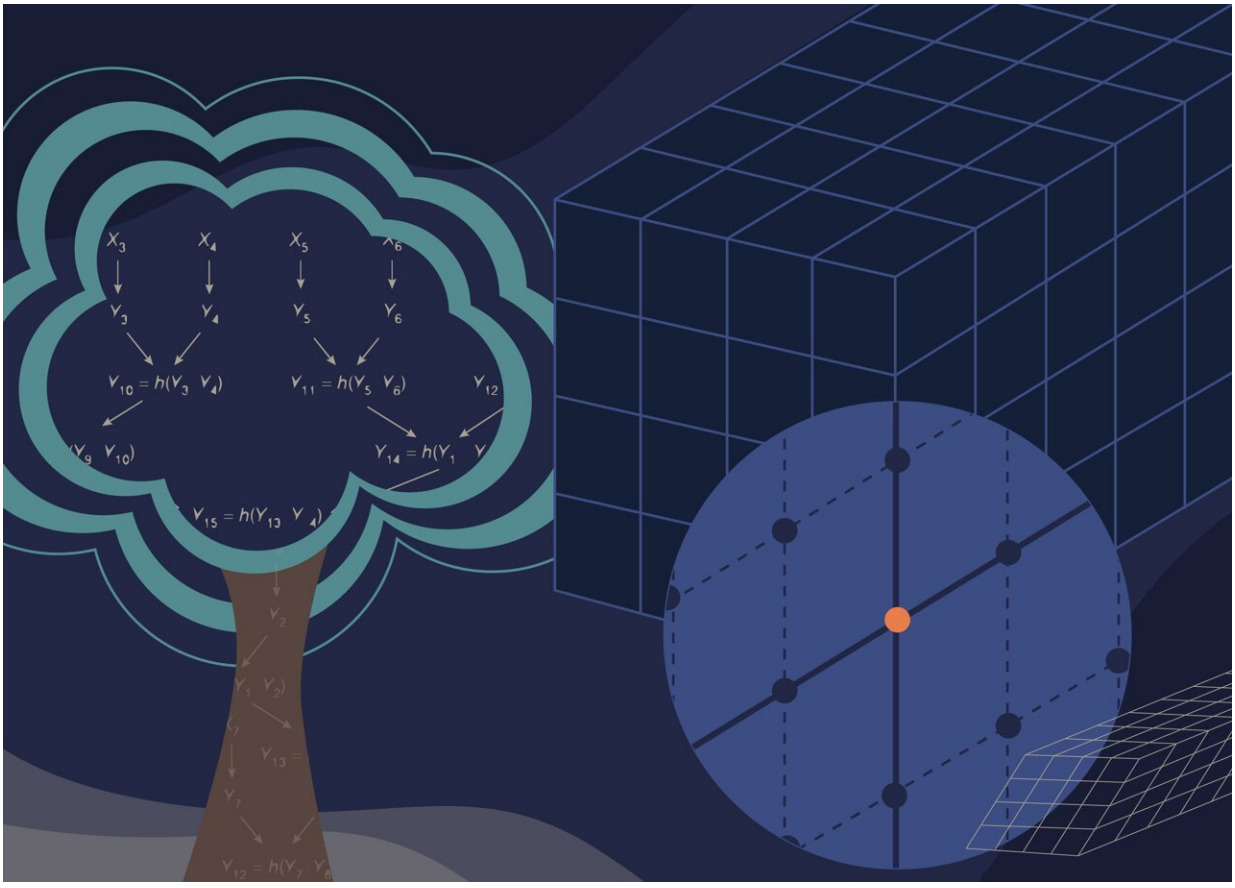
NIST announces first four quantum-resistant cryptographic algorithms

July 5 2022



The first four algorithms NIST has announced for post-quantum cryptography are based on structured lattices and hash functions, two families of math problems that could resist a quantum computer's assault. Credit: N. Hanacek/NIST

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has chosen the first group of encryption tools that are designed to withstand the assault of a future quantum computer, which could potentially crack the security used to protect privacy in the digital systems we rely on every day—such as online banking and email software. The four selected encryption algorithms will become part of NIST's post-quantum cryptographic standard, expected to be finalized in about two years.

"Today's announcement is an important milestone in securing our sensitive data against the possibility of future cyberattacks from quantum computers," said Secretary of Commerce Gina M. Raimondo. "Thanks to NIST's expertise and commitment to cutting-edge technology, we are able to take the necessary steps to secure electronic information so U.S. businesses can continue innovating while maintaining the trust and confidence of their customers."

The announcement follows a six-year effort managed by NIST, which in 2016 called upon the world's cryptographers to devise and then vet encryption methods that could resist an attack from a future quantum computer that is more powerful than the comparatively limited machines available today. The selection constitutes the beginning of the finale of the agency's post-quantum cryptography standardization project.

"NIST constantly looks to the future to anticipate the needs of U.S. industry and society as a whole, and when they are built, quantum computers powerful enough to break present-day encryption will pose a serious threat to our information systems," said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. "Our post-quantum cryptography program has leveraged the top minds in cryptography—worldwide—to produce this first group of quantum-resistant algorithms that will lead to a standard and significantly increase the security of our digital information."

Four additional algorithms are under consideration for inclusion in the standard, and NIST plans to announce the finalists from that round at a future date. NIST is announcing its choices in two stages because of the need for a robust variety of defense tools. As cryptographers have recognized from the beginning of NIST's effort, there are different systems and tasks that use encryption, and a useful standard would offer solutions designed for different situations, use varied approaches for encryption, and offer more than one algorithm for each use case in the event one proves vulnerable.

Encryption uses math to protect sensitive electronic information, including the secure websites we surf and the emails we send. Widely used public-key encryption systems, which rely on math problems that even the fastest conventional computers find intractable, ensure these websites and messages are inaccessible to unwelcome third parties.

However, a sufficiently capable quantum computer, which would be based on different technology than the conventional computers we have today, could solve these math problems quickly, defeating encryption systems. To counter this threat, the four quantum-resistant algorithms rely on math problems that both conventional and quantum computers should have difficulty solving, thereby defending privacy both now and down the road.

The algorithms are designed for two main 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. All four of the algorithms were created by experts collaborating from multiple countries and institutions.

For general encryption, used when we access secure websites, NIST has selected the CRYSTALS-Kyber algorithm. Among its advantages are comparatively small encryption keys that two parties can exchange

easily, as well as its speed of operation.

For digital signatures, often used when we need to verify identities during a digital transaction or to sign a document remotely, NIST has selected the three algorithms CRYSTALS-Dilithium, FALCON and SPHINCS+ (read as "Sphincs plus"). Reviewers noted the high efficiency of the first two, and NIST recommends CRYSTALS-Dilithium as the primary algorithm, with FALCON for applications that need smaller signatures than Dilithium can provide. The third, SPHINCS+, is somewhat larger and slower than the other two, but it is valuable as a backup for one chief reason: It is based on a different math approach than all three of NIST's other selections.

Three of the selected algorithms are based on a family of math problems called structured lattices, while SPHINCS+ uses hash functions. The additional four algorithms still under consideration are designed for general encryption and do not use structured lattices or hash functions in their approaches.

While the standard is in development, NIST encourages security experts to explore the new algorithms and consider how their applications will use them, but not to bake them into their systems yet, as the algorithms could change slightly before the standard is finalized.

More information: Algorithms: csrc.nist.gov/Projects/post-qu … /round-3-submissions

Provided by National Institute of Standards and Technology

cryptographic-algorithms.html