IBM TO DEPLOY QUANTUM-PROOF CRYPTOGRAPHY C DEVELOPED WITH CWI AND R

Together with CWI, Radboud University and other international partners, IBM Resear developed quantum-safe algorithms for securing d

Press release from CWI
August 29th 2019 | 863 reader

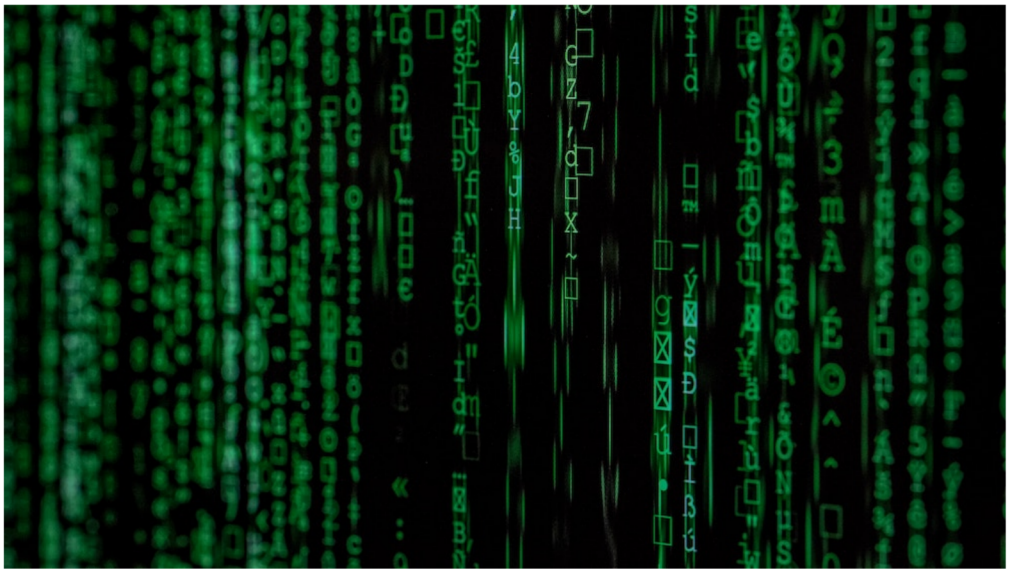

Photo by Markus Spiske on Unsplash

The new algorithms, which are part of the CRYSTALS suite, are based on the hardness c mathematical problems that have not succumbed to any algorithmic attacks, either classic quantum. The team made them open-source and submitted them to National Institute of Standards and Technology (NIST) as a candidate for standardization. IBM has now implemented CRYSTAL in one of the tape drives, making it the world's first quantum computing safe tape drive protot

CRYSTALS (CRYptographic Suite for Algebraic latticeS), contains a secure key encapsulation mechanism calle Kyber, and a secure digital signature algorithm, calle Dilithium. IBM tested CRYSTALS successfully on a prototype IBM TS1160 tape drive using both Kyber and Dilithium to enable the world's first quantum computing safe tape drive. To help clients asses potential risks, IBM Security is also offering a quantum data risk assessment service to help clients develop a quantum- cryptography implementation strateg

Quantum computing is an emerging technology that takes advantage of quantum mechanical phenomena to solve c problems that are effectively impossible to solve on classical computers. There are serious concerns that data protecte current encryption methods may become insecure within the next 10-30 years. While years away, data can be harvested t stored and decrypted in the future with a powerful enough quantum computer. Although the industry is still finalizi quantum cryptography standards, businesses and other organizations already can start preparing today. IBM will begin t quantum-safe cryptography services on its public cloud in 202

At CWI, cryptographer Léo Ducas is working on this research. He is a member of the Cryptology research group at CW headed by Prof. Ronald Cramer. This group investigates fundamental cryptographic questions from a broad scie perspective. CRYSTALS (Cryptographic Suite for Algebraic Lattices) is developed jointly in collaboration with several acader and commercial partners including ENS Lyon, Ruhr-Universität Bochum, Centrum Wiskunde & Informatica (CWI) in Amster and Radboud University. It has been included by OpenQuantumSafe.org to further develop open standards

YOU CAN READ TOO...

▸ CWI Research connects Quantum Computing and optin- 09/28/201

How do you get from Amsterdam to Den Haag as fast as possible? What is the shortest route that passes through several cit Optimization problems like these are everywhere around us. CWI PhD student Sander Gribling studied if and how qua computers can help solve such questions. He and his.