Executive-People
TECH BUSINESS PLATFORM
BRAND OF DUTCH IT CHANNEL

23-08-2019 | door: Wouter Hoeffnagel

Cryptografische algoritmen van IBM voor beveiliging van quantumcomputers

IBM Research introduceert nieuwe cryptografische algoritmen 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.

Cryptografische primitives

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, 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 doneert IBM de nieuwe algoritmes aan de open source community. Daarnaast gaat het bedrijf een aantal open source projecten ondersteunen, waaronder OpenQuantumSafe.org.

Terug naar nieuws overzicht