of random synthetic data subjected to a rigorous systematic analysis of ranges and numerical precision was implemented, in accordance with the guidelines and methodological standards of the Institute of Electrical and Electronics Engineers (IEEE).

This validation was structured across six distinct operational domains, which allowed for a controlled evaluation of the algorithm's behavior against scale variations, ensured numerical stability against the propagation and accumulation of noise inherent to homomorphic operations, and certified the robustness and validity of the model in diversified computational scenarios without relying on empirical biases from a pre-existing dataset.

5. Results and Discussion

Homomorphic Correctness Validation Results Table 1 presents the results of the homomorphic correctness validation, comparing the ciphertext product with the corresponding plaintext product. The simulation was conducted under the input parameters N, q, and scale factor Δ.

5.1 Numerical Results

As a first numerical result, the validation of homomorphic correctness is presented. As shown in Figure 1, a reduced set of inputs consisting of two representative cases extracted from these parameter ranges is summarized. The systematic analysis of random numbers within the domains established by the Institute of Electrical and Electronics Engineers made it possible to identify, on the one hand, the intervals where homomorphic correctness is guaranteed during the execution of the model and, on the other hand, those ranges where modular overflow occur.

This analysis constitutes a fundamental methodological step prior to the proposed security evaluations. Consequently, the value intervals that lack homomorphic correctness or exhibit modular overflow are excluded as viable configurations for tests aimed at evaluating their resistance against BKZ (Block Korkin-Zolotarev) attacks, with the objective of determining the model security level.

© IEOM Society International

Table 1. Homomorphic correctness validation results in the Proposed model simulation

Input a	Input b	Plaintext Product	Decrypted Product	Total error	Homomorphic correctness	Modular boundary
Domain 1: baseline behavior						
2.0	3.0	6.0	5.98715	0.01285	Valid	Secure
2.5	4.0	10.0	9.99768	0.00232	Valid	Secure
Domain 2: Hight sensitivity						
0.33333	3.0	0.99521	0.99999	0.00478	Valid	Secure
0.5	0.5	0.25159	0.25	0.00159	Valid	Secure
Domain 3: Architectural boundaries						
7.0	7.0	49.0	48.95578	0.04422	Valid	Secure
16384.0	16384.0	268435456.0	-0.00256	268435456.0	Fail	Overflow
Domain 4: Identity and zeros						
0.00001	0.00001	0.0	-0.00238	0.00238	Valid	Secure
1.0	1.0	1.0	0.99454	0.00546	Valid	Secure
Domain 5: Extreme asymmetry						
8192.0	4.0	32768.0	-8.0112	32776.0112	Fail	Overflow
1000000.0	0.001	1000.0	-284.62845	1284.62845	Fail	Overflow
Domain 6: Strict compliance						
0.1	0.1	0.1	0.00729	0.00271	Valid	Secure
0.6	0.6	0.36	0.35916	0.00084	Valid	Secure

As a second numerical result proposed model security verification results shown in Table 2 display the security verification results of the proposed model with parameters N —polynomial degree — and q — modulus —, yielding the corresponding verification values of β — block size — and λ —security level.

As a result of subjecting the model to the BKZ algorithm, using random test cases selected from the previously determined valid ranges (Table 1) — which neither compromise homomorphic correctness nor exhibit modular overflow — it was determined that for all cases presented in Table 2, the block size is $\beta = 983$ and the achieved security level is $\lambda = 287.0$. These results were obtained using the values base parameters $N = 4096$ and $q = 2^{15} = 32768$.

Table 2. Verification results of parameter β to determine the security level λ.

Sample (n)	Input a	Input b	Plaintext Product	Decrypted Product	Total error
1	1.82	2.12	3.8584	3.6797	0.17871
2	2.22	2.91	6.4602	6.5195	0.05933
3	3.19	1.70	5.4230	5.5273	0.10434
4	1.57	3.53	5.5421	5.9844	0.44228
5	3.44	2.54	8.7376	9.0156	0.27802
6	2.09	2.60	5.4340	5.5625	0.12850
7	2.12	2.36	5.0032	5.1836	0.18039
8	2.65	2.72	7.2080	6.7617	0.44628
9	3.52	3.58	12.6016	12.6758	0.07418
10	2.28	2.98	6.7944	6.4414	0.35299
11	1.44	1.10	1.5840	1.3047	0.27931

© IEOM Society International

Sample (n)	Input a	Input b	Plaintext Product	Decrypted Product	Total error
12	1.61	3.77	6.0697	5.9141	0.15564
13	3.10	1.50	4.6500	4.8438	0.19375
14	3.50	1.61	5.6350	5.8438	0.20875
15	2.79	1.74	4.8546	5.0391	0.18446
16	1.83	1.57	2.8731	2.9297	0.05659
17	2.64	1.93	5.0952	5.4258	0.33058
18	1.30	1.74	2.2620	2.6914	0.42941
19	3.70	1.19	4.4030	4.8008	0.39778
20	3.23	1.10	3.5530	4.0312	0.47825

5.2 Graphical Results

In order to identify the trade-off space between NIST security and approximate homomorphic correctness, an analysis of their compliance ranges was conducted, resulting in the following Figure 2 as a function of the modulus q and the polynomial degree N.

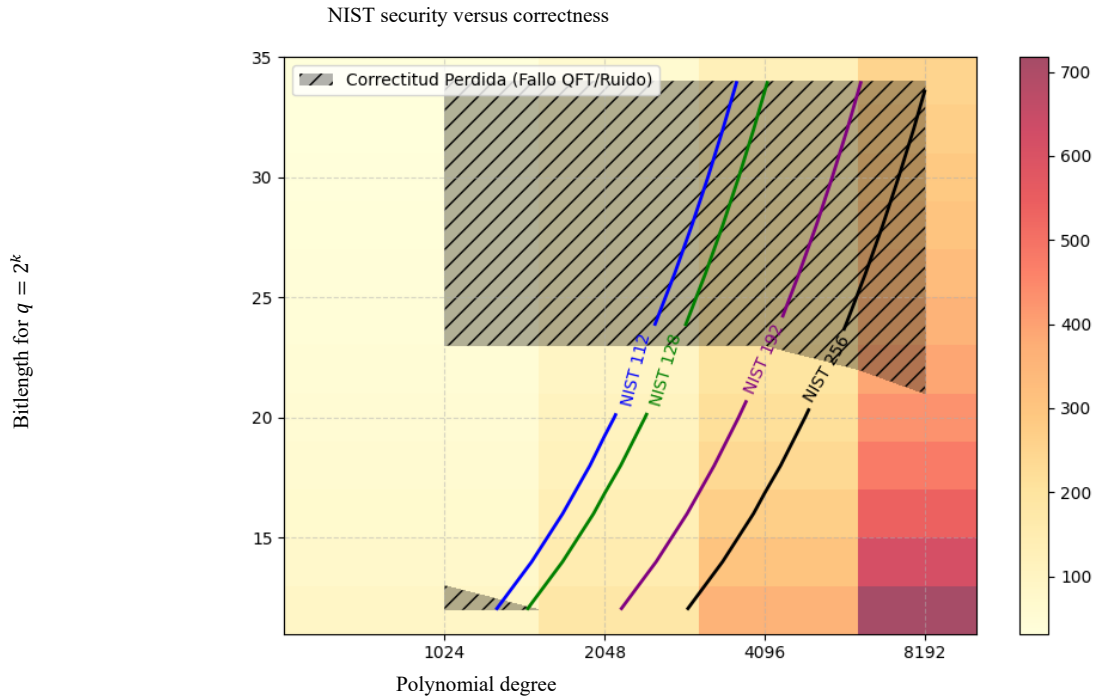
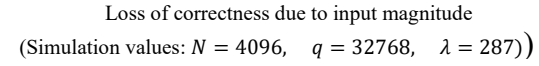


Figure. 2. Parametric heatmap of NIST security and approximate homomorphic correctness of the proposed model.

In other hand, the impact analysis of cryptographic noise growth on modular overflow boundaries and security level preservation shown in Figure 3 illustrates the range within which approximate homomorphic correctness is maintained relative to the multiplication input parameters. This result was obtained by tabulating the total error as a function of the input values a and b for specific values of N and q.



© IEOM Society International

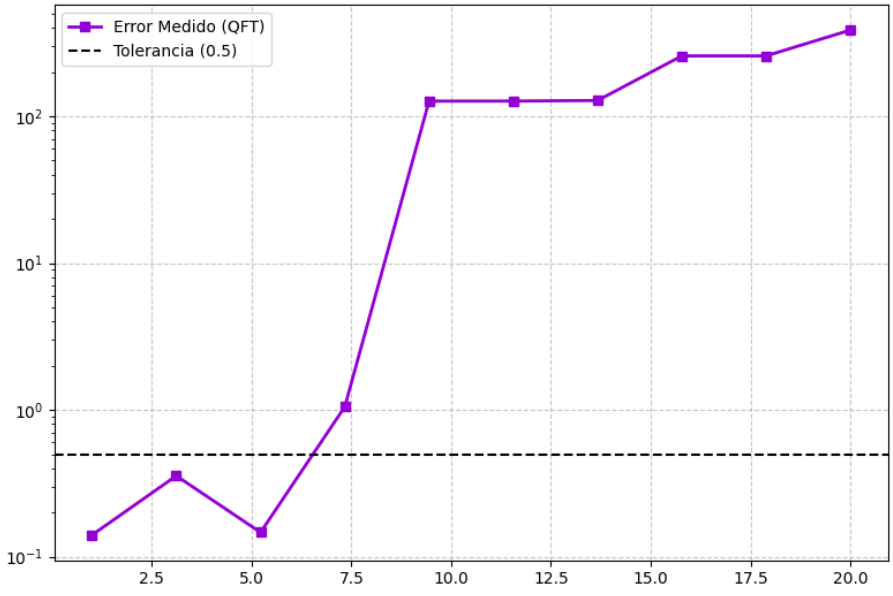


Figure 3. Dynamics of total error based on input values of quantum multiplication.

5.3 Proposed Improvements

Future work includes exploring other classical and quantum cryptosystems to contrast results regarding the trade-off between security level, homomorphic correctness, and noise propagation, as well as evaluating architectures that exceed the NIST Level 5 standard and analyzing the parameterization of the cryptosystem used. Additionally, future efforts involve deepening the processing of expanded input magnitudes to mitigate their inherent computational overhead, and evaluating hybrid secure multiplication models using exact cryptosystems, such as BGV and BFV, combined with quantum techniques.

5.4 Validation

To validate the reliability, correctness, noise behavior, and cryptographic resilience of the proposed hybrid quantum-classical model, empirical and security validation tests were conducted.

First, an empirical boundary and noise identification validation was performed. During the systematic random sweep across the established domains, noise propagation within the encrypted multiplication pipeline was closely monitored. The core input parameters—specifically the polynomial degree ($N = 4096$) and the modulus ($q = 2^{15} = 32768$)—were identified as the critical control variables for effective noise management. The validation confirms that restricting input parameters to the designated non-overflow intervals successfully bounds the noise growth, guarantees consistent homomorphic correctness, and prevents decryption failures caused by modular overflow.

Second, security consistency validation was assessed by subjecting multiple random test instances—selected strictly from these verified operational ranges—to the BKZ algorithm. The validation demonstrates uniform cryptographic stability across all test cases, consistently yielding a block size of $\beta = 983$ and a security level of $\lambda = 287.0$. These combined metrics empirically and analytically confirm that the model maintains both strict mathematical precision, optimal noise containment, and robust resistance against lattice attacks.

6. Conclusion

The quantum model preserves the approximate homomorphic correctness of ciphertext multiplication operations intact upon contrasting the product results in the quantum domain with the plaintext results. Homomorphic correctness is guaranteed when the size of the polynomial coefficients remains below the maximum boundary of the modulus q, thereby neutralizing the risk of data corruption due to modular overflow.

© IEOM Society International

A quantum model that preserves security and confidentiality in ciphertext multiplication has been successfully designed, demonstrating that for parametric ranges of N >= 4096 and a modulus q = 32768 (15 bits), the model provides resistance against attacks exceeding Level 5 of the NIST standard. This prioritization of security profiles the model to operate with high precision over bounded arithmetic magnitudes. Cryptographic noise growth constitutes the central factor in the balance between the arithmetic capacity and the security of the model.

The analysis demonstrated that its propagation directly conditions the modular overflow boundaries (q/2). Furthermore, any increase in the modulus q intended to absorb this variable degrades the model's resistance against basis reduction attacks (BKZ algorithm). Therefore, to guarantee the preservation of a security level higher than the NIST standard (Level 5), it is concluded that the input magnitudes and the ring dimension must be jointly calibrated, parameterizing the operands within the ranges of a, b ∈ [1, 5] and ensuring N ≥ 4096.

The obtained quantum – classical hybrid model enables the secure multiplication of ciphertexts by integrating the QFT into the homomorphic evaluation stage of the classical CKKS cryptosystem. This convergence is founded on the intrinsic compatibility between the polynomial representation generated by the CKKS cryptosystem and the input vector structure required by the QFT. As avenues for future research, we plan to expand the comparative analysis to other classical and quantum cryptosystems, examining in depth the existing trade-off between homomorphic correctness, the inherently associated noise propagation, and the resulting level of security. Furthermore, efforts will focus on mitigating the computational overhead derived from processing expanded input magnitudes and on exploring models that combine quantum techniques with exact cryptosystems.

References

Biamonte, J. D., et al., Implementing semiclassical Szegedy walks in classical–quantum circuits for homomorphic encryption, *arXiv preprint*, arXiv:2412.01966, 2024.

Broadbent, A. and Jeffery, S., Quantum homomorphic encryption for circuits of low T-gate complexity, *Advances in Cryptology – CRYPTO 2015*, pp. 609-629, 2015.

Chen, Y. and Nguyen, P. Q., BKZ 2.0: Better lattice security estimates, *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 1-20, 2011.

Cheon, J. H., Kim, A., Kim, M. and Song, Y., Homomorphic encryption for arithmetic of approximate numbers, *Advances in Cryptology – ASIACRYPT 2017*, vol. 10624, pp. 409-437, Springer, 2017.

Faneela, Ahmad, J., Ghaleb, B., Jan, S. U. and Buchanan, W. J., Cross-platform benchmarking of the FHE libraries: novel insights into SEAL and OpenFHE, *arXiv preprint arXiv:2503.11216*, 2025.

Gao, S., Huang, R.-C., Liu, B.-X., Cheng, Z.-W., Xie, H.-L., Zhang, Z.-X. and Yang, Y.-G., Quantum algorithm for polynomial multiplication and its applications, *EPJ Quantum Technology*, vol. 12, no. 119, 2025.

Gentry, C., Fully homomorphic encryption using ideal lattices, *STOC*, 2009. Katz, J. and Lindell, Y., *Introduction to Modern Cryptography*, 3rd Edition, CRC Press, Boca Raton, 2020.

Kim, S., et al., Accelerating number theoretic transformations for bootstrappable homomorphic encryption on GPUs, *Proceedings of the 2020 IEEE International Symposium on Workload Characterization (IISWC)*, IEEE, 2020.

Koblitz, N., *A Course in Number Theory and Cryptography*, 2nd Edition, Springer-Verlag, New York, 1994.

Li, Z.-Z., Zhang, Z., Li, Y.-J. and Wang, D.-F., Multi-party quantum homomorphic encryption scheme based on quantum teleportation, *Journal of Information Security and Applications*, vol. 93, no. 104157, 2025.

Lyubashevsky, V., Peikert, C. and Regev, O., On ideal lattices and learning with errors over rings, *Journal of the ACM*, vol. 60, no. 6, pp. 1-35, 2013. Mahadev, U. and Brakerski, Z., Analysis of quantum fully homomorphic encryption schemes (QFHE) and hierarchical memory management for QFHE, *IEEE Transactions on Quantum Engineering*, vol. 2, pp. 1-15, 2021.

Ma, S., Zhu, C., Quan, D., and Nie, M., A Distributed Architecture for Secure Delegated Quantum Computation, Entropy, vol. 24, no. 6, Article 794, 2022. doi:10.3390/e24060794.

Mahadev, U. and Brakerski, Z., Analysis of quantum fully homomorphic encryption schemes (QFHE) and hierarchical memory management for QFHE, *IEEE Transactions on Quantum Engineering*, vol. 2, pp. 1-15, 2021.

Nielsen, M. and Chuang, I., *Quantum Computation and Quantum Information*, Cambridge University Press, 2010.

Oppenheim, A. V., Willsky, A. S. and Nawab, S. H., *Signals & Systems*, 2nd Edition, Prentice Hall, Upper Saddle River, NJ, 1997. Regev, O., On lattices, learning with errors, random linear codes, and cryptography, *Journal of the ACM*, vol. 56, no. 6, 2009.

Regev, O., On lattices, learning with errors, random linear codes, and cryptography, *Journal of the ACM*, vol. 56, no. 6, 2009.

© IEOM Society International

Rivest, R. L., Adleman, L. M. and Dertouzos, M. L., On Data Banks and Privacy Homomorphisms, *Foundations of Secure Computation*, Academic Press, pp. 169-180, 1978.

Ruiz-Perez, L. and Garcia-Escartin, J. C., Quantum arithmetic with the quantum Fourier transform, *Quantum Information Processing*, vol. 16, no. 6, p. 152, 2017.

Savadatti, S., Cherukuri, A. K., Jonnalagadda, A. and Vasilakos, A. V., Analysis of quantum fully homomorphic encryption schemes (QFHE) and hierarchical memory management for QFHE, *Complex & Intelligent Systems*, vol. 11, no. 264, pp. 1-28, 2025, https://doi.org/10.1007/s40747-025-01851-7.

Tebaa, M., El Hajji, S. and El Ghazi, A., Homomorphic encryption applied to the cloud computing security, *Proceedings of the World Congress on Engineering*, vol. 1, pp. 4-6, 2012.

Biographies

Dr. Lauro Enciso Rodas is the Rector of the National University of San Antonio Abad del Cusco (UNSAAC), Peru, for the 2026–2031 term. He got a Master of Science degrees in Computer Science at Western Illinois University (USA) in Computer Engineering at University of Central Florida (USA), a Doctoral degree in Systems Engineering at National University of Federico Villarreal (Peru). He is a Full Professor at UNSAAC since 1977 and previously served as Dean of the Faculty of Electrical, Electronic, Informatics, and Mechanical Engineering, where he contributed to academic management, graduate education, and research development. He played a leading role in establishing the Master's and Doctoral programs in Computer Science at UNSAAC, significantly strengthening graduate education and research capacity in southern Peru. Dr. Enciso Rodas is an active researcher with an ORCID iD (0000-0001-6266-0838) and a Scopus Author ID (57192392387). His research has been published in IEEE conferences, the International Conference on Industrial Engineering and Operations Management (IEOM), CEUR Workshop Proceedings, and other international venues, with research contributions in artificial intelligence, computer vision, convolutional neural networks, clustering algorithms, operations research, cloud computing, digital transformation, and information systems. He has supervised undergraduate and graduate theses and has participated in institutional and interdisciplinary research projects focused on scientific innovation and technological development. Fluent in Spanish, English, Quechua, and Italian, Dr. Enciso Rodas actively promotes international collaboration, scientific research, technological innovation, and academic excellence as key pillars of UNSAAC's strategic development.

Karla Cathernie Rojas Pedraza holds a Master of Science in Informatics from the National University of San Antonio Abad del Cusco (UNSAAC), Peru, where she is a Professor in the Department of Informatics and Systems Engineering. Prior to joining academia, she held leadership positions as an Information Technology Auditor in the Peruvian financial sector, with responsibilities in information security, cybersecurity, IT governance, business continuity, regulatory compliance, and technology risk management. Her research interests include cybersecurity, homomorphic encryption, quantum computing, post-quantum cryptography, privacy-preserving computation, and secure data processing. Her current research focuses on the design of hybrid classical–quantum models for secure computation over encrypted data, with applications in cloud computing and critical information systems.

© IEOM Society International