NEDERLAND CRYPTOLAND

STARTPUNT ROUTEKAART CRYPTOCOMMUNICATIE: VERKENNING VAN VIER BELANGRIJKE UITDAGINGEN IN DE CRYPTOGRAFIE

Authors

Yoram Meijaard (TNO)
Maran van Heesch (TNO)
Ronald Cramer (CWI en Universiteit Leiden)
Jelger Groenland (Innovatiemakelaar Cryptocommunicatie)

Mei 2021

CWI dcypher Ministerie van Economische Zaken en Klimaat TNO

MANAGEMENT SAMENVATTING

Cryptografie is een *fundament* voor de Nederlandse samenleving. Onze sterk gedigitaliseerde samenleving is namelijk afhankelijk is van de vertrouwelijkheid, beschikbaarheid en integriteit die cryptografie kan bieden. Daarnaast heeft cryptografie een grote rol in de strategische autonomie van Nederland.

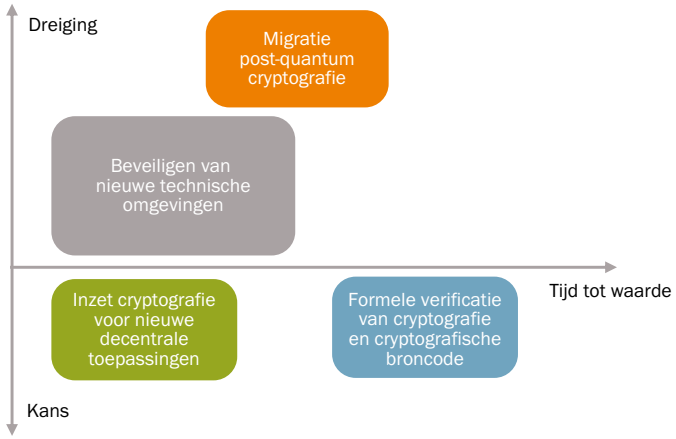
Om cryptografie in de praktijk in te kunnen zetten in de vorm van een *cryptografisch eindproduct*, zijn drie aspecten van belang: (1) de onderliggende wiskunde, (2) soft- en hardware implementatie, en (3) inbedding van het cryptografisch eindproduct in de organisatie. In de praktijk zijn cryptografische eindproducten een totaalpakket van wiskunde, software en hardware. Alle schakels zijn een opzichzelfstaande specialistische discipline, die samenkomen in de *valorisatieketen cryptografie*.

Binnen de wiskunde wordt er een onderscheid gemaakt tussen *unilaterale cryptografie*, waarin twee partijen informatie uitwisselen die geheimgehouden wordt ten opzichte van een derde partij, en *multilaterale cryptografie*, waarin meerdere partijen gezamenlijk berekeningen uitvoeren met geheimhouding van informatie ten opzichte van elkaar. Verder is het zonder een goede implementatie van het cryptografische protocol in zowel software als hardware onmogelijk om cryptografie veilig te gebruiken. Er zijn veel eisen waar een goede implementatie aan zou moeten voldoen; lastig is dat deze elkaar soms tegenspreken. Tot slot is de correcte inbedding in de organisatie en hiermee het correcte gebruik van het cryptografisch eindproduct, van belang. Certificering kan handvatten bieden om het juiste product voor het juiste veiligheidsniveau in te zetten, maar vereist dat het cryptografisch eindproduct controleerbaar is.

Er zijn veel verschillende cryptografische eindproducten, welke ieder een eigen functionaliteit hebben. Om deze te kunnen categoriseren maken we onderscheid tussen *data at rest*, *data in use* en *data in transit*. Binnen Nederland wordt er voornamelijk gebruik gemaakt van twee bekende taxonomieën van cryptografische eindproducten, namelijk de taxonomie van het Nationaal Bureau voor Verbindingsbeveiliging (NBV) en van de Common Criteria. Om deze lijsten te vergelijken zijn in deze verkenning beide taxonomieën gekoppeld aan de drie te onderscheiden categorieën. Het valt op dat niet alle productcategorieën van de Common Criteria zijn afgedekt door producten die door het NBV geëvalueerd zijn. Belangrijk hierbij is dat de ontwikkeling en acceptatie van nieuwe digitale technologie niet altijd aansluit bij de bestaande cryptografische eindproducten, de onafgedekte productcategorieën duiden op plekken waar deze aansluiting onvolledig is.

Binnen Nederland hebben we een actief cryptografisch landschap. Nederland heeft een sterke wetenschappelijke leiderschapspositie met veel internationaal erkende vooraanstaande wetenschappers. Er zijn een aantal middelgrote bedrijven die cryptografische eindproducten leveren. Het valt op dat in de taxonomie van de Common Criteria van producten die goedgekeurd zijn voor gebruik in Nederland, dat deze vooral door buitenlandse bedrijven geleverd worden.

In het cryptografie landschap zijn er constant nieuwe ontwikkelingen. Er zijn op dit moment vier ontwikkelingen die, naar ons inzien, de grootste uitdagingen vormen en de grootste kansen bieden voor de komende jaren op het domein van cryptografie (zie Figuur).



Figuur: Uiteenzetting van de vier high-impact ontwikkelingen in de cryptografie, uitgesplitst in kansen en dreigingen en uitgezet over de tijd. 1. beveiligen nieuwe technische omgevingen (grijs), 2. migratie naar post-quantum cryptografie (oranje), 3. inzet cryptografie voor nieuwe decentrale toepassingen (groen), 4. formele verificatie (blauw).

1. *Beveiligen van nieuwe technische omgevingen:* door de constante ontwikkeling en adoptie van nieuwe technische omgevingen is het nodig om deze voldoende te beveiligen voordat deze geschikt zijn om te gebruiken in situaties waarin veiligheid van groot belang is. Deze productontwikkeling is in principe uit te voeren met gangbare unilaterale cryptografie en is op korte termijn realiseerbaar.

2. *Migratie naar post-quantum cryptografie:* de ontwikkeling van de quantumcomputer brengt veelgebruikte cryptografische systemen in gevaar. Er wordt gewerkt aan post-quantum cryptografie die bestendig is tegen de quantumcomputer. De migratie naar post-quantum cryptografie is een uitdaging voor de gehele valorisatieketen, zowel op de korte als op de lange termijn. Een bijkomende kans is dat door middel van de structurele migratie de crypto-agility van de systemen verhoogd kan worden.

3. *Inzet van cryptografie voor nieuwe decentrale toepassingen:* de ontwikkeling van multilaterale cryptografie gaat heel hard en leidt tot nieuwe decentrale oplossingen, zoals secure multi-party computation. Het gebruik hiervan biedt kansen voor de Nederlandse economie. Op de korte termijn worden er verschillende markttoepassingen in Nederland verwacht.

4. *Formele verificatie van cryptografie en cryptografische broncode:* Formele verificatie is een methode om met een computer geautomatiseerd controles uit te voeren op software implementaties. Het toepassen van technieken uit de formele verificatie op cryptografische protocollen en broncode biedt een garanties over de veiligheid van cryptografische producten. De verwachtingen zijn zeer hoog, maar de toepassing wordt pas op de lange termijn verwacht.

Nederland zal stappen moeten ondernemen om deze kansen volledig te kunnen benutten en de uitdagingen het hoofd te bieden. In de Routekaart Cryptocommunicatie van het Ministerie van Economische Zaken en Klimaat werken we uit welke stappen er gezet moeten worden. Als auteurs willen we u, de lezer, via deze verkenning uitnodigen tot samenwerking aan de Routekaart, Cryptocommunicatie. Zo kunnen we gezamenlijk toewerken tot Nederland Cryptoland, waarbij een economisch actief en gezond ecosysteem, strategische autonomie en digitale veiligheid de uitgangspunten vormen.

INHOUD

1. INLEIDING EN ACHTERGROND

Cybersecurity is belangrijk voor consumenten, industrie en overheden om veilig en met vertrouwen gebruik te maken van computers, het internet en allerlei digitale systemen. Cybersecurity bevat veel aspecten, zoals monitoring van informatiestromen en toegangsmanagement, maar duidelijk is dat cryptografie een kritiek bouwblok is voor cybersecurity. Cryptografie is een *fundament* voor de Nederlandse samenleving, die afhankelijk is van de vertrouwelijkheid, beschikbaarheid en integriteit die cryptografie kan bieden.

Cryptografie is een zeer breed onderwerp. De basis van cryptografie ligt in de wiskunde, in de open en gepubliceerde wetenschap. De toepassing van cryptografie uit zich, onder andere, in veilige communicatie. Deze communicatie systemen zijn geïmplementeerd in software en hardware, ontwikkeld achter gesloten deuren. De stap van wiskundige perfectie naar de echte wereld brengt eigen aspecten met zich mee; zo moet de gebruikte hardware veilig zijn en net als alle componenten die door toeleveranciers aangeleverd zijn. Om cryptografie goed toe te passen moet er met al deze aspecten goed omgegaan worden. In de praktijk zijn cryptografische eindproducten een totaalpakket van wiskunde, software en hardware. Alle schakels zijn een opzichzelfstaande specialistische discipline die samenkomen in de *valorisatieketen cryptografie*.

In Nederland wordt cryptografie onder andere toegepast om hoog gerubriceerde informatie veilig te houden. Zodoende speelt cryptografie een grote rol in de strategische autonomie van Nederland. Strategische autonomie betekent dat Nederland, voor sectoren die van strategisch belang zijn, zelf in staat is een keuze te maken tot zelfbeschikking, samenwerking of afhankelijkheid van het buitenland. De keuzemogelijkheid staat hierin centraal. Factoren die strategische autonomie in de weg staan zijn bijvoorbeeld een gebrek aan kennis of economische activiteit in een bepaalde sector. Cryptografie is een onderwerp waarop Nederland strategische autonomie wil hebben. Dat wil zeggen dat Nederland niet zelfvoorzienend hoeft te zijn, maar wel in staat moet zijn om een bewuste keuze te maken over welke cryptografische technologie in Nederland ontwikkeld wordt en welke buiten-Nederland ontwikkelde technologie geïmporteerd en gebruikt kan worden.

In het cryptografisch landschap zijn er constant nieuwe ontwikkelingen. Sommige ontwikkelingen bedreigen het huidige beveiligingsniveau en andere bieden juist nieuwe kansen voor het Nederlandse bedrijfsleven en academische sector. Het ministerie van Economische Zaken en Klimaat wil samenwerking in het Nederlandse cryptografie landschap stimuleren om van alle ontwikkelingen te profiteren door vraag en aanbod bij elkaar te brengen en waar nodig actief innovatie in de valorisatieketen te stimuleren.

Er is daarom voor gekozen om rond het thema cryptocommunicatie een gedragen innovatie routekaart te ontwikkelen. Cryptocommunicatie is daarbij de toegepaste vorm van cryptografie in alle vormen van digitale communicatie. Deze terminologie geeft aan dat de routekaart breder is dan wiskunde alleen, maar aanvullende waarde vindt in de toepassing van cryptografie in informatietechnologie en andere domeinen. Cryptocommunicatie maakt daarnaast duidelijk dat het hier niet om het domein van de cryptomunten en digitale assets gaat, maar om de toepassing in het veilig uitwisselen van informatie tussen partijen via digitale kanalen.

De routekaart cryptocommunicatie richt zich op ‘hoe’ Nederland moet handelen om goed met al deze ontwikkelingen om te gaan. Deze verkenning geeft een eerste invulling aan ‘wat’ de ontwikkelingen in cryptografie zijn en wat de thema’s zijn voor de routekaart. In deze verkenning worden de begrippen en relevante aspecten van cryptografie en cryptocommunicatie in kaart gebracht. Op basis daarvan kan pas een start worden gemaakt met een routekaart cryptocommunicatie.

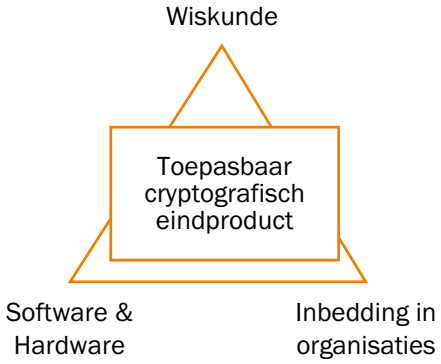
1.1 LEESWIJZER

In hoofdstuk 2 beschrijven we wat er nodig is om cryptografie in de praktijk in te kunnen zetten in de vorm van een *cryptografisch eindproduct* en in hoofdstuk 3 beschouwen we de verschillende typen cryptografische eindproducten. In hoofdstuk 4 brengen we het Nederlandse cryptolandschap in kaart. In hoofdstuk 5 beschrijven we de vier high-impact ontwikkelingen (kansen én dreigingen) in de cryptografie waarop Nederland zal moeten gaan acteren. Tot slot in hoofdstuk 6 concluderen we het document en in hoofdstuk 7 nodigen we de lezer uit om actief bij te dragen aan de Routekaart Cryptocommunicatie.

“CRYPTOGRAFIE STAAT AAN DE BASIS VAN DE DIGITALE VEILIGHEID EN IS BELANGRIJK VOOR DE STRATEGISCHE AUTONOMIE VAN NEDERLAND. HET CRYPTOGRAFIE LANDSCHAP IS CONSTANT IN BEWEGING, WAARDOOR NIEUWE DREIGINGEN ÉN KANSEN ZICH CONTINUE PRESENTEREN.”

2. CRYPTOGRAFIE: VAN PROTOCOL TOT EINDPRODUCT

Deze sectie beschrijft de verschillende facetten van een toepasbaar cryptografisch eindproduct, zie Figuur 1. Een overzicht wordt gegeven van de wiskunde achter cryptografie met bijbehorend nomenclatuur. De risico's en eigenschappen van de informatiekundige toepassing van cryptografie worden behandeld. Tot slot komt de inbedding van cryptografische eindproducten in de processen van een organisatie aan bod.



Figuur 1. De drie aspecten van cryptografie.

2.1 WAT IS CRYPTOGRAFIE

Cryptografie is de wetenschap die bouwstenen levert voor het 'veilig' omgaan met informatie. Wat veilig is verschilt per context, maar heeft vaak één of meerdere van de volgende eigenschappen:

- Beschikbaarheid, de data is beschikbaar voor degene die het nodig heeft.
- Integriteit, de data is onaangetast door derden.
- Vertrouwelijkheid, de data kan niet door derden ingezien worden.
- Onweerlegbaarheid, het is duidelijk van wie de data afkomstig is.

In de theorie kan cryptografie onderverdeeld worden in ten minste twee deelgebieden die essentieel van elkaar verschillen en elk hun eigen methodes omvatten. In *unilaterale cryptografie* wisselen twee partijen informatie uit die geheimgehouden wordt ten opzichte van een derde partij, dit in contrast met *multilaterale cryptografie* waarin meerdere partijen gezamenlijk berekeningen uitvoeren met geheimhouding van informatie ten opzichte van elkaar.

Unilaterale cryptografie is de oudste en meest ontwikkelde stroming en is op te delen in drie technieken: *symmetrische cryptografie* waarin beide/alle partijen informatie versleutelen en ontsleutelen met dezelfde geheime sleutel, *asymmetrische cryptografie* waarin iedere partij een eigen publieke en bijbehorende private sleutel gebruikt, en *cryptografische hash-functies* waarmee een nagenoeg unieke digitale vingerafdruk van de data gemaakt kan worden.

Het paradoxale van symmetrische cryptografie is dat er vooraf een sleutel afgesproken moet worden, maar het medium waarover de sleutel gecommuniceerd wordt pas veilig is als de sleutel is afgesproken. Deze catch-22 wordt het sleuteluitwisselingsprobleem genoemd. Asymmetrische cryptografie is geïntroduceerd om dit probleem op te lossen. Door gebruik te maken van de publieke sleutel van een ontvangende partij kan een bericht versleuteld worden, zodanig dat het bericht alleen ontsleuteld kan worden met de private sleutel van de ontvangende partij. Bovendien biedt asymmetrische cryptografie ook de mogelijkheid om digitale handtekeningen te zetten.

Een voordeel van symmetrische cryptografie is de hoge snelheid ten opzichte van asymmetrische cryptografie. Daarom gebruiken moderne cryptosystemen eerst asymmetrische cryptografie voor authenticatie van partijen en om een sleutel uit te wisselen, en versleutelen vervolgens met symmetrische cryptografie data. Deze gecombineerde cryptosystemen zijn overal te vinden in onze digitale maatschappij, van het versleutelen van banktransacties tot internetbezoeken, van het versturen van instant messages tot inloggen in elke webwinkel.

Cryptografische hash-functies spelen een belangrijke rol in het maken van digitale vingerafdrukken van data. Deze vingerafdruk is uniek[1] en kleine veranderingen in de data creëren een totaal andere vingerafdruk. Hiermee kan bijvoorbeeld de integriteit van een gedownload programma gecontroleerd worden. Cryptografische hash-functies spelen bovendien een belangrijke rol als heuristische benadering van willekeurigheid waarmee verschillende cryptografische systemen versterkt worden.

Multilaterale cryptografie heeft andere toepassingsgebieden. Er zijn situaties waarin meerdere partijen een gezamenlijk doel hebben, maar er geen sprake is van wederzijds vertrouwen, waardoor informatie niet gedeeld wordt tussen de partijen. Om toch tot een resultaat te komen wordt er dan een *vertrouwde derde partij* ingezet om alle informatie op te halen bij alle partijen en onafhankelijk tot een conclusie te komen. Neem als voorbeeld een veiling waarin alle deelnemers in het geheim hun bod doen bij de veilingmeester, die vervolgens bepaalt wie het hoogste bod heeft uitgebracht. Achteraf is het voor iedere deelnemer niet te herleiden wie welk bod heeft uitgebracht, maar de veilingmeester kent alle biedingen. De deelnemers vertrouwen dat de veilingmeester inderdaad het hoogste bod heeft geaccepteerd en dat de veilingmeester geen misbruik heeft gemaakt van het inzicht in de biedingen.

De vertrouwelijkheid van de *vertrouwde derde partij* presenteert een probleem, immers is vertrouwelijkheid zeer lastig te verifiëren en heeft elke deelnemer er geen controle over. Voor deze *vertrouwensparadox* biedt unilaterale cryptografie geen oplossing. Echter, technieken uit de multilaterale cryptografie kunnen de *vertrouwde derde partij* emuleren waardoor de cryptografie de vertrouwelijkheidsrol overneemt. Multilaterale cryptografie stelt meerdere partijen in staat tot het gezamenlijk uitvoeren van een willekeurige berekening zonder trusted third party, mét behoud van de vertrouwelijkheid van de individuele input en met een verifieerbaar correct resultaat.

2.2 TECHNISCHE ASPECTEN VAN EEN CRYPTOGRAFISCH EINDPRODUCT

De basis van cryptografie ligt in de wiskunde, maar is voor de toepassing afhankelijk van de gebruikte software en hardware. Cryptografie wordt in de regel geïmplementeerd in software en hardware en dit brengt eigen gevaren met zich mee. Voorbeelden hiervan zijn:

– *Side-channels* die informatie lekken over de gebruikte cryptografie en bijbehorende sleutels, bijvoorbeeld door minuscule verschillen in uitvoeringstijd.
– *Glitches*, kortlevende fouten in de hardware die cruciale cryptografische stappen kunnen doen overslaan.

Het gevolg is dat een cryptografische methode wiskundig gezien veilig is, maar in de implementatie toch kwetsbaar blijkt te zijn.

1. *In de literatuur wordt gesproken over collision resistance wanneer het vinden van twee inputs voor een hash-functie met dezelfde vingerafdruk zeer lastig is. In de praktijk zijn deze vingerafdrukken nagenoeg uniek.*

In de praktijk zijn cryptografische eindproducten een totaalpakket van wiskunde, software en hardware. Alle schakels zijn een opzichzelfstaande specialistische discipline die samenkomen in de *valorisatieketen cryptografie*. In gezamenlijkheid leidt de valorisatieketen tot een uiteindelijk cryptografisch eindproduct. Aan een cryptografisch eindproduct zitten verschillende eigenschappen, waarvan sommigen elkaar zelfs tegenwerken. We onderscheiden de volgende eigenschappen:

- De *functionaliteit* die het product levert, hierop wordt in hoofdstuk 3 dieper ingegaan.
- Het *beveiligingsniveau* is de mate van veiligheid die het product levert.
- De *complexiteit* is de mate van ingewikkeldheid van een product.
- De *modulariteit* is de mate waarin een product splitsbaar is in losse onderdelen.
- De *performance* van het product, bijvoorbeeld gemeten in de te behalen snelheid en throughput.
- De *crypto-agility* van het product is de mate waarin de cryptografie achteraf aangepast kan worden.
- De *controleerbaarheid* is de mate waarin het voor een gebruiker of externe controleur mogelijk is de eigenschappen van een eindproduct te verifiëren.
- De *gebruiksvriendelijkheid* is de mate van gemakt waarmee het cryptografisch eindproduct gebruikt kan worden.

Een voorbeeld van crypto-agility is het veranderen van het gebruikte cryptografisch protocol, bijvoorbeeld van 3DES naar AES. Dit kan nuttig zijn wanneer nieuwe inzichten leiden tot andere eisen aan de gebruikte cryptografie. Deze eigenschap beschrijft als het ware een plug 'n play optie, waarmee functionaliteit van het product behouden wordt maar veiligheidseigenschappen veranderen.

De verschillende eigenschappen kunnen elkaar versterken of tegenwerken. Complexiteit en controleerbaarheid werken elkaar tegen: een zeer complex product is lastig te controleren. Modulariteit kan in zekere mate de complexiteit van het product verlagen, door het eindproduct op te delen in behapbare brokken. De complexiteit van een softwareproduct is typisch hoger dan die van een hardware product en de crypto-agility van een software product typisch hoger dan een hardware product. Er zijn echter redenen om voor een hardware product te kiezen: in een hardware product is de performance typisch beter en het behaalde beveiligingsniveau hoger. De context waarin een cryptografisch eindproduct gebruikt wordt dicteert welke afweging tussen de tegenwerkende eigenschappen geschikt is.

2.3 CRYPTOGRAFIE IN HET OPERATIONEEL PROCES

Cryptografie wordt overal toegepast waar digitaal omgegaan wordt met informatie, zoals communicatie, dataopslag, ondertekenen en software-updates. Het gebruik van eindproducten in een organisatie vereist correcte inbedding binnen bedrijfsprocessen en technische infrastructuur. Daarvoor is het van groot belang dat het product gekozen wordt dat de juiste functionaliteit biedt én dat het op de juiste manier gebruikt wordt.

Cruciaal bij het selecteren van het juiste cryptografische eindproduct is de *zekerheid* dat het product aan de veiligheidseisen van de organisatie voldoet. Cryptografische eindproducten staan centraal in de veiligheid van de organisatie, waardoor een zekere mate van wantrouwen en voorzichtigheid aanwezig is. Om zekerheid te verschaffen dat een product aan de eisen voldoet moet het product in zekere mate *controleerbaar* zijn.

Organisaties moeten de keuze voor een bepaald product zelf maken. *Certificering* biedt handvatten voor organisaties om een cryptografisch eindproduct te kiezen dat past bij het beoogde veiligheidsniveau. Bekende voorbeelden van certificatie zijn de toetsen door het Nationaal Bureau voor Verbindingsbeveiliging (NBV)[2] en de Common Criteria[3]. Het NBV is een tak van de Nederlandse AIVD en fungeert als poortwachter voor het inzetten van producten in het staatsgeheime domein. De Common Criteria is een internationale standaard waartegen gecertificeerd kan worden door verschillende partijen. De evaluatie van het NBV zal in deze verkenning aan bod komen in sectie 3.

2. *https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/geevalueerde-producten*
3. *https://www.commoncriteriaportal.org/*

Een voorwaarde voor het gebruik van cryptografische eindproducten in een organisatie is identity, key en access management. Identity management is het proces waarmee de identiteit van een gebruiker wordt vastgesteld. Key management is het proces waarmee de cryptografische sleutels gegenereerd worden en gekoppeld worden aan de vastgestelde identiteiten. Access management is het proces waarmee toegang tot informatie voor bepaalde identiteiten geregeld wordt. Het correct inregelen van deze systemen in grote organisaties in een niet-triviale taak.

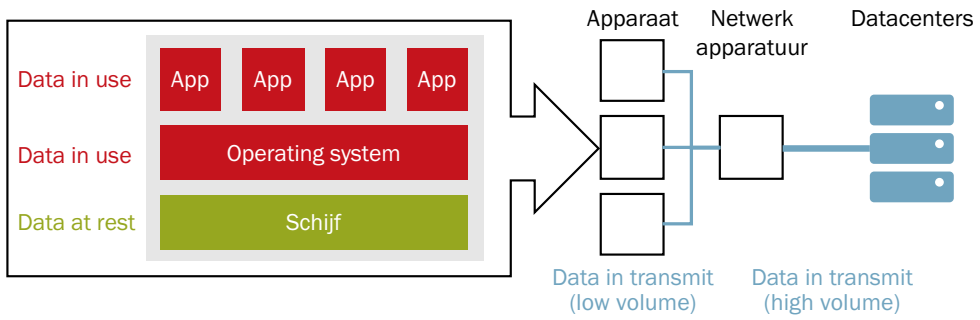
“IN DE PRAKTIJK ZIJN CRYPTOGRAFISCHE EINDPRODUCTEN EEN TOTAALPAKKET VAN WISKUNDE, SOFTWARE EN HARDWARE.
ALLE SCHAKELS ZIJN EEN OPZICHZELFSTAANDE SPECIALISTISCHE DISCIPLINE DIE SAMENKOMEN IN DE *VALORISATIEKETEN CRYPTOGRAFIE*.”

3. CRYPTOGRAFISCHE EINDPRODUCTEN IN DE PRAKTIJK

In deze sectie wordt dieper ingegaan op de functionaliteiten van cryptografische eindproducten. Hiertoe introduceren we een referentiemodel voor de toepassing van cryptografie. Dit referentiemodel kan gebruikt worden om de gewenste functionaliteit van het cryptografisch eindproduct in context te plaatsen. Aan de hand van het referentie model beschouwen we de taxonomieën van cryptografische productcategorieën zoals gebruikt door het Nationaal Bureau Verbindingsveiligheid (NBV) en de Common Criteria. Tot slot gebruiken wij de taxonomie van het NBV om een eerste indicatie te geven aan welke functionaliteiten er bij de Rijksoverheid behoefte is.

3.1 REFERENTIEMODEL CRYPTOGRAFIE

In de praktijk zijn er veel verschillende toepassingen van een cryptografisch eindproduct. In Figuur 2 is een referentiemodel gegeven waaraan de verschillende functionaliteiten van cryptografische eindproducten opgehangen kunnen worden. Dit referentiemodel is een adaptatie van het referentiemodel zoals gebruikt in een voorgaand TNO-rapport[4] en benadrukt de verschillende stadia waarin data zich kan bevinden.



Figuur 2: Referentie model cryptografische eindproducten.

Binnen een *apparaat*, zoals een laptop of mobiele telefoon, bevindt zich een gelaagde architectuur, zie Figuur 2. Op de *schijf* wordt data opgeslagen, die wordt gebruikt door het *operating system* en bijbehorende *apps*. Tussen verschillende apparaten wordt data uitgewisseld, zowel op lagere snelheid als op hoge snelheid zoals tussen *datacenters* gebeurt.

Het referentiemodel omschrijft drie verschillende stadia waarin data zich kan bevinden: data is in ruste, in transport, of in gebruik. Daarnaast zijn er drie uitspringende plekken waar cryptografie wordt toegepast: binnen de apparatuur van een eindgebruiker, binnen netwerkapparatuur en binnen datacenters. De verschillende plekken in het netwerk brengen verschillende veiligheidseisen met zich mee, waardoor er behoefte is aan een zeer divers productportfolio.

4. *TNO-rapport "Verdieping Valorisatieketens: Basis voor de routekaart 'Veilig werken in een onveilige cloud'"*

3.2 TAXONOMIEËN FUNCTIONALITEIT CRYPTOGRAFIE

Er worden verschillende taxonomieën gebruikt om onderscheid te maken tussen de functionaliteiten van een eindproduct. In deze sectie beschouwen we twee bestaande taxonomieën van cryptografische eindproducten, namelijk de taxonomie van het NBV en de Common Criteria. De keuze hiervoor is de toepasbaarheid binnen Nederland: de evaluatie van het NBV is leidend is voor de Rijksoverheid en de Common Criteria speelt een grote rol voor het Nederlands bedrijfsleven. De taxonomieën zijn overgenomen van de lijst NBV geëvalueerde producten[5], zie Tabel 1, en de lijst van Common Criteria gecertificeerde producten, zie Tabel 2. In beide tabellen is aangeven waar de producten gebruikt worden binnen het referentiemodel, zie Figuur 2.

De taxonomie van het NBV brengt een onderverdeling aan tussen producten voor *media en bestandsvercijfering*, producten voor *netwerkbeveiliging* en producten voor *mobiele communicatie*. In de overige categorie staan *keyboard, video and mouse (KVM) switches*, producten die gebruikt worden om met één toetsenbord, scherm en muis tegelijk aan te sluiten op meerdere computers. Een typische toepassing van een KVM-switch is in een datacenter, zodat er efficiënt toegang is tot de vele servers in één serverrek.

Tabel 1: Taxonomie geëvalueerde beveiligingsproducten Nationaal Bureau voor Verbindingsbeveiliging (NBV).

Taxonomie productcategorieën Nationaal Bureau voor Verbindingsbeveiliging	Referentiemodel
Media en bestandsvercijfering	Data at rest
Offline beveiliging	Data at rest
Laptopbeveiliging	Data at rest
Beveiliging externe media	Data at rest
Netwerkbeveiligingsproducten	Data in transit
Beveiligde mobiele communicatieproducten	Data in transit
Overige beveiligingsproducten	N.v.t.

De nadruk van deze taxonomie lig op het hoog-gerubriceerde, ook wel het *high-assurance*, domein waarin met staatsgeheime informatie omgegaan moet worden. In het domein van laag-gerubriceerde informatie wordt gewerkt met departementaal vertrouwelijke informatie.

De taxonomie van de Common Criteria kent meer categorieën dan de taxonomie van het NBV, zie Tabel 2. Interessant is om de zien dat alle categorieën van het NBV terugkomen in de taxonomie van Common Criteria, met de kanttekening dat *netwerkbeveiliging* bij de common criteria opgedeeld is in verschillende categorieën, zoals *boundary protection* en *network devices*. Daarentegen komen er in de taxonomie van de Common Criteria productcategorieën voor die niet in de taxonomie van het NBV terugkomen.

Tabel 2: Taxonomie cryptografische productcategorieën van de Common Criteria.

Taxonomie productcategorieën Common Criteria	Referentiemodel
Access Control Devices and Systems	Data in transit
Boundary Protection Devices and Systems	Data in transit
Data Protection	Data at rest
Databases	Data at rest
Detection Devices and Systems	Data in transit
ICs, Smart Cards and Smart Card-Related Devices and Systems	Data at rest
Key Management Systems	Data in transit, rest and use
Multi-Function Devices	Data in use
Network and Network-Related Devices and Systems	Data in transit
Operating Systems	Data in use
Products for Digital Signatures	Data in transit, rest and use
Secure mobile devices	Data in transit
Trusted Computing	Data in use
Other Devices and Systems	N.v.t.

5. *https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/geevalueerde-producten*

Uit de tabellen is het gemakkelijk te zien dat er verschillen zijn tussen de twee taxonomieën. Ten eerste komen in de taxonomie van het NBV, Tabel 1, geen *data in use* producten voor, zoals trusted computing, operating systems en multi function devices. Deze producten komen wel voor in de taxonomie van de Common Criteria, Tabel 2. Verder zijn in de taxonomie van de Common Criteria ondersteunende producten, zoals access control, key management en digital signatures wel opgenomen. Merk op dat deze toepassingen in zekere mate ook in de bestaande cryptografische eindproducten zullen zitten. Verder valt op dat in beide taxonomieën oplossingen voor cloud-computing nog niet als categorie zijn aangeduid.

Alle bovenstaande oplossingen zijn implementeerbaar met gangbare unilaterale cryptografie. In hoofdstuk 5.1 zal verder ingaan op het uitbreiden van het bestaande product portfolio.

“CRUCIAAL BIJ HET SELECTEREN VAN HET JUISTE CRYPTOGRAFISCHE EINDPRODUCT IS DE **ZEKERHEID** DAT HET PRODUCT AAN DE VEILIGHEIDSEISEN VAN DE ORGANISATIE VOLDOET.”

4. HET CRYPTOGRAFISCH LANDSCHAP VAN NEDERLAND

Vanuit de strategische autonomie van Nederland is het belangrijk om een goed beeld te hebben van het volledige cryptografisch ecosysteem in Nederland. In deze sectie wordt een eerste aanzet gegeven voor de kennispositie van de Nederlandse universiteiten en een eerste indicatie gegeven van de bedrijven die in Nederland op cryptografisch gebied actief zijn. Hierbij is de nadruk gelegd op de bedrijven die oplossingen bieden voor data at rest, in transit en in use. Bedrijven die andersoortige oplossingen bieden, of een andere rol spelen in het cryptografisch ecosysteem in Nederland worden niet beschouwd.

Deze kennispositie van de universiteiten is de fundering voor de valorisatieketen cryptocommunicatie. De ontwikkelde kennis geeft mogelijkheden voor het bedrijfsleven om snel van nieuwe ontwikkelingen gebruik te maken en tot een cryptografisch eindproduct te komen. De afstemming tussen onderzoek en valorisatie kan verder uitgediept worden en in kaart gebracht in de Routekaart Cryptocommunicatie van het Ministerie van Economische Zaken en Klimaat.

4.1 KENNISPOSITIE NEDERLAND

De kennispositie van Nederland is goed: er is een sterk academisch ecosysteem van internationaal gerenommeerde universiteiten en kennisinstellingen waarin cryptografie in de volle breedte wordt onderzocht. Er is op alle relevante deelgebieden van de cryptografie internationaal leiderschap voorhanden binnen de wetenschappelijke vakgroepen, instituten en kennisinstellingen. Dat wil zeggen, academici aan Nederlandse instellingen doen toonaangevend onderzoek in hun respectievelijke deelgebieden. Specifiek rondom post-quantum cryptografie en multilaterale cryptografie heeft Nederland internationaal leiderschap en een uitstekende kennispositie.

Een eerste indruk van welke deelgebieden van de cryptografie aan welke universiteit onderzocht wordt is gegeven in Tabel 3. Dit overzicht is gemaakt op basis van de publieke websites van de universiteiten en de daaraan verbonden onderzoeksgroepen. De onderzochte deelgebieden van cryptografie corresponderen met de onderverdeling van cryptografie zoals gegeven in sectie 2.1, aangevuld met quantum cryptografie (vooruitlopend op sectie 5.2) en hardware cryptografie zoals gegeven in sectie 2.2.

Tabel 3: Eerste aanzet overzicht cryptografie aan Nederlandse kennisinstellingen. Groen betekent dat dit deelgebied onderzocht wordt door vaste staf van de kennisinstelling en geel dat er onderzoek gerelateerd aan het deelgebied plaatsvind.

Kennisinstellingen	Deelgebieden cryptografie
CWI	
Radboud Universiteit	
Rijksuniversiteit Groningen	
TU Delft	
TU Eindhoven	
Universiteit Leiden	
Universiteit Twente	
Universiteit van Amsterdam	
Vrije Universiteit	
TNO	

4.2 EERSTE INDRUK LEVERANCIERS PRODUCTEN

Het is lastig om een compleet overzicht samen te stellen van alle welke (internationale) bedrijven allemaal actief zijn als leverancier van cryptografische eindproducten op de Nederlandse markt. Een eerste inschatting kan worden gedaan door te kijken naar de producenten die door de NBV geëvalueerde producten leveren of producten leveren die een Common Criteria certificering hebben voor het NL-schema. Deze informatie wordt gegeven in respectievelijk Tabel 4 en Tabel 5.

Tabel 4: Overzicht van internationale bedrijven die Nederland door het NBV geëvalueerde producten leveren. Dikgedrukte bedrijven komen uit Nederland.

Toeleveranciers geëvalueerde producten Nationaal Bureau voor Verbindingsbeveiliging		
APITech	**Fox Crypto**	Microsoft
Black Box	Hiddn	Sectra
Blancco	Ironkey	Secunet
Compumatica	iStorage	Sophos
		Technolution

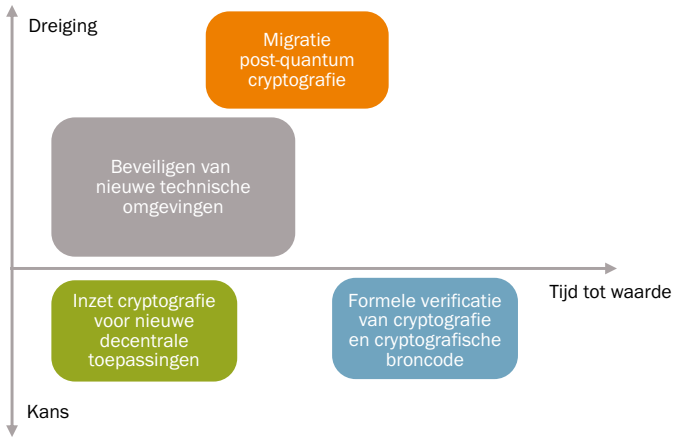
Tabel 5: Overzicht van (internationale) bedrijven producten leveren volgens het Common Criteria NL-schema.

Toeleveranciers producten Common Criteria			
A.E.T. Europe	DocuSign	Infineon Technologies	Sony
AllWipe	Eurowitcel	JR EAST MECHATRONICS	STMicroelectronics
Arm	Fox-IT	nCipher Security	Symantec
Blue Coat Systems	G+D Mobile Security	NetIQ	Thales
CEC Huada Electronic Design	HID Global	Nexor	Toshiba
Check Point Software Technologies	HiSilicon	NXP Semiconductors	Utimaco
Cisco Systems	Huawei Technologies	SafeNet	Waterfall Security Solutions
Cryptomathic A/S	Idemia	Samsung Electronics	ZTE Corporation

Het is opmerkelijk dat er beperkte overlap is tussen bedrijven die goedgekeurde producten leveren aan de Nederlandse overheid en aan de Nederlandse markt. Een waarschijnlijke verklaring hiervoor is dat Nederland een beperkte marktomvang heeft én dat de internationale concurrentie sterk is. Nederland kan met deze internationale concurrentie niet zomaar mee concurreren op R&D gebied. Dit laat zien dat wil Nederland strategische autonomie hebben, dan moet er meer geïnvesteerd worden in cryptografie.

5. AANSTAANDE ONTWIKKELINGEN CRYPTOGRAFIE

In deze sectie worden de vier ontwikkelingen geschetst die van grote impact zullen zijn op de Nederlandse samenleving op zowel de lange als de korte termijn. In Figuur 3 wordt een overzicht gepresenteerd van deze vier ontwikkelingen. Hierbij is onderscheid gemaakt is tussen of de ontwikkeling een kans voor Nederland biedt of een bedreiging vormt. Ook is een schatting gemaakt over hoever de ontwikkelingen in de toekomst liggen. In de opeenvolgende secties worden deze ontwikkelingen uitgebreid behandeld.



Figuur 3: Uiteenzetting van de vier hoofdontwikkelingen in de cryptografie, uitgesplitst in kansen en dreigingen en uitgezet over de tijd tot waarde. 1. beveiligen nieuwe technische omgevingen (grijs), 2. migratie naar post-quantum cryptografie (oranje), 3. inzet cryptografie voor nieuwe decentrale toepassingen (groen), 4. formele verificatie (blauw).

De formulering van deze ontwikkelingen is tot stand gekomen in samenwerking met vertegenwoordiging van de industrie, overheid en kennisinstellingen uit Nederland. Bij de gevoerde gesprekken zijn geen verdere ontwikkelingen naar voren gekomen.

De ontwikkelingen zijn in de basis gelijk qua omvang, met uitzondering van *beveiligingen van nieuwe technische omgevingen*. Er zijn dusdanig veel nieuwe technische omgevingen die nog aangepast moeten worden voordat deze inzetbaar zijn in situaties met hoge veiligheidseisen, dat deze ontwikkeling breder is neergezet.

5.1 BEVEILIGEN VAN NIEUWE TECHNISCHE OMGEVINGEN

In toenemende mate worden er nieuwe digitale producten aangeboden waarin de unilaterale veiligheid niet gegarandeerd is. Deze technieken worden zonder problemen gebruikt buiten het gerubriceerde domein. Echter, hierdoor ontstaat van nature een discrepantie tussen technologie waarmee men gewend is te werken en technologie die voldoet aan strikte veiligheidseisen. Dit is echt een zeer reëel probleem in de praktijk, voor zowel overheid als het bedrijfsleven.

Deze ontwikkeling begint met een aantal concrete voorbeelden van normaal geworden digitale technologie ontwikkelingen waarin de unilaterale veiligheid nog in zekere mate ontwikkeld moet worden. De voorbeelden zijn ingedeeld naar gelang het referentiemodel in sectie 3.1.

DATA IN TRANSIT

- **Koppelstukken** die scheiding aanbrengen tussen netwerken van verschillende veiligheidsniveaus, eventueel met de mogelijkheid om data uit te wisselen, bijvoorbeeld (geavanceerde) datadiodes.
- High performance encryptie die in staat is om op hoge bandbreedte data op hoog-gerubriceerd niveau data uit te wisselen. Concreet betekent dit het doorontwikkelen van bestaande lijnversleuteling.
- **Industriële toepassingen** voor het beveiligen van SCADA/ICS systemen. Traditioneel zijn dit opzichzelfstaande systemen zonder internettoegang, maar tegenwoordig worden deze systemen in toenemende mate gekoppeld aan het bedrijfsnetwerk. Voorbeelden van hoe cryptografie kan helpen om de risico's van gekoppelde SCADA/ICS systemen te mitigeren zijn toegang beperking middels datadiodes, authenticatie van de verschillende systemen en de integriteit van de uitgewisselde data. Expliciet willen wij er aandacht op richten dat het nut van versleutelen van informatie in een SCADA/ICS systeem in twijfel getrokken wordt[6].
- **Internet of Things (IoT) toepassingen** om veilig om te gaan met IoT apparatuur en netwerken. Deze apparatuur is veelal niet in staat om met sterke cryptografische protocollen om te gaan, concreet zou hier 'lichtgewicht' cryptografie voor ontwikkelt moeten worden.

DATA AT REST

- **Gegevensdragers** waarmee data veilig verplaatst kan worden klinkt als een opgelost probleem. Echter, het is momenteel niet mogelijk om gegevensdragers als USB-sticks in te zetten om data op hoog-gerubriceerd niveau te verplaatsen. Dit is ook niet een triviaal probleem, aangezien een onderschepte USB stick op veel manieren aan te vallen is. Een veilige gegevensdrager moet hiertegen bestendig zijn.
- **Cloudopslag** waarmee data veilig in de cloud opgeslagen kan worden. In het normale leven is data opslaan in de cloud geen enkel probleem. Dit veranderd wanneer de opgeslagen data gerubriceerd is, aangezien de grote cloudproviders buitenlandse bedrijven zijn. TNO heeft een rapport gepubliceerd die hier handvatten voor aanbied, zoals het lokaal versleutelen van het bestand of een nieuwe vertrouwde clouddienst gebruiken[7].

DATA IN USE

- **Werkplekken** waarmee veilig thuis of op verschillende locaties gewerkt kan worden zijn schaars. Op laag-gerubriceerd niveau is een thuiswerkplek mogelijk met inperking van de functionaliteit van de geïnstalleerde software. Echter, op hoog-gerubriceerd niveau is dit zeker niet mogelijk. Concreet betekent dit het ontwikkelen van werkplekken met minder connectiviteit in de geïnstalleerde software, veilige interne opslagmedia en een veilige verbinding naar buiten.
- **Videobellen** als logische opvolger van veilige telecommunicatie. De corona-crisis heeft duidelijk gemaakt hoe belangrijk videobellen is. De veiligheid van video-bel applicaties hangt af van de onderliggende dienstverlening. Voor laag-gerubriceerd domein zijn er oplossingen beschikbaar, maar voor hoog-gerubriceerd niveau zal deze ontwikkeling nog moeten komen.

OVERIG

- **Hardware acceleratie** kan voor intensivering van cryptografie zorgen. De hiervoor specifiek ontworpen processoren versnellen het versleutelen waardoor cryptografisch zware processen mogelijk worden. Deze processoren zijn al op grote schaal beschikbaar, maar het is voor nu onduidelijk in hoeverre kennis met betrekking tot hardware acceleratie voor cryptografie in Nederland aanwezig is.
- **Identiteit, authenticatie en key management systemen** vormen de basis van de cryptografische oplossingen. Specifiek dienen deze oplossingen ruimte te bieden voor het granulair verlenen van toegang tot digitale diensten. Zeker in het geval van koppelstukken tussen netwerken van verschillend rubriceringsniveau is goede administratie van de identiteit, rol en bijbehorende sleutels van de gebruiker van cruciaal belang.

6. *https://ieeexplore.ieee.org/document/8340732*
7. *TNO-rapport "Verdieping Valorisatieketens: Basis voor de routekaart 'Veilig werken in een onveilige cloud'"*

De meeste voorbeelden zijn in principe oplosbaar met gangbare unilaterale cryptografische technieken. Daardoor hoeft er nog weinig fundamentele kennis opgebouwd worden om deze toepassingen te realiseren. Wél moet er geïnvesteerd worden in de implementatie fase van de ontwikkeling, immers vereisen deze oplossingen meer dan alleen zuivere cryptografie. Om de toepassingen op hoog-gerubriceerd domein van toepassing te laten zijn zal de ontwikkeling aan strikte eisen moeten voldoen en bovendien controleerbaar dienen te zijn.

De voorbeelden beslaan een zeer divers pallet aan productcategorieën, waardoor dit thema enigszins groter uitpakt dan de andere thema's. Echter, juist vanwege die breedte is dit thema van grote impact op de samenleving. Een algeheel verhoogd veiligheidsniveau is van grote waarde voor de strategische autonomie van Nederland en is bovendien realiseerbaar op de (relatief) korte termijn.

5.2 MIGRATIE NAAR POST-QUANTUM CRYPTOGRAFIE

De grootste bedreiging voor veel van de op dit moment gebruikte asymmetrische cryptografie is de ontwikkeling van de quantumcomputer. Quantumcomputers met voldoende rekenkracht zijn in staat om de wiskundige fundering van veelgebruikte asymmetrische cryptografie te breken. Mogelijk al rond 2035 is de kans groot dat quantumcomputers krachtig genoeg zullen zijn om een gevaar te vormen voor de cryptografie[8].

Het gevolg hiervan is dat van alle asymmetrisch versleutelde informatie de vertrouwelijkheid kwijt is, inclusief van alle sleutels asymmetrisch uitgewisseld zijn. Zodoende komt ook de vertrouwelijkheid van alle informatie die met deze sleutels zijn versleuteld in gevaar. Voor statelijke actoren is het mogelijk en relatief goedkoop om alle versleutelde informatie van vandaag op te vangen, op te slaan en te wachten totdat deze te ontsleutelen is met behulp van de quantumcomputer. Door deze *store now, decrypt later* aanpak is geheimhouding voor 15+ jaar zo goed als onmogelijk.

Er zijn meerdere opties om quantum-onveilige cryptografie te vervangen door quantum veilige cryptografie. De mogelijkheid van een quantum gebaseerd communicatienetwerk wordt onderzocht en concreet wordt er gekeken naar *quantum key distribution*. Hiermee kan, gebruikmakend van quantumeffecten, er tussen twee partijen een sleutel afgesproken worden. Deze sleutel kan vervolgens gebruikt worden om data symmetrisch mee te versleutelen. Hoewel dit een veelbelovende technologie is, zal de ontwikkeling ervan niet op tijd komen om te beschermen tegen het *store now, decrypt later* scenario. Verder is er voor deze technologie een geheel nieuwe infrastructuur nodig en kan deze technologie niet alle aspecten van de asymmetrische cryptografie afdekken. Een andere oplossingsrichting is om enkel symmetrische cryptografie te gebruiken, zoals gebruikelijk was voordat asymmetrische cryptografie werd geïntroduceerd.

Een oplossingsrichting met een kortere terugverdientijd is het migreren naar post-quantum cryptografie. Dit is cryptografie die bestendig is tegen aanvallen met quantumcomputers en niet gebaseerd is op quantum mechanica maar op wiskundige protocollen—net als de cryptografie die we gewend zijn te gebruiken. Het gaat dan om wiskundige problemen die ook voor de quantumcomputer moeilijk op te lossen zijn. Hier wordt al decennia onderzoek naar gedaan. Nederland speelt hierin een internationaal leidende rol en heeft zeer veel ervaring met post-quantum cryptografie.

Momenteel loopt een wereldwijd standaardisatieproces van post-quantum cryptografie[9]. Voorstellen waarin de Nederlandse kennisinstellingen centraal betrokken zijn doen hierin mee. Dit standaardisatieproces gaat een aantal methodes aanwijzen waarmee de functionaliteit van asymmetrische cryptografie vermoedelijk gewaarborgd kan worden. Deze vermoedens zijn gebaseerd op de decennia aan academisch werk dat is verricht naar de veiligheid van post-quantum cryptografie.

8. *TNO position paper "Migration to quantum-safe cryptography: about making decisions on when, what and how to migrate to a quantum-safe situation"*

9. *https://csrc.nist.gov/projects/post-quantum-cryptography*

De voorstellen die uit het standaardisatieproces komen zullen op een zekere manier hun weg moeten vinden naar eindproducten. Het is aannemelijk dat er hybride cryptosystemen komen waarbij post-quantum cryptografie gecombineerd wordt met bestaande asymmetrische cryptografie. Hierdoor is er ruimte voor verdere cryptanalyse[10] en side-channel analyse van de post-quantum methodes in de praktijk. Deze analyses kan er bijvoorbeeld toe leiden dat de sleutel-lengtes aangepast worden.

De transitie naar post-quantum cryptografie zal niet vanzelf gaan; de gehele Nederlandse valorisatieketen zal hierop actie moeten ondernemen. In zekere mate kan dit parallel: terwijl de wetenschap zich stort op de ontwikkeling van post-quantum cryptografie, kan de industrie zich nu al richten op de crypto-agility van de eindproducten, zodat de migratie in de toekomst makkelijker plaats kan vinden.

5.3 INZET VAN CRYPTOGRAFIE VOOR NIEUWE DECENTRALE TOEPASSINGEN

De ontwikkeling van multilaterale cryptografie biedt nieuwe mogelijkheden buiten de veelgebruikte unilaterale cryptografie: veilig berekeningen uitvoeren in afwezigheid van wederzijds vertrouwen met behoud van geheimhouding van de individuele input. In feite vindt er decentralisatie plaats: de controle over data komt te liggen bij de gebruiker in plaats van in een gecentraliseerde cloud-omgeving. Deze decentralisatie wordt vanuit de technologie gepusht. De kansen die deze ontwikkeling biedt voor het bedrijfsleven en de overheid zijn nog onbekend.

In de praktijk staan de toepassingen van multilaterale cryptografie voor de deur. In de komende jaren gaat er ontdekt worden wat de mogelijkheden en toepassingen van multilaterale cryptografie in de praktijk gaat zijn. Op internationaal niveau experimenteert het bedrijfsleven volop met deze technieken[11] en ook in Nederland worden toepassingen onderzocht van *secure multi-party computation*, *secure sovereign identity*, en *zero-knowledge proofs*. Onze verwachting is dat er in Nederland op korte termijn in verschillende domeinen toepassingen van decentrale technieken op de markt zullen verschijnen.

Een concreet voorbeeld van decentralisatie is data uitwisseling in de zorg[12]. Alle medische data is zeer vertrouwelijk en persoonlijk. De data is echter wel waardevol en kan bijdragen aan het onderzoeken van allerlei ziekten. Via decentralisatie beschikken patiënten zelf over hun data en kunnen zij bepalen welke data zij wel of niet delen met onderzoekers. Bovendien, doordat patiënten zelf over hun decentrale data beschikken, kan de data gedeeld worden ongeacht welke zorginstelling die data normaliter zou opslaan. Hierdoor kan data die over meerdere zorginstellingen vergaard is op een privacy vriendelijke manier geanalyseerd worden en hoeven er geen databases integraal aan elkaar gekoppeld te worden. Decentralisatie brengt zo, op een verantwoorde manier, nieuwe kansen en mogelijkheden.

Decentralisatie is een technologische ontwikkeling met impact ook op de langere termijn, daarom is het van cruciaal belang dat decentralisatie veilig blijft voor bekende toekomstige dreigingen zoals quantumcomputers. Er is veel ontwikkeling gaande om deze decentralisatie mogelijk te maken met post-quantum cryptografie.

10. *Cryptanalyse behelst een wiskundige/algoritmische studie van hoeveel veiligheid (per bit sleutellengte) een cryptografisch systeem biedt.*
11. *Voorbeelden zijn: https://polkadot.network/, https://web3.foundation/ en https://dfinity.org/*
12. *https://www.tno.nl/en/tno-insights/articles/privacy-friendly-data-technology-expands-oncology-research-opportunities/*

5.4 FORMELE VERIFICATIE VAN CRYPTOGRAFIE EN CRYPTOGRAFISCHE BRONCODE

In de praktijk worden cryptografische eindproducten vertrouwd met ontzettend gevoelige informatie. Dit vertrouwen berust op het cumulatieve werk van cryptografen. Door jarenlang cryptografische methodes te onderzoeken via cryptanalyse worden alle kanten van een methode onderzocht. Met de tijd schept dit kritische onderzoek vertrouwen in de cryptografische methode. Dit is een zeer kostbaar en arbeidsintensief proces, wat voor een deel geautomatiseerd kan worden door formele verificatie.

Een vergelijkbaar probleem speelt zich af in de software: het vertrouwen van programmeurs dat hun code doet wat het zou moeten komt voort uit uitgebreid testen van de software. Een andere route is formele verificatie van de software. Dit is een techniek uit de informatica die gebruikt wordt om te bepalen of software de eigenschappen heeft die het zou moeten hebben, bijvoorbeeld dat de software geen dode-eindes heeft. Dit is een niet-triviale taak, omdat de complexiteit van software tegenwoordig zeer hoog is. Toch zijn wetenschappers erin geslaagd om zeer complexe softwarepakketten formeel te verifiëren[13].

Het is de verwachting dat ontwikkelingen in formele verificatie in toenemende mate toepasbaar zullen worden op cryptografische implementaties en veilige software in het algemeen. Op langere termijn is het de verwachting dat op alle niveaus van een cryptografisch eindproduct het in toenemende mate mogelijk wordt om menselijk vertrouwen bij te staan door formele verificatie. Op verschillende niveaus zijn voorbeelden beschikbaar van formeel geverifieerde security software, zoals operating system[14], veelgebruikte cryptografische protocollen[15] en compilers[16].

Hoewel formele verificatie veel ontwikkeling heeft doorgemaakt, behoeft de toepassing op cryptografie nog fundamenteel onderzoek. Specifiek richt de wetenschap zich nu tot:
- Verificatie van het cryptografisch protocol, waarbij wordt gekeken of het protocol inderdaad voldoet aan bepaalde veiligheidsclaims.
- Verificatie van de software implementatie, waarbij wordt gekeken of de implementatie inderdaad aansluit op het protocol, dat daarin geen fouten zijn gemaakt, en de implementatie geen mogelijke side-channels bevat.

Het inzetten van formele verificatie zou de mogelijkheid kunnen scheppen om open-source cryptografie van extra zekerheid te voorzien. Dit maakt het mogelijk om meer gebruik te maken van verschillende open-source implementaties, en daardoor aanvullende hoogkwalitatieve alternatieven bieden voor (internationale) bedrijfsontwikkelde software. Bovendien speelt formele verificatie een belangrijke rol bij het controleren van bedrijfsontwikkelde software, die veelal zodanig complex is dat een door mensen uitgevoerde verificatie slechts beperkt mogelijk is.

De belofte van formele verificatie van cryptografie is enorm en biedt grote kansen voor Nederland. Doordat er nog veel fundamenteel onderzoek nodig is, zal de echte waarde van formele verificatie van cryptografie op langere termijn tot uiting komen.

13. *MIT 6.822, Spring 2021*
14. *Zoals seL4, een formeel geverifieerd operating system.*
15. *Zoals miTLS, een formeel geverifieerde TLS implementatie uit Microsoft Research's Project Everest.*
16. *CS 6120: CompCert: Formally Verified C Compiler (cornell.edu)*

6. CONCLUSIE

Cryptografie staat aan de basis van de digitale veiligheid en is belangrijk voor de strategische autonomie van Nederland. Het cryptografie landschap is constant in beweging, waardoor nieuwe dreigingen én kansen zich continue presenteren. Nederland heeft een sterk ecosysteem op het gebied van cryptografie en bevind zich daarmee in een goede positie om op deze dreigingen en kansen in te spelen.

Nieuw in deze verkenning zijn de vier grote ontwikkelingen in de cryptografie, met bijbehorende bedreigingen en kansen voor Nederland. Ten eerste biedt op korte termijn het beveiligen van nieuwe technische omgevingen ruimte voor nieuwe productontwikkeling. Ten tweede vereist de migratie naar post-quantum cryptografie nu al grote flexibiliteit van de gehele valorisatieketen. Ten derde biedt de inzet van cryptografie voor nieuwe decentrale toepassingen nieuwe economische kansen. Ten vierde biedt in de toekomst formele verificatie van cryptografie nieuwe mogelijkheden voor de ontwikkeling van cryptografie, omdat deze techniek het vertrouwen in de gebruikte cryptografie zal vergroten.

In de beschreven ontwikkelingen liggen zowel kansen als uitdagingen. Decentralisatie bied op de korte termijn nieuwe economische kansen, net zoals formele verificatie op de langere termijn. Het is hierbij wel van belang te blijven investeren in kennis en ontwikkeling zodat deze economische kansen ook benut worden.

Het zullen grote uitdagingen worden om de dreiging van quantumcomputers en nieuwe digitale omgevingen te mitigeren. Het is gevaarlijk te onderschatten hoe groot deze dreigingen zijn en er is geen enkele partij die zelfstandig alle oplossingen kan bewerkstelligen. Sterke samenwerking in de gehele valorisatieketen is daarom het uitgangspunt.

De Nederlandse uitgangspositie is goed om de toekomstige kansen te benutten en bedreigingen te mitigeren. Wel is het zo dat expertise rondom cryptografie en zeker de implementatie daarvan zeer schaars is. Aanvullende investeringen zijn daarom nodig om voldoende kennis en capaciteit op te bouwen. Onze concrete aanbevelingen voor het richten van deze investeringen zijn als volgt:

1. Breng in kaart welke:
    a. spelers actief zijn in het Nederlands bedrijfsleven, zowel aanbieder als afnemer. Hoofdstuk 4 geeft hiervoor een eerste aanzet.
    b. hindernissen het bedrijfsleven ondervind in het op de markt brengen van een nieuw cryptografisch eindproduct. Denk hierbij aan de tijd die het kost om een cryptografisch eindproduct te laten evalueren, het bijbehorende risico en de schaarste van personeel.
    c. hindernissen nieuwe bedrijven ondervinden om toe te treden tot de markt. Denk hierbij aan de strikte veiligheidseisen waaraan een nieuw bedrijf moet voldoen.
2. Welke rol de overheid kan innemen om de hindernissen weg te nemen.

Deze punten zullen worden opgenomen in de Routekaart Cryptocommunicatie van het Ministerie van Economische Zaken en Klimaat.

7. ROUTEKAART CRYPTOCOMMUNICATIE

Gegeven de complexiteit van de ontwikkelingen en de uitdagingen waarvoor de valorisatieketen staat is het tijd om als ecosysteem samen een realisatieroute uit te werken. Als auteurs willen we u, de lezer, via deze verkenning uitnodigen tot samenwerking aan de Routekaart Cryptocommunicatie van het Ministerie van Economische Zaken en Klimaat. In deze routekaart zullen de behoeftes, uitdagingen en mogelijkheden van het ecosysteem in kaart worden gebracht. De plannen opgesteld in de routekaart zullen de eerste aanzet tot strategische investeringen in cryptografie vormen.

Het proces om te komen tot een gedragen routekaart start mei 2021 en is gebaat bij uw deelname. Middels interviews en co-creatie sessies zal er invulling gegeven worden aan de routekaart. De onderwerpen besproken in deze verkenning vormen een eerste aanzet tot de onderwerpen die in de routekaart tot uiting zullen komen. Uw input en deelname bij het vormgeven van de routekaart is van harte welkom. Zo kunnen we gezamenlijk toewerken tot Nederland Cryptoland.

Contact Routekaart:
Samenwerkingsplatform dcypher:
https://dcypher.nl/cms/view/5a12a72d-097e-473c-aa84-a428543ea2b3/contact-us