Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1703–1712
DOI : 10.47974/JDMSC-2170

Real-world applications of quantum computing for cryptographic key generation

Monica Kalbande [†]
Department of Electronics Engineering
Yeshwantrao Chavan College of Engineering
Nagpur 441110
Maharashtra
India

Meghana Lokhande *
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Pune 411044
Maharashtra
India

Amruta Mhatre [§]
Department of Computer Science Engineering and Data Science
St. John College of Engineering and Management
Palghar
Maharashtra
India

Araddhana Arvind Deshmukh [‡]
Department of Computer Science & Information Technology (Cyber Security)
Symbiosis Skill and Professional University
Pune 412101
Maharashtra
India

[†] *E-mail:* monicakalbande@gmail.com
* *E-mail:* meghana.lokhande@pccoepune.org (Corresponding Author)
[§] *E-mail:* amrutam@sjcem.edu.in
[‡] *E-mail:* aadeshmukhskn@gmail.com

Prashant Ashok Patil [@]
Department of Mechanical Engineering
Dr. D. Y Patil Institute of Technology
Pune 411018
Maharashtra
India

Pragya Maheshwari [#]
Department School of Management and Technology
Ramdeobaba University
Nagpur 440013
Maharashtra
India

Abstract

Using the rules of quantum physics to improve security protocols, quantum computing has the Quantum computing has the potential to fundamentally alter how cryptography keys are made. Classical computers have a difficult time dealing with discrete logarithms or figuring huge numbers, which are illustrations of troublesome scientific issues that are utilized in conventional cryptography. Quantum computers, on the other hand, utilize quantum superposition and ensnarement to handle gigantic sums of information at once, which may make these ancient security strategies futile. For illustration, Shor's strategy makes it conceivable to figure huge numbers in polynomial time, which is terrible for RSA security. Quantum key conveyance (QKD), on the other hand, could be a totally other way to do things. It employments quantum trap to securely send cryptographic keys, making beyond any doubt that any endeavour to tune in in changes the quantum state, appearing that somebody is there. Putting QKD and other quantum-safe strategies to utilize in genuine life can make communication networks much more secure against future quantum dangers. Quantum computing is additionally thought to create it possible to form unused cryptographic strategies that utilize quantum standards to form them more secure and more proficient. As quantum innovation makes strides, it'll be imperative to include these quantum-based strategies to current security frameworks to keep information secure from modern computer powers and keep solid cryptographic guards.

Subject Classification: *68M25.*

Keywords: *Quantum key distribution (QKD), Quantum cryptography, Post-quantum cryptography, Quantum random number generation (QRNG), Quantum algorithms, Quantum entanglement, Quantum superposition.*

[@] *E-mail:* **prashant.p@dypvp.edu.in**
[#] *E-mail:* **pragyarathi2811@gmail.com**

1. Introduction

Quantum computing may be an enormous alter within the field of data innovation that could have a tremendous effect on numerous regions, counting security [1]. The foremost critical thing almost this alter is that quantum computers can handle information in ways that customary computers can't [2], [3]. Quantum computers make use of quantum bits, also known as qubits, which, due to the phenomenon of superposition, are capable of existing in more than one state at the same time. This is often distinctive from customary frameworks that utilize bits as the essential unit of information [4]. In addition, quantum interaction makes it possible for qubits to be coupled to one another in such a way that the state of one qubit can very quickly modify the state of another qubit, even if the qubits are located at a great distance from one another [5]. Since of these quantum qualities, quantum computers can unravel difficult math issues at speeds that have never been seen some time recently [6]. This might debilitate current encryption frameworks that are implied to keep private information secure. Conventional encryption strategies, like RSA and ECC (Elliptic Bend Cryptography), depend on how hard issues like discrete logarithms and numbers factorization are to illuminate [7], [8]. Quantum calculations, particularly Shor's calculation, can fathom these issues rapidly, in spite of the fact that, which may be a enormous issue for conventional encryption strategies [9]. As a result, quantum key distribution (QKD) has gotten to be a cutting-edge way to share cryptographic keys securely by utilizing quantum mechanics. QKD employments essential thoughts from quantum physics to discover individuals who are tuning in in on discussions. This keeps the key sharing handle genuine and secure [10]. As quantum computing innovation progresses, it'll be essential to include quantum-resistant secure strategies and QKD to current security frameworks in order to keep information secure from future quantum dangers and make sure that security arrangements are solid and adaptable.

2. System Architecture

2.1 *Model Development for Quantum Key Distribution (QKD)*

In this step, we use math to create a model for Quantum Key Distribution (QKD), like the BB84 system, overview of proposed model shown in figure 1. One way to describe a qubit state is as $(|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle)$, where α and β are complex numbers such that $(|\alpha|^2 + |\beta|^2 = 1)$. Measurement in the BB84 protocol involves bases represented by unitary matrices $(U_\theta, \in \theta\ \{0°, 45°, 90°, 135°\}$. The chance $P\{correct\}$ of finding the key right is given by

$$P(correct) = \frac{1}{2}[1 - \frac{1}{2}(1 - \frac{1}{N}\sum_{i=1}^{N} e^{-2\,\lambda\Delta d_i})]$$

where N is the number of transmitted bits, λ is the constriction coefficient, and Δd_i is the remove between Alice and Weave for the i-th qubit. To do the security examination, you have got to unravel differential conditions that appear how the rate of key creation changes with remove R_key:

$$\frac{dR_{key}}{d\,d} = -\eta \cdot R_{key}$$

where η is how well the location strategy works. Once you increase this condition by the association remove, you get:

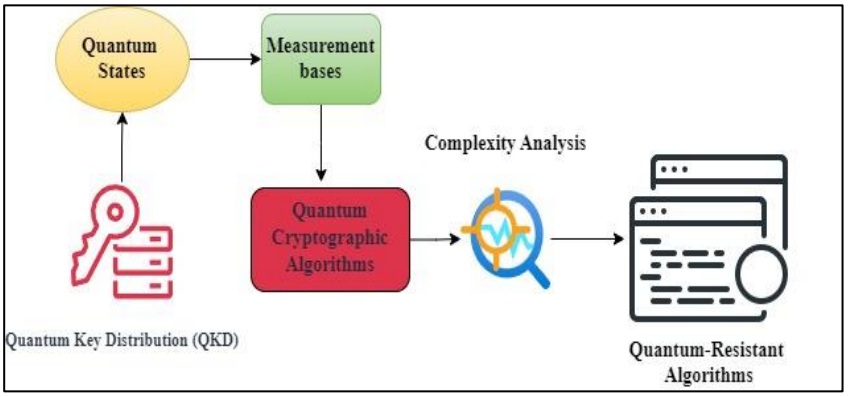

Figure 1
Architectural Block Diagram of Proposed Model

$$R_{key}(d) = R_{key}(0)e^{-\eta d}$$

This show makes a difference us get it how quantum states are sent and checked, as well as how commotion and separate influence key rates.

2.2 *Development Model for Quantum Cryptographic Algorithms*

We make numerical models for quantum cryptographic calculations in this step. One case is Shor's strategy for numbers factorization. Utilizing quantum material science, Shor's strategy rapidly breaks down a huge number N into its prime variables [11]. The most errand of the strategy is to find the period r of a function (f(x)= a^x mod N), where a could be a number picked at arbitrary that's coprime to N. The Quantum Fourier Change (QFT) is utilized to discover the period r, which works on a blend of states:

$$|x\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|k\rangle$$

The QFT is shown by the following matrix:

$$QFT|x\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{2\pi i\, k\, x/\, r}\ |k\rangle$$

The period r can be extracted with high probability, enabling factorization of N. When compared to traditional algorithms, Shor's algorithm is only $O((\,log\ N)^3)$ hard to understand. Differential equations that show the likelihood of different test results can be used to look at the performance:

$$\frac{dP(r)}{d\,t} = -\gamma P(r)$$

where P(r) is the chance of seeing a certain time r and γ is the constant of decay. By integrating this differential equation over time, you can see how well the method works.

2.3 *Quantum-Resistant Algorithms*

This cryptographic method that is unbreakable by quantum computers, like lattice-based cryptography. Although quantum assaults can defeat conventional cryptography systems, these approaches are designed to withstand them [12]. The Most brief Vector Issue (SVP) and the Learning with Blunders (LWE) issue are two illustrations of difficult grid issues that are utilized in scheme-based learning. The issue for LWE is to find the mystery vector s given a set of boisterous direct conditions:

$$A\,s + \ e = \ b$$

where A could be a list of open variables, e may be a clamor vector, and b is the list of values that were really seen. The security of LWE depends on how difficult it is to illuminate this framework, which is appeared by the clamor dispersion and framework measurements.

$$\frac{dE}{dt} = \ -\alpha E$$

The mistake term is indicated by E, and the attenuation constant for the commotion level is given by α. Once you coordinated this condition, you get the mistake bound over time:

$$E(t) = \ E(0)e^{-\alpha t}$$

In expansion, the taking after condition can be utilized to figure out how difficult the grid issue is by assessing how difficult it is to unravel:

$$Complexity \approx 2^{\,dim \cdot log(n)}\text{e}$$

3. Result and Discussion

Classical, quantum, and quantum-resistant encryption systems all work differently, as shown in the table 1. Classical RSA and ECC have low key generation rates and security levels. Because it is exponentially hard to compute, RSA is especially sensitive to quantum attacks. Even though ECC is more efficient, it still doesn't have quantum protection. NTRU and XMSS, on the other hand, are slower but offer stronger security with bigger key sizes, making them good for cryptographic needs that will still be around in the future.

Table 1
Performance metric of comparing quantum-based and classical cryptographic systems

System	Key Generation Rate (Kbps)	Security Level (Bits)	Computational Complexity	Resistance to Quantum Attacks	Key Size (Bits)
Classical RSA (2048-bit)	0.1	128	Exponential	Low	2048
Classical ECC (256-bit)	1.0	128	Polynomial	Low	256

Contd...

Quantum Key Distribution (BB84)	10	256+	Polynomial	High	Varies
Quantum-Resistant Lattice-Based (NTRU)	0.5	256	Polynomial	High	2048+
Quantum-Resistant Hash-Based (XMSS)	0.2	256	Polynomial	High	4096+

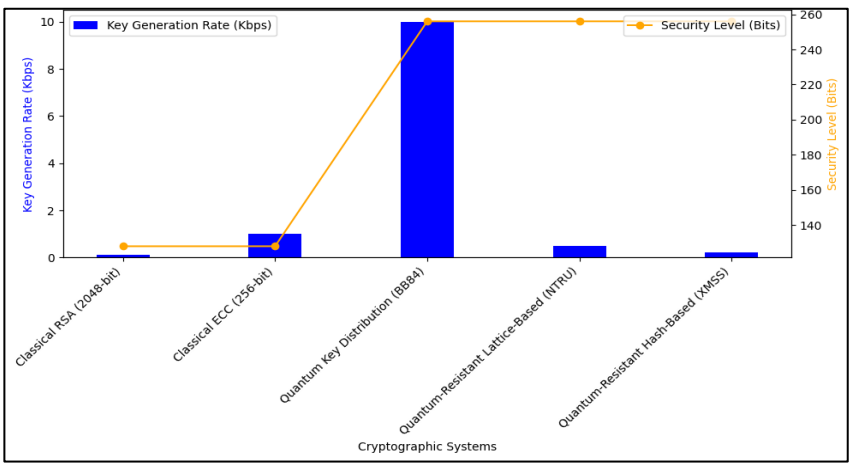

Figure 2
Representation of Comparison of Cryptographic System

Different encryption systems have different amounts of protection and key creation rates, which are shown in Figure 2. The blue bars show the key creation rate in Kbps. Quantum Key Distribution (BB84) has the fastest rate at 10 Kbps, and Classical ECC is in second place at 1.0 Kbps. This type of RSA has the slowest rate, at 0.1 Kbps. The orange line shows the level of security in bits. It shows that QKD and quantum-resistant algorithms (NTRU and XMSS) provide a high level of security with 256 bits, which is a lot more than the 128 bits that standard RSA and ECC offer.

Table 2
Results for quantum cryptographic algorithms and quantum-resistant algorithms

Algorithm	Key Strength (bits/qubits)	Scalability (%)	Resource Efficiency (%)	Security Assurance (%)
Quantum Key Distribution (QKD)	512 qubits	85%	70%	95%
Lattice-based Cryptography	256 bits	80%	65%	90%

Contd...

Hash-based Cryptography	256 bits	75%	60%	85%
Code-based Cryptography	256 bits	70%	55%	88%
Multivariate Polynomial Cryptography	256 bits	72%	58%	87%

The table 2 presents a comparative investigation of quantum cryptographic calculations, especially Quantum Key Dispersion (QKD), nearby quantum-resistant calculations such as lattice-based, hash-based, code-based, and multivariate polynomial cryptography. QKD stands out with it utilize of 512 qubits, giving the next level of key quality compared to the conventional bit-based approaches utilized by quantum-resistant calculations.

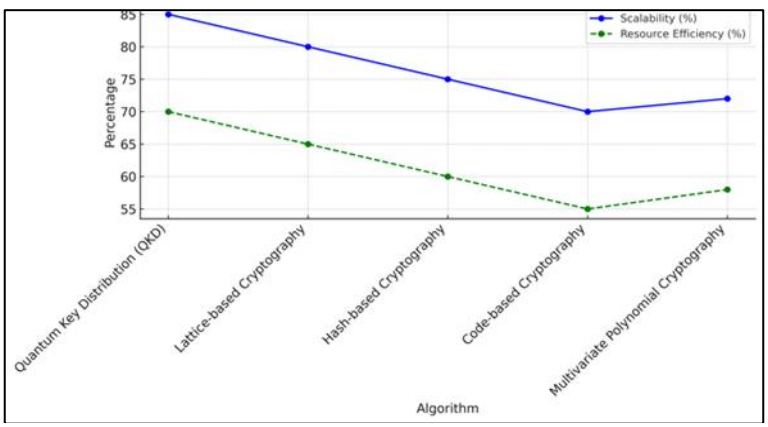

Figure 3
Comparison of cryptographic algorithm: scalability and Resource Efficiency

This quantum approach comes about in noteworthy preferences in security affirmation, accomplishing an exceptional 95% due to the inalienable properties of quantum mechanics that make listening in recognizable, shown in figure 3. QKD too exceeds expectations in versatility, with an 85% rating, permitting it to handle large-scale key dissemination viably. In any case, it requires specialized framework like quantum channels, which can restrain its broad appropriation and contribute to its direct asset proficiency of 70%. In spite of this, QKD's potential for future-proof security makes it a driving choice for situations where most extreme security is basic.

Quantum-resistant calculations, on the other hand, offer common sense options to classical cryptographic strategies whereas being versatile against quantum assaults. Lattice-based cryptography leads in this category with an 80% versatility rating and a 90% security affirmation. Hash-based, code-based, and multivariate polynomial cryptography give changed adaptability and asset

proficiency, with security affirmations extending from 85% to 88%, comparison of different metrics shown in figure 4.

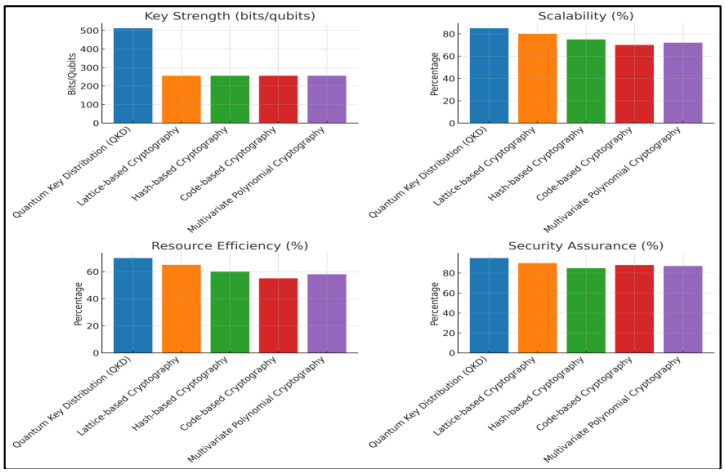

Figure 4
Representation of comparing different cryptographic algorithms

4. Conclusion

Adding cryptographic methods that is unbreakable by quantum computers to blockchain networks makes them very immune to new threats that come from quantum computers. Using these methods makes security better and protects the long-term safety and privacy of data. But this higher level of security comes with a few enormous costs, like slower exchange speeds, longer hold up times, and more asset utilize. Indeed with these issues, ponder utilize of quantum-resistant ways is fundamental to create blockchain frameworks prepared for long run. The comes about appear that more consider and improvement is required to find the most excellent blend between security and speed. This will permit for secure and compelling blockchain systems within a long time after quantum computing. This work lays the basis for secure blockchain frameworks to keep getting superior.

References

[1] C. S. Dhanush and K. Jain, "Comparison of post-quantum cryptography algorithms for authentication in quantum key distribution classical channel," in Proc. 2nd Int. Conf. Augmented Intell. Sustain. Syst. (ICAISS), Trichy, India, pp. 1219–1225 (2023).

[2] E. Lella, A. Aloisio, M. Guarnieri, and R. Rinaldi, "Cryptography in the quantum era," in Proceedings of the IEEE 15th Workshop on Low Temperature Electronics (WOLTE), Matera, Italy, pp. 1–4 (2022).

[3] I. Anantraj, B. Umarani, C. Karpagavalli, C. Usharani, and S. J. Lakshmi, "Quantum computing's double-edged sword: Unravelling the vulnerabilities in quantum key distribution for enhanced network security," in Proc. Int. Conf. Next Generat. Electron. (NEleX), Vellore, India, pp. 1–5 (2023).

[4] L. Sun, W. Wang, and M. Q. Wang, "MILP-aided bit-based division property for primitives with non-bit-permutation linear layers," *IET Inf. Secur.,* vol. 14, no. 1, pp. 12–20 (2020).

[5] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," (2020). [Online]. Available: [https://researcher.watson.ibm.com/researcher/files/ca-CharlieBennett/BB84highest.pdf].

[6] K. Jain, A. Aji, and P. Krishnan, "Medical image encryption scheme using multiple chaotic maps, "*Pattern Recognit. Lett.,* vol. 152, pp. 356–364 (2021).

[7] G. Alagic, D. Apon, D. Cooper, Q. Dang, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, U.S. Department of Commerce, National Institute of Standards and Technology, Tech. Rep. (2020).

[8] K. Jain, P. Krishnan, and V. V. Rao, "A comparison-based approach on mutual authentication and key agreement using DNA cryptography," in Proc. Int. Conf. Electr., Comput. Commun. Technol. (ICECCT), pp. 1–6 (2021).

[9] J. Gomes, S. Khan, and D. Svetinovic, "Fortifying the blockchain: A systematic review and classification of post-quantum consensus solutions for enhanced security and resilience," *IEEE Access*, vol. 11, pp. 74088–74100 (2023).

[10] G. Alagic, D. Apon, D. Cooper, Q. Dang, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, National Institute of Standards and Technology (NIST), U.S. Department of Commerce (Jul. 2020).

[11] M. G. Dhote, B. M. Nanche, P. N. Mahalle, S. S. Ali, M. Gulhane, and V. S. Karwande, "Deep learning for optimized path planning in autonomous vehicles by integrating reinforcement learning with convolutional neural networks," *J. Inf. Optim. Sci.,* vol. 46, no. 4-B, pp. 1129–1139 (2025), doi: 10.47974/JIOS-1897.

[12] Godbole, R. Dhabliya, V. Deshpande, S. A. Sivakumar, B. M. Shankar, and V. Khetani, "Ethical hacking and penetration testing: Strengthening cybersecurity posture through offensive security measures," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 4, pp. 1295–1305 (2024), doi: 10.47974/JDMSC-1983.

Received November, 2024