Future quantum computers may pose threat to today's most-secure communications

April 9 2020

Credit: CC0 Public Domain

Quantum computers that are exponentially faster than any of our current classical computers and are capable of code-breaking applications could be available in 12 to 15 years, posing major risks to the security of

current communications systems, according to a new RAND Corporation report.

The security risks posed by this new category of computers can be managed if the U.S. government acts quickly, and a centrally coordinated, whole-of-nation approach is the best way to manage those challenges, according to RAND researchers.

"If adequate implementation of new security measures has not taken place by the time capable quantum computers are developed, it may become impossible to ensure secure authentication and communication privacy without major, disruptive changes," said Michael Vermeer, lead author of the report and a physical scientist at nonprofit, nonpartisan RAND. "The United States has the means and very likely enough time to avert a quantum disaster and build a safer future, but only if it begins preparations now."

Standard protocols for postquantum cryptography that can maintain the current level of computing security are expected to be drafted and released within the next five years.

However, the nationwide or global transition necessary to implement the standard protocols and mitigate the vulnerability from quantum computing is expected to take decades—far longer than the time that experts estimated would be available for the task, the report finds.

The report says that the sooner an interoperable standard for postquantum cryptography can be widely implemented, the more the eventual risk will be diminished.

Building cyber-resilience and cryptographic agility into the digital infrastructure also will offer an opportunity to adopt structural improvements in the use of cryptography in communication and

information systems that could improve the nation's ability to respond to both current and future cyber threats.

If the United States acts in time with appropriate policies, risk reduction measures, a whole-of-government approach and a collective sense of urgency, it has an opportunity to build a future communications infrastructure that is as safe or safer than the status quo, according to RAND researchers.

The nation could reap the enormous benefits expected from quantum computing while enhancing privacy and security.

"The advent of quantum computers presents retroactive risk because information being securely communicated today without postquantum cryptography may be captured and held by others now in order to be decrypted and revealed later once quantum computers are created. This presents a vulnerability that urgently needs to be addressed," said Evan Peet, a co-author of the report and an economist at RAND.

More information: The report, "Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption," is available at http://www.rand.org.

Provided by RAND Corporation