

Quantum eMotion and Jmem Technology Join Forces to Deliver the First-Ever Full-Stack Quantum-Resilient Security Chip

Montreal, Quebec and Taipei, Taiwan--(Newsfile Corp. - September 29, 2025) - Quantum eMotion Corp. (TSXV: QNC) (OTCQB: QNCCF) (FSE: 34Q0) ("QeM" or the "Company"), a Canadian pioneer in quantum-based cybersecurity, and Jmem Technology Co., Ltd. (Jmem Tek), a Taiwanese IC design company specializing in hardware security solutions that integrate Physical Unclonable Function (PUF) with post-quantum cryptography (PQC), today announced a strategic alliance to co-develop a quantum-resilient System-on-Chip (SoC).

This unique platform will integrate three essential layers of protection into a single SoC:

- QeM's patented Quantum Random Number Generator (QRNG) — an ultrafast, diode-based entropy source delivering true randomness [1][2].
- Jmem Tek's proprietary Physical Unclonable Function (PUF) — an exclusive, silicon-anchored fingerprint that creates an unclonable hardware root of trust with invisible keys, delivering a level of security unmatched in the industry [3].
- NIST-aligned Post-Quantum Cryptography (PQC) Module — ensuring long-term resilience against quantum-computer-enabled attacks [4].

A Global First in Embedded Cybersecurity

"This collaboration with Jmem Tek represents a strategic step in the evolution of secure hardware," said Dr. Francis Bellido, CEO of Quantum eMotion. "By integrating quantum entropy, hardware-based identity, and post-quantum encryption into a single compact chip, we are advancing a solution that addresses security requirements not yet met by existing technologies. This positions QeM to participate in the growing demand for quantum-safe protection, as billions of connected devices and critical systems are expected to transition to stronger security standards over the coming years. Together with JMEM Tek, we are working to deliver a platform that combines technical differentiation with long-term commercial potential for our partners, investors, and customers."

He added: "Unlike photonic approaches, an electron-based QRNG can be miniaturized for chip-level integration—a capability protected by QeM's patents—which provides a practical and scalable path to embedding true quantum entropy at the semiconductor level."

John Chang, CEO of JMEM Tek, commented: "From day one, our mission has been to anchor trust directly in silicon. By combining JMEM Tek's proven PUF-based Root-of-Trust with QeM's quantum entropy and NIST-aligned PQC, we are setting a new benchmark for hardware security. This strategic collaboration is not only quantum-resilient, but also practical, scalable, and ready to protect the world's most critical systems everywhere against tomorrow's threats today."

Competitive Edge Over Current Solutions

- Software-based security relies on pseudo-randomness, leaving it vulnerable to sophisticated attacks [1].
- Photonic QRNGs, while quantum in principle, remain costly, power-hungry, and unsuitable for broad chip-level deployment.
- Conventional secure chips lack quantum entropy, leaving them exposed to Q-Day risks [4].
- CMOS-compatible quantum entropy for seamless integration into mobile, IoT, and server devices.
- Intrinsic hardware identity secured at the silicon level and establishing a Root-of-Trust platform optimized for PQC.
- Native PQC support aligned with NIST/FIPS standards.
- End-to-end protection in a single platform, from key generation through execution.

Strategic Impact

The QeM-Jmem Tek device directly addresses the urgent need for hardware-anchored, quantum-safe security across critical sectors — including blockchain, fintech, digital health, IoT, defense, and national infrastructure.

As quantum computing advances toward Q-Day, this device provides governments, enterprises, and manufacturers with a future-proof, standards-aligned security core — built on quantum physics, not mathematical approximations.

Potential market

The potential market for a full-stack quantum-resilient security chip is vast, spanning multiple high-value sectors. In the near term, adoption will be strongest in defense, finance, blockchain, and hardware security modules, representing a multibillion-dollar opportunity [5]. As telecom networks, cloud providers, and IoT ecosystems transition to post-quantum standards, demand will expand rapidly across data centers, 5G/6G infrastructure, and billions of connected devices [5]. By positioning itself as a foundational "root of trust" technology—similar to today's ARM cores or TPMs—the chip can capture a significant share of an addressable market expected to grow from a few billion dollars today to tens of billions over the next decade.

Summary

By integrating an ultrafast electron-tunneling QRNG, PQC, and PUF into a single silicon platform, QeM and Jmem Tek are delivering the industry's first unified quantum-resilient SoC.

This breakthrough enables:

- Fast and secure entropy for cryptographic operations.
- Tamper-proof hardware identity for supply-chain trust.
- Stronger protection against side-channel attacks.
- Reduced system complexity, cost, and attack surface.

The result is a uniquely future-proof SoC platform that positions QeM and Jmem Tek at the forefront of the global cybersecurity market.

References

1. QeMPatent US 10,921,010 B2 (2021). *Quantum Random Number Generator using Electron Tunneling*.
2. QeMPatent US 11,271,282 B2 (2022). *Methods and Systems for High-Speed Quantum Random Number Generation*.
3. Maiti, A. (2021). *Physical Unclonable Functions and Applications*. ACM Computing Surveys.
4. NIST (2023). *Post-Quantum Cryptography Standardization - Selected Algorithms*.
5. Precedence Research (2024). *Quantum Cryptography Market Forecast 2025-2034*.

About Jmem Technology Co., Ltd.

Jmem Technology, based in Taiwan, is a trusted innovator in secure semiconductor design. Specializing in Physical Unclonable Function (PUF) technology, Post-Quantum Cryptography (PQC), and hardware root-of-trust architectures, Jmem Tek delivers IP and System-on-Chip (SoC) solutions that enable next-generation cybersecurity across data centers, IoT, automotive, and defense applications.

For further information, please visit our website: <https://jmemtek.com> or contact:

John Chang, Chief Executive Officer, Co-Founder

Tel: +886 2-2325-3808

Email: marketing@jmemtek.com

Website: <https://jmemtek.com>

About Quantum eMotion Corp.

The Company aims to address the growing demand for affordable hardware and software security for

connected devices. QeM has become a pioneering force in classical and quantum cybersecurity solutions thanks to its patented Quantum Random Number Generator, a security solution that exploits the built-in unpredictability of quantum mechanics and promises to provide enhanced protection for high-value assets and critical systems.

The Company intends to target highly valued Financial Services, Healthcare, Blockchain Applications, Cloud-Based IT Security Infrastructure, Classified Government Networks and Communication Systems, Secure Device Keying (IOT, Automotive, Consumer Electronics) and Quantum Cryptography.

For further information, please visit our website at <https://www.quantumemotion.com/> or contact:

Francis Bellido, Chief Executive Officer

Tel: 514.956.2525

Email: info@quantumemotion.com

Website: www.quantumemotion.com

Neither TSX Venture Exchange nor its Regulation Services Provider (as that term is defined in the policies of the TSX Venture Exchange) accepts responsibility for the adequacy or accuracy of this release. This press release may contain forward-looking statements that are subject to known and unknown risks and uncertainties that could cause actual results to vary materially from targeted results. Such risks and uncertainties include those described in the Corporation's periodic reports, including the annual report or in the filings made by Quantum from time to time with securities regulatory authorities.



To view the source version of this press release, please visit

<https://www.newsfilecorp.com/release/268333>