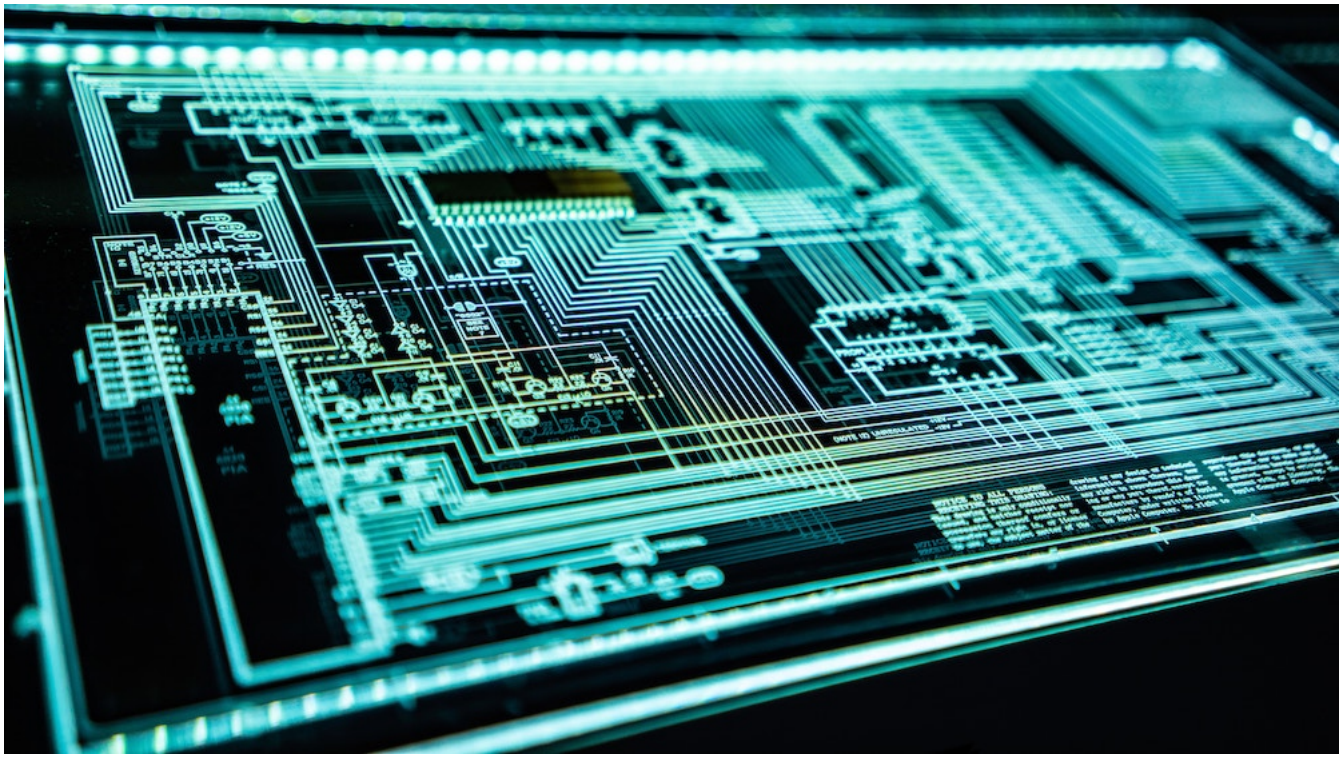
Quantum computing is all but set to transform the IT industry-- and to help enterprises prepare for such change, Sectigo offers a set of 15 educational resources for security professionals in the form of a white paper, podcasts and articles.



The computing architecture takes advantage of quantum mechanics to deliver capabilities beyond what is possible using traditional binary computing. However, quantum computers are destined to render the cryptographic underpinnings of current digital systems insecure once they reach a certain level of maturity. After all, quantum computers are (at least in theory) highly effective at factorising numbers, making them extremely capable at breaking the RSA and ECC (Elliptic Curve Cryptography) underpinning digital systems. And no, increasing key sizes is not a viable solution. Instead, Public Key Infrastructure (PKI) systems need to migrate to quantum-resistant encryption algorithms before quantum computers break current encryption methods.

PKI is necessary for the secure operation of all confidential and mission-critical digital processes in the global economy, and the impact of insecure PKI is so vast it can bring about what Sectigo dubs the Quantum Apocalypse. Currently thought leaders from industry, academia

and government are working together on quantum-resistant cryptographic solutions, with the National Institute of Standards and Technology (NIST) leading the effort to identify substitutes for the RSA and ECC.

Successful quantum-resistant algorithms must be difficult to break using brute-force attacks from both traditional and quantum architectures, while still meeting the performance standards of current algorithms. Thus, they must be fast both the encryption and decryption (via private keys) side when using traditional computers, while impractical to decrypt (without private keys) using quantum or traditional architectures. They should also generated encrypted data of reasonable size for storage and transmission across networks and the internet, and compatible with a wide range of software, hardware and services.

“While no one can definitively say when quantum computers will reach the point of defeating RSA and ECC, many estimates place that date in the next 10 or 15 years. Any organisation that does not migrate by then will be vulnerable,” Sectigo concludes. “At Sectigo, we are working with our large base of enterprises, schools, and government agencies to help them achieve crypto agility by putting in place the systems and automation capabilities necessary to ensure rapid and comprehensive migration to these new standards once they arrive.”

Go The Search for Quantum-Resistant Cryptography: Understanding the Future Landscape