**TU Eindhoven leidt miljoenenproject om data te beveiligen tegen quantumcomputer**

**Het is een wedstrijd over tientallen jaren, waarvan we de uitkomst mogelijk pas jaren later gaan vernemen, of zelfs helemaal niet. Wetenschappers van onder meer de TU Eindhoven werken aan cryptografietechnieken die bestand zijn tegen de ongekende rekenkracht van de quantumcomputer, die ergens na 2025 wordt verwacht. Als die computer er eerder is dan de cryptografietechnieken, dan kan die straks met terugwerkende kracht alle data ontcijferen die we versleutelen met hedendaagse technieken**.

TU/e-hoogleraar Cryptology Tanja Lange leidt een [onderzoeksconsortium](http://pqcrypto.eu.org/partners.html) van elf universiteiten en bedrijven die samen 3.9 miljoen euro krijgen uit het EU-programma Horizon 2020 om cryptografietechnieken te ontwikkelen die bestand zijn tegen de brute rekenkracht van quantumcomputers. Lange presenteerde [het onderzoeksproject PQCRYPTO](http://pqcrypto.eu.org/) begin deze maand voor het eerst op een drukbezochte workshop van het National Institute of Standards and Technology in de VS.

De verwachting is dat er ergens na 2025 quantumcomputers zullen zijn, computers die qua rekenvermogen ver boven de mogelijkheden reiken van het soort computers waar we nu mee werken, en die andere soorten aanvallen mogelijk maken. De huidige cryptografietechnieken, zoals [RSA](http://nl.wikipedia.org/wiki/RSA_%28cryptografie%29) en [ECC](http://en.wikipedia.org/wiki/Elliptic_curve_cryptography), gebruiken sleutels die in met de huidige computertechnologie niet binnen 100 jaar te kraken zijn. Maar als de quantumcomputer echt zo krachtig wordt als verwacht, dan zullen ze die sleutels binnen dagen of zelfs uren kunnen breken. “2025 lijkt nu nog ver weg, maar we zijn straks misschien alsnog te laat”, waarschuwt hoogleraar Lange, die al sinds 2006 aan de bel trekt over deze dreiging. “Het invoeren van nieuwe cryptosystemen duurt 15 tot 20 jaar, na standaardisatie. En we zitten pas in de onderzoeksfase.”

In de documenten die zijn gelekt door Edward Snowden staat dat de Amerikaanse NSA tientallen miljoenen stopt in de ontwikkeling van dergelijke computers. Saillant is dat een inlichtingendienst zoals de NSA hoogstwaarschijnlijk niet publiek zal maken wanneer ze quantumcomputers klaar hebben en in gebruik nemen. Dat geeft ze namelijk de gelegenheid om ongestoord beveiligde data en boodschappen uit het verleden in te zien, als ze die in het verleden hebben opgeslagen.

Omdat quantumcomputers dan tot alle data toegang kunnen krijgen, ook data uit het verleden die dan nog topgeheim zijn, pleit Lange ervoor dat data die meer dan tien jaar geheim moet blijven, nu al versleuteld wordt met post-quantumcryptografie. Denk aan medische dossiers en bepaalde staatsgeheimen. Die ‘quantumbestendige’ technieken zijn er dus deels al, maar ze vergen veel te veel capaciteit en stroom van bijvoorbeeld je smartphone of smart card. De kunst is het om cryptografietechnieken te ontwikkelen die de snelheid van de huidige generaties apparaten niet zichtbaar verlaagt, maar wel bestand zijn tegen de rekenkracht van quantumcomputers. Daar gaat het Europese consortium de komende drie jaar aan werken. De focus ligt daarbij op kleine apparaten zoals smartphones, op internetdataverkeer, en op opslag in de cloud.

**Noot voor de redactie (niet voor publicatie)**
Voor meer informatie kunt u contact opnemen met prof.dr. Tanja Lange, tanja@pqcrypto.eu.org.