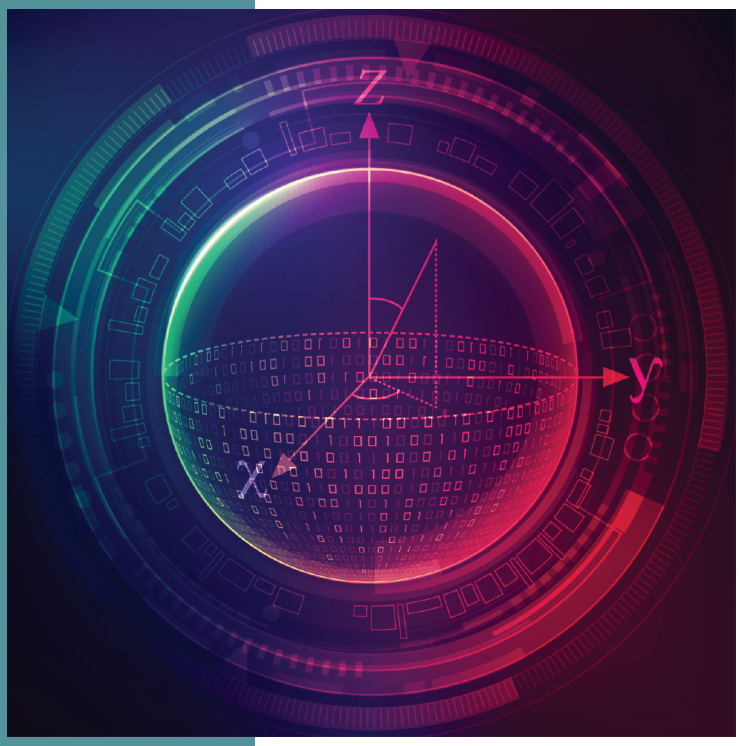
Securing Data in the Quantum Era



©Getty

Whenever you log in to a website, send an email, or make an online purchase, you're counting on your data being sent securely, without hackers being able to crack the code. Our standard cryptographic systems hinge on mathematical problems that stump present-day computers, like finding the prime factors of a very large number. But in the coming decades, powerful quantum computers are expected to be able to rapidly solve some such problems, threatening the security of our online communications. To develop new methods that can withstand even the most sophisticated quantum computer, cryptographers are using a wide range of mathematical tools—many of which were originally developed without any real-life applications in mind.

The National Institute of Standards and Technology is leading an effort to standardize algorithms, or step-by-step processes, for protecting our data in the quantum future. NIST researchers are testing the security, speed, and cost of dozens of proposed algorithms. The mathematics involved includes high-dimensional lattices, linear error-correcting codes, isogenies between elliptic curves, and more. NIST's goal is to identify the best quantum-resistant algorithms for digital signatures (which verify the authenticity of a document), public-key encryption (which allows anyone to send a message, but only the intended recipient to read it), and the generation of cryptographic keys (which are used for encryption and decryption). Then, cryptographers will develop standardized versions of these algorithms. In the coming years, the new, quantum-safe methods will gradually replace today's security systems everywhere from government computers to the phone in your pocket.

For More Information: "How the United States Is Developing Post-Quantum Cryptography" by Jeremy Hsu, *IEEE Spectrum*, September 6, 2019.

Watch an interview with an expert!

MM/158

AMS American Mathematical Society

*The **Mathematical Moments** program promotes appreciation and understanding of the role mathematics plays in science, nature, technology, and human culture.*

www.ams.org/mathmoments