security.nl presented by: Certified Secure

Nieuws

CWI-onderzoeker betrokken bij kwantumbestendige encryptie-algoritmes

donderdag 7 juli 2022, 10:54 door **Redactie**, 2 **reacties**

Het Amerikaanse National Institute of Standards and Technology (NIST) koos deze week **vier encryptie-algoritmes** die bestand zijn tegen de rekenkracht van kwantumcomputers en een onderzoeker van het Nederlandse **Centrum Wiskunde & Informatica** (CWI) is bij twee van deze algoritmes betrokken.

Met de komst van kwantumcomputers zullen veelgebruikte asymmetrische cryptografische algoritmes, zoals RSA en ECC, niet meer veilig zijn. Om data in de toekomst tegen aanvallen van kwantumcomputers te beschermen onderzocht het NIST de afgelopen vijf jaar verschillende benaderingen in een soort wedstrijdproces. De nadruk ligt op public-key versleutelingssystemen en op systemen voor digitale handtekeningen.

CWI-onderzoeker Léo Ducas is betrokken bij de twee algoritmes die het NIST koos, het public-key encryptieschema (CRYSTALS-KYBER) en die voor digitale handtekeningen (CRYSTALS-DILITHIUM). De vier door het NIST gekozen algoritmes zullen onderdeel worden van de post-kwantum cryptografische standaard van het instituut, die naar verwachting over twee jaar is afgerond.

"De selectie van onze algoritmen als standaard betekent dat ze wereldwijd zullen worden toegepast en de privacy van miljarden gebruikers zullen beschermen; fundamenteel onderzoek krijgt zelden zo'n directe en brede impact. De hele gemeenschap van cryptografisch onderzoek verdient hier eer; de door ons voorgestelde schema's zijn de kristallisatie van tientallen jaren wetenschappelijke inspanning", aldus Ducas. Het CWI is het nationaal onderzoeksinstituut voor wiskunde en informatica.