https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

National Institute of Standards and Technology
U.S. Department of Commerce

NEWS (https://www.nist.gov/news-events/news)

NIST Releases First 3 Finalized Post-Quantum Encryption Standards

August 13, 2024

- NIST has released a final set of encryption tools designed to withstand the attack of a quantum computer.
- These post-quantum encryption standards secure a wide range of electronic information, from confidential email messages to e-commerce transactions that propel the modern economy.
- NIST is encouraging computer system administrators to begin transitioning to the new standards as soon as possible.

Credit: J. Wang/NIST and Shutterstock

GAITHERSBURG, Md. — The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has finalized its principal set of encryption algorithms

(https://www.federalregister.gov/public-inspection/2024-17956/issuance-of-federal-information-processing-standards) designed to withstand cyberattacks from a quantum computer.

Researchers around the world are racing to build quantum computers that would operate in radically different ways from ordinary computers and could break the current encryption that provides security and privacy for just about everything we do online. The algorithms announced today (https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved) are specified in the first completed standards from NIST's post-quantum cryptography (PQC) standardization project, and are ready for immediate use.

The three new standards are built for the future. Quantum computing technology is developing rapidly, and some experts predict that a device with the capability to break current encryption methods could appear within a decade (https://www.rand.org/pubs/commentary/2023/09/when-a-quantum-computer-is-able-to-break-our-encryption.html), threatening the security and privacy of individuals, organizations and entire nations.

Want to learn more about post-quantum cryptography? Check out our explainer. (https://www.nist.gov/cybersecurity/what-post-quantum-cryptography)

"The advancement of quantum computing plays an essential role in reaffirming America's status as a global technological powerhouse and driving the future of our economic security," said Deputy Secretary of Commerce Don Graves. "Commerce bureaus are doing their part to ensure U.S. competitiveness in quantum, including the National Institute of Standards and Technology, which is at the forefront of this whole-of-government effort. NIST is providing invaluable expertise to develop innovative solutions to our quantum challenges, including security measures like post-quantum cryptography that organizations can start to implement to secure our post-quantum future. As this decade-long endeavor continues, we look forward to continuing Commerce's legacy of leadership in this vital space."

The standards — containing the encryption algorithms' computer code, instructions for how to implement them, and their intended uses — are the result of eight-year effort (https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information) managed by NIST, which has a long history (https://www.nist.gov/cryptography) of developing encryption. The agency has rallied the world's cryptography experts to conceive, submit and then evaluate cryptographic algorithms that could resist the assault of quantum computers. The nascent technology could revolutionize fields from weather forecasting to fundamental physics to drug design, but it carries threats as well.

Encryption carries a heavy load in modern digitized society. It protects countless electronic secrets, such as the contents of email messages, medical records and photo libraries, as well as information vital to national security. Encrypted data can be sent across public computer networks because it is unreadable to all but its sender and intended recipient.

Encryption tools rely on complex math problems that conventional computers find difficult or impossible to solve. A sufficiently capable quantum computer, though, would be able to sift through a vast number of potential solutions to these problems very quickly, thereby defeating current encryption. The algorithms NIST has standardized are based on different math problems that would stymie both conventional and quantum computers.

“These finalized standards include instructions for incorporating them into products and encryption systems,” said NIST mathematician Dustin Moody, who heads the PQC standardization project. “We encourage system administrators to start integrating them into their systems immediately, because full integration will take time.”

Moody said that these standards are the primary tools for general encryption and protecting digital signatures.

NIST also continues to evaluate two other sets of algorithms that could one day serve as backup standards.

One of these sets consists of three algorithms designed for general encryption but based on a different type of math problem than the general-purpose algorithm in the finalized standards. NIST plans to announce its selection of one or two of these algorithms by the end of 2024.

The second set includes a larger group of algorithms designed for digital signatures. In order to accommodate any ideas that cryptographers may have had since the initial 2016 call for submissions (https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information), NIST asked the public for additional algorithms in 2022 (https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals) and has begun a process of evaluating them. In the near future, NIST expects to announce about 15 algorithms from this group that will proceed to the next round of testing, evaluation and analysis.

While analysis of these two additional sets of algorithms will continue, Moody said that any subsequent PQC standards will function as backups to the three that NIST announced today.

“There is no need to wait for future standards,” he said. “Go ahead and start using these three. 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. But for most applications, these new standards are the main event.”

More Details on the New Standards

Encryption uses math to protect sensitive electronic information, including secure websites and emails. Widely used public-key encryption systems (https://csrc.nist.gov/glossary/term/public_key_cryptography), which rely on math problems that

computers find intractable, ensure that these websites and messages are inaccessible to unwelcome third parties. Before making the selections, NIST considered not only the security of the algorithms' underlying math, but also the best applications for them.

The new standards are designed for two essential tasks for which encryption is typically used: general encryption, used to protect information exchanged across a public network; and digital signatures, used for identity authentication. NIST announced its selection of four algorithms (https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms) — CRYSTALS-Kyber, CRYSTALS-Dilithium, Sphincs+ and FALCON — slated for standardization in 2022 and released draft versions of three of these standards (https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers) in 2023. The fourth draft standard based on FALCON is planned for late 2024.

While there have been no substantive changes made to the standards since the draft versions, NIST has changed the algorithms' names to specify the versions that appear in the three finalized standards, which are:

- **Federal Information Processing Standard (FIPS) 203** (https://csrc.nist.gov/pubs/fips/203/final), intended as the primary standard for general encryption. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation. The standard is based on the CRYSTALS-Kyber algorithm, which has been renamed ML-KEM, short for Module-Lattice-Based Key-Encapsulation Mechanism.
- **FIPS 204** (https://csrc.nist.gov/pubs/fips/204/final), intended as the primary standard for protecting digital signatures. The standard uses the CRYSTALS-Dilithium algorithm, which has been renamed ML-DSA, short for Module-Lattice-Based Digital Signature Algorithm.
- **FIPS 205** (https://csrc.nist.gov/pubs/fips/205/final), also designed for digital signatures. The standard employs the Sphincs+ algorithm, which has been renamed SLH-DSA, short for Stateless Hash-Based Digital Signature Algorithm. The standard is based on a different math approach than ML-DSA, and it is intended as a backup method in case ML-DSA proves vulnerable.

Similarly, when the draft FIPS 206 standard built around FALCON is released, the algorithm will be dubbed FN-DSA, short for FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm.

Information technology (https://www.nist.gov/topic-terms/information-technology), Cybersecurity (https://www.nist.gov/topic-terms/cybersecurity), Cryptography (https://www.nist.gov/topic-terms/cryptography) and Privacy (https://www.nist.gov/topic-terms/privacy)

Media Contact

- Chad Boutin (https://www.nist.gov/people/chad-boutin)
  charles.boutin@nist.gov (https://www.nist.govmailto:charles.boutin@nist.gov)
  (301) 975-4261

Related News

NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers (https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers)

Related Links

What Is Post-Quantum Cryptography? (https://www.nist.gov/cybersecurity/what-post-quantum-cryptography)
FIPS 203 (https://csrc.nist.gov/pubs/fips/203/final)
FIPS 204 (https://csrc.nist.gov/pubs/fips/204/final)
FIPS 205 (https://csrc.nist.gov/pubs/fips/205/final)
Post-Quantum Cryptography Standardization Project (https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization)
Released August 13, 2024, Updated August 26, 2024