TECHNOLOGY FEATURE Cybersecurity / Emerging Technologies

Post-Quantum Cryptography: Future Proofing the Here and Now.

Computing is on the verge of a silent revolution-and it could shatter the core of digital security that we know of today. Is our world prepared to enter a post-quantum world?

By **Syed Taseer Abbas Naqvi** / Cybersecurity Analyst & Technology Researcher | Published: July 2026
syedtaseerabbas797@gmail.com | Position: Cybersecurity Analyst

Introduction

Imagine this it is the year 2030. A major financial institution suddenly discovers that its encrypted customer information that is believed to be utterly safe, has been hacked. Not in the conventional sense of the term, but by an extremely strong quantum computer quietly running in the background. Hours later, sensitive transactions are revealed, identities are stolen and trust starts crumbling.

It is a dramatic (or maybe a bit futuristic) but this is not too distant according to the experts. The field of quantum computing is moving more rapidly than anticipated and even though quantum computing promises an amazing breakthrough, it also presents a daunting challenge, the possible ability to crack the encryption systems upon which we base our daily lives.

This cannot be ignored by countries such as Pakistan, where digital development is gaining momentum in many areas such as banking, government services, and telecommunication. Actually we need to begin preparing to do it now not later.

> ***" This is the actual threat of quantum computing not the strength that is posed by the technology but the lack of preparedness of our existing security frameworks to handle quantum computing."***

Technology Overview

The essence of quantum computing is an entirely new approach to information processing. Conventional computers operate using simple bits 0s and 1s. Instead, quantum computers employ so-called qubits. These qubits can be in many states simultaneously and enable quantum machines to work through many possibilities simultaneously.

That may be abstract, but the effect is very tangible. Quantum systems could potentially address problems that take the classical computers thousands of years to be solved.

And complication arises here.

Majority of the encryption systems used in the present such as RSA and ECC relies on mathematical problems which are extremely hard to crack using classical systems. However, quantum algorithms, and in particular the Shor algorithm, are built to efficiently solve precisely such problems.

Visualize it this way, take a lock on which you have stored your treasures over the years, but it becomes unlocked in your hands. Such is what quantum computing may do to contemporary encryption. Think of it like this: imagine a lock that has protected your valuables for years suddenly becoming easy to pick. That's essentially what quantum computing could do to modern encryption.

The Quantum Threat to Modern Encryption
Why Current Systems Are at Risk

Much of the current digital security is grounded on a single fact, namely; some mathematical problems are highly intractable by the normal computers. This has been a good assumption over the years with classical computers. However, this may not be the case with quantum computers.

As soon as quantum technology is powerful enough, it can potentially:

- Crack frequently used encryption schemes.
- Access confidential information which has been stored over years.
- Hack into secure communication of various industries

A single area of growing concern is the so-called "harvest now, decrypt later" where attackers will gather encrypted data today and store it until quantum computers are powerful enough to decrypt it in the future. That is, what appears to be a safe piece of information today might not be safe in the future.

A Race That Has Already Started
Due to this danger, governments and technology firms in all corners of the world are not resting. A problem that was perceived to be experienced in the future is presently a big cybersecurity concern.

What is Post-Quantum Cryptography?
Then what is the answer?

It is in this that Post-Quantum Cryptography (PQC) comes in. PQC is concerned with coming up with new encryption systems capable of safeguarding data against the conventional computing and also in the case of the quantized computers in the future.

PQC relies on innovative methods as opposed to the ancient methods of math, which are thought to be far more inaccessible by quantum computers. A few of them are:

- Lattice-based methods
- Hash-based cryptography
- Multivariate polynomial techniques

It is a very straightforward concept: develop security systems that will be robust today and will be robust tomorrow.

Real-World Use Cases and Industry Response

Tech Giants Are Already Moving

The large tech firms Google, IBM and Microsoft are already developing quantum resistant technologies. It is not research any more it is the preparations to the next step in cybersecurity.

Meanwhile, other organizations like the NIST are coming up with international post-quantum cryptography standards. These standards will serve to guide governments, companies and institutions as they will start to transition to safer encryption systems.

Critical Sectors Taking It Seriously

One of the first industries that started to take this issue seriously are those which operate with sensitive data like banking and government. Several are already looking into the ways on how they can prepare their systems before quantum threats become a tangible threat.

Challenges in Implementation

Naturally, it is not a matter of flicking the switch to switch to post-quantum cryptography.

Technical Hurdles

Typically, new cryptographic systems have trade-offs:

- Larger key sizes
- Reduced performance in a few instances.
- Incompatible with the available systems.

The Bigger Challenge: Transition

Modernising the world digital infrastructure is an enormous project. Everything, including the financial systems, communication network, and so forth, requires proper planning, investment and coordination

Pakistan & Global Cybersecurity Preparedness

The digital world in Pakistan is rapidly transforming. Every day, online banking, cloud services and e-governance platforms are becoming increasingly prevalent.

However, with quantum readiness, there is much to be desired.

Where Pakistan Stands

- There is increased awareness on cybersecurity.
- The use of digital is on the rise.
- Quantum-resistant systems research is, however, limited.

A Window of Opportunity

The good news? There is an opportunity to put a step forward in Pakistan.

Investments in knowledge, promotion of research, and development of international relations will help the country to become a serious participant in the next-generation cybersecurity.

Key Findings & Impact

It is not a choice but a necessity that the transition to post-quantum cryptography is necessary.

Most affected industries are in the industries of:

- Banking/ Finance: Data security, safeguarding of transactions and customer records.
- Government: Top secret communications and national security.
- Healthcare: Data privacy concerning the patients.
- Telecommunications: Transmission of data that is secure.

Organizations that postpone change expos are at risk of being exposed to breaches in the future, particularly those associated with the actual collection of data and decryption at a later time.

What's Next?

Although quantum computers are not currently that widely available, it is high time to get ready. Who will be the leaders and who will be the laggards in this new age will depend upon early adoption, investment of research and policy development.

The future of cyber security will not only be relying on enhanced systems, but wiser thinking.

And preparation is no better defense than in the race of quantum threats, preparation is the only real defense.

About the Author

Syed Taseer Abbas Naqvi is a technology researcher and cybersecurity analyst focusing on the new digital threats and next-generation computing systems. His research covers the convergence of cybersecurity, quantum-technologies and digital infrastructures of the future. One can contact him through syedtaseerabbas797@gmail.com.

Keywords: Post-Quantum Cryptography; Quantum Computing; Cybersecurity; Encryption; Emerging Technologies; Pakistan Tech

References

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

[2] IBM Research, 2025. Quantum Computing and Cryptography Overview.