Nascent Quantum Computing Poses Threat to Cybersecurity

A scalable, fault-tolerant quantum computer would pose a major threat to widely used algorithms

Sara Castellanos Sep 13, 2017 2:34 pm ET

LONDON – The threat of a cyber attack by hackers or rogue nation states with access to quantum computers is becoming real enough that scientists and public officials are convening here this week in part to urge companies to develop a plan for defense.

More than 150 cryptographers, business executives and public officials attended the first day of the three-day Quantum Safe Workshop, hosted by organizations including the University of Waterloo's Institute for Quantum Computing, the European Telecommunications Standards Institute and

United Kingdom's Quantum Technology Hub for Quantum Communications.

When the conference was first founded in 2013, the possibility of a quantum computing cyber threat becoming a reality within a decade was not as serious. Now, as companies are advancing toward building the world's first large-scale quantum computer sooner than previously thought, the threat to widely used encryption algorithms could materialize within 10 years, said Michele Mosca, co-founder of the Institute for Quantum Computing at the University of Waterloo.

"Every year the dial is turning, it's heating up non-trivially," Dr. Mosca said in an interview at the event.

Classical computers, including supercomputers, use binary digits, or bits, which can either be 0s or 1s. Quantum computers use quantum binary digits, or qubits, which represent and store information in both 0s and 1s simultaneously. The computers have the potential to sort through a vast number of possibilities — more than the number of atoms in the universe — to come up with a probable solution. The calculations could be completed as fast as a fraction of a second.

A scalable, fault-tolerant quantum computer has not been built yet, though Dr. Mosca says there's a chance it could be built within 10 years, which would pose a major threat to widely used algorithms including RSA.

The RSA algorithm is vulnerable because it's based on integer factorization, which is essentially reverse multiplication. It would take classical computers, even supercomputers, several years to quickly factor large numbers that are 500 or 600 digits long, which means solving for integer factorization is impractical and inefficient. Quantum computers, though, are capable of solving integer factorization problems perhaps trillions of times faster than a classical computer, as WSJ has previously reported.

RSA, named after its developers Ron Rivest, Adi Shamir and Leonard

Adleman, is at the heart of today's encryption methods and is used for securing e-mail, online banking, e-commerce and electronic communications such as those in the health-care industry. Executives at RSA Security LLC, the cybersecurity company founded by RSA's inventors and now a subsidiary of Dell EMC Infrastructure Solutions Group, told the WSJ previously that new cryptographic algorithms will be available in the future.

Panelists at the conference said the threat of a quantum computing-based attack also applies to devices connected to the internet, ranging from TVs to cars and connected lights.

Brian LaMacchia, head of the security and cryptography team at Microsoft Research and a Microsoft Corp. distinguished engineer, said executives should begin taking an inventory of all of the systems using public key cryptosystems such as RSA and develop a formal plan for how to guard them against quantum computers.

"Understand that a transition is coming and make sure you're not creating a future problem for yourself," Dr. LaMacchia said in an interview at the event. He added that more Microsoft enterprise customers are now asking for briefings on quantum computing and cryptography systems that could potentially help thwart a quantum computing attack.

He also urged companies looking to procure new cybersecurity services from vendors to ask what their plans are for integrating so-called quantum-safe or quantum-resistant algorithms that could potentially thwart a quantum computing attack. "If you don't ask for it, they aren't necessarily going to provide it," he said.

The topic is becoming top of mind for some service providers, including British Telecommunications plc, owned by BT Group PLC.

The company is currently exploring a technique called quantum key distribution that uses quantum mechanics to transmit photons in two states at once. "Any hacker trying to read the secret encryption key that is carried by the photons, forces the photon to adopt one of the two states. This is easily detected and the hacker tracked down. This stops encryption keys being stolen and prevents attacks by quantum computers," said Andrew Lord, head of optical research at BT.

Quantum key distribution and new quantum-resistant algorithms for encryption should be explored simultaneously and companies, public officials and researchers shouldn't wait, said Sir Peter Knight, chair of the Quantum Metrology Institute at the United Kingdom's National Physical Laboratory, at the event.

"One needs to start working on it now," he said. "A decade is not a long time."