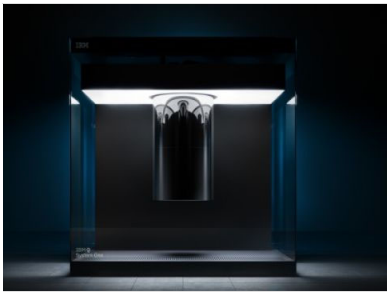
IBM deelt algoritmen voor quantum-beveiliging

26 AUGUSTUS 2019 11:12 | PIM VAN DER BEEK



IBM's quantumcomputer.

IBM deelt conceptversies van algoritmen voor de toekomstige beveiliging van quantumcomputers. Het gaat om cryptografische algoritmen die ontworpen zijn door wetenschappers van het CWI (Centrum Wiskunde & Informatica in Amsterdam (CWI) en de Radboud Universiteit van Nijmegen. Zij maakten een algoritme voor een digitale handtekening en een inkapselingsmechansime. Beide concepten worden gedeeld met de opensource-gemeenschap.

De nieuwe cryptografische algoritmen voor de toekomstige beveiliging van quantumcomputers zijn tijdens de tweede editie van het Post-Quantum Cryptography Standardization Conferentie gedeeld. Dat evenement wordt georganiseerd door NIST (National Institute of Standards and Technology).

IBM Research meldt dat het in samenwerking met academische en commerciële partners, waaronder het Centrum Wiskunde & Informatica (CWI) en de Radboud Universiteit, twee cryptografische conceptversies voor quantumcomputing heeft ontwikkeld. 'Het gaat om Kyber, een veilig inkapselingsmechanisme en Dilithium, een algoritme voor digitale handtekeningen. Deze twee concepten vormen samen de Cryptographic Suite for Algebraic Lattices, ook wel ‘Crystals’ genoemd’, licht de onderzoekstak van IBM toe.

'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 is te beginnen met de ontwikkeling van toekomstbestendige tools en beveiligingsmethodes.'

Lattice Cryptography IBM Research

Opensource

Om de ontwikkeling te versnellen, zal IBM de nieuwe algoritmes doneren aan de opensourcecommunity. Daarnaast zal het bedrijf een aantal opensourceprojecten rondom beveiliging ondersteunen. De concept-algoritmen moeten een basis vormen voor verschillende beveiligingstoepassingen voor quantumcomputers.