NIST standaardiseert kwantumveilige cryptografiemethoden

Felix Speulman
28 augustus 2024

Start met lezen

Deze maand heeft het Amerikaanse National Institute of Standards and Technology (NIST) drie kwantumveilige cryptografiemethoden gestandaardiseerd voor wereldwijd gebruik. Kwantumveilige cryptografie, ook wel post-quantum cryptografie (PQC) genoemd, is nodig in een toekomst waarin kwantumcomputing zodanig toegankelijk is dat deze door kwaadwillenden gebruikt kan worden om gangbare versleuteling te ontcijferen.

De huidige, klassieke versleutelingsmethoden zijn bestand tegen aanvallen vanaf bestaande (klassieke) computers. De veiligheid van deze methoden 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 zeer efficiënt oplossen, waardoor ze klassieke encryptie naar verwachting in korte tijd zullen kunnen breken.

Gegevens die met de huidige stand der techniek worden versleuteld, kunnen in de toekomst met behulp van een kwantumcomputer worden onderschept en ontcijferd.

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.

NIST heeft nu deze drie standaarden gepubliceerd. Het gaat om 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 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 organisaties hadden het belang van de nieuwe methoden al erkend. CRYSTALS-Kyber is vanaf 2023 geïmplementeerd door ruim 17 procent van Cloudflare-klanten, aldus het bedrijf. 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 uiteraard Cloudflare zelf.

Léo Ducas, crypografisch expert en werkzaam bij de Cryptologiegroep van het Centrum Wiskunde & Informatica (CWI) heeft samen met internationale collega's van verschillende instellingen meegewerkt aan het ontwerp van wat nu de twee primaire standaarden CRYSTALS-Kyber (ML-KEM) en CRYSTALS-Dilithium (ML-DSA) zijn.

"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".

Gerelateerde artikelen

Meer artikelen »