NIST kiest voor Kyber, Dilithium en SPHINCS+ als 'standaard' in post-quantumcryptografie

05 juli 2022 · Onderzoeksbericht

CRYSTALS-KYBER, CRYSTALS-Dilithium en SPHINCS+, drie beveiligingsalgoritmes van onderzoekers van onder andere de Radboud Universiteit, zijn door het Amerikaanse National Institute of Standards and Technology (NIST) gekozen als drie van de nieuwe standaarden voor post-quantumcryptografie. De achterliggende technologie moet ervoor zorgen dat de versleuteling van gevoelige communicatie ook in de komende decennia veilig blijft.

Achter de drie algoritmes zit een internationaal team van onderzoekers, waaronder Peter Schwabe, hoogleraar Cryptographic Engineering aan de Radboud Universiteit, tevens verbonden aan het Max Planck Institute for Security and Privacy. Schwabe werkt samen met onderzoekers van onder andere de TU/Eindhoven en het Centrum voor Wiskunde en Informatica. "Dit project effent het pad voor de volgende generatie encryptie- en handtekeningalgoritmen, die wereldwijd digitale communicatie beveiligen. Het was een geweldige ervaring voor onze groep om bij te dragen aan deze enorme internationale inspanning en nu de eerste grote mijlpaal bereikt te zien."

De competitie werd zes jaar geleden uitgeschreven door NIST , en begon met 69 voorstellen. Na verschillende voorrondes waarbij de algoritmes geëvalueerd zijn, heeft NIST uiteindelijk voor meerdere winnaars gekozen, waaronder drie waar de Radboud Universiteit bij betrokken is. Schwabe: ‘Er is bewust gekozen voor meer dan één winnaar, dat biedt meer flexibiliteit. De verschillende algoritmes zijn gebaseerd op verschillende onderliggende wiskundige problemen. Daardoor hebben ze een verschillende performance afhankelijk van het doel waar ze voor gebruikt worden.

Toekomstbestendig

De dreiging van quantumcomputers is voor nu puur een theoretische: de meeste wetenschappers verwachten dat het nog jaren duurt voor er een quantumcomputer gebouwd kan worden. Toch is het volgens Daan Sprenkels, die binnen de Radboud Universiteit onderzoek doet naar post-quantumcryptografie, belangrijk om nu al voorbereid te zijn. ‘Sommige informatie is altijd gevoelig, en moet daarom voor langere tijd beschermd blijven. Denk bijvoorbeeld aan communicatie van een ambassade. Stel dat er over vijftig jaar een quantumcomputer gebouwd is, dan zou alle communicatie die beschermd is met huidige encryptiemethodes opeens op straat liggen. Door al eerder versleuteling op basis van post-quantumcryptografie toe te passen, blijft deze gevoelige informatie ook veilig in de toekomst.’

Onderzoekers van de Radboud Universiteit zijn de afgelopen decennia vaker betrokken geweest bij essentiële beveiligingsstandaarden. Joan Daemen, sinds 2015 verbonden als hoogleraar Symmetrische cryptografie aan de Radboud Universiteit, is medeverantwoordelijk voor het Rijndael-algoritme dat NIST in 2000 als winnaar selecteerde voor een eerdere cryptografiecompetitie voor de Advanced Encryption Standard, of AES. Deze standaard wordt ook nu nog gebruikt voor bijvoorbeeld de beveiliging van versleutelde WhatsApp-berichten of beveiligde websites.

Gaat over persoon Schwabe, dhr. prof. dr. P. (Peter), Sprenkels, dhr. D. (Daan), MSc

Contactgegevens

Meer weten? Neem contact op met de onderzoekers zelf of met Persvoorlichting & Wetenschapscommunicatie via 024 361 6000 of media@ru.nl.

Doelgroep: Alumni, Medewerkers, Medewerkers » Promovendus, Medewerkers » Wetenschappelijk, Partners, Partners » Educatieve instelling, Partners » Geldverstrekker, Partners » MKB, Partners » Wervingspartner, Pers

- Thema: Innovatie, Privacy

Deel deze pagina

Adres

Houtlaan 4
6525 XZ Nijmegen

T: +31 (0) 24 361 61 61