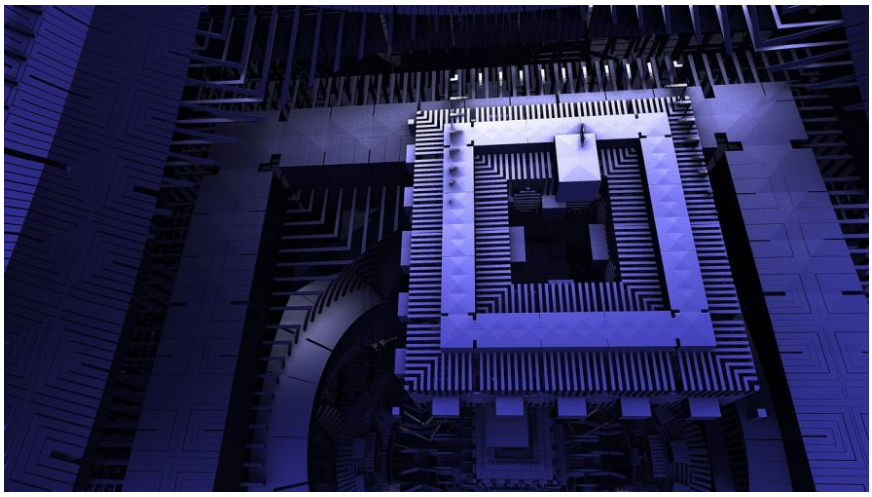
Belangrijke stap in de beveiliging van quantum computers

26 AUGUSTUS 2019



IBM Research (http://www.research.ibm.com/) heeft tijdens de tweede Post-Quantum Cryptography Standardization Conferentie (https://c212.net/c/link/?t=0&l=en&o=2559875-1&h=295488520&u=https%3A%2F%2Fcsrc.nist.gov%2FProjects%2FPost-Quantum-Cryptography&a=Second+Post-Quantum+Cryptography+Standardization+Conference), georganiseerd door het NIST (National Institute of Standards and Technology), nieuwe cryptografische algoritmen aangekondigd die ondersteuning bieden bij de toekomstige beveiliging van quantumcomputers. De algoritmen zijn in samenwerking met verschillende academische en commerciële partners, waaronder het Centrum Wiskunde & Informatica (CWI) en de Radboud Universiteit, tot stand gekomen.

Omdat quantumsystemen steeds krachtiger worden, zullen er ook nieuwe uitdagingen en kansen komen op het gebied van security. Door de hoge snelheid van quantumcomputers zal data minder goed beveiligd zijn met de huidige asymmetrische-encryptiemethoden. Dankzij de nieuwe cryptografische algoritmen van IBM kan er nu begonnen worden met de ontwikkeling van toekomstbestendige tools en beveiligingsmethodes.

In samenwerking met verschillende academische en commerciële partners, waaronder het Centrum Wiskunde & Informatica (CWI) en de Radboud Universiteit, hebben IBM-onderzoekers twee cryptografische primitives voor quantumcomputing ontwikkeld. Kyber (https://pq-crystals.org/kyber/index.shtml), een veilig inkapselingsmechanisme, en Dilithium (https://pq-crystals.org/dilithium/index.shtml), een algoritme voor digitale handtekeningen. Deze twee primitives vormen samen de ‘Cryptographic Suite for Algebraic Lattices’ ook wel ‘CRYSTALS (https://pq-crystals.org/index.shtml)’ genoemd.

Om de ontwikkeling te versnellen zal IBM de nieuwe algoritmes doneren aan de open source community. Daarnaast zal het bedrijf ook een aantal open source projecten ondersteunen zoals OpenQuantumSafe.org (https://c212.net/c/link/?t=0&l=en&o=2559875-1&h=1151854895&u=https%3A%2F%2Fopenquantumsafe.org%2F&a=OpenQuantumSafe.org).