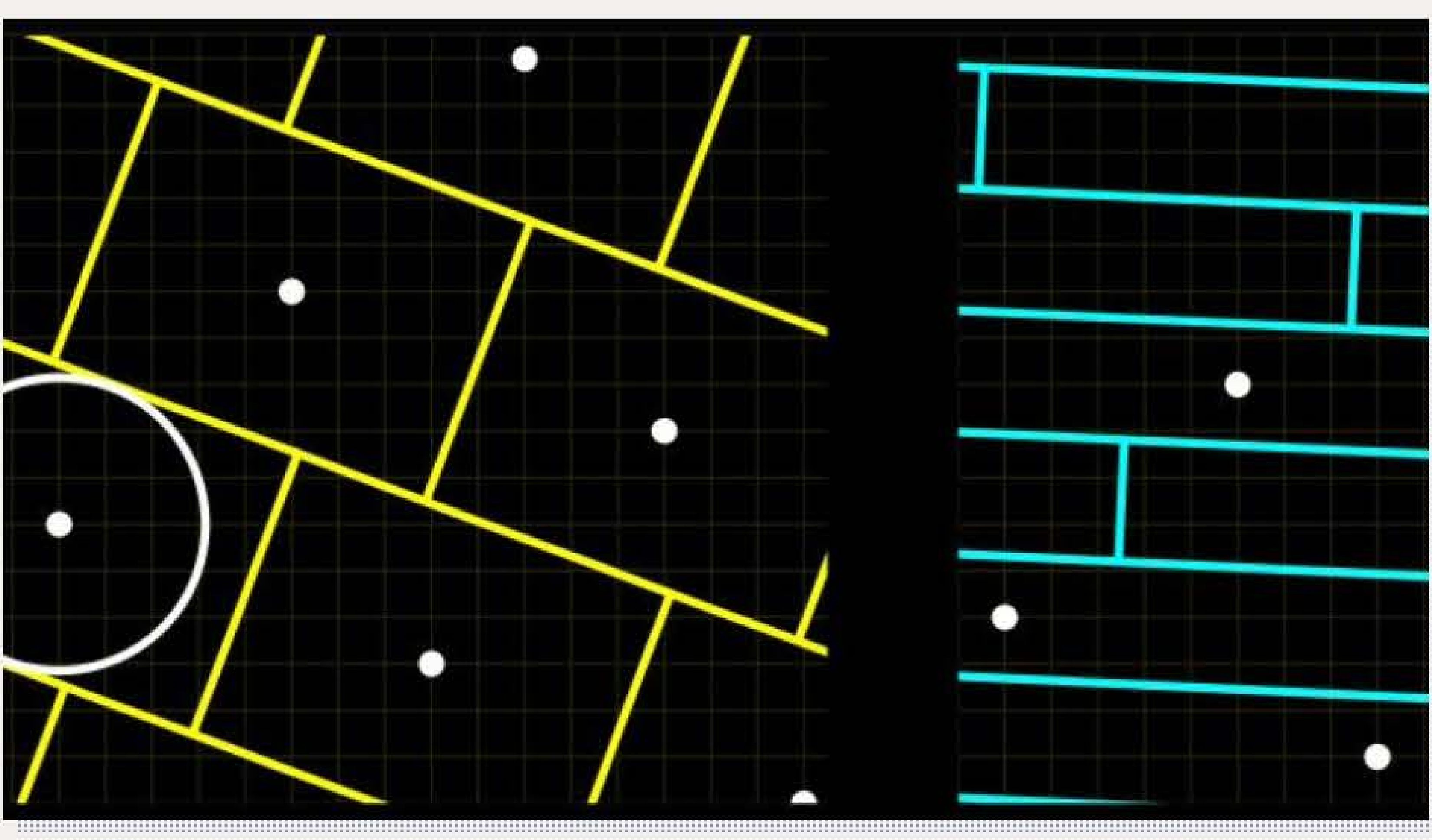
Nieuws • Quantum + • Security + • Leiderschap +
16 minuten geleden leestijd 2 minuten 0 reacties

Kwantumveilige encryptie leunt sterk op Nederlandse ontwikkeling

Het Amerikaanse National Institute of Standards and Technology (NIST) heeft drie kwantumveilige cryptografiemethoden nu gestandaardiseerd voor wereldwijd gebruik. Deze standaardisatie volgt op een competitie die 8 jaar geleden is aangekondigd. Twee van de drie winnende methodes voor dataversleuting hebben hun oorsprong deels in Nederland.

- Lees ook: Hoe zit het met al die varianten van kwantumcomputing?

Jasper Bakker
redacteur
Meer van deze auteur



Léo Ducas, CWI

Kwantumveilige cryptografie, ook wel post-quantum cryptografie (PQC) genoemd, is een belangrijke ontwikkeling om beveiliging van data en van digitale communicatie te kunnen behouden. De ontwikkeling van kwantumcomputers zet namelijk huidige, non-kwantum versleutelingsmethoden op losse schroeven. De meest krachtige encryptie van nu zou door een toekomstig kwantumsysteem in principe binnen afzienbare tijd gekraakt kunnen worden.

Versleuteling van nu later kunnen kraken

Klassieke versleutelingsmethoden zijn namelijk ontworpen om bestand te zijn tegen aanvallen die via bestaande (klassieke) computers worden gedaan, legt het CWI uit. De veiligheid van die methoden is afhankelijk van complexe wiskundige taken zoals priemfactorisatie, waarbij een groot getal wordt opgesplitst in zijn priemfactoren. Klassieke computers hebben daar een immense hoeveelheid energie en tienduizenden jaren voor nodig.

Toekomstige kwantumcomputers zijn echter in staat om dit soort specifieke wiskundige taken zeer efficiënt op te lossen. Dit heeft als gevolg dat gevoelige gegevens die nu in versleutelde staat worden verzonden of opgeslagen op een later tijdstip door een kwantumcomputer kunnen worden ontcijferd. Om dat gevaar in te perken, heeft het NIST in 2016 een wereldwijde competitie opgezet, waarna wetenschappers van over de hele wereld voorstellen hebben ingediend voor kwantumveilige versleutelingsmethoden.

Nederlands wetenschapscentrum

In totaal zijn er 82 voorstellen ingediend, die in verschillende rondes zijn beoordeeld door de wereldwijde onderzoeksgemeenschap voor cryptografie. Uiteindelijk zijn twee jaar terug één encryptiemethode en drie methoden voor digitale handtekeningen gekozen voor standaardisatie. Dit zijn: CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+ en FALCON.

De twee eerstgenoemde - en volgens het CWI de belangrijkste - POC-methoden zijn mede-ontworpen door Léo Ducas van de Cryptologie-groep aan het CWI (Centrum voor Wiskunde en Informatica). Dat Nederlandse wetenschapsinstituut staat aan de wieg van veel meer digitale doorbraken en innovaties. Die betreffen toekomstgerichte, fundamentele zaken zoals bijvoorbeeld diepgaande security in chips, visie op duurzame ICT en baanbrekende databasevernieuwing.

Naast 'gewone ICT-security', voor bijvoorbeeld software libraries, geniet ook post-kwantum beveiliging natuurlijk aandacht van het CWI. Terwijl het acht jaar heeft geduurd voordat de NIST-competitie voor kwantumveilige versleuteling is afgerond, wordt er wel verwacht dat de nieuwe standaarden snel wijdverbreid gebruikt gaan worden.

Directe en hele brede impact

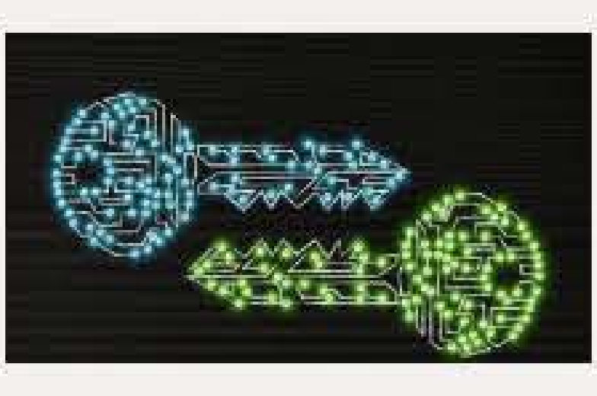
Ducas is daar verheugd over: "De standaardisatie van ons schema [voor kwantumveilige versleuteling - red.] betekent dat het wereldwijd zal worden ingezet en de privacy van miljarden gebruikers zal beschermen; fundamenteel onderzoek krijgt zelden zo'n directe en brede impact." De CWI-wetenschapper stelt wel dat de eer voor deze prestatie naar de hele cryptografische onderzoeksgemeenschap moet gaan; "de schema's die wij hebben voorgesteld zijn slechts de kristallisatie van tientallen jaren wetenschappelijke inspanning".

Het gaat overigens niet slechts om toekomstige implementatie, want het belang van post-kwantum versleuteling wordt wijdverbreid erkend en sommige ICT-aanbieders hebben al een voorschot genomen op de NIST-standaardisatie. Zo is CRYSTALS-Kyber al vanaf 2023 geïmplementeerd, inmiddels door 17,1% van Cloudflare's klanten, wat neerkomt op meer dan een half biljoen verbindingen per dag die eindigen bij dat content distribution network (CDN). Het CWI meldt nu dat de grootste early adopters diensten zijn zoals Apple's iMessage, Google's webbrowser Chrome, Signal, Zoom en Cloudflare.

GERELATEERDE ARTIKELEN

Achtergrond • Ethiek PRO
De kwantumcomputersector moet hype loslaten en zich richten op verantwoorde ontwikkeling
Kwantum computing niet overlaten aan commerciële sector, maar ook niet aan alleen wetenschappers en techneuten.
3 min

Nieuws • post-kwantumbeveiliging
Chrome beschermt encryptiesleutels tegen dreigend kwantumgeweld
Google wil bescherming bieden tegen 'harvest now, decrypt later'-gevaar.
1 min 1



Nieuws • Security
Postkwantumencryptie-algoritme gekraakt met eenvoudige aanval
Onderzoekers breken model binnen een uur met alleen PC.
2 min

GERELATEERDE ARTIKELEN

Nieuws • Phishing, QR-codes Partner
Populariteit HR-gerelateerde phishing houdt aan, QR-codes in phishing een groeiend probleem
Dit blijkt uit het Q2 2024 top-clicked phishing rapport.
2 min

Nieuws • KnowBe4, security awareness Partner
KnowBe4 zet National Social Engineering Day op de Nationale Dag Kalender
6 augustus was het Nationale Social Engineering Day.
2 min

MEER WHITEPAPERS

Whitepaper • Cloud
PCI Cloud for the Edge en HPE: het beste van twee werelden
De concurrentie voorblijven? Ga voor future-proof IT met PCI Cloud for the Edge en HPE en ontdek de voordelen van een multi-cloud.

Whitepaper • Cloud
Ontdek best practices voor het beveiligen van containerized apps en Kubernetes-clusters
Implementeer en voer veilige container-gebaseerde applicaties een stuk eenvoudiger uit.

Whitepaper • Security
Fysieke security van datacenters net zo belangrijk als cybersecurity
Dit is waarom fysieke security van datacenters zo essentieel is.

MEER WHITEPAPERS →

Reacties

Bold _italic_

Typ uw reactie

Plaats reactie

AG CONNECT TECH SINDS 1967

AG Connect is sinds 1967 de essentiële bron van ideeën en informatie die betekenis geven aan een wereld in constante transformatie. Wij laten zien hoe tech elk aspect van ons leven verandert, van onze organisaties, ons werk en onze carrière tot onze cultuur, wetenschap en maatschappij.

Lees ons manifest >

Over ons
Abonneren
Adverteren
Contact
Colofon

Community
Events
Nieuwsbrieven
Vacatures
Whitepapers

Volg ons

Redactionele partner