

Cyber security in het quantumtijdperk

Voor een quantumveilige toekomst



Martijn Boerkamp

Na alle positieve verhalen in het nieuws over quantumcomputers zou je denken dat deze computers alleen maar goede doeleinden hebben. Maar wat als iemand een quantumcomputer gebruikt om jouw informatie te hacken? Een nieuw project zoekt hiervoor oplossingen en zorgt daarmee voor een quantumveilige toekomst.

DELFT -Een consortium bestaande uit een aantal instituten, waaronder: TNO, TU Delft en het Amsterdamse Centrum voor Wiskunde en Informatica (CWI), samen met een aantal bedrijven, zoals Microsoft en KPN, heeft een subsidie van 1.8 miljoen euro gekregen voor onderzoek naar cybersecurity in het quantumtijdperk. Het project richt zich op de bescherming van digitale informatie tegen aanvallen van quantumcomputers.

De quantum Terminator

Het klinkt een beetje als in de film Terminator, waarin een kwaadaardig computersysteem de mensheid bedreigt. Maar de realiteit kan er misschien dichtbij komen. Quantumcomputers zijn al lange tijd dé belofte om veel goede dingen te doen. Van de fundamenteel andere rekenkracht van quantumcomputers wordt verwacht dat ze heel snel en/of zeer complexe berekeningen gaan maken. Heel handig voor toekomstig onderzoek naar persoonlijke medicijnen of klimaatverandering. Maar wat als je het op een kwaadaardige manier inzet? Tegen misbruik van een quantumcomputer zijn we namelijk nog niet gewapend.

Encryptie

Tegenwoordig verzenden we bijna alleen maar 'versleutelde' informatie. Hierbij zorg je ervoor dat de informatie alleen in te zien is, wanneer je daar eerst een complexe berekening voor doet, maar die alleen uit te voeren is als je daar de juiste sleutel voor hebt. Dit proces noemen ze 'encryptie'. Die digitale sleutel is eigenlijk alleen

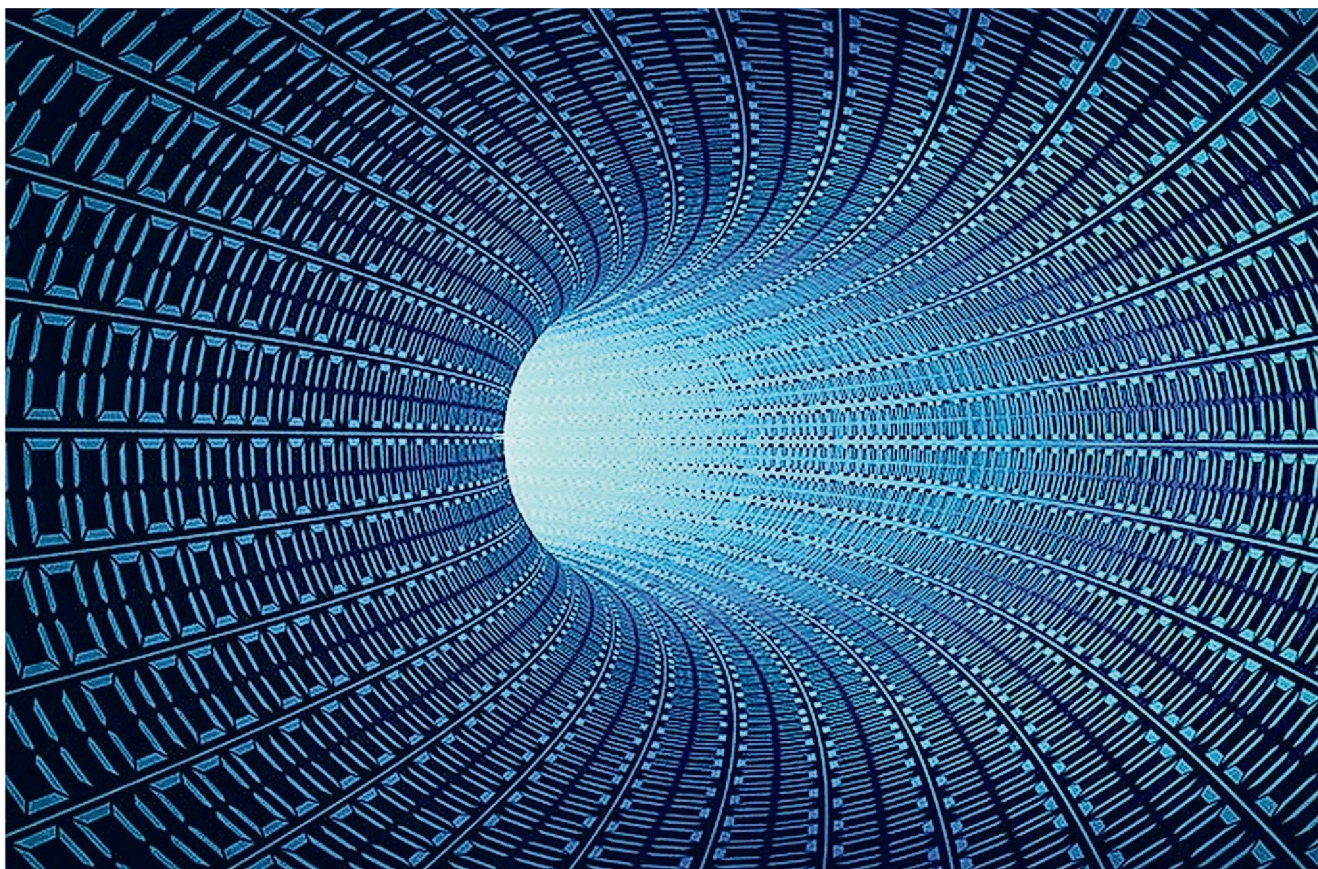
voor de verzender en ontvanger. Je kan natuurlijk je best doen om de berekening op te lossen zonder de sleutel. Maar als je digitale sleutel écht goed in elkaar zit, dan doet zelfs de beste computer er miljoenen jaren over om het op te lossen. Maar een krachtige quantumcomputer rekent dat zo uit, dus veel van de huidige systemen zijn in een quantumtijdperk plotseling onveilig.

Het project

Maran van Heesch werkt als Quantum Security Specialist bij TNO en heeft het project mee opgezet. "In de toekomst gaan we gebruik maken van zogenoemde 'post-quantum cryptografie': een type versleuteling waar zelfs een quantumcomputer niet tegen opgewassen is. Maar voordat we zover zijn, moeten we in de overgangsfase aandacht besteden om de huidige systemen een extra laag van beveiliging geven, zodat ze ook veilig zijn tegen aanvallen met behulp van quantumcomputers. Organisaties kunnen daarna de overgang maken richting een volledig quantumveilig systeem. We zijn uiteraard heel blij met deze subsidie. Hiermee kunnen we echt de nodige stappen maken richting een quantumveilige toekomst."

CYBER SECURITY IN HET TIJDPERK VAN QUANTUM COMPUTERS





Veilig de toekomst in met quantumcomputers Foto: bron: TNO