PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 07 • June 2026

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Quantum-Safe Cryptography: Protecting the Digital World Beyond the Quantum Era

With the rapid approach of quantum computing technology towards practicality, the underlying cryptographic systems supporting today's digital world stand at the brink of vulnerability and require immediate transition to quantum-safe solutions.

By **Farah Deeba** | University of Agriculture | Published: June 2026
fd1093416@email.com | Position: e.g., Student

Introduction

Begin Today's digital world thrives on trust. Trust that information is safeguarded, transactions are secure, and communication is confidential. Cryptography, the foundation stone of all security measures within this digital realm, faces an imminent challenge. The advent of quantum computing is more than a technological advancement; it heralds a paradigm shift that could undermine the cryptographic systems upon which our entire digital ecosystem depends.

Traditional cryptographic methods like RSA and ECC (Elliptic Curve Cryptography) depend on mathematical challenges that are practically insolvable by classical computers. In contrast, quantum computers rely on qubits and quantum phenomena, enabling them to compute some tasks exponentially faster than classical computers. This poses a critical challenge to existing cryptographic systems.

The impending danger is not imaginary in nature. Countries across the globe have been making serious investments towards developing quantum computer technology. Although large scale quantum computers capable of breaking modern day encryption codes have not been made public yet, the time frame remains uncertain, and failing to respond appropriately can lead to serious ramifications.

Pakistan's rapidly growing digital environment which involves sectors such as fintech, e-governance, telecommunications, and start-ups has a lot at stake here. With the nation speeding towards its digital transformation, securing its digital ecosystem in light of cyber threats becomes essential for its success.

> ***"Transitioning into quantum-safe cryptography is not a matter of if, but when—and one will only regret waiting too long until it is realized that their data is now vulnerable."***

Technology Overview

Quantum-safe cryptography, which is also referred to as post-quantum cryptography (PQC), pertains to cryptography algorithms which cannot be broken using quantum computing techniques as well as classical computing.

In order to appreciate the need for such a shift, one needs to consider how quantum computing poses risks to current cryptography approaches. Among the most important quantum computing algorithms is the algorithm proposed by Peter Shor, which enables efficient integer factorization—a process critical to RSA encryption. Another example is Grover's algorithm, which is capable of optimizing the efficiency of brute force attacks on symmetric algorithms, such as AES.

Therefore, what is being referred to as "harvest now, decrypt later" is the ability to decrypt data that was encrypted using current methods and then saved for decryption using quantum computing technology. Financial, healthcare, government, and other sensitive information can therefore be considered already compromised.

However, quantum-safe cryptography offers an alternative to these mathematical algorithms through new frameworks, some of which include:

1. Lattice-Based Cryptography

The idea behind this is that the lattice problems, including the Shortest Vector Problem (SVP), are still hard even for quantum computers. Cryptographic solutions, such as CRYSTALS-Kyber and CRYSTALS-Dilithium, can be considered representatives of this group and are chosen by international organizations to be implemented in the future.

2. Hash-Based Cryptography

These algorithms use a cryptographic hash function to implement digital signature mechanisms. These approaches are well-known and secure, although not very scalable in terms of performance.

3. Code-Based Cryptography

It uses error-correcting codes as its foundation, and it has been researched for quite a long time now. Nevertheless, usually, code-based solutions require relatively large sizes of keys.

4. Multivariate Cryptography

Here the problem of solving systems of non-linear polynomial equations remains hard enough for quantum computers.

5. Isogeny-Based Cryptography

This approach can be considered relatively new and advanced; however, a number of algorithms of this type have been recently compromised.

In practice, quantum computing security is achieved not only through algorithm replacement but through much more complicated steps.

Pakistan, a country where digital infrastructure is quickly developing, can benefit from incorporating quantum-safe measures at an early stage. It would make sense for banks, telecom companies, and government organizations to start preparing for potential migration. environment.

[Insert Image Here — 1200 × 600 p

x

recommended]

Figure 1:

Key Findings & Impact

Present Quantum-safe cryptography is a major shift that will affect various sectors of the economy and different nations in the coming decades.

1. Imminent Threats to Cryptography

While experts disagree on when the threat will become imminent, most agree that within 10 to 20 years, quantum computers able to crack the RSA-2048 code will appear. In light of how long it takes before some sensitive information ceases to be classified, the problem is urgent.

Businesses that will neglect this problem will face exposure of their long-term confidential data. It becomes even more pressing in the case of:

- Banks and financial services
- Healthcare data systems
- Government and military communication
- Research data

2. Standardization Activities Globally

- The International community through agencies like the National Institute of Standards and Technology (NIST) has spearheaded activities aimed at standardizing post-quantum cryptography algorithms.
- A number of algorithms have been chosen following years of analysis, thus representing an important step in global cybersecurity.
- This standardization is a blueprint for the adoption of quantum-safe cryptography in other parts of the world, including Pakistan.

3. Challenges Faced While Implementing the Algorithm

- Although quantum-safe cryptography offers more security than conventional cryptography, it comes with challenges, which include:
- Increased key size
- Slower processing speed than conventional cryptography
- Incompatibility with other software systems
- Businesses need to consider these aspects before implementing the quantum-safe algorithm.

4. Possibilities for Pakistan's Technology Ecosystem

- The shift towards quantum-safe cryptography offers an excellent chance for Pakistan to improve its standing in the international tech scene.
- Startups and Innovations:
- Tech companies in Pakistan can create products that ensure quantum-safe cryptography and cybersecurity for developing countries.
- Research and Academia:
- Education institutes can help with quantum safe cryptography research.
- Policy and Regulations:
- Government organizations can design progressive cybersecurity policies for the country.

Talent Management:

With the growing need for cybersecurity specialists, Pakistan needs to invest in talent development.

5. Economic and Strategic Impact

- Cybersecurity threats may lead to huge financial, reputation, and even national security issues. However, Pakistan can capitalize on quantum-safe cryptography to:
- Improve trustworthiness of digital systems
- Bring in foreign investments
- Increase national security infrastructure
- Become a cybersecurity leader in the region

What's Next?

While the process of transitioning to quantum-safe cryptography may prove complicated, it has begun already.

Step 1: Cryptography Audit & Security Risk Assessment

First, it is necessary to find out what kind of cryptographic solutions the enterprise uses. This may include data protection, authentication, communication channels, and software and services integrated from outside sources.

Step 2: Implementation of Hybrid Cryptographic Systems

Many companies decide to move to hybrid systems combining classical algorithms with quantum-safe ones. It helps maintain backward compatibility with existing systems and provide better security for the future.

Step 3: Upgrade the IT Infrastructure

Traditional infrastructure might not be capable of supporting new algorithms. It may be necessary to invest in upgrading it.

Step 4: Collaboration & Exchange of Knowledge

Collaborations between different organizations will be vital to accelerating implementation.

Step 5: Continuous Monitoring & Adjustment

Quantum-resistant cryptography continues to evolve, so enterprises need to monitor its progress and adapt their security measures accordingly.

Indeed, as the quantum age nears, we can expect a new world of possibilities and threats in computation, innovation, and even security. Although the potential risks seem ominous, the opportunities cannot be overlooked.

Adopting quantum-safe cryptography does not only involve being reactive; it is about preparing for the challenges that await us in the future.

For Pakistan, as it works toward being technologically advanced and ready for the digital age, quantum-safe encryption will be necessary to ensure a bright future.

For those who invest in the future of security today, tomorrow will belong to them.

About the Author

She is passionate about bridging global developments with Pakistan's tech community and discusses future-proof technologies. You can reach out to her at fd1093416@gmail.com.

Keywords: Quantum Computing; Post-Quantum Cryptography; Cybersecurity; Cryptography; Digital security; Pakistan Tech; Future technology; Data Protection.

References

[1] NIST (2024). Post-Quantum Cryptography Standardization, National Institute of Standards and Technology.

[2] Bernstein, D. et al. (2023). Post-Quantum Cryptography, Springer.

[3] Chen, L. et al. (2024). Report on Post-Quantum Cryptography, NISTIR Series.

[4] Mosca, M. (2022). Cybersecurity in an Era with Quantum Computers, IEEE Security & Privacy.