Twee Nederlandse bijdrages aan kwantumveilige cryptografiemethodes

Geplaatst door Redactie Engineersonline

20 aug. 2024 4 minuten

Het Amerikaanse National Institute of Standards and Technology (NIST) heeft recent drie kwantumveilige cryptografiemethoden gestandaardiseerd voor wereldwijd gebruik. Léo Ducas van de Cryptologie-groep van het Centrum Wiskunde & Informatica (CWI) is mede-ontwerper van twee methoden. De derde post-quantum cryptografiemethode (PQC-methode) is mede ontwikkeld door TU/e-onderzoekers Andreas Hülsing en Tanja Lange.

TAGS: kwantum quantum

Links: Léo Ducas van het CWI heeft meegewerkt aan het ontwerp van de CRYSTALS-Kyber (ML-KEM) en CRYSTALS-Dilithium (ML-DSA) kwantumveilige cryptografiemethodes die nu zijn vastgelegd als standaard. (Foto: CWI)
Rechts: TU/e-onderzoeker Andreas Hülsing heeft samen met collega Tanja Lange mee-ontwikkeld aan de kwantumveilige cryptografiemethode SPHINCS+ (SLH-DSA). (Foto: TU/e)

De huidige vooruitgang in quantum computing bedreigt de veiligheid van onze digitale communicatie. Verschillende huidige encryptiemethoden zijn gebaseerd op het oplossen van moeilijke wiskundige taken, zoals het ontbinden van een getal in een paar zeer grote priemgetallen, waarbij elk priemgetal meer dan tweehonderd cijfers kan hebben. Met een desktopcomputer of laptop kost je dat mogelijk duizenden jaren. Maar een kwantumcomputer doet daar maar een paar uur over. Dus gevoelige data die nu versleuteld worden verzonden of opgeslagen, kan je dan onderscheppen en 'zo' ontcijferen.

Competitie

De nu gestandaardiseerde PQC-methodes zijn het resultaat van de Post-Quantum Cryptography Standardization competitie die het NIST in 2016 opende. Wetenschappers van over de hele wereld dienden voorstellen in voor nieuwe encryptiemethoden en methoden voor digitale handtekeningen, ontworpen om bestand te zijn tegen kwantumaanvallen. NIST heeft nu de standaarden gepubliceerd met als nieuwe officiële namen: CRYSTALS-Kyber (ML-KEM), CRYSTALS-Dilithium (ML-DSA) en SPHINCS+ (SLH-DSA).

Een vierde standaard, Falcon (FN-DSA), zal naar verwachting later worden afgerond. De komende jaren zullen nog meer standaarden aan het portfolio worden toegevoegd. De standaarden zijn bedoeld om de nieuwe encryptiemethoden soepel te kunnen implementeren in online applicaties, zonder het risico te lopen dat de huidige beveiligingsmaatregelen worden verstoord.

Eer

Léo Ducas is een vooraanstaand internationaal expert op het gebied van roostergebaseerde cryptografie. Hij behaalde zijn PhD aan de École Normale Supérieure van Parijs in 2013. Sinds 2015 is hij werkzaam bij de Cryptologiegroep van het CWI. Sinds 2021 is hij ook parttime hoogleraar Mathematische Cryptologie aan het Mathematisch Instituut van de Universiteit Leiden.

Samen met internationale collega's van verschillende instellingen heeft Léo Ducas meegewerkt aan het ontwerp van wat nu de twee primaire standaarden CRYSTALS-Kyber (ML-KEM) en CRYSTALS-Dilithium (ML-DSA) zijn. Hij zegt: "De standaardisatie van ons schema betekent dat het wereldwijd zal worden ingezet en de privacy van miljarden gebruikers zal beschermen; fundamenteel onderzoek krijgt zelden zo'n directe en brede impact. De eer moet naar de hele cryptografische onderzoeksgemeenschap gaan; de schema's die wij hebben voorgesteld zijn slechts de kristallisatie van tientallen jaren wetenschappelijke inspanning."

Directe impact

SPHINCS+ is mede ontwikkeld door TU/e-onderzoekers Andreas Hülsing – die ook het voorstel leidde – en Tanja Lange. Beiden zijn werkzaam aan de faculteit Mathematics and Computer Science.

"Cryptografische algoritmen die NIST standaardiseert, worden over de hele wereld gebruikt", zegt Hülsing. "Elke beveiligde verbinding met een bank wordt waarschijnlijk beschermd door ten minste twee van zulke gestandaardiseerde algoritmen. Met de publicatie van deze nieuwe NIST-standaarden worden beide algoritmen vervangen door een van de nieuw geselecteerde algoritmen."

Hülsing en Lange hebben aanzienlijk bijgedragen aan SPHINCS+. Dit is een handtekeningenschema om de authenticiteit van documenten of digitale berichten zoals e-mails te verifiëren. Dilithium is ook een handtekeningenschema, maar bedoeld voor andere toepassingen.

Hülsing: "SPHINCS+ is een tragere handtekeningbenadering en kan het beste gebruikt worden om documenten digitaal te ondertekenen. In zo'n geval is tijd geen kritiek punt (..). Aan de andere kant is Dilithium veel sneller en beter geschikt voor het authenticeren van een server in een online protocol omdat dit hogere eisen stelt aan de snelheid en de geldigheid van het bewijs alleen voor dat moment hoeft te gelden."

Early adopters

Veel bedrijven hebben het belang van de implementatie van deze nieuwe veilige encryptiemethoden al erkend, zelfs voordat de standaarden werden gepubliceerd. Kyber, een key encapsulation mechanism (KEM) dat helpt bij het starten van een online vertrouwelijk overleg tussen twee partijen die elkaar nog niet hebben ontmoet, is al door verschillende klanten geadopteerd sinds het werd uitgerold in 2023. 17,1% van de klanten die Cloudflare gebruiken (per 5 augustus 2024 – volgens Cloudflare) gebruiken bijvoorbeeld Kyber. Dit komt overeen met meer dan een half biljoen verbindingen per dag die worden beveiligd met behulp van PQC. De grootste early adopters zijn diensten zoals iMessage (Apple), Google Chrome, Signal, Zoom en Cloudflare. Met de publicatie van deze normen wordt een impuls verwacht in de acceptatiegraad van deze methoden.

TAGS: kwantum quantum

Het laatste nieuws

Strategische samenwerking en joint venture SICK en Endress+Hauser

Twee Nederlandse bijdrages aan kwantumveilige cryptografiemethodes

Bladvormige zonneconcentratoren bieden flexibele en schaalbare oplossingen voor hernieuwbare energie

Altair en L&T Technology Services starten Digital Twin Centre of Excellence

Zeiss optimaliseert buitendienst- en serviceactiviteiten

Meer nieuws

Geef een reactie

Het e-mailadres wordt niet gepubliceerd.Vereiste velden zijn gemarkeerd met *

Reactie *

Naam *

E-mail *

Mijn naam, e-mail en site bewaren in deze browser voor de volgende keer wanneer ik een reactie plaats.

Reactie plaatsen

Anderen lazen ook

Actueel

Meer leren over quantummechanica dankzij

Naast muziek en dans is er op Lowlands plaats voor nog een discipline: wetenschap. Wetenschappers van de Universiteit Leiden gebruiken het festival om onderzoek te doen naar quantumdeeltjes. Voor prom[...]

quantum

Actueel

Spin qubits gaan op de trampoline

Onderzoekers van QuTech hebben spin-qubits ontwikkeld die salto's maken voor universele quantumlogica. Deze prestatie maakt efficiënte aansturing van grote halfgeleider qubit-arrays mogelijk. D[...]

kwantum

Actueel

Nieuwe fotonen voor andere optische technologieën

Fotonen gedragen zich verbazingwekkend veel gevarieerder dan elektronen, terwijl je ze veel makkelijker kan controleren. Nieuwe inzichten beloven slimme Led-verlichting, informatie bestuurd met kwantu[...]

fotonica kwantum LED-verlichting