Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1781–1790
DOI : 10.47974/JDMSC-2178

Design and deployment of cryptographic systems for quantum-secure cloud applications

Shikha Bhardwaj *
Department of Engineering Science
Bharati Vidyapeeth's College of Engineering
Pune 412115
Maharashtra
India

Shuchita Vaidya †
Symbiosis School for Online and Digital Learning
Symbiosis International University
Pune 411016
Maharashtra
India

Neha Shahare §
Department of Electronics and Telecommunication
KJEI'S KJ College of engineering Management and Research
Pune 411048
Maharashtra
India

Shantanu Pandurang Kanade ‡
Symbiosis School for Online and Digital Learning
Symbiosis International Deemed University
Pune 411016
Maharashtra
India

* *E-mail:* shikha.shrivas@bharatividyapeeth.edu (Corresponding Author)
† *E-mail:* pc.hss@ssodl.edu.in
§ *E-mail:* nehashahare.kjcoemr@kjei.edu.in
‡ *E-mail:* shantanu.kanade@ssodl.edu.in

© Taru Publications

Uday Shankar Patil [@]
Department of Civil Engineering
Bharati Vidyapeeth's College of Engineering
Lavale
Pune 412115
Maharashtra
India

Atre Pradeep Prabhakar [#]
Department of Engineering Science
Bharati Vidyapeeth's College of Engineering
Pune 411043
Maharashtra
India

Abstract

Conventional cryptographic frameworks are in threat since quantum computing is getting way better and quicker. This can be why quantum-secure cryptographic arrangements for cloud apps have to be be made and utilized. This paper looks at how to form and utilize quantum-resistant encryption frameworks that are culminate for safe computer settings. To begin with, we see at how current security strategies can be broken by quantum assaults. At that point, we list the foremost vital conditions for quantum-resistant alternatives. At that point, we see at distinctive post-quantum security strategies, such as hash-based, code-based, and lattice-based ones, to see how well they work and whether they are suitable for cloud computing. The arrange for rollout incorporates including these quantum-secure strategies to cloud frameworks that are as of now in put. This will cause less unsettling influence whereas expanding security. We conversation around genuine issues like how well the calculation works, how well it works with existing frameworks, and how well it can be scaled up. Case thinks about appear both the issues that came up and the arrangements that were found amid the switch to quantum-secure cryptography. The proposed model about appear how vital it is to be proactive around securing cloud apps against future quantum dangers. They moreover provide analysts and specialists a total system for building solid cryptographic frameworks in a world after quantum computing.

Subject Classification: *68M01.*

Keywords: *Quantum-secure cryptography, Post-quantum security methods, Hash-based encryption, Lattice-based cryptography, Cloud computing security.*

[@] *E-mail:* **uday.patil@bharatividyapeeth.edu**
[#] *E-mail:* **pradeep.atre@bharatividyapeeth.edu**

1. Introduction

Quantum computing may be a colossal step forward within the control of computers, but it moreover postures huge issues for the field of cryptography. Quantum calculations like Shor's and Grover's are a coordinate threat to conventional security calculations that depend on how difficult it is to illuminate certain numerical issues. These calculations might make current encryption strategies futile [1]. Since cloud computing is presently a vital portion of advanced innovation, it is exceptionally important to keep it secure from modern threats. Since quantum computers could be able to break common cryptographic conventions, it is imperative to be proactive about creating and propelling quantum-resistant cryptographic frameworks that work well within the cloud [2],[3]. This article talks almost how to create and utilize quantum-secure security frameworks to settle the issues that quantum computing causes. To begin with, we see at the essential thoughts behind quantum computing and what they cruel for current security benchmarks. After that, we see at post-quantum security strategies, such as hash-based, code-based, and lattice-based plans, and choose on the off chance that they can be utilized in cloud frameworks [4]. The objective is to form it simple to include these progressed strategies to current cloud instruments without influencing speed or security. This incorporates genuine issues like framework design and operation. This consider looks at case ponders and execution strategies to allow a full direct on how to secure cloud applications in a post-quantum world, which can make beyond any doubt they are well ensured against future quantum dangers [5].

2. Quantum Computing and Cryptographic Protocol

2.1 *Shor's Algorithm and Public-Key Cryptography*

Dwindle Shor, a researcher, made Shor's Calculation in 1994. It may be a major risk to public-key security frameworks. Cutting edge advanced frameworks depend on public-key cryptography, which employments the reality that it's difficult to figure huge numbers or fathom discrete logarithms, to keep communication secure [8].

Shor's Algorithm and Public-Key Cryptography Model

Finding the prime factors of a composite number N is the objective of Shor's Algorithm, which was developed by Shor. This is delivered in the form of:

$$N = p1^{e1} * p2^{e2} * \dots * pk^{ek} \quad (1)$$

Shor's Algorithm relies on finding the period r of a function f(x) modulo N. The function is defined as:

$$f(x) = a^x mod\ N \quad (2)$$

To find the period r, Shor's Algorithm uses quantum parallelism to create a superposition of states:

$$\left(\frac{1}{sqrt(Q)}\right) * \Sigma_{\{x=0\}}^{\{Q-1\}|x\rangle} \otimes |a^x mod\ N\rangle \quad (3)$$

The quantum Fourier transform is used to extract the period r. The QFT of the state |x⟩ is given by:

$$QFT|x\rangle = \left(\frac{1}{sqrt(Q)}\right) * \Sigma_{\{k=0\}}^{\{Q-1\}} e^{\frac{2\pi i x k}{Q}} |k\rangle \quad (4)$$

Upon measurement, the result provides an approximate value of k. The period r is then found by solving:

$$k = \frac{m * r}{Q} \quad (5)$$

6. Factoring the Number

Once the period r is obtained, it is used to factor N by finding the greatest common divisor (gcd) of N and:

$$\gcd\left(a^{\frac{r}{2}} - 1, N\right) and \gcd\left(a^{\frac{r}{2}} + 1, N\right) \quad (6)$$

These gcd calculations yield the non-trivial factors of N.

2.2 *Grover's Algorithm and Symmetric Key Cryptography*

Lov Grover came up with Grover's Algorithm in 1996. It is different from symmetric key cryptography in a way [6]. Grover's Algorithm can very quickly cut down on the time needed to do a brute-force search on protected data, but it's not as powerful as Shor's Algorithm [7]. In particular, it lets quantum computers search a library that isn't organized or brute-force an encryption key in a way that is close to the square root of the number of possible keys.

Grover's Algorithm and Symmetric Key Cryptography Model

The initial state is a uniform superposition of all possible keys, expressed as:

$$|\psi\rangle = \left(\frac{1}{\sqrt{(N)}}\right) * \Sigma_{\{k=0\}}^{\{N-1\}|k\rangle} \quad (7)$$

The oracle operator O flips the sign of the amplitude for the correct key k*. It can be described by:

$$O|k\rangle = (-1)^{f(k)}|k\rangle \quad (8)$$

where $f(k) = 1\ if\ E(K,x) = C$ (i.e., k is the correct key), and f(k) = 0 otherwise.

The diffusion operator D amplifies the amplitude of the correct key. It can be expressed as:

$$D = 2|\psi\rangle\langle\psi| - I \quad (9)$$

$$D = 2 * \left(\frac{1}{N}\right) * \Sigma_{\{i=0\}}^{\{N-1\}} \Sigma_{\{j=0\}}^{\{N-1\}} |i\rangle\langle j| - I \quad (10)$$

Applying the oracle O and diffusion operator D iteratively to the state, we get:

$$|\psi'\rangle = D * O * |\psi\rangle \quad (11)$$

The number of iterations θ required is approximately:

$$\theta = \frac{\pi}{4} * \sqrt{\left(\frac{N}{M}\right)} \quad (12)$$

After θ iterations, the probability of measuring the correct key is given by the amplitude squared:

$$P(k*) = |\langle k* | (D * O)\hat{}\theta \, |\psi\rangle|\hat{}2 \quad (13)$$

The probability of finding the correct key upon measurement is maximized by:

$$P(k*) = \left(\frac{1}{N}\right) * \left[1 - \cos\left(\frac{2\pi M}{N}\right)\right] \quad (14)$$

The expected value E of the number of iterations needed to find the key can be expressed as:

$$E = \left(\frac{N}{M}\right) * \left[\frac{\pi}{4} * \sqrt{\left(\frac{N}{M}\right)}\right] \quad (15)$$

The evolution of the quantum state after t iterations of the operator U can be expressed by:

$$|\psi(t)\rangle = U^t * |\psi(0)\rangle \quad (16)$$

3. Design Considerations for Quantum-Secure Systems

Adding quantum-secure algorithms to systems that are already in place needs careful planning and changes to make sure that everything works well and is safe. Quantum-secure methods, like hash-based, code-based, or lattice-based encryption schemes, are made to protect against threats using quantum computers [9], [10].

$$SVP(L) = v \in L\{0\} min \parallel v \parallel \quad (17)$$

Their merging into current systems, which mostly use old-fashioned secure ways, is, however, very difficult. The first step is to see if these methods can work with the standards and facilities that are already in place.

$$\frac{d}{nd}\left[1 - \exp\left(-\frac{n2}{2b+1}\right)\right] = \frac{n}{2b+1} \exp\left(-\frac{n2}{2b+1}\right) \quad (18)$$

3.1 *System Architecture and Design Principles*

Quantum-secure frameworks have to be built with scale, speed, and in reverse compatibility in intellect when they are arranged out. Executing calculations that offer efficient computing and capacity needs is one of the foremost imperative things to think around, since quantum-resistant strategies can utilize more assets than their conventional adaptations, the framework engineering appeared in figure 1. The plan of the framework ought to incorporate secure ways to handle keys and customary overhauls to keep up with changes in quantum technology.

Solid testing and endorsement strategies are too required to create beyond any doubt that the modern strategies work well in an extend of working circumstances and do not make any new security gaps. The common plan ought to put both keeping working effectiveness and ensuring against quantum dangers within the future at the best of the list.

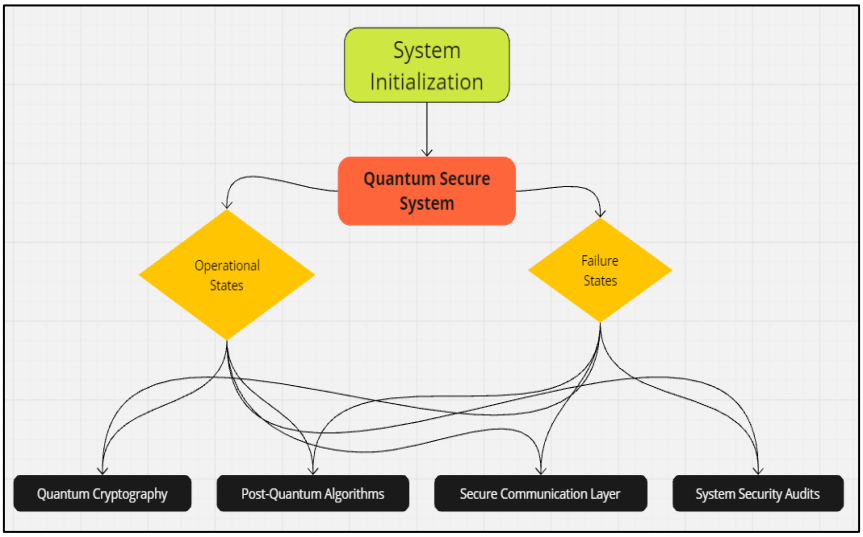


Figure 1
Overview of System Architecture

4. Deployment Model

4.1 *Transitioning from Classical to Quantum-Secure Systems*

Moving from conventional to quantum-secure frameworks could be a prepare that happens over time and has several critical steps. To begin with, businesses have to be take a see at their current security scene and figure out which frameworks have to be updated or supplanted [11]. This needs a cautious see at current measures and how effortlessly they can be broken by quantum assaults. After that, businesses got to choose and attempt quantum-secure strategies that meet their proficiency and security needs.

4.2 *Hybrid Approaches*

Combining quantum-safe calculations with standard encryption strategies is what crossover strategies do. They make a bridge between classical and quantum-resistant security. Amid the exchange stage, this strategy lets companies utilize the most excellent parts of both conventional and quantum-secure strategies.

$$EncHybrid(m, kLattice, kAES) = EncLattice(kAES, kLattice) \parallel EncAES(m, kAES)$$

In half breed frameworks, quantum-resistant calculations are utilized for modern or touchy assignments, whereas conventional strategies are kept for more seasoned frameworks. By gradually getting freed of strategies that aren't secure, this approach makes a difference control hazard by changing to modern security needs.

$$S = \min\big(H(kLattice), H(kAES)\big)$$

5. Evaluation and Testing

The table 1 appears a comparison between a classical calculation (RSA) and a quantum-secure calculation (Lattice-Based Encryption), centered on critical execution measures such as throughput, key estimate, encryption speed, translating speed, scaling, and integration exertion.

Table 1
Result Comparison between Classical Algorithm (RSA) And A Quantum-Secure Algorithm

Test Parameter	Quantum-Secure Algorithm	Classical Algorithm
Algorithm Name	Lattice-Based Encryption	RSA
Throughput (ops/sec)	5000	10000
Key Size (bits)	512	2048
Encryption Speed (MB/s)	30	60
Decryption Speed (MB/s)	28	58
Scalability	90	80
Integration Effort	60	30

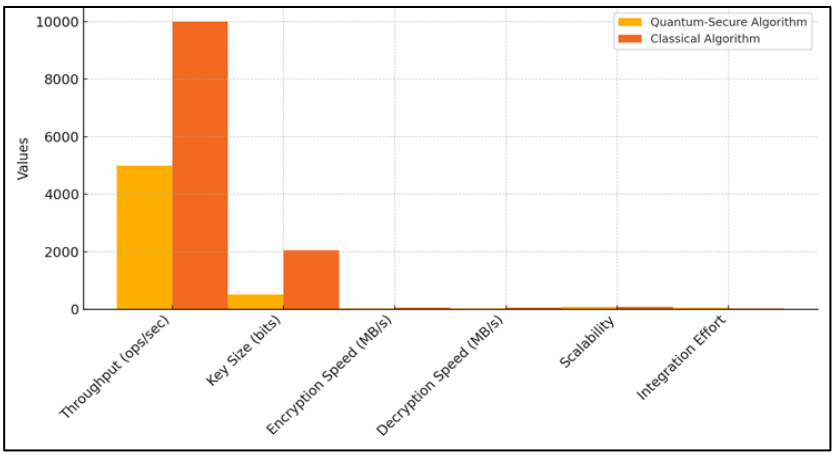
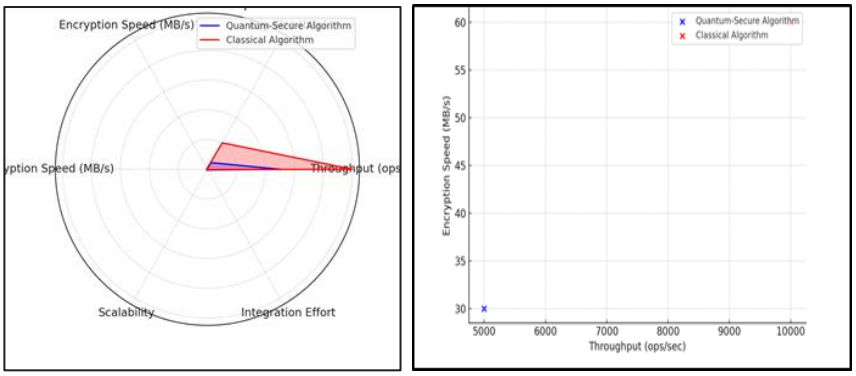


Figure 2
Comparing various parameters between the Quantum-Secure and Classical Algorithms

The quantum-secure lattice-based encryption calculation can as it were handle 5,000 operations per moment, whereas the standard RSA strategy can handle 10,000 operations per moment.



(a) **(b)**

Figure 3
Representation of (a) Key Size and Throughput (b) Throughput vs Encryption Speed

In terms of genuine computing speed, this implies that RSA is as of now more productive. Key Measure tells you how huge the encryption key is in bits, appeared in figure 2. The key estimate for lattice-based encryption is as it were 512 bits, whereas the key measure for RSA is 2,048 bits. Speed of Encryption and Unscrambling appears how quick information can be secured and decoded. With speeds of 60 MB/s and 58 MB/s, separately, RSA is quicker at both scrambling and decoding than lattice-based encryption, which is 30 MB/s and 28 MB/s. This appears how well RSA works at scrambling and unscrambling information outline in figure 3 (a) and (b).

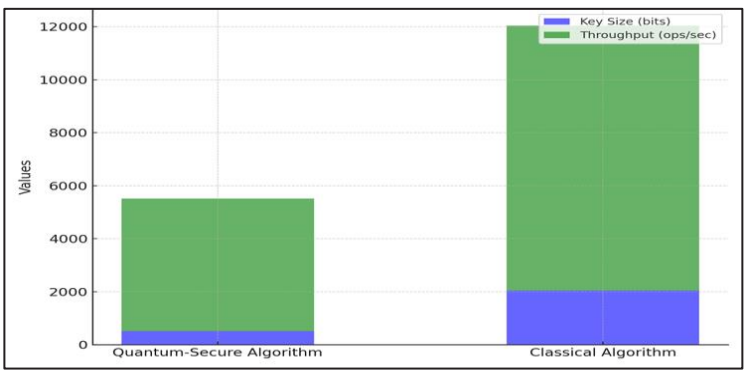


Figure 4
Compare Key Size and Throughput together for each algorithm

The quantum-secure strategy gets a better score for adaptability (90) than RSA does (80) as shown in figure 4. This means that lattice-based encryption can be superior at taking care of more work or greater records, which is

important as the sum of information increments. Integration Exertion figures out how difficult it'll be to include the strategy to current frameworks and how much work it'll take. When compared to lattice-based encryption (60), RSA is less demanding to combine (30). This implies that whereas lattice-based encryption might give way better security within the future, it is harder to utilize and requires more assets right presently.

6. Conclusion

The move to quantum-secure cryptographic systems is fundamental for protecting cloud applications against the potential threats posed by quantum computing. This paper has explored the integration of quantum-secure calculations, such as lattice-based encryption, into existing cloud establishments, highlighting the require for cautious thought of execution, security, and comfort. Quantum-secure systems offer a overwhelming defense against future quantum ambushes, in show disdain toward of the reality that they show challenges in terms of utilization complexity and integration effort. Effective course of action models, tallying hybrid approaches, donate a pathway for organizations to move effectively from classical to quantum-secure cryptographic methodologies. By leveraging hybrid models, organizations can calm perils in the midst of the move organize though moving forward their security posture. The comparative examination of execution estimations between quantum-secure and classical calculations underscores the trade-offs between provoke capability and long-term security benefits. As quantum computing development impels, contributing in quantum-secure cryptographic courses of action will be critical for keeping up the insight and protection of cloud-based systems.

References

[1] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, "600-km repeater-like quantum communications with dual-band stabilization," *Nat. Photonics,* vol. 15, pp. 530–535 (2021).

[2] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W\.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu et al., "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nat. Photonics*, vol. 15, pp. 570–575 (2021).

[3] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W\.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang et al., "Quantum Key Distribution over 658 km Fiber with Distributed Vibration Sensing," *Phys. Rev. Lett.*, vol. 128, p. 180502 (2022).

[4] A. Aguado, E. Hugues-Salas, P. A. Haigh, J. Marhuenda, A. B. Price, P. Sibson, J. E. Kennard, C. Erven, J. G. Rarity, M. G. Thompson et al., "Secure NFV Orchestration over an SDN-Controlled Optical Network with Time-Shared Quantum Key Distribution Resources," *J. Light. Technol.,* vol. 35, pp. 1357 (2017).

[5] R. N. Wadibhasme, A. U. Chaudhari, P. Khobragade, H. D. Mehta, R. Agrawal, and C. Dhule, "Detection and prevention of malicious activities in vulnerable network security using deep learning," in Proc. 2024 Int. Conf. Innovations Challenges Emerging Technol. (ICICET), Nagpur, India, pp. 1–6 (2024), doi: 10.1109/ICICET59348.2024.10616289.

[6] M. A. Khan, H. Alhakami, W. Alhakami, A. V. Shvetsov, and I. Ullah, "A smart card-based two-factor mutual authentication scheme for efficient deployment of an IoT-based telecare medical information system," *Sensors*, vol. 23, p. 5419 (2023).

[7] J. Lee, J. Oh, D. Kwon, M. Kim, K. Kim, and Y. Park, "Blockchain-enabled key aggregate searchable encryption scheme for personal health record sharing with multi-delegation," *IEEE Internet Things J.*, vol. 11, pp. 17482–17494 (2024).

[8] V. Sucasas, G. Mantas, M. Papaioannou, and J. Rodriguez, "Attribute-based pseudonymity for privacy-preserving authentication in cloud services," *IEEE Trans. Cloud Comput.*, vol. 11, pp. 168–184 (2023).

[9] S. N. Ajani, P. Khobragade, P. V. Jadhav, R. A. Mahajan, B. Ganguly, and N. Parati, "Frontiers of Computing - Evolutionary Trends and Cutting-Edge Technologies in Computer Science and Next Generation Application," *J. Electr. Syst.,* vol. 20, no. 1s (2024). [Online]. Available: https://doi.org/10.52783/jes.750

[10] H. Wang, J. Liang, Y. Ding, S. Tang, and Y. Wang, "Ciphertext-policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health," *Comput. Stand. Interfaces,* vol. 84, p. 103696 (2023).

[11] D. Goyal, A. Kumar, Y. Gandhi, and V. Khetani, "Securing wireless sensor networks with novel hybrid lightweight cryptographic protocols," *J. Discrete Math. Sci. Cryptogr.*, vol. 27, no. 2-B, pp. 703–714 (2024), doi: 10.47974/JDMSC-1921.

Received November, 2024