How the United States Is Developing Post-Quantum Cryptography

When practical quantum computing finally arrives, it will have the power to crack the standard digital codes that safeguard online privacy and security for governments, corporations, and virtually everyone who uses the Internet.That’s why a U.S. government agency has challenged researchers to develop a new generation of quantum-resistant cryptographic algorithms.

Many experts don’t expect a [quantum computer](https://spectrum.ieee.org/tech-talk/computing/hardware/race-for-the-quantum-prize-rises-to-national-priority) capable of performing the complex calculations required to crack modern cryptography standards to become a reality [within the next 10 years](https://spectrum.ieee.org/tech-talk/computing/hardware/the-us-national-academies-reports-on-the-prospects-for-quantum-computing). But the [U.S. National Institute of Standards and Technology (NIST)](https://www.nist.gov/) wants to stay ahead by getting new cryptographic standards ready by 2022. The agency is overseeing the second phase of its [Post-Quantum Cryptography Standardization Process](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization) to narrow down the best candidates for quantum-resistant algorithms that can replace modern cryptography.

“Currently intractable computational problems that protect widely-deployed cryptosystems, such as RSA and Elliptic Curve-based schemes, are expected to become solvable,” says [Rafael Misoczki](https://www.linkedin.com/in/rafael-misoczki-phd-24b33013/), a cryptographer at the Intel Corporation and a member of two teams (named Bike and Classic McEliece) involved in the NIST process. “This means that quantum computers have the potential to eventually break most secure communications on the planet.”

Misoczki was one of more than 250 registered attendees who signed up for the [Second PQC Standardization Conference](https://csrc.nist.gov/Events/2019/second-pqc-standardization-conference) held at the University of California, Santa Barbara from 22 to 25 August. The event featured presentations from almost all of the teams working on 26 candidate algorithms, which were winnowed down from 69 first-round candidates.

NIST hopes these [second-round candidates](https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions) will evolve beyond mere proofs of concept and begin benchmarking tests. The stakes are high, given that a quantum computing breakthrough could threaten to undermine security for hundreds of billions of dollars in e-commerce alone—not to mention the trillions of dollars at risk in the broader digital economy. Still, many researchers have cautioned that NIST should take its time to evaluate the new class of candidates for [post-quantum cryptography](https://spectrum.ieee.org/tech-talk/computing/networks/the-practical-limits-of-quantum-cryptography) before selecting any finalists.

## **Meet the Quantum-Resistant Algorithms**

The NIST process is considering algorithms that fall into two general categories, Misoczki explains. The first category includes key-establishment algorithms that enable two parties that have never met to agree on a shared secret. This category also includes public-key encryption algorithms—such as RSA and Elliptic Curve cryptography—that do the same thing, but are less efficient.

A second category involves algorithms for digital signatures that ensure the authenticity of data. Such digital signatures feature in code-signing applications that establish confidence that a program was created by the intended developer and not by a hacker.

Both categories require new algorithms based upon mathematical problems which even quantum computers couldn’t crack. There are several approaches to post-quantum cryptography algorithms under consideration, and each has pros and cons. For example, “families such as code-based cryptography enjoy a long history of public scrutiny, while [lattice-based cryptography](https://spectrum.ieee.org/tech-talk/computing/embedded-systems/circuit-secures-the-iot-against-quantum-attack) offers very fast algorithms,” Misoczki says.

The tradeoffs between each approach can have significant real-world implications for computing applications and devices. Lattice-based cryptography is even faster than modern cryptographic approaches such as RSA, but its bigger data size could make a difference if bandwidth is relatively scarce.

That’s why it makes sense for NIST to standardize algorithms from several different approaches, says [Vadim Lyubashevsky](https://researcher.watson.ibm.com/researcher/view.php?person=zurich-vad), a cryptography researcher at the IBM Zurich Research Laboratory in Switzerland and participant in the NIST process. “Even if we were sure they were all secure, no candidate is best in every area,” Lyubashevsky says.

Much remains unknown about these candidate algorithms that will likely replace large parts of the world’s infrastructure underpinning secure global communication, says [Peter Schwabe](https://cryptojedi.org/peter/), a computer security researcher at Radboud University in the Netherlands. More development and testing is needed to assess each algorithm’s actual cryptographic security against the best possible attacks, measure its security-performance tradeoffs, develop techniques to implement the algorithms securely, and find things that can go wrong when deploying them.

“What seems quite clear by now is that the new schemes have massively different performance characteristics than the ones we use today and many have subtly different security properties,” Schwabe says.

## **Cooperative Spirit vs. Competitive Streak**

The NIST challenge has brought together both academic researchers focused on theoretical work and tech industry experts familiar with real-world performance needs and security demands. The agency initially described it as a “competition-like process,” but seems eager to encourage a cooperative spirit among participants.

Some researchers have joined multiple teams working on different algorithms. For example, Lyubashevsky is a member of groups working on algorithms such as CRYSTAL-KYBER, CRYSTALS-DILITHIUM, and Falcon. Schwabe belongs to seven teams focused on specific algorithms: CRYSTALS-KYBER, CRYSTALS-DILITHIUM, Classic McEliece, NewHope, SPHINCS+, NTRU, and MQDSS.

Teams openly share frameworks and feedback on a single mailing list—an approach that has benefits and drawbacks. “Certain vocal and at times outright impolite personalities dominate the mailing list, causing others to hesitate to contribute their work or questions,” wrote one anonymous participant in response to a NIST survey.

Most of the community seems dedicated to working together, says Misoczki, who has observed “more of a cooperative environment rather than a competitive situation” despite some differences of opinion.

Schwabe also described the community’s cooperative spirit, but noted that some individuals seem to have more of a competitive streak. “Unfortunately, some participants are not that cooperative, and have a focus on pushing for ‘their’ (often patented) schemes rather than working as a community on finding the best scheme(s) to standardize and use in the future,” Schwabe wrote in an email.

Some of the competing algorithms represent relatively minor variations on the same cryptographic approaches. Lyubashevsky suggested that NIST keep the participants focused on the common standardization goal by asking for specific cryptographic features that the agency wants in candidate algorithms.

“It would be good to say ‘look, forget the names of people attached to these things, here are the features we want to see,’” Lyubashevsky says.

## **New Post-Quantum Cryptography Standards**

NIST plans to draft standards for post-quantum cryptography around 2022. But researchers have urged the agency to avoid rushing the process of vetting all the candidate algorithms. Their anonymous feedback came from a [NIST survey](https://csrc.nist.gov/CSRC/media/Presentations/nist-pqc-standards-next-steps/images-media/liu-nist-pqc-next-steps-2019.pdf) that was shared at the end of the Second PQC Standardization Conference in August.

“NIST should not be aiming to conclude the process and have standards written by 2022,” wrote one survey respondent. “This is simply too fast to get proper answers…. Much more research is needed.”

Another survey respondent proposed that “NIST should hold off creating any standard before 2025 and fund research efforts to look at all the candidates until that time,” in order “to give researchers a chance to innovate.”

One survey respondent painted an especially dire picture of the possible consequences of rushing ahead: “Attempting to end this process in just a couple more years is dangerous and could lead to disastrous results and/or a loss of perceived legitimacy of the process and output.”

Many pointed to the [need for more cryptanalysis](https://spectrum.ieee.org/searchContent?q=cryptanalysis) to thoroughly investigate the possible weaknesses of each algorithm. One person urged NIST to sponsor more academic research at U.S. universities to further develop “the science of quantum cryptanalysis.”

“The problem with cryptography in general is that cryptanalysis is such an unrewarding process,” Lyubashevsky says. "ither you fail and no one knows that you tried and failed, or you succeed and you get your five minutes of fame, and then that algorithm that you wrote is never used again.”

NIST may be partly counting on the idea that different teams will try to break each other’s algorithms. But Lyubashevsky suggested that the agency should also look into requiring researchers to check another group’s work, or perhaps make cryptanalysis part of the conditions for funding the theoretical work in developing the algorithms.

## **When Will Computers Crack Cryptography?**

Nobody knows exactly when quantum computing will render modern cryptographic algorithms useless. One complication is that the first government or organization to develop a practical quantum computer could gain a lot by simply keeping quiet, breaking modern cryptography systems and hoovering up the world’s secrets.

“I see a good chance that the first large universal quantum computers will be available only to government agencies who will not exactly advertise that they have such computing capabilities,” Schwabe says. He sees a “realistic chance that within 20 years there will be quantum computers that break the cryptography we have in wide use today.”

What cryptography researchers do know is that it can take a long time for the world’s governments and industries to adopt the latest cryptographic standards. Even though Elliptic Curve Cryptography was first proposed in the late 1980s, much of the world still relies on older RSA cryptography that appeared in the late 1970s. That’s why there is still some urgency behind NIST’s standardization effort for post-quantum cryptography, even if practical quantum computing remains a few decades away.

“Predicting when large-scale quantum computers will become available is a hard question,” Misoczki says. “On the other hand, the crypto community knows that transitioning crypto algorithms takes several years, even decades.”

Luckily, forward-thinking organizations holding extremely sensitive data don’t need to wait for the NIST standardization process to play out before taking steps to future-proof their systems. Instead, they could simply go ahead and adopt some of the candidate algorithms in the NIST process that have been published publicly online and are free to use.

“If you really have sensitive data, do it now, migrate yourself,” Lyubashevsky says. “If you don't have such data, then I think it'd be good to wait five years and let the competition run its course to come up with a nice standard that most people are happy with.”

As for those willing to wait, Lyubashevsky expressed confidence that cryptographers working together with NIST would be ready for a future with [quantum computing](https://spectrum.ieee.org/searchContent?q=quantum+computing).

“We’ll definitely have post-quantum cryptography before quantum computers are ready,” Lyubashevsky says. “I think if we take the next five years to really get the standards of post-quantum cryptography right, it’s enough time for virtually every application.”