

16-08-2024

Drie kwantumveilige cryptografiemethoden gestandaardiseerd



Deel dit bericht



Het Amerikaanse National Institute of Standards and Technology (NIST) kondigde dit deze week aan dat drie kwantumveilige cryptografiemethoden nu gestandaardiseerd zijn voor wereldwijd gebruik. 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 wereldwijd gebruikt gaat worden.

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 procent 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".

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 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.

Tags: Cryptografie, Kwantum computing, Quantum Computing, Security

Company: CWI, NIST

Generatieve AI in Business Analyse door **Christian Gijssels**



Gerelateerde Berichten



15/08 - IBM: kosten datalekken stijgen naar nieuwe hoogten



14/08 - SAP Enterprise Cloud Services kiest CyberArk voor beveiliging



01/08 - Conscia en Splunk willen optimale ondersteuning bieden bij datastrategie



03/07 - Belgische cybersecurityspeler Jarviss wil Nederlandse markt veroveren

Cursus Sparx Enterprise Architect 16 – Fundamentals en Best Practices



NIEUWSARCHIEF

ADEPT EVENTS



15-10-2024

Generatieve AI in Business Analyse door Christian Gijssels

15 oktober 2024 Workshop met BPM-specialist Christian Gijssels over AI-Gedreven Business Analyse met ChatGPT. Kunstmatige Intelligentie, ongetwijfeld een van de meest baanbrekende technologieën tot nu toe, opent nieuwe deuren voor analisten met i...



07-11-2024

The Data-Process Connection door Alec Sharp [halve dag online]

7 november (online seminar op 1 middag)Praktische tutorial met Alec Sharp Alec Sharp illustreert de vele manieren waarop conceptmodellen (conceptuele datamodellen) procesverandering en business analyse ondersteunen. En hij behandelt wat elke data...



18-11-2024

Business-oriented Data Modelling Masterclass met Alec Sharp

18 t/m 20 november 2024Praktische workshop met internationaal gerenommeerde spreker Alec Sharp over het modelleren met Entity-Relationship vanuit business perspectief. De workshop wordt ondersteund met praktijkvoorbeelden en duidelijke, herbruikbare ...



21-11-2024

A Data Strategy for Becoming Data Driven

21 november 2024 Praktische en interactieve workshop met Nigel Turner Data-gedreven worden lukt niet door alleen nieuwe technologie en tools aan te schaffen. Het vereist een transformatie van bestaande business modellen, met cultuurverandering, een h...



28-11-2024

Cursus Sparx Enterprise Architect 16 - Fundamentals en Best Practices

28 november 2024Workshop met BPM-specialist Christian Gijssels over business analyse, modelleren en simuleren met de nieuwste release van Sparx Systems' Enterprise Architect, versie 16.Intensieve cursus waarin de belangrijkste basisfunctionaliteiten v...



02-12-2024

Data Management Fundamentals door Winfried Etzel [Live en/of Online]

De DAMA DMBok2 beschrijft 11 disciplines van Data Management, waarbij Data Governance centraal staat. De Certified Data Management Professional (CDMP) certificatie biedt een traject voor het inleidende niveau (Associate) tot en met hogere niveaus van...



03-04-2025

Concept Modelling for Business Analysts door Alec Sharp [halve dag]

3 april 2025 (halve dag)Praktische workshop met Alec Sharp [Halve dag] Deze workshop door Alec Sharp introduceert conceptmodellering vanuit een non-technisch perspectief. Alec geeft tips en richtlijnen voor de analist, en verkent datamodellering op C...



10-04-2025

Working with Business Processes Masterclass door Alec Sharp

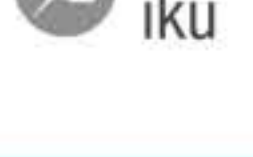
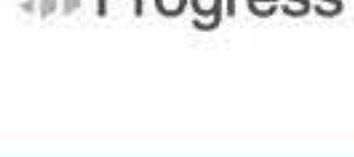
10, 11 en 14 april 2025Praktische driedaagse workshop met internationaal gerenommeerde spreker Alec Sharp over herkennen, beschrijven en ontwerpen van business processen. De workshop wordt ondersteund met praktijkvoorbeelden en duidelijke, herbruikba...

Working with Business Processes Masterclass met **Alec Sharp**



Bekijk de volledige Adept Events >

PARTNERS



VOLG ONS



NIEUWSBRIEF

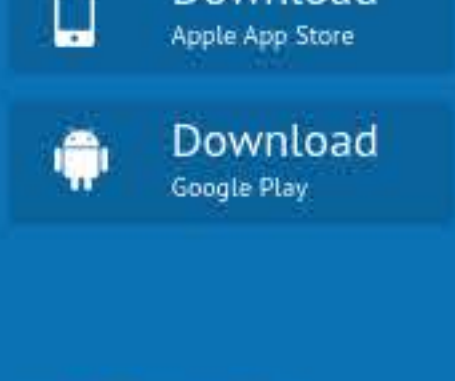
Meld u hier aan

SAMENWERKINGEN

BI-Platform
Adept Events
Data Warehousing & Business Intelligence Summit

APP

Download gratis de mobiele apps



INFORMATIE

Welkom
About Release
Adverteren
Over Release
Contact
Colofon
PDF artikelen archief
Privacy