IBM voorziet tapedrive van beveiliging tegen kraken door quantumcomputers

Amerikaanse en Zwitserse onderzoekers van IBM hebben met hulp van het Centrum Wiskunde & Informatica en de Radboud Universiteit data op tapeopslag beveiligd met algoritmen die moeten beschermen tegen kraken door quantumcomputers.

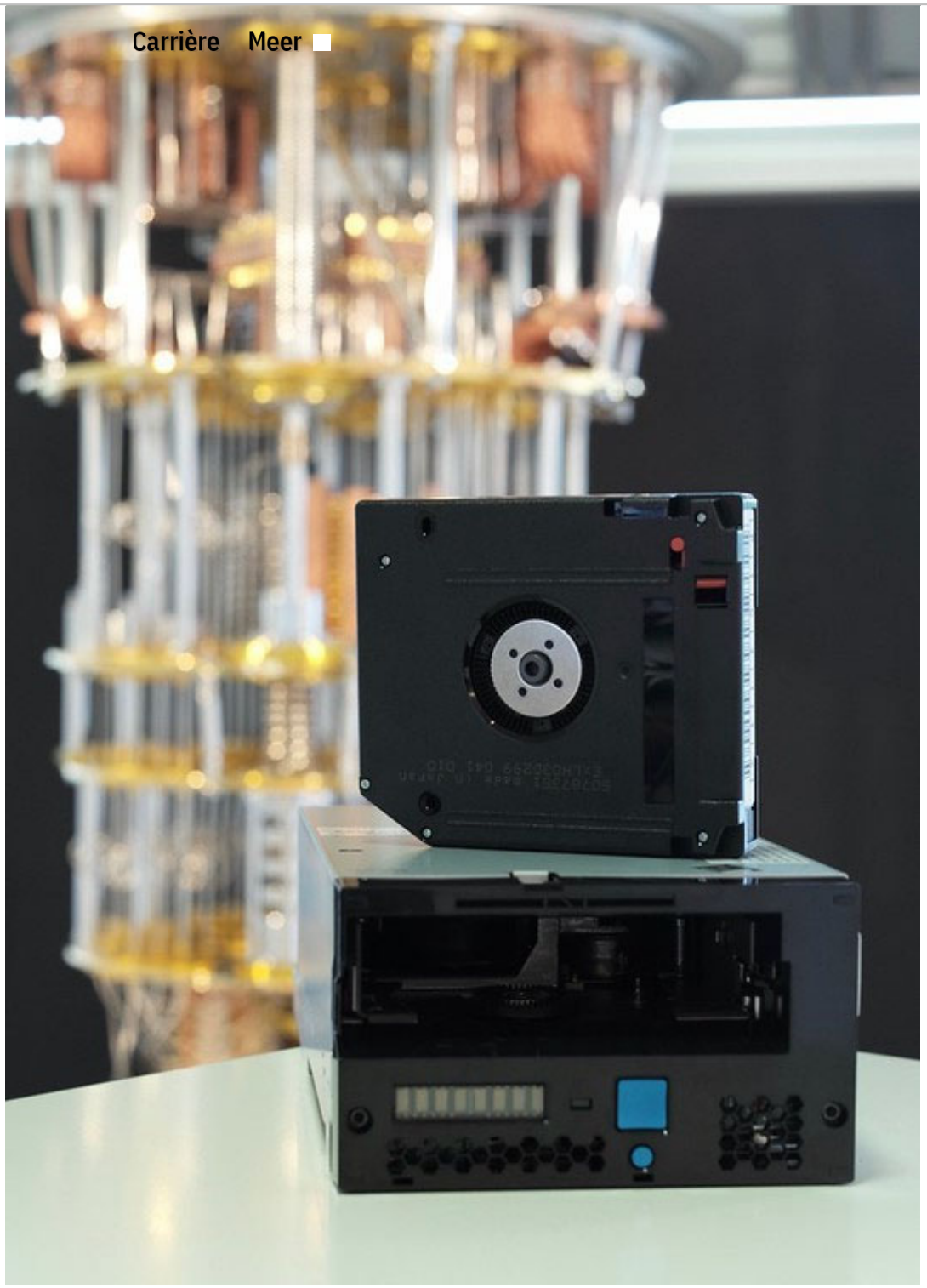
Bij het ontwikkelen van een prototype van beveiligde opslag dat bestand is tegen krakende quantumcomputers kozen IBM-onderzoekers uit Zwitserland en de VS voor een tapedrive, de TS1120 Enterprise Tape Drive. De reden is dat dit type opslag door grote organisaties nog steeds veel gebruikt wordt voor opslag voor tientallen jaren. De reden is dat de kosten voor tapes laag zijn, terwijl de opslagcapaciteit hoog is. De tapedrives bevatten van nature al een beveiligingslaag omdat ze *airgapped* zijn: zolang de drive ze niet opstart, is de data niet uit te lezen of te wijzigen.

De wetenschappers wilden onderzoeken wat er nodig is om te zorgen dat beveiligde tapeopslag ook over tien tot dertig jaar nog weerstand kan bieden tegen kraakpogingen. De verwachting van IBM is dat in dat tijdsbestek asymmetrische encryptie onvoldoende bescherming biedt tegen bijvoorbeeld de opkomst van de quantumcomputer. Die computers kunnen dankzij hun parallelle rekenkracht aanzienlijk sneller grote getallen ontbinden in priemfactoren. De beveiliging van publieke-sleutelencryptie berust op priemgetallen. Het is de vraag of en zo ja wanneer een werkende quantumcomputer daarvoor gereed kan zijn, maar bij IBM denken ze dus dat dit in tien tot dertig jaar het geval kan zijn. IBM is zelf een van de bedrijven die wereldwijd vergevorderd zijn met onderzoek naar quantumcomputers.

Om publieke-sleutelcryptografie tegen quantumkraken te beschermen heeft IBM twee *lattice-based cryptosystems* ontwikkeld, samen met het ENS Lyon, de Ruhr-Universität Bochum, het Centrum Wiskunde & Informatica en de Radboud Universiteit. Deze algoritmes maken voor de bescherming gebruik van een rooster en het *shortest vector*-probleem. Het gaat om Kyber, een algoritme dat bedoeld is om sleutels veilig 'in te kapselen' en om Dilithium voor veilige digitale handtekeningen. Het concern schaart de algoritmes onder wat het 'Crystals' noemt, CRYptographic Suite for Algebraic LatticeS. Beide zijn kandidaat om door het NIST tot standaard voor de zogenoemde *post quantum cryptography* aangewezen te worden.

IBM heeft de beveiliging via een firmware-update aan de TS1120 toegevoegd en meldt dat de software in de toekomst voor bestaande tapedrives vrijgegeven kan worden. Waarschijnlijk is het prototype deels bedoeld om aan te tonen dat de beveiliging in de praktijk in te zetten is, om daarmee de kandidatuur van Kyber en Dilithium bij de NIST-standaardisatie kracht bij te zetten.

Meer over *post quantum cryptography* lees je in het achtergrondartikel De dreiging van quantumcomputers en de noodzaak van resistente encryptie.



« Vorig nieuwsartikel Volgend nieuwsartikel »

Lees meer