PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 13 • ISSN: 3136-2729

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Pakistan's Race Against Quantum Clock: Securing Tomorrow's Communication Today

Imagine adversaries quietly collecting encrypted data right now banking details, government secrets, health records waiting for the day a quantum computer cracks open everything we thought we safe. That day is coming faster than most realize and ignoring it could prove costly

By **Eman Kanwal** | University of Agriculture, Faisalabad | Published: July 2026
ekanwal247@email.com | Position: Computer Scientist

Introduction

Our digital world is based on a number of mathematical conjectures, which have been stable for several decades now. With every login to a website offering online banking, encrypted communication, or signing of any document online, one is counting on the hardness of solving certain mathematically defined problems, such as factoring huge numbers, calculating discrete logarithms, and finding points on an elliptic curve. All those conjectures have worked fine until quantum computing was introduced.

Quantum computers leverage superposition and entanglement to efficiently traverse huge search spaces at once. Regarding the mathematics of RSA and ECC, a potent enough quantum computer using Shors algorithm can break encryption that would take an equivalent supercomputer many years to crack – in just hours. Furthermore, Grover's algorithm presents a threat to symmetric key cryptography and hash functions by reducing their effective security by half. Collectively, these two algorithms present a formidable assault on our cryptography systems.

This is not an issue only for the future. There is already evidence from security researchers and intelligence organizations about a strategy called "harvest now, decrypt later." The attackers harvest large amounts of encrypted data currently being generated, keep it in storage, and intend to use quantum computers when their ability becomes available to decrypt all this information. Information sent securely in 2026 can potentially become encrypted in 2035 or 2040. Thus, the danger exists right now and is not theoretical.

For Pakistan, there is an additional problem related to its current transition to a more technologically advanced economy. Post-Quantum Cryptography (PQC) is the way to go. While quantum key distribution needs special hardware and new infrastructure, PQC works using regular computing devices, from phones to servers, as well as embedded systems. It relies on mathematical hardness assumptions different from those used by classical and quantum computers.

> ***"Building post-quantum secure system isn't about fearing quantum computers; it's about refusing to let today's shortcuts become tomorrow's national vulnerabilities."***

Vol. 01, Issue 13 • ISSN: 3136-2729

Technology Overview

The fundamental definition of Post-Quantum Cryptography is a fresh wave of encryption technologies that will be safe from the attacks of powerful quantum computers. While the theory of quantum networking is based on quantum physics principles, the development of PQC algorithms involves only software programming performed on conventional classical hardware, such as desktops, laptops, tablets, and smartphones.

Post Quantum Cryptography (PQC), therefore, constitutes a brand-new class of algorithms that have been created with the sole purpose of protecting against any attacks. PQC is a brand-new generation of cryptography algorithms that will stay safe even when quantum computers become widespread. While quantum networks are yet to be practically realized, PQC can work on existing devices like;

1. **Lattice-Based Cryptography**: The most successful construction techniques that have emerged in the field of PQC thus far are lattice-based techniques. A lattice is an orderly structure of points in n-dimensional space. The difficulty of these cryptograms relies on the following two challenging problems:
    - **Shortest Vector Problem (SVP):**

      Finding the shortest non-zero vector within a lattice. The SVP problem is conjectured to be NP-hard even for quantum computers.
    - **Learning With Errors (LWE):**

      Distinguishing between inner products in a lattice with noise and truly random samples. This problem was introduced in 2005.Considered one of the strongest practical option.
2. **Hash-Based Signatures:** Hash-based signature schemes are solely based on the collision resistance and image resistance of hash functions. They have the strongest security assumptions of all PQC families - they only rely on properties of hash functions that have been investigated for more than 50 years.
3. **Code-Based Encryption:** Cryptography based on error-correcting codes is a form of encryption that secures data using mathematical error-correcting codes. These codes were originally designed to detect and correct errors in data transmission, but have been modified for communication purposes. This technique is regarded as a key in post-quantum cryptography as it is thought to be secure against quantum computers.
4. **Hybrid-Security Models:** A hybrid security model is a Cyber security strategy that integrates several security methods, technologies or cryptography schemes to deliver enhanced and adaptable security measures. Rather than a one-size-fits-all approach, it combines traditional security measures with contemporary techniques like multi-factor authentication, cloud security measures, artificial intelligence-based monitoring, and innovative encryption. Combine current encryption with PQC during transition.

Post quantum secure communication system may help in secure messaging applications, Banking transactions, Government record systems, software updates and authentication and health care data protection.

Vol. 01, Issue 13 • ISSN: 3136-2729

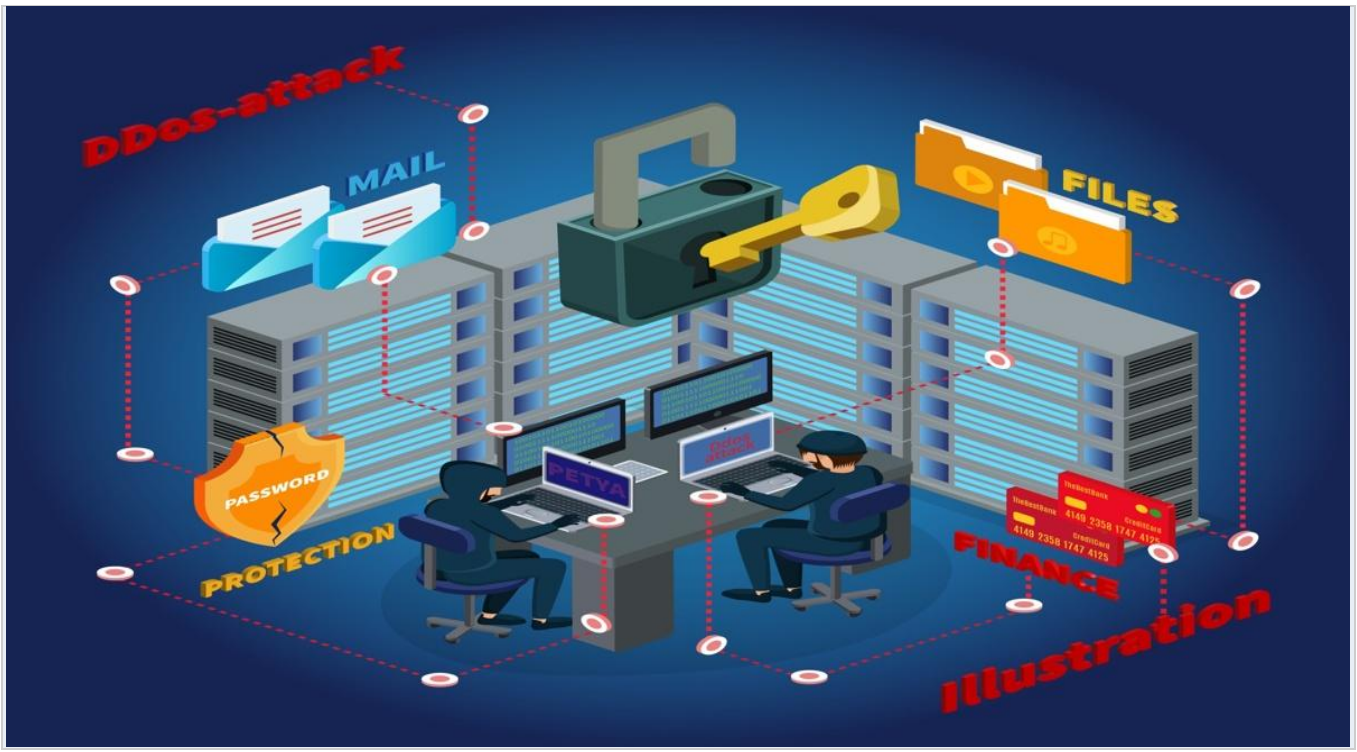

Figure 1: Illustration of a post quantum secure network connecting users, institutions and cloud services.

Key Findings & Impact

The world is moving to post-quantum security. Standards organizations, governments, cloud providers and technology vendors are experimenting with migration plans because cryptography upgrades can be a lengthy process. Emerging digital markets can save time and money by starting early. Inaction can lead to panic upgrades, last minute replacements and security vulnerabilities.

These systems employ quantum-safe algorithms to protect communication channels, ensuring secure and future-proof messaging. A key discovery is that current encryption systems, like RSA and ECC, could be susceptible to attack by large-scale quantum computers. Quantum-resistant algorithms such as lattice-based and code-based cryptography offer more secure options for messaging; cloud computing, banking and government communications. A further consequence is the need for infrastructure upgrades, as some post-quantum cryptography algorithms have larger key sizes and computational demands. In conclusion, post-quantum secure communication systems offer a key to a more secure and future-proof world.

Early transitions to post-quantum systems could help businesses, countries and governments build significant opportunities for the future. Improved protection is a major advantage, as information encrypted now may not be compromised for decades, even with more powerful quantum computers. This is particularly important for critical data like banking information, health data and public records. Increased trust in banking is another important benefit, as financial institutions and businesses can increase confidence by securing customer data, transactions and online payments with enhanced security measures. When customers know their information is secure, they're more willing to take advantage of online services. Economic opportunities may also rise, as Pakistani startups and tech firms can build indigenous security software, services, secure apps and products for local and global markets. Also, education is important, because Pakistani universities and training programs can

train students in a rapidly-growing field. Studying post-quantum security can prepare young people with up-to-date skills for a future career in computer security.

Early adoption of post-quantum systems can create major advantages:

- **Stronger Banking Confidence:** Banks and other companies can improve trust by protecting customer transactions.
- **Business opportunities:** Pakistani startups may develop local security tools, consulting services and secure products.
- **Skill Development:** Universities can train students in one of the fastest-growing fields of security.

Stronger security is an organizational challenge rather than a technical one. Institutions must sustain day-to-day operations while balancing security, performance, cost, and compatibility. Larger keys or signatures are used by some PQC algorithms compared to prior systems, which may have an impact on processing performance, bandwidth, or storage in specific settings. Thus, thorough testing is crucial. Migration seems promising, but it will take time.

Organizational and Policy Challenges:

- Most Pakistani people who make decisions about technology do not know about the harvest-decrypt-later threat or the NIST standardization timeline. If the people in charge do not understand

this then the companies will not make the post quantum cryptography migration a priority because they will not give it an enough budget. This is a problem because of the awareness gap about post quantum cryptography.

- There are not people in Pakistan who are good at classical cryptography. To do lattice cryptography and other things like that you need to have a lot of math knowledge, which is usually learned in graduate school. But the universities in Pakistan are not teaching this kind of thing regularly. There is a shortage of qualified specialists in post quantum cryptography.
- Pakistan does not have a plan for how to use post cryptography so companies are not being told when they have to start using it or what kind of algorithms are okay to use. Without the government telling them what to do companies do not have a reason to spend money on post cryptography until they really need to which is a problem because of the regulatory vacuum.
- For the government and smaller banks it will cost a lot of money to get post quantum cryptography systems, including special hardware and training for the staff. This is a problem because of the budget constraints.
- If companies start using post cryptography systems before they are fully tested they might get stuck with systems that do not work with other systems or they might find out that the system they chose is not secure which is the vendor lock-in risk, for post quantum cryptography.

What's Next?

Transitioning to -quantum security is not going to be simple. It needs to be done with planning and not rushed into. Many of the quantum security algorithms use bigger keys, which mean they need more bandwidth, more storage space and more power to process.

Older systems may not be able to handle these methods so when we upgrade them we have to be careful. We do not want to disrupt the service or leave any gaps in security. Post-quantum security is a challenge. We also have a problem because there are not skilled professionals who understand post-quantum security and how to implement it. This means that organizations have to spend money to train their engineers IT staff and security teams so they can handle the change, to quantum security. The best way to do this is to have crypt-agility. This means designing systems that can easily switch from one encryption method to another when needed.

For the few years the focus will be on changing things slowly rather than making big changes all at once. Most companies will probably start with a mix of new security methods, where the traditional way of keeping things secret works together with the new post-quantum algorithms. This way companies can still work with the systems they already have and at the time they can get used to the new technologies. Using both new security methods at the same time can give companies extra protection right away and it can also reduce the risks of making big changes too quickly. This approach gives businesses time to see how things work find out what is not working well and make changes to how they do things one step, at a time with the -quantum algorithms and the traditional security methods the companies can make this transition smoothly.

Experts say that companies should start getting ready rather than waiting for something bad to happen. If someone steals information today they could save it and figure out the code later when quantum technology gets better. That is why it is very important to get ready Companies can take a steps to reduce the risk of something bad happening later. They can check their systems to see if they are working well. They can find out if they are using encryption methods that are not strong enough. They can try out solutions that will work even

when quantum technology gets stronger. They can also make a plan for how to switch to these solutions. Pakistan has a lot of people in the technology field and the technology sector is growing. More and more people are using technology in Pakistan. If the country plans carefully invests in the skills and gets the public and private sectors working together it could become a leader in the region for secure communication technologies and digital trust.

The time of quantum technology is. Companies that get ready early will be in the best position to protect them. The quantum era is. Those who act early will be in the strongest position to protect their future and that is why the quantum era and the steps taken for the quantum era are very important, for the quantum era.

Conclusion

Post-quantum secure communication systems are not about being ready for the future they are also about being responsible now. The choices that organizations make today will have an impact on how safe they will be in the years to come. As technology keeps getting better it is more important than ever to protect data, customer information, financial transactions and national infrastructure. Organizations that start getting ready will be safer and smarter in the digital world. They will have time to try out solutions teaching their teams and upgrading their systems in a calm and planned way instead of rushing to fix things later. If organizations start preparing for post-quantum secure communication systems they will be more competitive in the digital era. Getting ready early for -quantum secure communication systems can also help build trust with customers, partners and investors who think strong security and long-term reliability are important.

Countries and businesses that move quickly on -quantum secure communication systems can create new ideas new job opportunities and become leaders in new technologies. Being ready for -quantum secure communication systems is not just about making a technical change it is about making a smart investment in being strong growing and feeling confident in the digital world, for the future of post-quantum secure communication systems.

About the Author

Eman kanwal is an emerging technology writer with the interests in Cyber security, AI and modern communication systems. Their works focuses on explaining complex topics in clear and practical language .They can be reached at ekanwal247@gmail.com

Keywords: post-quantum cryptography; Cyber security; Secure communication; Quantum computing Pakistan Tech

References

[1] NIST.Post-Quantum Cryptography Standardization Project.

[2] ETSI Reports on Quantum-Safe Security..