VISION by protiviti

In Focus

August 28,
2024

NIST unveils post-quantum cryptography standards. What does it mean?

By Konstantinos Karagiannis

Director, Quantum Computing Services, Protiviti

Earlier this month, the National Institute of Standards and Technology (NIST) approved three post-quantum cryptography (PQC) standards that constitute the first significant steps towards protecting critical services from quantum computers being used to break the encryption of sensitive and classified information for both business and government.

Why it matters

The rapid evolution of quantum computing has brought numerous concerns around cybersecurity, particularly data encryption. The theoretical power offered by quantum computers can decrypt the most complicated encryption schemes in use today in just a matter of seconds. NIST sees these new standards as a blueprint for governments and private sector organisations worldwide to deploy to mitigate the potential threats quantum computing may present.

Acknowledging the threats of quantum computing, businesses and government agencies have been working to protect data. Back in 2016, NIST launched a process where industry and government leaders could collaborate on the development of PQC standards. IBM researchers developed two of the three standards, while the third was co-developed by a researcher who recently joined IBM. Some major businesses, including Apple, Meta and Google have been quick to act and have been working with hybrid post-quantum solutions featuring draft versions of the finalised standards and are actively implementing new encryption technologies to mitigate potential threats.

What they say

Laurie E. Locascio, Under Secretary of Commerce for Standards and Technology and NIST Director

"Quantum computing technology could become a force for solving many of society's most intractable problems, and the new standards represent NIST's commitment to ensuring it will not simultaneously disrupt our security. These finalised standards are the capstone of NIST's efforts to safeguard our confidential electronic information."

Duston Moody, NIST mathematician and head of the PQC standardisation project

"We encourage system administrators to start integrating [the standards] into their systems immediately because full integration will take time. There is no need to wait for future standards. We need to be prepared in case of an attack that defeats the algorithms in these three standards, and we will continue working on backup plans to keep our data safe."

What we say

Eventually, we're going to cross that line of about 4,000 or so logical qubits that can crack encryption. When that happens, certain secrets will be exposed, and we can't just flip a switch and rewrite everything. We can't just have everyone set up with new encryption standards overnight—that all takes time. These NIST standards are a significant step in that process to help protect sensitive and classified information for both the public and private sectors. The U.S. government set a deadline of 2035 to be ready, but that feels too far off. I see 2030 as when we have a potential for machines capable of cracking encryption—and maybe sooner—so the private sector, especially, should be moving quickly on this, and these standards are a good starting point.

The bottom line

Even though quantum computers that can crack encryption could be a decade away, attackers are harvesting encrypted data, regulators will soon come calling, and migration to PQC will take time. Business and government leaders should begin the process of migrating data to post-quantum cryptography, including inventorying and managing data to become "crypto-agile" as soon as possible.

- **Know your crypto**: Understand the cryptographic algorithms and protocols currently in use within your organisation.
- **Abstract it out**: Design your systems in a way that allows for easy replacement of cryptographic algorithms.
- **Manage your data**: Ensure that your data is protected and that you have a clear understanding of where and how cryptographic keys are used.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk, and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2024 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, and with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About VISION by Protiviti

VISION by Protiviti is a global content resource exploring big, transformational topics that will alter business over the next decade and beyond. Written for the C-suite and boardroom executives worldwide, *VISION by Protiviti* examines the impacts of disruptive forces shaping the world today and in the future. Through a variety of voices and a diversity of thought, *VISION by Protiviti* provides perspectives on what business will look like in a decade and beyond.

protiviti®