Terra Quantum's TQ42 Library aligns with newly released NIST post-quantum cryptography standards

TQ42 Cryptography is the most comprehensive open-source PQC library available that fully aligns with the NIST PQC standards officially published yesterday

ST. GALLEN, SWITZERLAND, August 14, 2024 /EINPresswire.com/ -- Terra Quantum, a leader in quantum technology solutions, is proud to announce that its post-quantum cryptography library, TQ42 Cryptography, fully aligns with the NIST PQC standards officially published yesterday. TQ42 Cryptography is the most comprehensive, NIST-aligned open-source PQC library available.

Quantum computing poses an imminent threat to traditional encryption, and NIST's standards usher in a new era of data protection as organizations migrate from classical to post-quantum cryptography. NIST's standards should motivate organizations to take quantum threats seriously, which are crucial to quantum-resistant security. By standardizing PQC algorithms, NIST provides a roadmap for organizations worldwide to transition to quantum-resistant cryptographic systems.

> TQ42 Cryptography provides an accessible entry point for organizations to integrate quantum-resistant security measures into their applications, ensuring the long-term protection of sensitive data."
>
> *Markus Pflitsch, Founder and CEO of Terra Quantum*

TQ42 Cryptography provides a practical and comprehensive suite of PQC algorithms, which include the security features necessary to meet the NIST PQC standards, such as secure key exchange and robust digital signatures. This ensures it meets today's standards and is also prepared for tomorrow.

Terra Quantum is committed to creating innovative solutions that comply with rigorous standards and that businesses can confidently implement now. TQ42 Cryptography can be applied by businesses, large or small,

and scales to meet customer needs.

Markus Pflitsch, Founder and CEO of Terra Quantum, said: “As organizations begin to plan for the post-quantum future, adopting appropriate cryptography solutions is crucial for maintaining the security of valuable information. TQ42 Cryptography provides an accessible entry point to integrate quantum-resistant security measures into their applications, ensuring the long-term protection of sensitive data.”

Dr. Florian Neukart, Chief Product Officer at Terra Quantum, said: “Adding ML-KEM, ML-DSA, and SLH-DSA to our open-source library shows our ongoing commitment to democratizing access to post-quantum cryptography. By empowering developers and organizations worldwide with cutting-edge tools, we’re ensuring that the future of data protection is built on a foundation of openness, collaboration, and shared innovation.”

###

Background information

Read more about NIST’s recent announcement here:
https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved

TQ42 Cryptography launched in May 2024, expanding Terra Quantum’s quantum-as-a-service ecosystem of existing offerings that provide easy access to quantum computing tools. In its most recent releases, it added algorithms for ML-KEM, ML-DSA, and SLH-DSA, which passed test vectors for NIST’s new standards:

- ML-KEM (FIPS 203): Secure key encapsulation for post-quantum encryption
- ML-DSA (FIPS 204): Robust digital signatures for post-quantum authentication
- SLH-DSA (FIPS 205): Stateless hash-based signatures for expanded capabilities
- FN-DSA (Falcon): Selected by NIST for future standardization, already integrated into our library

TQ42 Cryptography caters to the needs of developers, security professionals, and technology executives by offering a user-friendly API, scalable architecture, and essential security features like key generation and file deletion capabilities. The library is available under two primary licensing options to accommodate the diverse needs of organizations at different stages of their post-quantum migration journeys: Free use is permitted under AGPLv3, and a Commercial license is available.

About Terra Quantum
Terra Quantum Group is a leading quantum technology company co-headquartered in Germany and Switzerland. It provides “Quantum as a Service (QaaS)” in three core areas, the first one being “Quantum Algorithms as a Service.” Here, customers are provided access to an extensive library of algorithms, such as hybrid quantum optimization and hybrid quantum neural

networks, which can be used for solving complex logistics problems or pattern recognition, among other things. Terra Quantum also develops new quantum algorithms for its customers or adapts existing algorithms to their specific needs. Secondly, through “Quantum Computing as a Service,” Terra Quantum offers its customers access to its proprietary high-performance simulated quantum processing units (QPU), the quantum ecosystem’s physical QPUs, while also developing native QPUs. The third division is “Quantum Security as a Service,” through which Terra Quantum offers its unique solutions for secure quantum and post quantum communications worldwide.

Visit us on LinkedIn and our webpage.

Mike Kilroy
HKA, Inc. Marketing Communications
+1 714-422-0927
email us here