NIST Confirms Quantum Bridge Compliance with Quantum-Safe Security Standards Through CAVP Certification

Quantum Bridge now certified for US standards on quantum-safe cybersecurity, and adds a second protocol to its solution to meet the guidance of other countries

TORONTO, ONTARIO, CANADA, January 14, 2025 /EINPresswire.com/ -- Quantum Bridge, maker of a range of advanced quantum-safe cybersecurity solutions, today announces that the US National Institute of Standards and Technology (NIST) has confirmed the company's technology meets its standards under the Cryptographic Algorithm Validation Program (CVAP). The approvals process is now complete, and this outcome verifies that Quantum Bridge offers its clients encryption which protects against the emerging threat of cyberattacks using quantum computers.

> This certification from NIST is a validation of the work Quantum Bridge has been doing for the last 5 years. We are confident that there is no safer data-security solution available on the market"
>
> *Mattia Montagna, CEO at Quantum Bridge*

NIST recently approved Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) encryption as one of four standards which it considers to be secure against cyberattacks using a quantum computer. Quantum Bridge has incorporated ML-KEM into its solution, and compliments that NIST standard with its own patented Distributed Symmetric Key Establishment (DSKE) technology. Customers can now have confidence that the company's data-protection solutions meet the highest global standards, and even exceed them in some areas.

"Receiving this certification from NIST is a validation of the work Quantum Bridge has been doing for the last 5 years. We are confident that there is no safer data-security solution available on the market," said Mattia Montagna, CEO at Quantum Bridge. "Not only do we meet the NIST standard, but we also add to it. Many governments are now recognizing that using a solution containing a combination of protocols is the best way to prevent cyberattacks of any kind, including those carried out with a quantum computer."

Indeed, on November 27 of last year, a joint statement was issued by 18 EU member states. The cybersecurity groups within each of these governments have "strongly recommended the deployment of PQC in hybrid solutions for most use-cases, i.e. combining a deployed

cryptographic scheme with PQC in such a way that the combination remains secure even if one of its components is broken." This is exactly the approach Quantum Bridge has taken, as demonstrated by the company and its partners during a technology showcase for G7 representatives at a workshop in Rome in the fall of 2024.

While they have shown a strong interest, government stakeholders are not the only ones looking to adopt quantum-safe solutions. This technology also appeals to telecommunications companies around the world, especially as it pertains to 5G and 6G infrastructure. That equipment will be in use for the next 10-20 years, making it more likely to be exposed to quantum threats in the future, and therefore requires protection. There is also a similar need for this technology to safeguard networks in the banking sector, as well as for protecting critical infrastructure such as the power grid.

"The primary objective at Quantum Bridge is to help our customers understand and effectively counter quantum threats," Montagna added. "Some of these interested parties are now testing our solution and others are in the planning stage, while some have already begun to deploy this technology to protect their data and systems."

Combining DSKE and ML-KEM in a single encryption solution creates a double-layered process for preventing quantum aided attacks, including 'harvest-now and decrypt later' attacks. DSKE encryption is highly scalable, has no distance limit, and provides information-theoretic security via novel protocols for data sharing in both network security and mobile applications. This hybrid approach corresponds perfectly with the recommendations of multiple European governments and agencies which have suggested that post quantum cryptography, combined with the adoption of symmetric keying such as DSKE, is their preferred method of protecting against the quantum threat.

About Quantum Bridge
Quantum Bridge was founded by Dr. Mattia Montagna and Professor Hoi-Kwong Lo, leveraging decades of expertise developed at the University of Toronto. The company offers a suite of unbreakable quantum-safe communication solutions for discerning customers who absolutely cannot afford a breach. Quantum Bridge is also actively researching cutting-edge engineering and theoretical problems related to achieving long-distance quantum communication, and is developing multiple proprietary technologies to make current internet and cellular networks quantum-resilient. For additional information on these or other data-security innovations from Quantum Bridge, please visit the company's website.

Steven La Barbera
FTG Media Inc.
+1 647-715-1774
email us here
Visit us on social media:
LinkedIn