WITOLD KEPINSKI - 19 AUGUSTUS 2024 Deel dit artikel

NIST standaardiseert kwantumveilige cryptografiemethoden

Drie kwantumveilige cryptografiemethoden zijn sinds deze week gestandaardiseerd voor wereldwijd gebruik. Léo Ducas van CWI's Cryptologie-groep is mede-ontwerper van de twee belangrijkste methoden.

Wetenschap Security Cybersecurity

Van competitie naar standaardisatie: drie kwantumveilige cryptografiemethoden zijn nu gestandaardiseerd voor wereldwijd gebruik. Het Amerikaanse National Institute of Standards and Technology (NIST) kondigde dit deze week aan. Kwantumveilige cryptografie wordt ook wel post-quantum cryptografie (PQC) genoemd. Léo Ducas van CWI's Cryptologie-groep is mede-ontwerper van de twee belangrijkste PQC-methoden die voor deze standaardisatie zijn geselecteerd. De nieuwe standaarden zijn acht jaar na de aankondiging van de competitie afgerond, en er wordt verwacht dat het snel wijdverbreid gebruikt gaat worden.

Waarom hebben we kwantumbestendige encryptiemethoden nodig?

De huidige voortuitgang in quantum computing bedreigt de veiligheid van onze digitale communicatie. Klassieke versleutelingsmethoden zijn ontworpen om bestand te zijn tegen aanvallen die via bestaande (klassieke) computers worden gedaan. Hun veiligheid hangt af van moeilijke wiskundige taken zoals priemfactorisatie: het opsplitsen van een groot getal in zijn priemfactoren. Als dit door klassieke computers zou worden uitgevoerd, zou dit een immense hoeveelheid energie en tienduizenden jaren vergen. Toekomstige kwantumcomputers kunnen dit soort specifieke wiskundige taken echter zeer efficiënt oplossen, wat betekent dat ze klassieke methoden in relatief korte tijd zouden kunnen breken. Dit houdt in dat gevoelige gegevens die nu versleuteld worden verzonden of opgeslagen, op een later tijdstip met behulp van een kwantumcomputer kunnen worden onderschept en ontcijferd.

Standaardisatieproces

Om deze risico's te beperken, publiceerde het NIST in 2016 zijn Post-Quantum Cryptography Standardization competitie. Wetenschappers van over de hele wereld dienden voorstellen in voor nieuwe encryptiemethoden en methoden voor digitale handtekeningen, ontworpen om bestand te zijn tegen kwantumaanvallen. De 82 ingediende voorstellen werden in verschillende rondes beoordeeld door de cryptografische onderzoeksgemeenschap. In 2022 werden één encryptiemethode en drie methoden voor digitale handtekeningen gekozen voor standaardisatie: CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+ en FALCON.

Standaarden helpen implementatie

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 de 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. Veel bedrijven hadden het belang van de implementatie van deze nieuwe veilige encryptiemethoden al erkend voordat de normen werden gepubliceerd. CRYSTALS-Kyber is vanaf 2023 geïmplementeerd, inmiddels door 17,1% van de klanten die Cloudflare gebruiken (per 5-8-2024, volgens Cloudflare). Dit komt neer op meer dan een half biljoen verbindingen per dag die eindigen bij Cloudflare, beveiligd met PQC. De grootste early adopters zijn diensten zoals iMessage (Apple), Google Chrome, Signal, Zoom en Cloudflare.

Miljarden gebruikers

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".

Over Léo Ducas

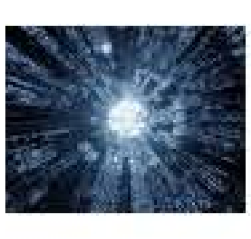
Léo Ducas is een vooraanstaand internationaal expert op het gebied van roostergebaseerde cryptografie. Hij behaalde zijn PhD aan de École Normale Superiéure van Parijs in 2013. Sinds 2015 is hij werkzaam bij de Cryptologiegroep van het Centrum Wiskunde & Informatica (CWI). Bij het CWI deed hij het werk aan de kwantumveilige protocollen voor NIST-standaardisatie. In 2016 ontving Ducas een NWO Veni Grant en de USENIX/Facebook Internet Defense Award, de laatste samen met co-auteurs, en in 2020 ontving hij een ERC-grant voor zijn onderzoek. Sinds 2021 is hij ook parttime hoogleraar Mathematische Cryptologie aan het Mathematisch Instituut van de Universiteit Leiden. Ducas' werk aan theoretische en praktische aspecten van roostercryptanalyse had een grote invloed op de manier waarop zulke kwantumveilige schema's worden ontworpen en geparametriseerd.

Tip de redactie

DUTCH IT EVENTS

Alle events

MEER OVER WETENSCHAP


Nieuws - Witold Kepinski - 02-08-2024
NWO honoreert aanvragen in de Open Competitie ENW-M
WETENSCHAP, QUANTUM COMPUTING,


Nieuws - Witold Kepinski - 13-07-2024
GPU-uitbreiding van supercomputer Snellius
HPC, WETENSCHAP, COMPUTE, ONDERWIJS,


Nieuws - Witold Kepinski - 25-06-2024
Noord-Nederland wil ook semicon industrie en bedrijven als ASML behouden
HARDWARE, INNOVATIE, CHIP, PROCESSOR, WETENSCHAP

Alles over wetenschap

OVER WITOLD KEPINSKI

Witold Kepinski (1969) is Editor-in-Chief en Director Content en mede-aandeelhouder van Dutch IT Channel en Dutch IT Leaders. Witold Kepinski is 25 jaar actief in de IT Media en Tech Business branche

Witold Kepinski geeft met een gespecialiseerd team van redacteuren, bloggers en videomakers inzicht in tech business trends en toepassingen waarmee IT-beslissers en Channel Partners impact maken.

Auteur pagina

WIL JIJ DAGELIJKSE UPDATES?

Schrijf je dan in voor onze nieuwsbrief!

Naam | Bedrijf | E-mailadres | Versturen

PROJECTEN
Digital Workplace 2024
Cloud & MSP Project 2024
Security 2024
Datacenters 2024

DUTCH IT CHANNEL
Alle evenementen
Ons Team
Homepage
Magazines
Colofon
Partner- en Reclamemogelijkheden
Events Sponsormogelijkheden 2024 NL
Events Sponsor Opportunities 2024 ENG
Partner and Advertising Opportunities

ONZE SAMENWERKINGEN
Canalys
CloudLunch
Gartner
NL Digital

NIEUWSBRIEF ONTVANGEN?
Naam
Bedrijf
E-mailadres
Versturen

CONTACT
Dutch IT Media
Nieuwe Parklaan 17
2597 LA Den Haag
redactie@dutchitchannel.nl
Per mail