PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 17 • ISSN: 3136-2729

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

Quantum computers vs Encryption: Is security about to collapse?

The *arrival of quantum computers threatens today's encryption, exposing sensitive data within critical sectors, as classical algorithms like Rivest-Shamir-Adleman and elliptic curve cryptography can be efficiently broken. Post-quantum cryptography involving lattice-based and hybrid schemes ensures post-quantum solutions.*

By **Muhammad Asif** | University of Agriculture, Faisalabad | Published: September, 2026
muhammadasifdogar9@gmail.com | Position: Software Engineer

Introduction

The approaching arrival of quantum computers is creating serious concerns about digital security. If current methods of encryption are broken, a large amount of sensitive data is exposed, basically disrupting trust in digital systems used in critical areas like banking, national security, and cloud computing(Swetha and Mohiddin, 2024; Bindu Ronald, 2024). Cryptography that is balanced like AES is still more flexible. It needs really big keys to stay safe from attacks by quantum computers. This is because quantum computers can break codes that regular computers cannot.

> ***"Today's strongest encryption protects our data from hackers—but tomorrow's quantum computers could unlock it in minutes."***

Technology Overview

Basically, quantum computing creates a serious threat to the security of current cryptographic systems that protect most digital information security today. Typical public key-encryption techniques like RSA and Elliptic curve cryptography (ECC) are considered secure because they depend upon mathematical problems such as factoring large numbers and solving discrete algorithms that are difficult to solve for classical computers. Although a method called Shor's algorithm can optimally solve these problems much faster on a properly powerful quantum computer, it could lead to the easy breaking of widely used encryption techniques, putting sensitive information at risk of exposure.

Key Findings & Impact

Quantum computing is going to cause problems for digital security if we do not do something about it soon. We need to act to stay safe. To deal with this problem, researchers think that companies should start using quantum cryptography, which is also known as PQC. This type of cryptography is made to keep us safe from quantum attacks. Quantum computing is a problem. We need to be safe from computing attacks. The way to do this is with quantum cryptography. One good way to be safe is to use encryption systems. These systems combine the strength of symmetric algorithms, like AES-256.

Post-quantum cryptography and these systems can also change encryption keys often. Our data is not safe if someone gets our key. They can read our data. So, we need to change the keys a lot. If we change the keys regularly, our data will be safe. This is true even if a key is breached.

Quantum computing is a problem. It is a threat to our data. We need to use cryptography to protect our data. Quantum cryptography will protect us from these attacks. We need to use it to keep our data safe from computing attacks. Indicate stronger protection against attacks without replacing current hardware or software.

What's Next?

Quantum computing basically threatens the security of the current encryption systems. The encryption domain is quickly advancing to use quantum-protected cryptographic solutions that are built to protect data against attacks by quantum computers. Crucially, lattice-based cryptography has become a leading approach because it offers strong security properties and comparative efficiency. Other encouraging approaches, such as hash-based, code-based, multivariate polynomial, and isogeny-based cryptographic schemes.

Organizations like NIST are steadily developing post-quantum cryptography standards to secure systems to work together efficiently and remain secure. New research is looking to link machine learning with post-quantum cryptography to make encryption more effective, improve key generation, and detect attacks in real time, developing security systems that can accommodate and scale.

About the Author

Muhammad Asif is a BS IT student and is interested in cybersecurity, cryptography, and post-quantum encryption. They can be reached at muhammadasifdogar9@gmail.com

Keywords: Cryptography; Cybersecurity; Post quantum encryption; Pakistan Tech

References

[1] Swetha, D., & Mohiddin - https://doi.org/10.14569/ijacsa.2024.0150964

[2] Loriya, H. (2024) - https://doi.org/10.52783/cana.v31.1589

[3] Selvi, F., & Alkan - https://doi.org/10.29109/gujsc.1682989

[4] Morales, A., Bishwas - https://doi.org/10.48550/arxiv.2502.02445