Hardware Info

[Pro] IBM meldt samen met CWI en de Radboud Universiteit belangrijke stap te zetten in de beveiliging van quantumcomputers

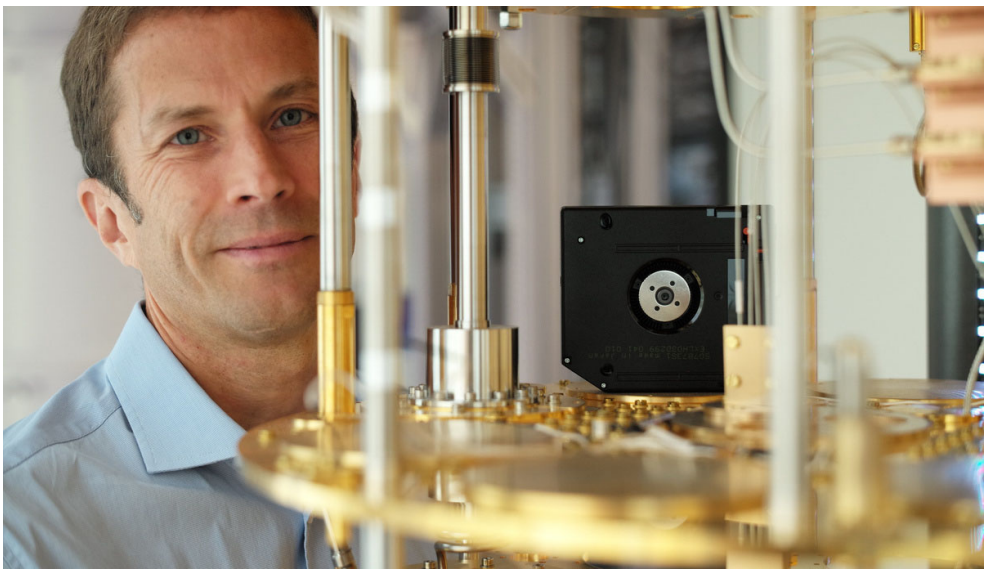
Richard Schouw 28 augustus 2019 07:00, 1 reactie

IBM Research heeft tijdens de tweede **Post-Quantum Cryptography Standardization Conferentie**, georganiseerd door het NIST (National Institute of Standards and Technology), nieuwe cryptografische algoritmen aangekondigd die ondersteuning moeten 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, wachten er volgens IBM steeds 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 nieuwe cryptografische algoritmen hoopt het bedrijf de aftrap te kunnen geven voor de ontwikkeling van toekomstbestendige tools en beveiligingsmethodes.

Vanuit het eerder genoemde samenwerkingsverband zijn twee cryptografische primitives voor quantumcomputing ontwikkeld. **Kyber**, een veilig inkapselingsmechanisme en **Dilithium**, een algoritme voor digitale handtekeningen. Deze twee primitives vormen samen de 'Cryptographic Suite for Algebraic Lattices' ook wel **'CRYSTALS**' 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**.



Mark Lantz, IBM Research

Bron: **IBM**