



- 
Nieuws
- 
Tools
- 
Duiding
- 
Leren

AIVD, CWI en TNO publiceren vernieuwd handboek voor quantumveilige cryptografie

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 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 Szabó.

AIVD 3 december 2024

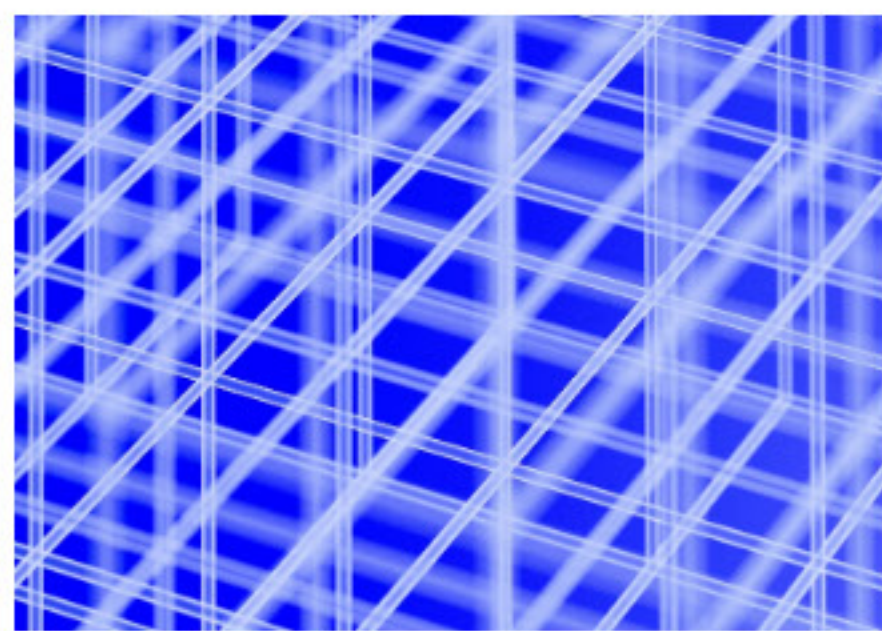
Nieuws-persbericht

aivd

inlichtingendienst

quantumtechnologie

versleuteling



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. De AIVD waarschuwt al sinds 2014 dat Q-Day kan plaatsvinden in 2030. 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, waarbij gebruik wordt gemaakt van de kennis die sinds de eerste druk is opgedaan.

Verder worden er praktische ervaringen rondom de migratie gedeeld én bevat het de nieuwe adviestool PQChoiceAssistant die bedrijven helpt bij hun keuze van PQC methode.

De AIVD kijkt altijd vooruit naar technologieën die belangrijk voor Nederland kunnen worden. De AIVD onderzoekt onder meer (het veilige gebruik) van post quantum cryptografie.

Artikel delen



Reacties

Er zijn nog geen reacties gegeven!

Laat een reactie achter

U moet **ingelogd zijn** om een reactie te plaatsen.

NIEUWS

Inwerkingtreding Wet gegevensverwerking door samenwerkingsverbanden

NIEUWS-PERSBERICHT

GI's en LNVT uiten zorgen over ontwikkeling Toekomstscenario in aanloop naar debat

NIEUWS-PERSBERICHT

Onderzoek impact Wegennetwerkregistratie DSM bij gemeenten

NIEUWS-PERSBERICHT

noyb is now qualified to bring collective redress actions

NIEUWS-PERSBERICHT

noyb is now approved as a so-called "Qualified Entity" to bring collective redress actions in courts throughout the European Union. Such action under Directive (EU) 2020/1828 can either...

Digitalisering Rijksinkoop, wat is de stand van zaken?

NIEUWS-PERSBERICHT

DIGITALE OVERHEID

Vertrouwen wij deze overheid met het aftapsysteem van de politie?

BLOG

Monitoring personeel normaliseert digitale surveillance

NIEUWS-PERSBERICHT

AP: Plan kabinet centrale database taxiritten groot privacyrisico

NIEUWS-PERSBERICHT

Politie Nederland tart rechtelijk bevel: intern databeleid schend Wpg structureel

ARTIKELEN



CHRISTIAN CORDOBA LENIS

Meld je aan voor de nieuwsbrief

Blijf altijd op de hoogte van het laatste nieuws.

AANMELDEN

Word lid van PONT | Data & Privacy

- ✓ Toegang tot Kennisbank
- ✓ Lees e-books
- ✓ Contact met vakgenoten
- ✓ Eigen nieuwsoverzicht

WORD LID

ALGEMEEN

- Over PONT | Data & Privacy
- Contact met PONT | Data & Privacy
- Schrijf voor PONT | Data & Privacy
- Algemene voorwaarden
- Privacystatement, disclaimer en auteursrecht
- Cookieverklaring
- Raad van Advies

SERVICE

- Nieuwsbrief
- Mijn PONT | Data & Privacy
- Lidmaatschappen
- Partner worden
- Vacature plaatsen
- Adverteren
- Incompany

NAVIGEER

- Events
- Dossiers
- Kennisbank
- Partners
- Auteurs

BERGHAUSER PONT MEDIAGROEP

- Over Berghauser Pont Mediagroep
- PONT Academy
- Bookshop
- PONT | Omgeving
- PONT | Zorg & Sociaal
- PONT | Klimaat



CONTACT

Berghauser Pont Mediagroep
Danzigerkade 225A
1013 AP Amsterdam

in x f