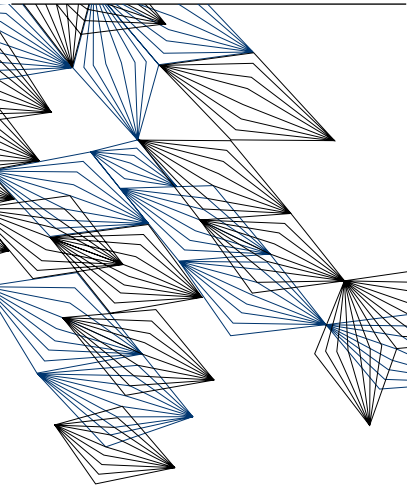
INAUGURELE REDE
19 OKTOBER, 2023



HET ONTSLUITEN VAN DE FASCINERENDE GEHEIMEN VAN CRYPTOGRAFIE

UNLOCKING THE FASCINATING SECRETS OF CRYPTOGRAPHY

PROF. DR. IR. THIJS VEUGEN

UNIVERSITY OF TWENTE.

PROF. DR. IR. THIJS VEUGEN

HET ONTSLUITEN VAN DE FASCINERENDE GEHEIMEN VAN CRYPTOGRAFIE

UNLOCKING THE FASCINATING SECRETS OF CRYPTOGRAPHY

INAUGURELE REDE PROF. DR. IR. THIJS VEUGEN

COLOPHON
Prof. Dr. Ir. Thijs Veugen

October 2023

De tekst van deze inaugurale rede is zowel beschikbaar in Nederlands als in Engels.
The text of this inaugural lecture is available in both Dutch and English.

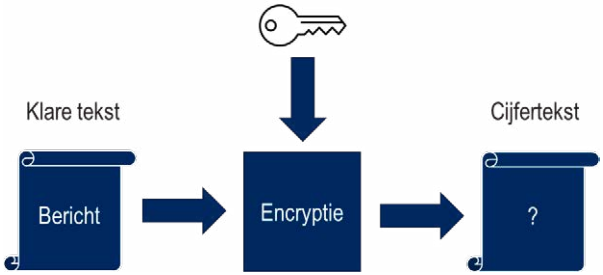
INHOUD

CONTENT

HET ONTSLUITEN VAN DE FASCINERENDE GEHEIMEN VAN CRYPTOGRAFIE

Geachte rector magnificus, beste familieleden, vrienden en collega's, van harte welkom. Fijn dat jullie de moeite hebben genomen, vaak na een lange reis, om hierbij aanwezig te zijn. En natuurlijk ook welkom aan de online toehoorders die meeluisteren.

Ik ga jullie vandaag de geheimen van cryptografie laten zien. Dit voortdurend vernieuwende vakgebied heeft steeds meer impact op onze samenleving. Aangezien mijn leerstoel Toegepaste Cryptografie betreft, ga ik jullie vooral laten zien welke mooie toepassingen je met cryptografie kunt maken. Ter afsluiting zal ik jullie meenemen langs mijn persoonlijke reis richting het hoogleraarschap.

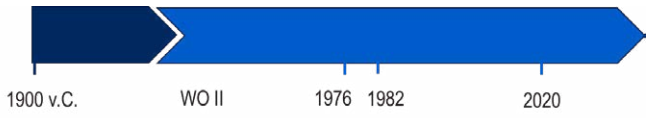


Figuur 1: Wat is encryptie?

Cryptografie betekent letterlijk 'geheimschrijven'. De naam komt uit het Grieks: 'crypto' betekent 'geheim' en 'grafie' is 'schrijven'. Tegenwoordig wordt met crypto vaak de digitale valuta bedoeld die je met cryptografische technieken kunt maken, maar cryptografie is veel meer dan dat.

Geheimschrijven doe je met een sleutel (zie Figuur 1). Die sleutel vertelt hoe je van een bericht een geheimschrift kunt maken. Dat proces heet encryptie of vercijfering. Het geheimschrift wordt doorgaans cijfertekst genoemd: het is geen leesbare tekst meer en bestaat vaak alleen uit cijfers. Alleen als je de sleutel weet kun je een cijfertekst ontcijferen om de originele leesbare tekst, de klare tekst, te lezen.

Ik zal in vogelvlucht het ontstaan van het vakgebied schetsen en de ontwikkelingen ervan tot aan de Tweede Wereldoorlog: het donkerblauwe deel van de tijdlijn in Figuur 2. Daarna beschrijf ik in chronologische volgorde drie revolutionaire ontwikkelingen die het vakgebied de laatste decennia heeft doorgemaakt en de mooie toepassingen die hieruit zijn ontstaan, elk corresponderend met een jaartal in het lichtblauwe deel van de tijdlijn in Figuur 2.

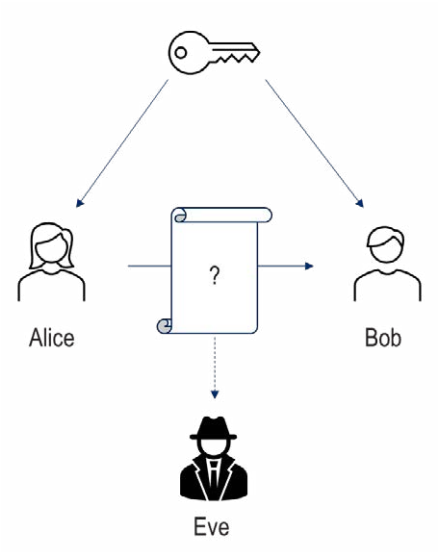


Figuur 2: Tijdlijn

Om een tipje van de sluier op te lichten: we zullen via het schrijven van geheimen naar het rekenen met geheimen gaan. Vervolgens zal ik mijn visie geven op de inhoudelijke uitdagingen de komende jaren en wat voor moois we allemaal nog van cryptografie kunnen verwachten.

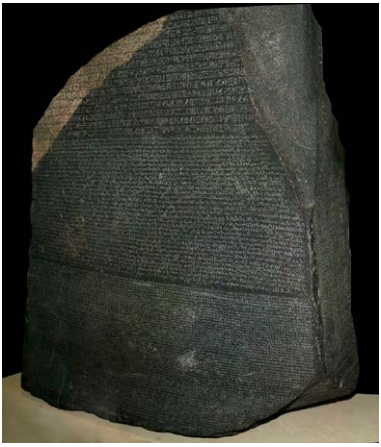
KLASSIEKE CRYPTOGRAFIE

Dit is het moment om Alice en Bob te introduceren (zie Figuur 3). In het modelleren van cryptografie sturen we berichten van A naar B. Om het iets levendiger te maken heeft men die ooit vervangen door personen: de A van Alice en de B van Bob. En om het plaatje compleet te maken hebben we ook de kwaadaardige Eve die probeert om de geheimen van Alice en Bob te achterhalen, zonder de sleutel te kennen.



Figuur 3: Alice en Bob

Het eerste stukje van mijn verhaal gaat over het ontstaan van cryptografie rond 1900 voor Christus en de ontwikkeling ervan tot aan de Tweede Wereldoorlog. Het eerste gebruik van klassieke cryptografie is gevonden in Egyptische stenen rond 1900 voor Christus die gegraveerd waren met cijferteksten. Waarschijnlijk was dit meer een spel om geleerden te amuseren dan om echt informatie te verbergen. In Figuur 4 is de bekende steen van Rosetta te zien die in 196 voor Christus werd gemaakt en in juli 1799 werd ontdekt in Egypte. Het is een soort vertaalsteen die een relatie legt tussen het hiëroglyfisch schrift en de Egyptische taal. Het bleek een belangrijke sleutel in de ontcijfering van oude Egyptische hiërogliefen.



Figuur 4: De steen van Rosetta

We weten dat Julius Caesar in de 1e eeuw voor Christus cryptografie gebruikte om geheime berichten te versturen. Hij deed dat door alle letters een vast aantal posities in het alfabet te verschuiven, zie Figuur 5. De “A” wordt een “D”, de “B” wordt een “E”, etc. De cryptografische sleutel in dit systeem is deze substitutietabel.

Klaar	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cijfer	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Bericht	V	E	N	I	V	I	D	I	V	I	C	I
Encryptie	Y	H	Q	L	Y	L	G	L	Y	L	F	L

Caesar

Figuur 5: Caesarcijfer

Stel bijvoorbeeld dat Caesar het bekende bericht “Veni, vidi, vici” zou willen vercijferen. Dan zoekt hij de letter “V” op in de tabel en ziet dat dat een “Y” wordt. De volgende letter “E” wordt een “H”, etc. Om van de encryptie terug te gaan naar het bericht kun je dezelfde tabel gebruiken. Als de sleutel voor encryptie (vercijferen) en decryptie (ontcijferen) hetzelfde is, noemen we dat een symmetrisch encryptiesysteem.

In het voorbeeld kun je zien dat er aardig wat structuur van het bericht doorsijpelt naar de cijfertekst, zoals bijvoorbeeld het om de twee posities

voorkomen van de letter “L” (dat is de “I” in het originele bericht). Dit soort structuur maakt het voor een kwaadwillende, onze Eve, gemakkelijker om de originele tekst te achterhalen zonder de tabel te kennen.

In de loop van de geschiedenis werden de encryptiesystemen gelukkig beter. In een overzicht van cryptografie kan het Enigma-apparaat uit Figuur 6 niet ontbreken: een ingewikkeld apparaat met allerlei rotoren waarmee de Duitsers in de Tweede Wereldoorlog hun militaire geheimen communiceerden.

Figuur 6: Enigma-apparaat

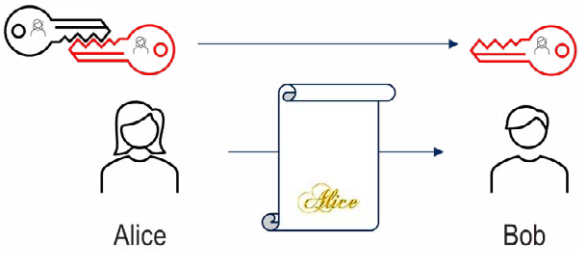
Het kraken van de Enigma-codering in Bletchley Park onder leiding van Alan Turing heeft mede geleid tot de ontwikkeling van de eerste elektronische computer die nu niet meer is weg te denken uit onze samenleving. Samen met de in die tijd niet geaccepteerde homoseksualiteit van de hoofdrolspeler bleek dit stukje geschiedenis een goede basis voor gedramatiseerde verfilming, zoals bijvoorbeeld het vermakelijke “The Imitation Game”[1]. Een ander populair voorbeeld van cryptografie is het boek “De Da Vinci code” waar schrijver Dan Brown de Cryptex verzon.

Na dit korte overzicht van de geschiedenis van cryptografie wordt het tijd om jullie kennis te laten met de eerste revolutionaire ontwikkeling van de laatste 50 jaar.

[1] https://www.imdb.com/title/tt2084970/

ASYMMETRISCHE CRYPTOGRAFIE

Het cijfer van Caesar en de Enigma zijn voorbeelden van symmetrische encryptie: de sleutel om een bericht te vercijferen is dezelfde als de sleutel waarmee je het bericht weer kunt terughalen. In het geval van Caesar is dat de tabel waarmee je elke letter kunt vercijferen dan wel ontcijferen.



Figuur 7: Asymmetrische cryptografie

Sinds 1976 bestaat er ook asymmetrische encryptie [1]. Alice maakt in dat geval twee verschillende sleutels: een zwarte en een rode sleutel (Figuur 7) die onlosmakelijk met elkaar zijn verbonden. Ze houdt een van de twee sleutels voor zichzelf (in dit geval de zwarte), en geeft de andere sleutel, de rode, aan Bob. Alice gebruikt de zwarte sleutel om het bericht te vercijferen en Bob gebruikt de rode om het bericht te ontcijferen.

Omdat Alice de enige persoon is die de zwarte sleutel kent, is die vercijfering vergelijkbaar met een digitale handtekening op dat bericht: niemand anders kan deze cijfertekst (lees: handtekening) maken. Bob kan met de rode sleutel controleren of de handtekening echt is: is de handtekening daadwerkelijk een versleuteling van het bijgevoegde bericht? Zo ja, dan moet Alice degene zijn die deze handtekening heeft gemaakt, want zij is de enige die de zwarte sleutel kent.

Waar het op neerkomt is dat er met de komst van asymmetrische encryptie conceptueel een volledig nieuwe functie met cryptografie is bewerkstelligd. In plaats van het beschermen van de vertrouwelijkheid van een bericht (ervoor zorgen dat niemand kan meelezen), kunnen we nu de onweerlegbaarheid van een bericht garanderen: als Alice een digitale handtekening zet op een bericht kan ze dat later niet meer ontkennen.

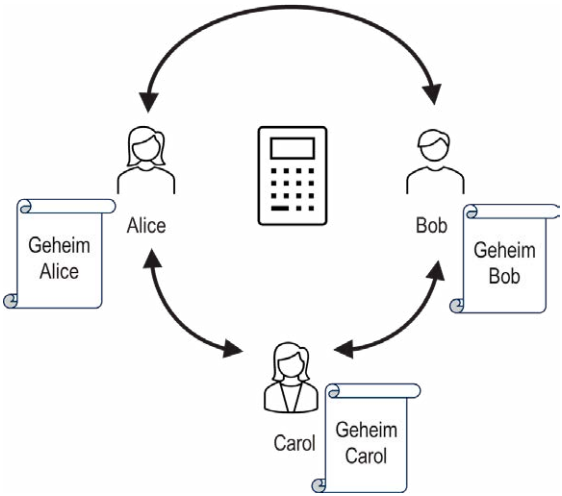
Dat opent een hele nieuwe wereld van toepassingen en vormt de veilige basis van de huidige elektronische wereld van transacties:

1. Inmiddels is er wetgeving om te garanderen dat digitale handtekeningen een rechtsgeldigheid hebben vergelijkbaar met geschreven handtekeningen. Zo kun je elektronisch berichten tekenen waar mensen je later op aan kunnen spreken.
2. Asymmetrische cryptografie heeft geleid tot elektronisch zakendoen en internetbankieren: een internet dat veilig genoeg is om digitale transacties te verrichten en elektronisch te betalen.
3. Als je met symmetrische cryptografie een berichtensysteem zoals Whatsapp zou willen opzetten, moet je zorgen dat elk paar gebruikers een geheime symmetrische sleutel met elkaar deelt. Hoe ga je dat voor elkaar krijgen als iedereen mee kan luisteren over internet? Ook dat wordt mogelijk gemaakt door asymmetrische cryptografie met een speciaal sleuteluitwisselingsprotocol [1].
4. En als laatste digitaal geld. In 1991 had ik het genoegen om mijn afstudeeronderzoek te doen bij het Centrum Wiskunde & Informatica in Amsterdam, onder begeleiding van David Chaum [2,3,4]. Deze Amerikaanse pionier heeft de moderne cryptografie naar Europa gebracht en was toen al bezig om digitaal geld te maken met behulp van cryptografie [5]. In zijn systeem kon de bank een digitale handtekening zetten op een speciaal gevormd lang getal. Zo kreeg je bijvoorbeeld een gulden die je vervolgens bij een winkel kon uitgeven. Het systeem was zo opgezet dat de bank niet kon achterhalen waar je je geld aan besteedde. Helaas was hij zijn tijd te ver vooruit en is het systeem nooit in de praktijk gebruikt. Hoe anders was het toen jaren later de verschillende cryptocoins ontstonden, gebaseerd op een ander concept buiten het beheer van banken om.

Het wordt tijd om jullie kennis te laten maken met de volgende recente wetenschappelijke ontdekking in de cryptografie. Een ontdekking die de deuren opent naar een hele nieuwe wereld van toepassingen: secure multi-party computation.

VEILIG REKENEN MET GEHEIMEN

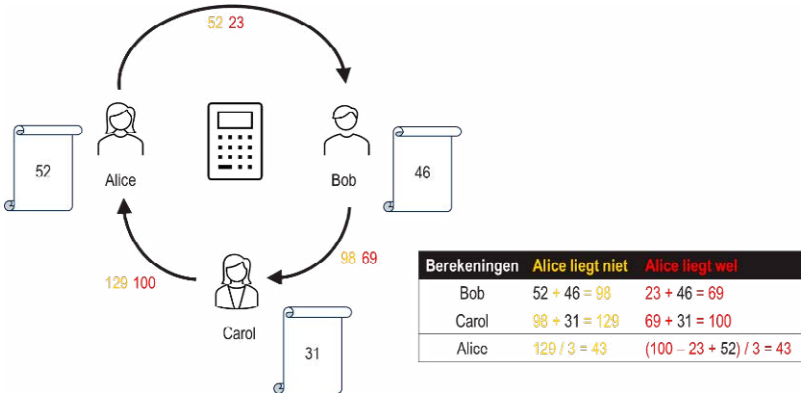
Na het ontstaan van asymmetrische cryptografie is dit de tweede revolutionaire ontwikkeling die de afgelopen decennia binnen cryptografie heeft plaatsgevonden. Alice en Bob hebben een vriend gekregen: Carol. Ze weten inmiddels hoe ze met symmetrische en asymmetrische cryptografie hun geheim kunnen communiceren. Nu willen ze gaan rekenen met hun geheimen zonder ze te communiceren.



Figuur 8: Secure multi-party computation

Dit deelgebied van cryptografie is ontstaan in 1982 [6] en heet "secure multi-party computation", oftewel veilig rekenen met meerdere partijen, en wordt vaak afgekort tot MPC. In Figuur 8 zien jullie drie partijen die elk hun eigen geheime informatie hebben. Ze willen samen iets uitrekenen met hun geheimen, gesymboliseerd door de rekenmachine in het midden, zónder dat ze elkaars geheimen te weten komen.

Ik zal met een voorbeeld uitleggen hoe dat er in de praktijk uitziet. Dit voorbeeld kent drie partijen, namelijk Alice, Bob en Carol. De zwarte getallen die je in Figuur 9 ziet zijn hun leeftijden. Ze zijn benieuwd wat hun gemiddelde leeftijd is, maar willen elkaar niet hun leeftijd verklappen. Hoe gaan we dat voor elkaar krijgen?



Figuur 9: Veilig uitrekenen van de gemiddelde leeftijd

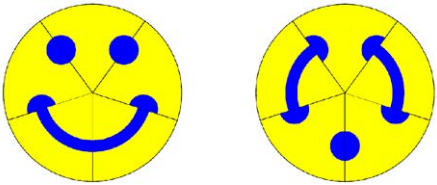
In een naïeve eerste poging, geïllustreerd door de gele getallen in Figuur 9, zou je kunnen zeggen dat Alice haar leeftijd (52) opstuurt naar Bob. Bob telt zijn eigen leeftijd (46) erbij op en geeft de som door aan Carol. Carol telt haar leeftijd (31) bij de som en geeft het totaal aan Alice. Alice deelt het totaal (129) door drie en ze leert de gemiddelde leeftijd (43). Zo'n serie van communicatiestappen noemen we een protocol. Hoewel de uitkomst correct is, zal de oplettende lezer hebben gezien dat dit protocol niet veilig is. Al in stap 1 gaat het mis, want Alice vertelt haar leeftijd aan Bob, en dat was juist niet de bedoeling.

De oplossing lijkt eenvoudig. Om te voorkomen dat Bob de echte leeftijd van Alice leert laten we Alice in de eerste stap liegen over haar leeftijd, geïllustreerd door de rode getallen in Figuur 9. In plaats van haar echte leeftijd (52) geeft ze aan Bob het getal 23. Bob zal haar wellicht een beetje raar aankijken, maar telt braaf zijn eigen leeftijd (46) erbij op en stuurt de som weer naar Carol. Carol weet dat 69 de som is van een gelogen leeftijd van Alice en een eerlijke leeftijd van Bob, maar heeft geen idee wat de afzonderlijke termen zijn. Net als de vorige keer telt Carol haar leeftijd (31) erbij op en stuurt het totaal naar Alice. Het enige dat nog resteert is dat Alice de door haar gelogen leeftijd vervangt door haar echte leeftijd en het nieuwe totaal door drie deelt.

Het nieuwe protocol geeft weer dezelfde correcte uitkomst en is bovendien

veilig: niemand komt de leeftijd van de ander te weten. We hebben nu een mooie oplossing bedacht om de gemiddelde leeftijd uit te rekenen zonder de verschillende leeftijden te onthullen. Dit lijkt een leuk theoretisch speeltje, maar wat als we de drie personen zouden vervangen door drie concurrerende bedrijven? En in plaats van leeftijden zouden rekenen met gevoelige bedrijfsmatige gegevens zoals omzet of de effectiviteit van producten? Dan hebben we ineens een manier om een norm te bepalen van bedrijfsprestaties in een bepaalde branche, waar bedrijven zich aan kunnen meten zonder dat ze concurrentiegevoelige data hoeven te delen.

Deze nieuwe vorm van cryptografie met meerdere partijen leidt tot allerlei verrassende toepassingen. Kijk eens naar een filmpje van een dating show waarbij je zonder schaamte het speelveld kunt verlaten als er geen match blijkt te zijn[2]. In het filmpje zie je een smiley puzzel die alleen lacht als er een match, zie Figuur 10. Het publiek van de dating show krijgt alleen te weten of er een match is of niet en de “nee” zeggers leren niet of de ander misschien toch warme gevoelens voor hun had. Ik heb de puzzel meegenomen naar de oratie om uit te proberen, maar er is ook een variant met speelkaarten om thuis te proberen[3].



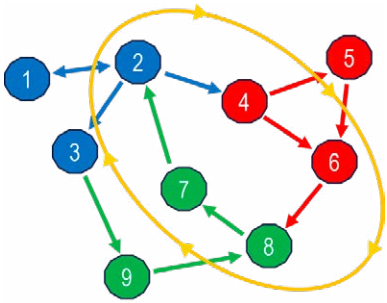
Figuur 10: Dating game

We hebben gezien hoe je veilig getallen kunt optellen met drie partijen. De afgelopen jaren zijn er veel wetenschappelijke ontwikkelingen geweest waardoor we nu op een veilige en redelijk snelle manier willekeurige berekeningen kunnen uitvoeren met een willekeurig aantal partijen, zonder individuele geheimen prijs te geven [7, 8]. Ik zal laten zien dat je hier vele mooie toepassingen mee kunt maken. We beginnen met het detecteren van financiële fraude en het bestrijden van armoede.

---

[2] https://vimeo.com/294584796
[3] https://www.win.tue.nl/~wstomv/misc/ZeroKnowledgeMatchMaker

Financiële fraude kost de samenleving veel geld. In Nederland gaat naar schatting jaarlijks voor 16 miljard euro aan zwart geld rond[4]. Het is erg lastig om dit soort illegale geldstromen te vinden. De huidige pakkans is slechts 0,083%[5]. In Figuur 11 zien jullie een klein financieel transactienetwerk. De bolletjes zijn bankrekeningen en de pijltjes zijn transacties. Bijvoorbeeld de pijl van bol 2 naar bol 4 betekent dat in een bepaalde tijdperiode geld is overgemaakt van bankrekening nummer 2 naar bankrekening nummer 4.



Figuur 11: Detecteren van witwasfraude

Een manier van witwassen is om illegaal verdiend geld rond te pompen langs verschillende rekeningen totdat het niet meer te traceren is en daarmee voor de buitenwereld wit is geworden zodat het legaal kan worden uitgegeven. Dat betekent dat je moet gaan zoeken naar verdachte geldstromen zoals de gele cirkel in Figuur 11: hier gaat geld van bol 2 via 4, 6, 8 en 7 weer terug naar 2. Het probleem is echter dat niet alle bolletjes van dezelfde bank zijn. Geld wordt niet witgewassen binnen één bank, maar via meerdere banken. In dit voorbeeld bestaat het netwerk eigenlijk uit drie banken, elk met hun eigen kleur (blauw, rood en groen), met aan elkaar geknoopte transactienetwerken. Om commerciële en juridische redenen mogen de banken hun transactienetwerken niet delen.

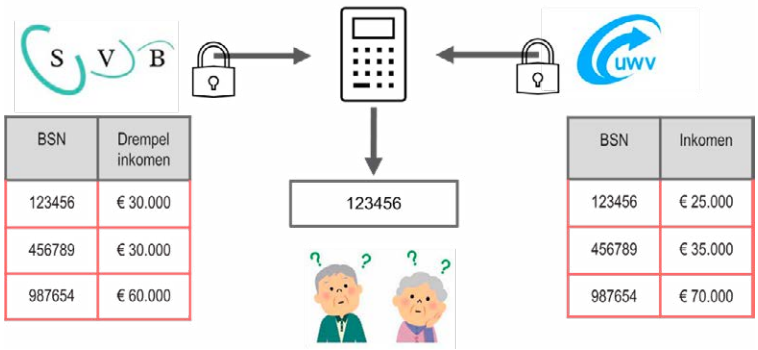
Om in dit soort gevallen toch nader onderzoek te kunnen doen naar geldstromen, is secure multi-party computation (MPC) de ideale techniek.

---

[4] https://www.uu.nl/nieuws/jaarlijks-16-miljard-euro-witgewassen-in-nederland
[5] https://www.groene.nl/artikel/pakkans-0-083-procent

Met behulp van MPC is het mogelijk om te zoeken in het volledige transactienetwerk zonder de drie afzonderlijke netwerken met elkaar te delen, en zo uiteindelijk de verdachte cirkels te vinden [6]. Ik vind het zelf een van de mooiste toepassingen van MPC. Een kleine verbetering van het detectiepercentage kan er al toe leiden dat veel geld bespaard wordt. Er is niet alleen geld te verdienen met MPC, het helpt ook om ervoor te zorgen dat toelagen adequaat worden toegekend. Een voorbeeld daarvan is onderstaande oplossing die we bij TNO voor UWV en SVB gemaakt hebben.

Er bestaat een regeling waarmee ouderen een aanvulling op hun AOW kunnen krijgen als hun inkomen onder een bepaalde drempel blijft. Daar blijkt weinig gebruik van te worden gemaakt. De overheid wil graag weten waarom, maar weet niet om welke mensen het gaat. Dat komt omdat de informatie uit twee verschillende databases moet komen die worden beheerd door verschillende organisaties, die de data niet mogen delen om privacyredenen. De Sociale VerzekeringsBank (SVB) (Figuur 12) weet welke mensen, geïdentificeerd door hun BurgerServiceNummer, AOW krijgen en wat hun drempel inkomen is; het Uitvoeringsinstituut WerknemersVerzekeringen (UWV) weet hun inkomen.

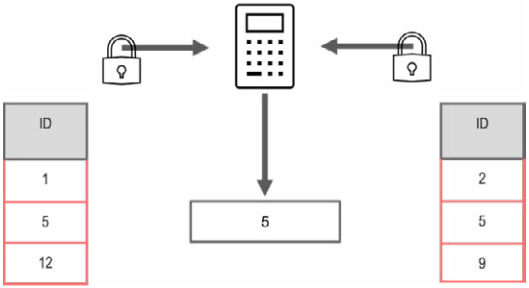


Figuur 12: Wie heeft recht op aanvullend AOW?

Alleen wanneer we op een privacyvriendelijke manier die data kunnen combineren, kunnen we bepalen wie recht heeft op de regeling. In het voorbeeld geldt dat voor de persoon met fictief BSN 123456, want dat is de enige met een inkomen onder het drempelinkomen. De informatie van alle andere AOW'ers wordt niet bekend en blijft in de lokale databases.

Wederom een mooi voorbeeld van MPC: twee partijen met data die niet gedeeld mag worden maar waar je met behulp van MPC wel mee kunt rekenen.

Een ander voorbeeld van MPC gaat over het vinden van gemeenschappelijke records van verschillende databases, zonder de databases te hoeven delen (Figuur 12). Het enige record dat in beide databases voorkomt is dat met het getal 5. Met MPC kun je dat gemeenschappelijke deel uitrekenen zonder dat je alle records hoeft uit te wisselen. De eigenaar van de linker database bijvoorbeeld leert dan niet dat de rechter database naast 5 ook de getallen 2 en 9 heeft. Beide eigenaren leren alleen dat ze het getal 5 gemeenschappelijk hebben. Dit basis principe is breed toepasbaar.



Figuur 13: Het veilig vinden van de overlap van databases

Denk bijvoorbeeld aan de situatie waarbij verschillende landen lijstjes hebben van verdachte personen. Die namen mogen niet zomaar gedeeld worden maar als er verdachten zouden zijn die in meerdere landen gezocht worden, zou dat welkome informatie zijn. Een ander voorbeeld in dezelfde categorie is het maken van aanbevelingen. Iedereen zal weleens een product gezocht hebben op internet. Google geeft je een lijstje suggesties van winkels en vervolgens ga je wel of niet in een van die winkels verder zoeken. Google komt echter niet te weten of je het product daadwerkelijk hebt gekocht door hun aanbeveling. Als die terugkoppeling wel gemaakt kon worden op een privacy-vriendelijke manier, zou dat de kwaliteit van aanbevelingen ten goede komen. Dat hoeft niet eens op individueel niveau: aggregaties per tijdsperiode per product bewerkstelligen hetzelfde effect.

Het is duidelijk dat verzekeringsmaatschappijen niet zomaar inzage kunnen krijgen in patiëntengegevens uit de gezondheidszorg. Binnen TNO hebben we twee projecten gedaan waar je met MPC die data veilig kunt combineren om de kwaliteit van leven beter te maken door betere zorg. Het eerste project uit Zuid-Limburg, samen met CBS, Zuyderland en zorgverzekeraar CZ, gaat over het bepalen van de effectiviteit van een bepaalde app. In het tweede project zoeken we, samen met ZorgTTP, Zilveren Kruis en Erasmus MC, risicofactoren voor een bepaalde groep van patiënten met hartfalen in Rotterdam [10].

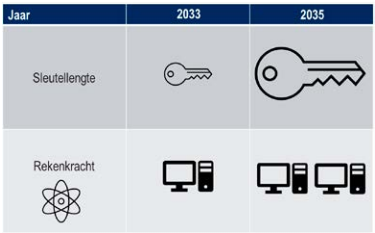
Ik zou nog een hele tijd door kunnen gaan met het noemen van toepassingen van MPC, maar het is tijd om naar de volgende ontwikkeling te gaan die de cryptografie op zijn grondvesten zal doen schudden.

DE DREIGING VAN DE KWANTUMCOMPUTER

Herinneren jullie je nog de naam Alan Turing? Hij was één van de grondleggers van de huidige computer. Zoals jullie wellicht weten wordt er momenteel hard gewerkt aan de ontwikkeling van de kwantumcomputer. Deze computer zal bepaalde berekeningen veel sneller kunnen uitvoeren dan de huidige computer. Dat schept weer kansen voor allerlei innovaties in de samenleving.

Helaas zal deze kwantumcomputer ook goed zijn in het kraken van cryptografie. Met name de berekeningen die ten grondslag liggen aan asymmetrische cryptografie liggen de kwantumcomputer goed. Hoewel de huidige kwantumcomputers nog te klein zijn, zullen ze op een gegeven moment krachtig genoeg zijn. Deze dreiging heeft nu al een revolutionair effect op het vakgebied. Collega-cryptografen zijn sinds een aantal jaren bezig met nieuwe asymmetrische systemen die bestand lijken tegen de kwantumcomputer [11].

Hoe zit dat precies? Want gewone computers worden ook elk jaar sneller. Waarom vormen die geen dreiging voor de cryptografie? Er is een wet, de wet van Moore, die de technologische vooruitgang van computers kwantificeert. Deze trend komt er grofweg op neer dat de rekenkracht van computers elke twee jaar verdubbelt. Eve heeft zo'n computer en probeert daarmee zonder kennis van de sleutel het vercijferde bericht tussen Alice en Bob te ontcijferen. Dat kan door alle sleutels één voor één te proberen en te kijken of dat een leesbaar bericht oplevert. Dat betekent dat hoe langer Alice en Bob die sleutel maken, hoe moeilijker het voor Eve wordt. Je kunt het vergelijken met het kraken van een kluis: hoe meer cijfercombinaties je moet proberen, hoe langer je bezig bent. Door de sleutel een klein beetje langer te maken, kunnen ze het ontcijferprobleem voor Eve zo moeilijk maken dat ontcijferen ondoenlijk is, zelfs wanneer Eve in de toekomst over een twee keer zo grote computer beschikt.



Figuur 14: Het probleem van de kwantumcomputer voor cryptografie

Laten we aannemen dat Eve over tien jaar een grote kwantumcomputer heeft. Het symbooltje dat je in Figuur 14 bij “Rekenkracht” ziet, stelt een atoom voor waarmee ik het kwantumeffect introduceer. Ook de kwantumcomputer zal steeds sterker worden. Alice en Bob zullen hun sleutel steeds langer moeten maken om dat effect bij te benen. Echter, de kwantumcomputer kan veel sneller alle mogelijke sleutels uitproberen dus de sleutel moet opeens een flink stuk langer worden. Dus we kunnen dezelfde cryptografische systemen blijven gebruiken, maar dat betekent dat de sleutels veel sneller moeten groeien dan we gewend zijn. Die extreem lange sleutels moeten worden gecommuniceerd en opgeslagen. Bovendien worden encryptie en decryptie hierdoor langzamer, waardoor het in de praktijk een vrijwel onwerkbaar systeem wordt. We ontkomen er dus niet aan om nieuwe cryptografische systemen te ontwikkelen die zelfs voor de kwantumcomputer te moeilijk zijn om te kraken. Die nieuwe systemen noemen we Post Quantum Cryptografie, oftewel PQC.

Eigenlijk is deze terminologie onjuist want ‘post’ is Latijn voor ‘na’, en we kunnen niet wachten tot de kwantumcomputer voldoende krachtig is, want kwaadwillenden (gesymboliseerd door onze Eve) kunnen nu vercijferde informatie opslaan en bewaren totdat de kwantumcomputer zover is. De gevolgen zullen op korte termijn merkbaar zijn bij alle personen en organisaties die werken met computers en internet. Alle computers, netwerken, etc. zullen moeten migreren naar kwantum-bestendige cryptografie. Dat is een ingewikkeld proces: je kunt niet zomaar kwetsbare cryptosystemen vervangen door veilige varianten. Zoals ik net geschetst heb, krijg je te maken met andere sleutellengten, langere encryptie- en decryptietijden en grotere cijferteksten waar onze computers en netwerken maar mee om moeten kunnen gaan.

Om te voorkomen dat onze geheimen straks op straat liggen, is het belangrijk dat organisaties hier nu al mee beginnen. In april van dit jaar overhandigden collega’s van TNO en CWI het handboek voor post-quantum cryptografie migratie [12], dat ze samen met de AIVD maakten, aan staatssecretaris Alexandra van Huffelen.

Wellicht dat het jullie inmiddels een beetje duizelt van al die sleutels, computers en wetenschappelijke doorbraken. Ik zet de genoemde geheimen van cryptografie even op een rijtje:
1. We zijn begonnen met het klassieke geheimschrijven, dat rond

de Tweede Wereldoorlog mede geleid heeft tot de komst van de elektronische computer;
2. Daarna volgde de belangrijke uitbreiding in 1976 van symmetrische naar asymmetrische cryptografie, waarmee we digitale handtekeningen konden maken, elektronische transacties konden verrichten en berichtensystemen als WhatsApp konden ontwikkelen;
3. In 1982 werd MPC ontdekt: we gingen van geheimen schrijven naar het rekenen met geheimen, en zagen de vele verrassende toepassingen die dat had;
4. Ten slotte werden we geconfronteerd met de dreiging van de kwantumcomputer en daarmee met de noodzaak voor nieuwe cryptografische systemen die die dreiging kunnen weerstaan.

DE TOEKOMST VAN CRYPTOGRAFIE

Welke geheimen heeft de cryptografie nog meer voor ons in petto de komende jaren? Ik geef jullie een overzicht van de belangrijkste uitdagingen die ik verwacht voor mijn vakgebied. Daarbij ga ik van de nabije toekomst naar de wat verdere toekomst.

1. Als eerste noem ik de groeiende behoefte aan privacybeschermende technieken. Dat is niet alleen secure multi-party computation, maar het betreft tevens daaraan gerelateerde technieken met vaktermen als federated learning, differential privacy, trusted execution environments, zero knowledge proofs en synthetic data [13,14]. Bij het grote publiek zijn die nog weinig bekend, waardoor we nieuwe kansen om data op een verantwoorde manier te verrijken nog te weinig benutten. Samen met collega's van de Universiteit Twente ga ik de komende jaren studenten hiervoor opleiden. Wat op dit moment nog ontbreekt is een goede manier om, gegeven een technische oplossing, de kwaliteit te meten van de geleverde privacybescherming;
2. Ten tweede de migratie van post-quantum cryptografie. Sinds 2016 wordt vanuit het Amerikaanse instituut NIST gewerkt aan de standaardisatie van post-quantum cryptografie. Dat proces lijkt binnenkort tot een einde te komen. Maar daarmee zijn we er nog lang niet [12]. Het is onduidelijk hoe alle cryptografische primitieven moeten worden geïmplementeerd binnen verschillende domeinen. Met name wanneer er beperkingen zijn in rekenkracht, geheugen of bandbreedte, zoals bij chipkaarten en sensoren;
3. Ten derde de opkomst van machine learning als onderdeel van kunstmatige intelligentie. Er dienen zich allerlei methoden aan om geavanceerde analyses te kunnen doen met tekst, geluid of beelden. Voordat een computer zover is moet deze eerst getraind worden met een heleboel data. De kwaliteit van die data is cruciaal. MPC en federated learning kunnen helpen om voldoende, mogelijk gevoelige data van goede kwaliteit uit verschillende bronnen beschikbaar te krijgen en vervolgens op een gedistribueerde manier veilig het model te trainen;
4. Als laatste noem ik computer aided crypto [15]. Het ontwikkelen van veilige protocollen en kwantum-bestendige producten wordt steeds ingewikkelder. De computer kan ons daarbij helpen door intensieve, formele evaluaties uit te voeren. Dan heb ik het zowel over het ontwerpen als het implementeren van die protocollen en producten. Dat scheelt de cryptografische industrie vele arbeidsuren en komt de productkwaliteit ten goede.

PERSOONLIJKE REIS

Tot zover de inhoudelijke ontwikkelingen. Zoals gebruikelijk bij een oratie neem ik jullie mee langs de weg die ik heb bewandeld om hier te mogen staan en laat ik zien welke mensen daar een belangrijke rol in hebben gespeeld.

De reis begint in Eindhoven in 1987. Mijn studievriend Marten van Dijk heeft mij destijds overgehaald om niet alleen wiskunde, maar ook informatica te gaan studeren. Daar pluk ik nog steeds de vruchten van, want zoals jullie vandaag hebben gezien, bevindt cryptografie zich op het grensvlak van wiskunde en informatica. Mijn eerste uitstapje boven de rivieren was mijn afstudeerstage bij het CWI in Amsterdam onder begeleiding van David Chaum. Zoals ik al eerder heb gezegd, had ik destijds de eer om met zijn moderne, cryptografische technieken te werken aan digitaal geld. Vervolgens ben ik gepromoveerd in de informatietheorie, een vakgebied dat nauw verwant is aan cryptografie. Van mijn promotor Piet Schalkwijk (die helaas in 2020 is overleden) en copromotor Frans Willems heb ik de beginselen van wetenschappelijk onderzoek geleerd.

Mijn eerste echte baan als wetenschappelijk programmeur was bij het CBS in Heerlen, waar ik mijn vrouw Suzanne heb ontmoet. Helaas had ik toen nog geen dating game, maar gelukkig zei ze “ja”. In mijn werk als programmeur ging ik al snel het onderzoek missen. Samen zijn Suzanne en ik toen van Maastricht naar Den Haag verhuisd.

In 1999 ben ik begonnen bij TNO in Den Haag, waar ik nog altijd met veel plezier werk. Door de wetenschappelijke ontwikkelingen die ik jullie heb laten zien, werd mijn vakgebied steeds relevanter en de hoeveelheid vakgenoten steeds groter. Er zijn veel mensen die mij gesteund hebben tijdens mijn carrière bij TNO. Als ik er een in het bijzonder moet noemen dan is dat Henk-Jan Vink. Hij was een van mijn eerste afdelingsmanagers, later ook directeur van mijn unit, en heeft er mede voor gezorgd dat ik nu hier sta.

In 2008 wilde ik graag naast TNO één dag per week op een universiteit werken. Dankzij Inald Lagendijk kreeg ik die kans bij de TU Delft. Daar heb ik jarenlang samen met Zekeriya Erkin gewerkt aan mooie toepassingen op het grensvlak van signaalverwerking en cryptografie. Na het avontuur aan de TU Delft mocht ik in 2016 voor één dag in de week aan de slag bij

de cryptogroep van het CWI, een van de beste onderzoeksgroepen van de wereld op het gebied van cryptografie. Ik dank Ronald Cramer voor het vertrouwen dat hij me al die jaren heeft gegeven en voor de vele projecten en evenementen die we samen van de grond hebben gekregen.

Sinds een aantal jaren heb ik bij TNO een bijzondere collega die ook hoogleraar is bij de Universiteit Twente: Paul Havinga. De deur van Paul Havinga staat altijd open voor goede raad en hij heeft een belangrijke rol gespeeld bij mijn aanstelling hier, waar ik hem voor dank. Ik ben blij en trots dat ik hoogleraar Toegepaste Cryptografie mag zijn aan de Universiteit Twente en hoop hier nog lang te werken aan de fascinerende geheimen van cryptografie.

Een laatste woord van dank aan mijn gezin. Suzanne heeft me altijd gesteund en mede dankzij haar heb ik mij ook op het niet-inhoudelijke vlak weten te ontwikkelen. Naast Suzanne wil ik ook mijn zonen Sam en Stef bedanken: voor de vele uren tafeltennis in de tuin, alle voetbalwedstrijden en andere sportwedstrijden die we samen gekeken hebben, zowel thuis op de televisie als in de Johan Cruijff Arena. Na een mooie wedstrijd was deze supernerd weer helemaal opgeladen!

Ik heb gezegd.

REFERENTIES

1. Diffie, W., Hellman, M.E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654.
2. Veugen, T. (1991). Some mathematical and computational aspects of electronic cash. In *MSc thesis*. Eindhoven University of Technology.
3. Veugen, T. (1993). On RSA signatures. Proceedings. *IEEE International Symposium on Information Theory*, p. 235.
4. Hirschfeld, R. (1993). Making Electronic Refunds Safer. In: Brickell, E.F. (eds) *Advances in Cryptology — CRYPTO' 92*. CRYPTO 1992. Lecture Notes in Computer Science, vol. 740. Springer, Berlin, Heidelberg.
5. Chaum, D., Fiat, A., Naor, M. (1990). Untraceable Electronic Cash. In: Goldwasser, S. (eds) *Advances in Cryptology — CRYPTO' 88*. CRYPTO 1988. Lecture Notes in Computer Science, vol. 403. Springer, New York, NY.
6. Yao, A.C. (1982). Protocols for Secure Computations. In *Proceedings of the IEEE Symposium on Foundations of Computer Science*, pp. 160–164.
7. Damgård, I. Pastro, V., Smart, N.P., Zakarias, S. (2012). Multiparty computation from somewhat homomorphic encryption. In *Advances in Cryptology – CRYPTO 2012* - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings, pp. 643-662.
8. Keller, M., Orsini, E., Scholl, P. (2016). MASCOT: faster malicious arithmetic secure computation with oblivious transfer. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, October 24-28, 2016, pp. 830-842. ACM.
9. Sangers, A., van Heesch, M., Attema, T., Veugen, T., Wiggerman, M., Veldsink, J., Bloemen, O., Worm, D. (2019). Secure multiparty PageRank algorithm for collaborative fraud detection. *Financial Cryptography and Data Security 2019*.
10. van Egmond, M.B., Spini, G., van der Galien, O. et al. (2021). Privacy-preserving dataset combination and Lasso regression for healthcare predictions. *BMC Medical Informatics and Decision Making*, vol. 21, no. 266.
11. NIST. (2022). Post-Quantum Cryptography - Selected Algorithms 2022. https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022.
12. TNO, CWI, AIVD. (2023). Het PQC-migratie handboek, maart 2023, https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-migratie-

handboek.
13. Smart, N. (2023), "Computing on Encrypted Data," in *IEEE Security & Privacy,* vol. 21, no. 4, pp. 94-98, July-Aug. 2023.
14. Information Commissioner's Office. (2023). Privacy-enhancing technologies (PETs), June 2023, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/
15. Barbosa, M., et al. (2021). "SoK: Computer-Aided Cryptography," *2021 IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, pp. 777-795.

UNLOCKING THE FASCINATING SECRETS OF CRYPTOGRAPHY

Dear Rector Magnificus, esteemed family members, friends, and colleagues, welcome. I'm glad that you have taken the effort, often after a long journey, to be present here today. And of course, a warm welcome to the online attendees who are joining us remotely.

Today, I am going to reveal the secrets of cryptography to you. This continuously evolving field has an increasingly significant impact on our society. Given that my chair is in Applied Cryptography, I will primarily show you the fascinating applications that can be created with cryptography. To conclude, I will take you on a journey through my personal path to becoming a professor.

Cryptography literally means 'secret writing.' The name originates from Greek: 'crypto' means 'secret' and 'graphy' is 'writing.' Nowadays, crypto often refers to digital currencies created using cryptographic techniques, but cryptography is much more than that.

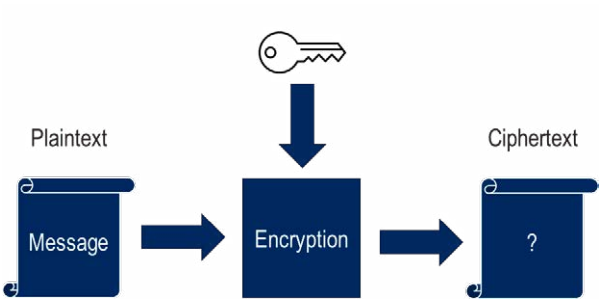


Figure 1: What is encryption?

Secret writing is done with a key (see Figure 1). This key explains how a message can be turned into a cipher. This process is called encryption, and the end result is a cipher: it is no longer a legible text and most of the time entirely consists of digits. Only knowing the key enables decrypting the ciphertext and reading the original text: the plaintext.

I will briefly outline the emergence of the field and its developments up to World War II: the dark blue part of the timeline in Figure 2. After that, I will describe in chronological order three revolutionary developments that the field has undergone in recent decades and the beautiful applications that have arisen from them, each corresponding to a year in the light blue part of the timeline in Figure 2.

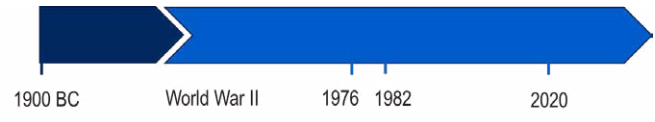


Figure 2: Timeline

To give you a glimpse of what's to come: we will transition from writing secrets to performing computations with secrets. Then, I will share my insights into the scientific challenges in the coming years and the exciting developments we can expect from cryptography.

CLASSICAL CRYPTOGRAPHY

This is the moment to introduce Alice and Bob (see Figure 3). In the modeling of cryptography, we send messages from A to B. To make it a bit more lively, these were once replaced by people: the A of Alice and the B of Bob. And to complete the picture, we also have the malicious Eve (from 'eval') who tries to uncover the secrets of Alice and Bob without knowing the key.

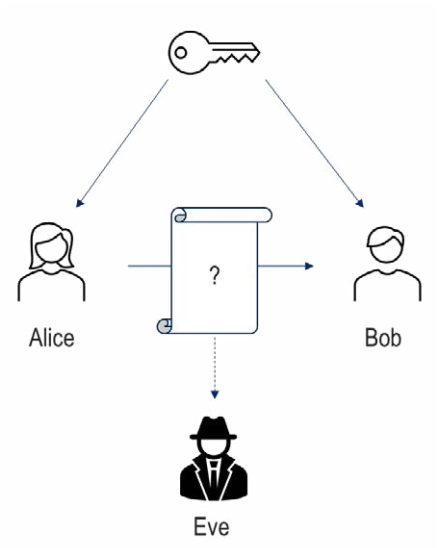


Figure 3: Alice and Bob

The first part of my story is about the origins of cryptography around 1900 BC and its development up to World War II. The earliest use of classical cryptography was found in Egyptian stones around 1900 BC, which were engraved with ciphertexts. This was probably more of a game to entertain scholars than to genuinely hide information. Figure 4 shows the famous Rosetta Stone, which was created in 196 BC and discovered in Egypt in July 1799. It's a kind of translation stone that relates hieroglyphic writing to the Egyptian language. It turned out to be a crucial key in deciphering ancient Egyptian hieroglyphs.

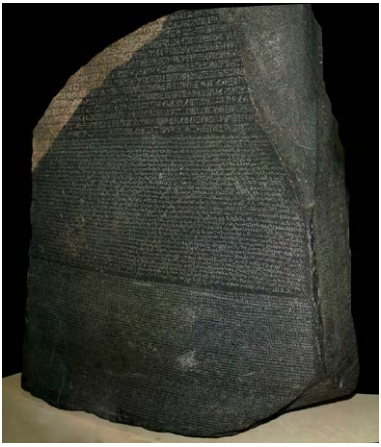
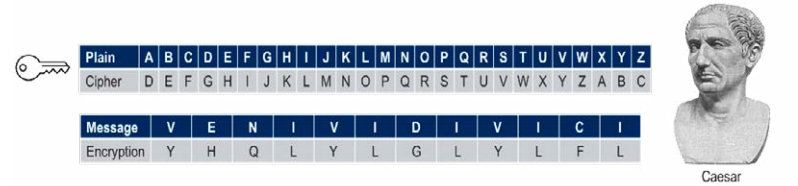


Figure 4: The Rosetta Stone

We know that Julius Caesar used cryptography to send secret messages in the 1st century BC. He did this by shifting all letters of the alphabet a fixed number of positions, as seen in Figure 5. The “A” becomes a “D,” the “B” becomes an “E,” and so on. The cryptographic key in this system is this substitution table.



Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Message	V	E	N	I	V	I	D	I	V	I	C	I
Encryption	Y	H	Q	L	Y	L	G	L	Y	L	F	L

Figure 5: Caesar’s cipher

For example, if Caesar wanted to encrypt the famous message “Veni, vidi, vici,” he would look up the letter 'V' in the table and see that it becomes 'Y.' The next letter 'E' becomes 'H,' and so on. To go from encryption back to message, one can use the same table. When the key for encryption and decryption is the same, we call it a symmetric encryption system.

In the example, one can see that quite a bit of the message's structure seeps into the ciphertext, such as the occurrence of the letter 'L' every two positions (which is the 'I' in the original message). This type of structure

makes it easier for a malicious actor, our Eve, to decipher the original text without knowing the table.

Over the course of history, encryption systems fortunately improved. In an overview of cryptography, the Enigma machine from Figure 6 cannot be omitted: a complex device with various rotors that the Germans used to communicate their military secrets during World War II.

Figure 6: Enigma machine

The cracking of the Enigma encryption at Bletchley Park under the leadership of Alan Turing played a significant role in the development of the first electronic computer, which is now an integral part of our society. Along with the homosexuality of the main character, which was not accepted at the time, this piece of history proved to be a good basis for dramatized adaptations, such as the entertaining movie "The Imitation Game[1]" Another popular example of cryptography is the book "The Da Vinci Code," in which author Dan Brown created the Cryptex.

After this brief overview of the history of cryptography, it's time to introduce you to the first revolutionary development of the last 50 years.

[1] https://www.imdb.com/title/tt2084970/

ASYMMETRIC CRYPTOGRAPHY

The Caesar cipher and the Enigma are examples of symmetric encryption: the key used to encrypt a message is the same as the key used to decrypt it. In the case of Caesar, this key is the table that allows you to encrypt or decrypt each letter.

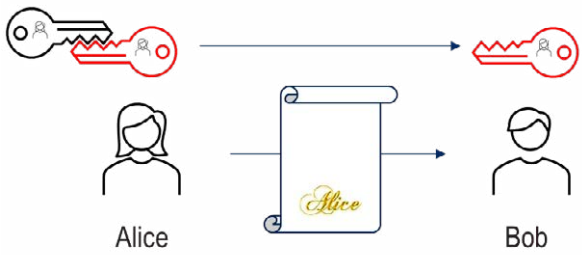


Figure 7: Asymmetric cryptography

Since 1976, asymmetric encryption has also existed [1]. In this case, Alice creates two different keys: a black key and a red key (Figure 7) that are intricately linked. She keeps one of the two keys for herself (in this case, the black one), and gives the other key, the red one, to Bob. Alice uses the black key to encrypt the message, and Bob uses the red key to decrypt it. Because Alice is the only person who knows the black key, that encryption is similar to a digital signature on that message: no one else can create this ciphertext (read: signature). Bob can verify with the red key whether the signature is genuine: is the signature indeed an encryption of the attached message? If so, Alice must be the one who created this signature because she is the only one who knows the black key.

What it boils down to is that with the advent of asymmetric encryption, a completely new function of cryptography has been achieved conceptually. Instead of just protecting the confidentiality of a message (ensuring that no one can eavesdrop), we can now guarantee the non-repudiation of a message: if Alice places a digital signature on a message, she cannot later deny it. This opens up a whole new world of applications and forms the secure foundation of the current electronic world of transactions:

1. There is now legislation in place to ensure that digital signatures have legal validity comparable to handwritten signatures. This means that you

can electronically sign messages that people can hold you accountable for later.

2. Asymmetric cryptography has paved the way for electronic commerce and online banking: an internet that is secure enough to conduct digital transactions and make electronic payments.
3. If you were to set up a messaging system like WhatsApp using symmetric cryptography, you would need to ensure that every pair of users shares a secret symmetric key with each other. How would you achieve that when anyone can eavesdrop over the internet? This is also made possible by asymmetric cryptography with a special key exchange protocol [1].
4. Finally, digital currency. In 1991, I had the privilege of doing my graduate research at the Centrum Wiskunde & Informatica in Amsterdam under the guidance of David Chaum [2,3,4]. This American pioneer brought modern cryptography to Europe and was already working on creating digital money using cryptography [5]. In his system, the bank could place a digital signature on a specially formatted long number. For example, you would receive a 'gulden' (Dutch currency) that you could then spend at a store. The system was designed in a way that the bank couldn't trace how you spent your money. Unfortunately, he was ahead of his time, and the system was never used in practice. How different it was when, years later, various cryptocurrencies emerged, based on a different concept outside the control of banks.

It's time to introduce you to the next recent scientific discovery in cryptography. A discovery that opens the doors to a whole new world of applications: secure multi-party computation.

SECURE COMPUTATION WITH SECRETS

After the advent of asymmetric cryptography, this is the second revolutionary development that has taken place in cryptography in recent decades. Alice and Bob have gained a new friend: Carol. They now know how to communicate their secret using symmetric and asymmetric cryptography. Now, they want to perform computations with their secrets without communicating them.

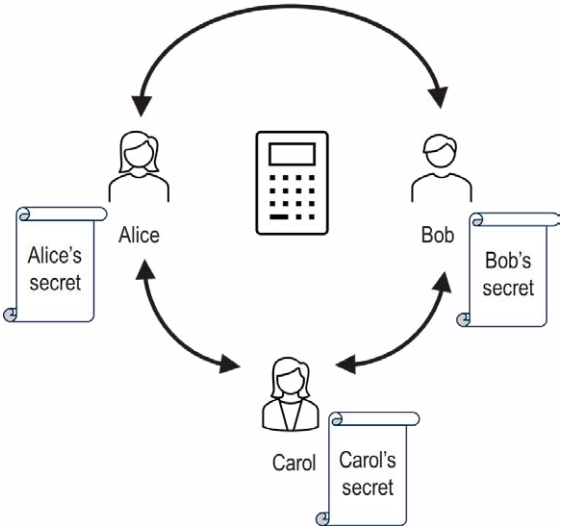
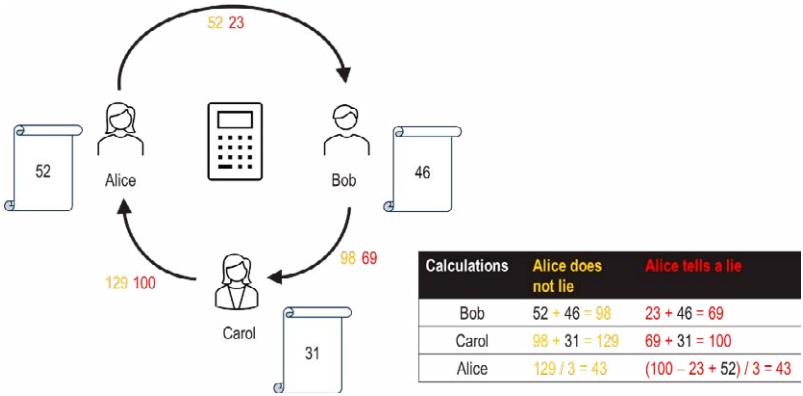


Figure 8: Secure multi-party computation

This subfield of cryptography originated in 1982 [6] and is called 'secure multi-party computation,' often abbreviated as MPC. In Figure 8, you can see three parties, each of whom has their own secret information. They want to compute something together with their secrets, symbolized by the calculator in the middle, without revealing each other's secrets.

I will explain with an example how this looks in practice. This example involves three parties, namely Alice, Bob, and Carol. The black numbers you see in Figure 9 represent their ages. They are curious about what their average age is but don't want to reveal their ages to each other. How are we going to achieve that?



Calculations	Alice does not lie	Alice tells a lie
Bob	52 + 46 = 98	23 + 46 = 69
Carol	98 + 31 = 129	69 + 31 = 100
Alice	129 / 3 = 43	(100 – 23 + 52) / 3 = 43

Figure 9: Safely calculating the average age

In a naive initial attempt, illustrated by the yellow numbers in Figure 9, you might think that Alice sends her age (52) to Bob. Bob adds his own age (46) to it and passes the sum to Carol. Carol adds her age (31) to the sum and passes the total back to Alice. Alice divides the total (129) by three and learns the average age (43). Such a series of communication steps is called a protocol. However, despite the correct outcome, the attentive reader will have noticed that this protocol is not secure. It goes wrong as early as step 1 because Alice reveals her age to Bob, which was precisely not the intention.

The solution seems simple. To prevent Bob from learning Alice's real age, we let Alice lie about her age in the first step, as illustrated by the red numbers in Figure 9. Instead of her real age (52), she tells Bob the number 23. Bob might give her a strange look but dutifully adds his own age (46) to it and sends the sum back to Carol. Carol knows that 69 is the sum of a lied-about age of Alice and an honest age of Bob, but has no clue what the separate terms are. Just like before, Carol adds her age (31) to the sum and sends the total back to Alice. All that remains is for Alice to replace the age she lied about with her real age and divide the new total by three.

The new protocol yields the same correct result and is also secure: no one learns the other's age. We've now come up with a nice solution for calculating the average age without revealing individual ages. This may

seem like a fun theoretical exercise, but what if we were to replace the three individuals with three competing companies? And instead of ages, we were dealing with sensitive business data like revenue or product effectiveness? Suddenly, we have a way to establish a benchmark for business performance in a specific industry, which companies can adhere to without sharing sensitive competitive data.

This new form of multi-party cryptography leads to various surprising applications. Take a look at a video from a dating show where you can exit the playing field without shame if there is no match. In the video, you see a smiley puzzle that only smiles if there is a match[2], as shown in Figure 10. The audience of the dating show only gets to know whether there is a match, and the 'no' responders don't find out if the other person might have had warm feelings for them after all. I brought the puzzle to the inaugural lecture to try out, but there is also a version with playing cards to try at home[3].

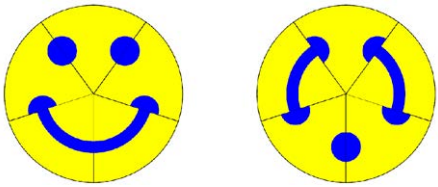


Figure 10: Dating game

We have seen how you can securely add numbers with three parties. In recent years, there have been many scientific developments that now allow us to perform arbitrary computations safely and reasonably quickly with any number of parties, without revealing individual secrets [7, 8]. I will demonstrate that this can lead to many valuable applications. We will start with detecting financial fraud and combating poverty.

Financial fraud costs society a significant amount of money. In the Netherlands, it is estimated that around €16 billion in undeclared income

---

[2] https://vimeo.com/294584796
[3] https://www.win.tue.nl/~wstomv/misc/ZeroKnowledgeMatchMaker

circulates annually[4]. Detecting and tracing these illegal financial flows can be extremely challenging. The current rate of apprehension is only 0.083%.[5] In Figure 11, you can see a small financial transaction network. The little balls represent bank accounts, and the arrows represent transactions. For instance, the arrow from ball 2 to ball 4 indicates that money was transferred from bank account number 2 to bank account number 4 during a certain time period.

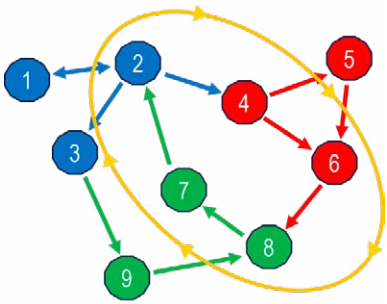


Figure 11: Detecting money laundering

One way of laundering illegally earned money is to move it through various accounts until it becomes untraceable, appearing legitimate to the outside world and thus allowing legal spending. This means you need to look for suspicious money flows, such as the yellow circle in Figure 11: here, money goes from ball 2 through 4, 6, 8, and 7 before returning to 2. The problem, however, is that not all balls belong to the same bank. Money isn't laundered within a single bank but rather through multiple banks. In this example, the network is actually composed of three banks, each with its own color (blue, red, and green), and the transaction networks are intertwined. For commercial and legal reasons, the banks are not allowed to share their transaction networks.

In cases like these, secure multi-party computation (MPC) is the ideal technique for conducting further investigations into money flows. With MPC, it is possible to search the entire transaction network without sharing

[4] https://www.uu.nl/nieuws/jaarlijks-16-miljard-euro-witgewassen-in-nederland
[5] https://www.groene.nl/artikel/pakkans-0-083-procent

the three separate networks with each other, ultimately helping identify suspicious circles [6]. I personally consider it one of the most beautiful applications of MPC. Even a small improvement in the detection rate can lead to significant savings. MPC not only helps in saving money but also ensures that allowances are allocated correctly. An example of this is the solution we developed at TNO for UWV and SVB.

There is a scheme that allows seniors to receive a supplement to their AOW pension if their income falls below a certain threshold. However, it appears that this benefit is underutilized. The government wants to understand why but doesn't know which individuals are affected. This is because the necessary information resides in two separate databases managed by different organizations, which cannot share data for privacy reasons. The Dutch Social Insurance Bank (Sociale Verzekeringsbank, SVB) (Figure 12) knows which individuals, identified by their Social Security Number (SSN), receive AOW and what their income threshold is. The Netherlands Employee Insurance Agency (Uitvoeringsinstituut WerknemersVerzekeringen, UWV) knows their income.

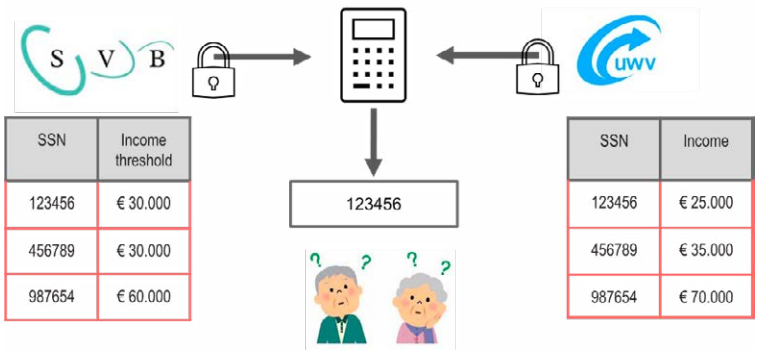


Figure 12: Who is entitled to supplementary AOW?

Only when we can combine that data in a privacy-friendly manner can we determine who is eligible for the scheme. In the example, this applies to the individual with the fictitious SSN 123456 because that is the only one with an income below the threshold. The information of all other AOW recipients remains undisclosed and in the local databases. Once again, a great example of MPC: two parties with data that cannot be shared but can be used for calculations with the help of MPC.

Another example of MPC involves finding common records in different databases without having to share the databases themselves (Figure 13). The only record that appears in both databases is the one with the number 5. With MPC, you can find the shared records without needing to exchange all the records. For example, the owner of the left database won't learn that the right database, in addition to 5, also has the numbers 2 and 9. Both owners will only learn that they have the number 5 in common. This basic principle has a wide range of applications.

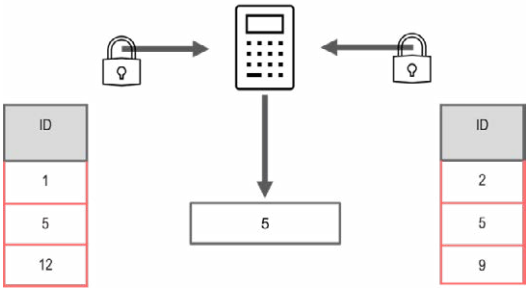


Figure 13: Safely finding the overlap of databases

Consider, for example, a situation where different countries have lists of suspicious individuals. These names cannot be shared freely, but if there are suspects wanted in multiple countries, that would be valuable information. Another example in the same category is making recommendations. Everyone has probably searched for a product on the internet at some point. Google provides you with a list of store suggestions, and then you decide whether or not to continue searching in one of those stores. However, Google doesn't find out whether you actually purchased the product due to their recommendation. If that feedback could be provided in a privacy-friendly manner, it would improve the quality of recommendations. It doesn't even have to be at an individual level: aggregations per time period per product achieve the same effect.

It is clear that insurance companies cannot simply access patient data from healthcare providers. Within TNO, we have undertaken two projects where you can securely combine that data using MPC to improve the quality of life through better healthcare. The first project, conducted in South Limburg in collaboration with Statistics Netherlands, Zuyderland, and health insurer CZ,

focuses on determining the effectiveness of a specific app. In the second project, in partnership with ZorgTTP, Zilveren Kruis, and Erasmus MC, we are identifying risk factors for a particular group of heart failure patients in Rotterdam [10].

I could go on for a while mentioning applications of MPC, but it's time to move on to the next development that will shake the foundations of cryptography.

THE THREAT OF THE QUANTUM COMPUTER

Do you remember the name Alan Turing? He was one of the pioneers of the modern computer. As you may know, there is currently a lot of work being done on the development of quantum computers. These computers will be able to perform certain calculations much faster than today's computers. This opens up opportunities for various innovations in society.

Unfortunately, this quantum computer will also excel in breaking cryptography. In particular, the calculations underlying asymmetric cryptography are vulnerable to quantum computers. Although current quantum computers are still too small, they will eventually become powerful enough. This threat is already having a revolutionary impact on the field. Fellow cryptographers have been working on new asymmetric systems for a number of years that appear to be resistant to quantum computers [11].

How does that work exactly? Because regular computers also get faster every year. Why don't they pose a threat to cryptography? There's a law, Moore's Law, that quantifies the technological advancement of computers. This trend roughly means that the computational power of computers doubles every two years. Eve has such a computer and is trying to decrypt the encrypted message between Alice and Bob without knowing the key. This can be done by trying all possible keys one by one and checking if they produce a readable message. This means that the longer Alice and Bob make the key, the harder it becomes for Eve. You can compare it to cracking a safe: the more possible combinations you have to try, the longer it takes. By making the key a little longer, they can make the decryption problem for Eve so difficult that it becomes practically impossible, even if Eve has a computer twice as powerful in the future.

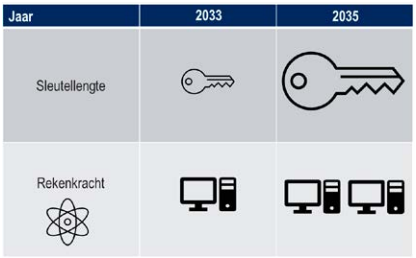


Figure 14: The problem of the quantum computer for cryptography

Let's assume that Eve has a large quantum computer in ten years. The symbol you see in Figure 14 just below 'Computational power' represents an atom, introducing the quantum effect. The quantum computer will also become increasingly powerful. Alice and Bob will need to make their key longer to keep up with that effect. However, the quantum computer can try all possible keys much faster, so the key suddenly needs to be much longer. So we can continue to use the same cryptographic systems, but it means that the keys need to grow much faster than we're used to. These extremely long keys need to be communicated and stored. Moreover, encryption and decryption become slower as a result, making it a practically unworkable system in practice. Therefore, we cannot escape the need to develop new cryptographic systems that are too difficult for even the quantum computer to crack. These new systems are called Post Quantum Cryptography, or PQC.

Actually, this terminology is incorrect because 'post' is Latin for 'after,' and we cannot wait until the quantum computer is powerful enough, as malicious actors (symbolized by our Eve) can now store and keep encrypted information until the quantum computer reaches that level. The consequences will be noticeable in the short term for all individuals and organizations working with computers and the internet. All computers, networks, etc., will need to migrate to quantum-resistant cryptography. This is a complex process: you can't simply replace vulnerable cryptosystems with secure variants. As I outlined earlier, you'll encounter different key lengths, longer encryption and decryption times, and larger ciphertexts that our computers and networks will need to handle.

To prevent our secrets from being exposed in the future, it's crucial for organizations to start addressing this issue now. In April of this year, colleagues from TNO and CWI presented the handbook for post-quantum cryptography migration [12], which they created in collaboration with the AIVD (Dutch General Intelligence and Security Service), to State Secretary Alexandra van Huffelen.

Perhaps by now, you may feel a bit overwhelmed by all the keys, computers, and scientific breakthroughs. Let me summarize the secrets of cryptography that have been discussed:

1. We began with classical cryptography, which around World War II played a role in the development of the electronic computer;

2. Then, in 1976, we had a significant expansion from symmetric to asymmetric cryptography, allowing us to create digital signatures, conduct electronic transactions, and develop messaging systems like WhatsApp;
3. In 1982, we discovered MPC, transitioning from secret writing to computing with secrets, and exploring its many surprising applications;
4. Finally, we faced the threat of quantum computers and the necessity for new cryptographic systems that can withstand that threat.

THE FUTURE OF CRYPTOGRAPHY

What other secrets does cryptography have in store for us in the coming years? I'll provide you with an overview of the main challenges I expect in my field, moving from the near future to the more distant future:

1. Firstly, I mention the growing need for privacy-preserving techniques. This includes not only secure multi-party computation but also related techniques with terms like federated learning, differential privacy, trusted execution environments, zero knowledge proofs, and synthetic data [13,14]. These are not widely known among the general public, which means we are underutilizing new opportunities to enrich data in a responsible manner. In the coming years, I will be working with colleagues from the University of Twente to train students in these areas. What is currently lacking is a good way to measure the quality of the privacy protection provided given a technical solution.
2. Secondly, the migration to post-quantum cryptography. Since 2016, the U.S. National Institute of Standards and Technology (NIST) has been working on the standardization of post-quantum cryptography. This process seems to be coming to an end soon [12]. However, we are far from done with this. It is unclear how all cryptographic primitives should be implemented in various domains, especially when there are constraints on computing power, memory, or bandwidth, such as in smart cards and sensors.
3. Thirdly, the rise of machine learning as part of artificial intelligence. Various methods are emerging to perform advanced analyses with text, sound, or images. Before a computer can do this, it must first be trained with a lot of data. The quality of that data is crucial. MPC and federated learning can help make enough, possibly sensitive, high-quality data available from various sources and then securely train the model in a distributed manner.
4. Lastly, I mention computer-aided crypto [15]. Developing secure protocols and quantum-resistant products is becoming increasingly complex. Computers can assist us by performing intensive, formal evaluations. This includes both designing and implementing these protocols and products. This saves the cryptographic industry many hours of labor and improves product quality.

PERSONAL JOURNEY

So far, the scientific developments. As is customary in an inaugural lecture, I will take you on the journey I have traveled to stand here today and show you the people who have played an important role in it.

The journey begins in Eindhoven in 1987. My study friend Marten van Dijk convinced me at the time not only to study mathematics but also computer science. I still reap the benefits of that decision, as you have seen today, cryptography is at the intersection of mathematics and computer science. My first trip to the North of the Netherlands was my internship at CWI in Amsterdam, supervised by David Chaum. As I mentioned earlier, I had the honor at the time of working with his modern cryptographic techniques for digital money. I then obtained my Ph.D. in information theory, a field closely related to cryptography. From my supervisor Piet Schalkwijk (who unfortunately passed away in 2020) and co-supervisor Frans Willems, I learned the fundamentals of scientific research.

My first real job as a scientific programmer was at the CBS in Heerlen, where I met my wife Suzanne. Unfortunately, I didn't have a dating game back then, but fortunately, she said “yes.” In my work as a programmer, I quickly began to miss research. So, Suzanne and I moved from Maastricht to The Hague together.

In 1999, I started working at TNO in The Hague, where I still enjoy working. Due to the scientific developments I have shown you, my field of expertise became increasingly relevant, and the number of colleagues in the field grew. There are many people who have supported me throughout my career at TNO. If I have to mention one in particular, it would be Henk-Jan Vink. He was one of my first department managers, later also the director of my unit, and played a significant role in getting me to where I am today.

In 2008, I wanted to work one day a week at a university alongside TNO. Thanks to Inald Lagendijk, I got that opportunity at the TU Delft. There, I worked for many years with Zekeriya Erkin on exciting applications at the intersection of signal processing and cryptography. After my time at TU Delft, I had the opportunity to work one day a week with the cryptography group at CWI in 2016, one of the world's leading research groups in cryptography. I want to thank Ronald Cramer for the trust he has placed in me over the years and for the many projects and events we have organized together.

For several years now, I have had a special colleague at TNO who is also a professor at the University of Twente: Paul Havinga. Paul Havinga's door is always open for good advice, and he played a significant role in my appointment here, for which I thank him. I am happy and proud to be a professor of Applied Cryptography at the University of Twente, and I hope to continue working here for a long time on the fascinating secrets of cryptography.

A final word of thanks to my family. Suzanne has always supported me, and thanks to her, I have also been able to develop myself as a person. In addition to Suzanne, I would like to thank my sons Sam and Stef: for the many hours of table tennis in the garden, all the football matches and other sports events we watched together, both at home on television and in the Johan Cruijff Arena. After a great match, this super nerd was completely recharged!

Ik heb gezegd.

REFERENCES

1. Diffie, W., Hellman, M.E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654.
2. Veugen, T. (1991). Some mathematical and computational aspects of electronic cash. In *MSc thesis*. Eindhoven University of Technology.
3. Veugen, T. (1993). On RSA signatures. Proceedings. *IEEE International Symposium on Information Theory*, p. 235.
4. Hirschfeld, R. (1993). Making Electronic Refunds Safer. In: Brickell, E.F. (eds) *Advances in Cryptology — CRYPTO' 92*. CRYPTO 1992. Lecture Notes in Computer Science, vol. 740. Springer, Berlin, Heidelberg.
5. Chaum, D., Fiat, A., Naor, M. (1990). Untraceable Electronic Cash. In: Goldwasser, S. (eds) *Advances in Cryptology — CRYPTO' 88*. CRYPTO 1988. Lecture Notes in Computer Science, vol. 403. Springer, New York, NY.
6. Yao, A.C. (1982). Protocols for Secure Computations. In *Proceedings of the IEEE Symposium on Foundations of Computer Science*, pp. 160–164.
7. Damgård, I. Pastro, V., Smart, N.P., Zakarias, S. (2012). Multiparty computation from somewhat homomorphic encryption. In *Advances in Cryptology – CRYPTO 2012* - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings, pp. 643-662.
8. Keller, M., Orsini, E., Scholl, P. (2016). MASCOT: faster malicious arithmetic secure computation with oblivious transfer. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, October 24-28, 2016, pp. 830-842. ACM.
9. Sangers, A., van Heesch, M., Attema, T., Veugen, T., Wiggerman, M., Veldsink, J., Bloemen, O., Worm, D. (2019). Secure multiparty PageRank algorithm for collaborative fraud detection. *Financial Cryptography and Data Security 2019*.
10. van Egmond, M.B., Spini, G., van der Galien, O. et al. (2021). Privacy-preserving dataset combination and Lasso regression for healthcare predictions. *BMC Medical Informatics and Decision Making*, vol. 21, no. 266.
11. NIST. (2022). Post-Quantum Cryptography - Selected Algorithms 2022. https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022.
12. TNO, CWI, AIVD. (2023). Het PQC-migratie handboek, maart 2023, https://www.aivd.nl/documenten/publicaties/2023/04/04/pqc-migratie-

handboek.
13. Smart, N. (2023), "Computing on Encrypted Data," in *IEEE Security & Privacy,* vol. 21, no. 4, pp. 94-98, July-Aug. 2023.
14. Information Commissioner's Office. (2023). Privacy-enhancing technologies (PETs), June 2023, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/
15. Barbosa, M., et al. (2021). "SoK: Computer-Aided Cryptography," *2021 IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, pp. 777-795.

WWW.UTWENTE.NL