

# AIVD, CWI en TNO publiceren vernieuwd handboek voor quantumveilige cryptografie

Information and sensor systems

Quantum-safe technologie

3 december 2024

Om organisaties voor te bereiden op Q-Day, de dag dat quantumcomputers in staat zijn om bepaalde veelgebruikte cryptografie te breken, publiceren de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), Centrum Wiskunde & Informatica (CWI) en TNO een vernieuwd handboek voor quantumveilige cryptografie.

Deze uitgebreide tweede editie (pdf) [📄](#) bevat, onder andere, de nieuwste ontwikkelingen en adviezen voor de overstap naar een quantumveilige omgeving, inclusief concreter advies voor het vinden van cryptografische componenten, het beoordelen van quantumrisico's en het inrichten van cryptografische wendbaarheid. Tijdens het Symposium 'Post-Quantum Cryptography' in Den Haag is het overhandigd aan de Staatssecretaris voor Digitale Zaken en Koninkrijksrelaties Zsolt Szabo.

Cryptografie wordt gebruikt om gegevens te beschermen die niet leesbaar mogen zijn door anderen. Toch is niet elke vorm van cryptografie veilig tegen aanvallen met quantumcomputers. Mogelijk vindt Q-Day al plaats in de komende vijf tot vijftien jaar, aldus sommige experts [L2](#). Kwaadwillenden, zoals vijandige statelijke actoren, kunnen dan bepaalde hedendaagse cryptografie grotendeels omzeilen. Dan gaat het bijvoorbeeld om RSA-beveiliging en ECC (elliptic curve cryptografie), die worden gebruikt voor versleuteling en digitale handtekeningen. Maar de risico's voor de huidige cryptografie beginnen vandaag al. Beveiligde data kunnen nu onderschept worden en dan vanaf Q-Day met een quantumcomputer worden ontcijferd.

Daarnaast duurt het overstappen op nieuwe cryptografie soms wel tien jaar of langer. Vandaar dat organisaties die werken met belangrijke versleutelde informatie – zoals staats- of bedrijfsgeheimen – nu al bezig moeten zijn met de overstap naar een quantumveilige omgeving. Dit handboek helpt organisaties om risico's te identificeren en geeft concrete stappen om te werken aan een migratiestrategie.



Uitreiking van het PQC handboek

## Tweede editie

Sinds de publicatie van de eerste editie is er meer kennis opgedaan op het gebied van [post-quantum cryptografie](#) (PQC). PQC is een verzameling van versleutelingsmethodes die, in tegenstelling tot huidige methodes, veilig moeten zijn tegen aanvallen met quantumcomputers. In deze herziene en uitgebreide tweede editie zijn de nieuwste ontwikkelingen en adviezen op het gebied van PQC opgenomen. Daarnaast zijn meerdere essentiële acties voor bedrijven en organisaties in de PQC -migratie nog gedetailleerder onderzocht.

Verder is er concreter advies opgenomen voor het inventariseren van cryptografische componenten in software die door organisaties wordt gebruikt, het beoordelen van quantumrisico's en cryptografische wendbaarheid. Het biedt nu ook een lijst met stappen die voor iedere organisatie handig zijn, ongeacht de quantumdreiging ("no-regret moves") en een gedetailleerd overzicht van de PQC-methodes en internationale wetgeving. Verder worden er praktische ervaringen rondom de migratie gedeeld én bevat het de nieuwe adviestool [PQChoiceAssistant](#) [L2](#) die bedrijven helpt bij hun keuze van PQC methode.

## Europese samenwerking

Sinds 2021 organiseren CWI's Cryptology onderzoeksgroep en TNO een serie symposia over [post-quantum cryptografie](#) [L2](#) met het thema 'Act now, not later.' Het doel hiervan is om de overheid, bedrijfsleven en wetenschap samen te brengen. Het evenement van 3 december in Den Haag, de 7e editie in deze serie, stond in het teken van internationalisering en werd georganiseerd met hulp van het ministerie van Binnenlandse Zaken. Een van de hoofdonderwerpen van die dag was de ontwikkeling van een Europese Roadmap om de Europese digitale infrastructuur quantumveilig te maken. Deze roadmap moet leiden tot een gecoördineerde transitie, met aandacht voor interoperabiliteit, standaarden en kennisdeling binnen Europa. Nederland speelt hierin een leidende rol, samen met Duitsland en Frankrijk. Die drie landen coördineren samen de EU werkgroep.

## Neem contact met ons op



Thomas Attema

Researcher Cryptology

In een maatschappij die wordt gedreven door data, is het essentieel om vertrouwelijke en privé informatie te beschermen. Tegelijkertijd zou de cryptografie die is ontwikkeld om deze informatie te beschermen, in de nabije toekomst kunnen worden gebroken door quantumcomputers. Thomas onderzoekt nieuwe cryptografietechnieken, die beveiligen tegen quantumcomputers en in staat zijn data op een privacy-vriendelijke manier te gebruiken.

Meer over Thomas

📍 Den Haag – New Babylon

✉ E-mail Thomas

Maaïke van der Wal

Integrator and PMC Lead

## Laat je verder inspireren

Alles

Nieuws

Artikel

Insight

Podcast

Insight

22 oktober 2024

Zonder inventarisatie geen migratie: bescherming tegen de quantumcomputer begint met inzicht

Het staat vast: de quantumcomputer komt eraan. Organisaties moeten inventariseren wat voor cryptografie ze gebruiken en daar wil TNO bij helpen.

Lees meer

Nieuws

4 april 2023

Het PQC-migratie handboek

Lees meer

Nieuws

23 september 2022

Quantumcomputer vormt ook bedreiging voor onze gegevensbescherming

Lees meer

Artikel

Cybersecurity door post quantum crypto

Lees meer

Podcast

6 mei 2019

7 afleveringen

ICT-Ontwikkelingen

Lees meer

|                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>Hier werken we aan</div> <div><div>Duurzaam</div><div>Gezond</div><div>Veilig</div><div>Digitaal</div><div>Sectoren</div><div>Werken bij</div></div> | <div>Newsroom</div> <div><div>Nieuws</div><div>Agenda</div><div>Webinars</div><div>Insights</div><div>Podcasts</div><div>Papers</div><div>Abonneren TNO Update</div></div> <div>Technologie en wetenschap</div> <div><div>Laboratoria</div><div>Onderzoeksapparaten</div><div>Technologieën</div><div>Early research programmes</div><div>Octrooien en licenties</div><div>Repository TNO Publicaties</div></div> | <div>Over TNO</div> <div><div>Missie en visie</div><div>Strategie</div><div>Organisatie</div><div>Onze mensen</div><div>Contact</div><div>TNO en de maatschappij</div><div>Communities</div></div> <div>Samenwerken</div> <div><div>Projecten in opdracht</div><div>Publiek privaat</div><div>MKB</div><div>Tech Transfer</div><div>Internationaal</div></div> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|