Tech Xplore

The new frontier in online security: Quantum-safe cryptography

November 14 2023

Credit: Pixabay/CC0 Public Domain

A team of experts led by Monash University researchers, in collaboration with Australia's national science agency CSIRO, has created an algorithm that can help strengthen online transactions that use

end-to-end encryption against powerful attacks from quantum computers.

Cryptography researchers from Monash University's Faculty of Information Technology and CSIRO's data and digital specialist arm Data61 have developed the most efficient quantum-secure cryptography algorithm, called "LaV," to enhance the security of end-to-end encryption, with potential application across instant messaging services, data privacy, cryptocurrency and blockchain systems.

End-to-end encryption is a way to secure digital communication between a sender and receiver using encryption keys. Mobile messaging services like WhatsApp and Signal use end-to-end encryption so that no one, including the communication system provider, telecom providers, internet providers or hackers can access the information being transmitted between the sender and the receiver.

It would take millions of years for a normal computer or even a supercomputer to hack into and gain access to data protected by end-to-end encryption. But a large-scale quantum computer could break current encryption within minutes and gain access to encrypted information more easily.

Lead researcher of the collaborative quantum security project, Dr. Muhammed Esgin, said the new cryptography tool will help make end-to-end encryption more secure, so online services can withstand hacks or interference from the most powerful quantum computers in the future.

"While end-to-end encryption protocols are quite well established and are used to secure data and messaging in some of the most popular instant messaging applications across the world, currently they are still vulnerable to more sophisticated attacks by quantum computers," Dr. Esgin said.

"This new cryptographic tool can be applied to various mobile applications and online transactions that use end-to-end encryption and is the first practical algorithm that can be used to fortify existing systems against quantum computers."

Co-author of the research and quantum-safe cryptography expert Associate Professor Ron Steinfeld said software for current technology is not being developed, keeping in mind the advent of much more powerful computing devices.

"Over the past few years we have seen many significant cyberattacks and data leaks in Australia alone, clearly showing that we need to pay much more attention to cybersecurity and mitigate vulnerabilities in our systems before such vulnerabilities are exploited by attackers," Associate Professor Steinfeld said.

"Government and Standards organizations worldwide are preparing for the possibility that large scale quantum computers, which can threaten the security of currently deployed encryption systems, could become a reality within the next decade or so.

"Our past experience has shown the process of updating encryption algorithms deployed in existing online systems can also take a decade or more to complete. This means that we need to urgently start updating our cybersecurity infrastructure to use quantum-safe cryptography, to ensure our systems are protected before the approaching quantum threat is realized," Associate Professor Steinfeld added.

This research was conducted in collaboration with researchers Dr. Dongxi Liu and Dr. Sushmita Ruj (now at the University of New South Wales) from CSIRO's Data61, and was presented at Crypto 2023, the 43rd International Cryptology Conference held earlier this year in Santa Barbara, U.S..

"The National Institute of Standards and Technology has been standardizing methods like encryption and digital signatures to protect basic internet security in a post-quantum world. However, these measures are not enough to protect advanced security applications. Our research is filling this gap," said Dr. Liu. "Our new algorithm has been implemented into code by Dr. Raymond Zhao from CSIRO's Data61 and is available open source."

As the next step, the research team is working on building a full quantum-secure key transparency protocol which can be readily deployed in encryption applications.

More information: Paper: Efficient Hybrid Exact/Relaxed Lattice Proofs and Applications to Rounding and VRFs

Provided by Monash University