EDITORIAL

The Quantum Countdown: A Global Call to Action for Post-Quantum Readiness

Mujeeb Ur Rehman[1,*]

[1] School of Computer Science and Informatics, De Montfort University, LE1 9BH Leicester, United Kingdom

Every now and then, a breakthrough in technology compels us to pause and to question the very systems we once believed were unbreakable. Quantum computing is one such breakthrough. No longer confined to academic theory or science fiction, it has swiftly moved from imagination to reality. What was once a distant possibility is now a fast-approaching force, casting a long shadow over the cryptographic foundations that protect our digital world.

With advancements in scalable qubit systems, error correction, and hardware acceleration, the threat to public-key cryptography is no longer distant. Algorithms like RSA and elliptic curve cryptography, which safeguard everything from banking transactions to national defence systems, are now vulnerable to the immense parallelism that quantum computing offers. Recognising this, the U.S. National Institute of Standards and Technology (NIST) finalised three post-quantum cryptographic algorithms in 2024: CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+, and placed HQC under formal review in early 2025 [1]. These standards promise quantum-resilient security without requiring quantum hardware—a pragmatic bridge from the present to a post-classical future. Yet standardisation is only the beginning. The scale of the challenge becomes clear when we examine the cost and readiness landscape. The U.S. Government Accountability Office projects that upgrading federal systems to post-quantum encryption will cost over $7.1 billion between 2025 and 2035 [2]. Globally, the figure will be far greater, given the breadth of digital services dependent on legacy encryption. Alarmingly, the cybersecurity community is aware of the risks but not acting fast enough. ISACA's 2025 Pulse Poll reports that 67% of cybersecurity professionals believe quantum computers will break current cryptographic systems within ten years, yet only 4% of organisations have a formal mitigation strategy in place [3]. Capgemini echoes this concern, finding that although 65% of organisations fear "harvest-now, decrypt-later" threats, 30% admit they have taken no steps to address them [4]. Meanwhile, the market for post-quantum solutions is accelerating. Grand View Research estimates the global post-quantum cryptography market to be valued at $1.15 billion in 2024, with projections of $7.82 billion by 2030—an annual growth rate of 37.6% [5]. A longer-term forecast suggests that figure could reach $29.95 billion by 2034 [6].

It is against this backdrop that *ICCK Transactions on Cybersecurity* happily launches its inaugural volume. In this first issue, we showcase work that advances the field of post-quantum resilience from lattice-based implementations for constrained devices to cryptographic agility frameworks for scalable enterprise deployment. These contributions are not

Submitted: 30 June 2025
Accepted: 21 July 2025
Published: 27 August 2025

Vol. 1, **No.** 1, 2025.
10.62762/TC.2025.873234

***Corresponding author:**
✉ Mujeeb Ur Rehman
mujeeb.rehman@dmu.ac.uk

Citation
Rehman, M. U. (2025). The Quantum Countdown: A Global Call to Action for Post-Quantum Readiness. *ICCK Transactions on Cybersecurity*, 1(1), 13–14.

© 2025 ICCK (Institute of Central Computation and Knowledge)

just theoretical: they are blueprints for readiness, resilience, and global digital trust.

As Editor-in-Chief, I request academia, industry, and policymakers to respond with urgency. The window for proactive preparation is narrowing, and reactive adaptation may come at too high a cost. Post-quantum cryptography is not simply a technological shift—it is a civilisational safeguard. The countdown has begun.

Data Availability Statement

Not applicable.

Funding

This work was supported without any funding.

Conflicts of Interest

The author declares no conflicts of interest.

Ethical Approval and Consent to Participate

Not applicable.

References

[1] *Post-quantum cryptography*. (n.d.). NIST Computer Security Resource Center | CSRC. Retrieved from https://csrc.nist.gov/Projects/post-quantum-cryptography

[2] U.S. Government Accountability Office. (2025). Securing federal systems from the quantum threat (GAO-25-107703). Retrieved from https://www.gao.gov/assets/gao-25-107703.pdf

[3] ISACA. (2025). Quantum computing pulse poll. Retrieved from https://www.isaca.org/about-us/newsroom/press-releases/2025/quantum-computings-rapid-rise-is-a-risk-to-cybersecurity-and-business-stability

[4] Capgemini Research Institute. (2025). Future encrypted—Why PQC tops the agenda. Retrieved from https://www.capgemini.com/us-en/news/press-releases/nearly-two-thirds-of-organizations-consider-quantum-computing-as-the-most-critical-cybersecurity-threat-in-3-5-years/

[5] Grand View Research. (2024). Post-quantum cryptography market size, share & trends analysis report. Retrieved from https://www.grandviewresearch.com/industry-analysis/post-quantum-cryptography-market-report

[6] TimesTech. (2025). Post-quantum cryptography market size to soar USD 29.95 Bn by 2034. Retrieved from https://timestech.in/post-quantum-cryptography-market-size-to-soar-usd-29-95-bn-by-2034/

Dr. Mujeeb Ur Rehman is an accomplished academic with over 11 years of teaching and research experience at leading institutions, including De Montfort University (UK), University of Glasgow (UK), York St John University (UK), and Riphah International University (Pakistan). He has supervised numerous PhD, MSc, and undergraduate research projects, and has authored more than 50 peer-reviewed publications in prestigious outlets such as IEEE Transactions, IET Journals, Elsevier, and Springer.
In 2022, he was recognised by the UK Government as an Exceptional Talent (Emerging Leader) for his pioneering contributions to cybersecurity and artificial intelligence. Dr Rehman has led or co-led projects with combined research funding exceeding £4.5 million, supported by institutions in the UK, Saudi Arabia, and beyond. His academic accomplishments include a Gold Medal in his MS programme and a Distinction in his undergraduate degree. He currently serves as the Editor-in-Chief of the ICCK Transactions on Cybersecurity. (Email: mujeeb.rehman@dmu.ac.uk)