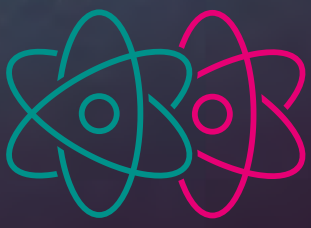
Essay

Verkenning quantum technologie

Aanbevelingen ter voorbereiding op een gezamenlijke toekomst met quantumtechnologie



ECP
Platform voor de InformatieSamenleving

Colofon

2019 © ECP | Platform voor de InformatieSamenleving

Met dank aan Turnaround Communicatie

Inhoud

Deze verkenning is een wegwijzer voor lezers zonder technische achtergrond of kennis van quantumtechnologie en schetst kort wat de stand van zaken is, wat de kansen en uitdagingen zijn zowel op technisch als maatschappelijk vlak, welke partijen actief zijn in het veld en waar meer informatie is te vinden.

Voorwoord

Aan de horizon verschijnt een nieuwe technologie: quantumtechnologie. De technologie en de ideeën over toepassing bestaan al een tijdje, maar door een aantal doorbraken wordt nu aan concrete toepassingen gewerkt. Deze verkenning is een wegwijzer voor lezers zonder technische achtergrond of kennis van quantumtechnologie en schetst kort wat de stand van zaken is, wat de kansen en uitdagingen zijn zowel op technisch als maatschappelijk vlak, welke partijen actief zijn in het veld en waar meer informatie is te vinden.

Quantumtechnologie is gebaseerd op de natuurwetten die het gedrag van de allerkleinste deeltjes beschrijven.[1] Die pakken anders uit dan de wetten die we gewend zijn: zo kunnen deeltjes op microniveau verschillende waarden[2] tegelijkertijd hebben en zich onder bepaalde voorwaarden gedragen als één – ongeacht hun onderlinge afstand. Deze eigenschappen van de kleinste deeltjes vormen de basis voor drie quantum-toepassingsgebieden: quantum computing en quantumsimulatie (rekenen), quantum sensing (meten) en quantuminternet (communiceren).

Met quantum computing bijvoorbeeld, kunnen we in de toekomst misschien precies uitrekenen hoe het perfecte geneesmiddel voor een specifieke persoon gemaakt kan worden, op moleculair niveau. Quantum computing zou ook de ontwikkeling van artificial intelligence kunnen versnellen en bepaalde problemen kunnen helpen oplossen waarvoor we nu onvoldoende rekenkracht hebben. Zo lijkt bij het verschijnen van deze publicatie een eerste experimentele quantumcomputer te zijn gerealiseerd die een algoritme kan draaien dat op klassieke computers praktisch niet uitgevoerd kan worden *(NRC, 2019; Sciencenews, 2019)*.

Quantumsensoren kunnen straks nog beter en preciezer signalen registreren en kunnen worden toegepast in de zorg (nauwkeuriger ziektebeelden) of bij navigatie (GPS-positiebepaling tot op de millimeter nauwkeurig, ook op plekken waar geen GPS voorhanden is). Toepassingen in de industrie, bouw en defensie liggen op korte termijn in het verschiet.

"De potentiële toekomstige impact van quantum op de informatietechnologie en daardoor ook op de maatschappij is enorm. De ontwikkelingen in quantumtechnologie gaan erg snel en Nederland is een koploper in technologieontwikkeling, maar wat kunnen we ermee? Laten we samen onderzoeken hoe we de quantumtechnologie ten goede van de maatschappij kunnen inzetten."

— Jean-Louis Roso, Senior business development manager TNO

Via het quantuminternet kunnen quantumcomputers informatie uitwisselen met behoud van quantumeigenschappen en zonder dat deze quantuminformatie afgeluisterd kan worden: de eerste quantum backbone in Nederland is naar verwachting binnen enkele jaren operationeel *(Computable, 2019)*.

Met quantumcomputers zal de rekenkracht zodanig toenemen dat er nieuwe methoden voor beveiliging van digitale informatie nodig zijn: het hoofdstuk 'informatieveiligheid en cryptografie' laat zien dat wetenschappers daar voortgang in boeken. Bovendien biedt quantumtechnologie zelf een deel van de oplossing.

Kansen op de korte en lange termijn

Quantumtechnologie heeft de potentie op de lange termijn grote maatschappelijke vraagstukken te helpen oplossen, maar er zijn ook al kansen voor de kortere termijn. Enkele eerste generatie-producten en -diensten zijn nu al verkrijgbaar, zoals kleinschalige special purpose quantumcomputers, bepaalde typen quantumsensoren en de eerste Quantum Key Distribution-oplossingen. Daarnaast bereiden ontwikkelingen in de post-quantum cryptografie ons alvast voor op de komst van de quantumcomputer. Deze ontwikkelingen zijn onder andere relevant voor de financiële, logistieke en telecomsector, maar ook van belang in relatie tot andere ICT-innovaties, zoals artificial intelligence en big data.

Vanuit de wetenschap wordt er volop ingezet op de ontwikkeling van quantumtechnologie. Een aantal doorbraken in de afgelopen decennia, onder andere op de TU Delft en bij QuTech in Delft, QuSoft in Amsterdam en QT/e in Eindhoven, hebben Nederland een voorsprong gegeven. Wereldwijd behoort QuTech bijvoorbeeld tot de top op het gebied van quantum computing en quantumcommunicatie. Een voorsprong die Nederland als kennisland graag wil behouden, onder andere met de Nationale Agenda Quantumtechnologie. Deze is op 16 september 2019 uit naam van het Nederlands quantumveld aangeboden aan staatssecretaris Mona Keijzer *(QuTech, 2019)*.

"Hoe het tijdpad van quantumtechnologie er precies uit zal gaan zien is misschien nauwelijks aan te geven, maar er is voldoende reden voor organisaties, branches en bedrijfssectoren, maar ook voor politici en beleidsmakers om zich nu al te verdiepen in de quantumtechnologie"

— Daniël Frijters (MA, BSc), Voorzitter ECP werkgroep Quantum

Nu al verdiepen!

Hoe het tijdpad van quantumtechnologie er precies uit zal gaan zien is op dit moment nog niet goed aan te geven, maar er is voldoende reden voor organisaties, branches en bedrijfssectoren, maar ook voor politici en beleidsmakers om zich nu al te verdiepen in de quantumtechnologie.

De agendering van randvoorwaarden, zoals encryptie en ethiek, pakt ECP | Platform voor de InformatieSamenleving met deze 'Verkenning quantumtechnologie' op. Samen met deelnemers en leden van de ECP-werkgroep Quantum willen we denk- en gespreksstof aanbieden die we nodig hebben om ons als samenleving en bedrijfsleven voor te bereiden op een gezamenlijke toekomst met quantumtechnologie.

Daniël Frijters (MA, BSc)
Voorzitter ECP werkgroep Quantum
MT-lid en programmamanager ECP

Jean-Louis Roso
Senior business development manager TNO

Drs. Jelle Attema
Secretaris en projectadviseur ECP

Drs. Ir. Maran van Heesch
Consultant quantum security TNO

In de werkgroep Quantum hebben (op persoonlijke titel) zitting:

Charlotte Rugers *op persoonlijke titel,* **Cor van der Struijf** *IBM,* **Daniël Frijters** *ECP,* **Freeke Heijman** *TU-Delft,* **Hans Bos** *Microsoft,* **Hugo Gelevert** *TNO,* **Ingrid Romijn** *QuTech/TUDelft,* **Jean-Louis Roso** *TNO,* **Jelle Attema** *ECP,* **Jos van Rijn** *Capgemini,* **Kristian Tap** *Capgemini,* **Maran van Heesch** *TNO,* **Niels Neumann** *TNO,* **Oscar Koeroo** *KPN,* **Victor Reijs** *SIDN Labs*

ECP zal naast deze publicatie samen met partners de maatschappelijke dialoog rondom dit thema vorm en inhoud geven in 2019 en 2020. Daarbij werkt ECP onder andere samen met de partijen achter de Nationale Agenda Quantumtechnologie.

Introductie quantumtechnologie

Quantumverschijnselen vormen de basis voor drie soorten quantumtechnologie: quantum computing/simulatie (rekenen, simuleren van fysische of chemische processen), quantumsensoren (registreren) en quantuminternet (transport van informatie). Quantumtechnologie is gebaseerd op de natuurwetten die het gedrag van de kleinste deeltjes beschrijven. Dat pakt op microniveau anders uit dan op macroniveau.[3] Elke quantumtoepassing benut specifieke eigenschappen van de microdeeltjes, en biedt eigen mogelijkheden en uitdagingen, met een eigen tijdpad. In het hoofdstuk “Toepassingsgebieden” wordt dieper ingegaan op toepassingsmogelijkheden: in dit hoofdstuk wordt nader ingegaan op de technische kant.

Quantum computing

Onze klassieke computers werken met nullen en enen en moeten bewerkingen op de nullen of de enen na elkaar (sequentieel) of door verschillende computers parallel laten uitvoeren *(TNO, 2019)*. Quantum computing maakt gebruik van het verschijnsel dat op microniveau een deeltje verschillende waarden tegelijk kan hebben[4]: een quantumbit of 'qubit' heeft niet de waarde van nul óf één, maar heeft tegelijkertijd de waarde nul én één (en alle waarden daartussenin).[5] Een bewerking op een qubit geeft daarom als resultaat de bewerking op zowel de nul als de één.

Een processor die deze eigenschappen gebruikt, kan bijvoorbeeld in één keer tegelijkertijd dezelfde berekeningen uitvoeren over een zeer grote hoeveelheid data.[6] Een quantumcomputer kan daardoor voor specifieke taken vele malen sneller zijn dan een conventionele computer. Het manipuleren — of bewerken — van qubits lukt echter alleen bij heel lage temperaturen.[7] Qubits zijn namelijk erg instabiel: de uitdaging is om een omgeving te creëren waarin deze wel qubits wel stabiel blijven; daar wordt dan ook veel onderzoek naar gedaan.

Het concept van de quantumcomputer werd reeds begin jaren tachtig al beschreven. Recente doorbraken, waarbij de Nederlandse wetenschap een belangrijke rol speelt, brengen de technologie binnen handbereik. Het hoofdstuk 'De toppositie van Nederland' gaat verder in op de rol van Nederland in dit domein.

Quantum sensoren

Quantumverschijnselen kunnen ook gebruikt worden voor nieuwe generaties sensoren: in dit domein worden al enkele jaren veel patenten geregistreerd *(Economist, 2019b)*.

Quantumsensoren kunnen de huidige technieken voor het maken van beelden verbeteren. Denk aan de MRI-scans in de medische sector. Of het maken van scans van de ondergrond. Bouwbedrijven worden bijvoorbeeld nu nog regelmatig verrast met wat zich in de grond bevindt, omdat testboringen en grondradars niet diep genoeg komen. Met quantum-technieken is dat wel mogelijk.

Rekenkracht

Om een idee te geven van de rekencapaciteit van quantumtechnologie, is het wellicht behulpzaam om het voorbeeld van Discover* van twintig jaar geleden aan te halen *(Tweakers, 2019)*. Stel je moet een map met documenten vinden, die iemand in de lade van zijn bureau in een groot kantoorgebouw heeft achtergelaten. Je weet alleen niet in welk bureau. Je kunt bij de onderste etage bij het eerste bureau beginnen met zoeken en zo één voor één alle bureaus afgaan. Dit is vergelijkbaar met hoe een klassieke rekenprocessor het aanpakt: serieel, bureau voor bureau, etage voor etage.

Je kunt ook teams samenstellen die tegelijk de bureaus van verschillende etages controleren en hun bevindingen doorgeven. Dit is vergelijkbaar met parallelle verwerking zoals gpu's (grafische processoren) die bijvoorbeeld bieden: een groot aantal processoren werkt tegelijkertijd, maar op verschillende etages, de verschillende bureaus af.

Een quantumcomputer pakt het helemaal anders aan. Een manier om het te vergelijken is dat je zoveel klonen van je zelf maakt, dat je op hetzelfde moment in alle laatjes van alle bureaus op alle etages tegelijk kunt kijken. Bij het vinden van de map met documenten verdwijnen alle klonen op de vinder na. Het is natuurlijk een ongenuanceerde vergelijking, maar ze geeft wel aan dat de quantumcomputer enorme snelheidswinst kan bieden, al is het maar voor een beperkte groep berekeningen.

Bekende voorbeelden van ontwikkelde algoritmen zijn die voor zoeken in ongestructureerde databases (algoritme van Grover) en die voor het berekenen van priemfactoren van een geheel getal (Shor's algoritme).

* http://discovermagazine.com/1999/jan/thegreatquantumn1574

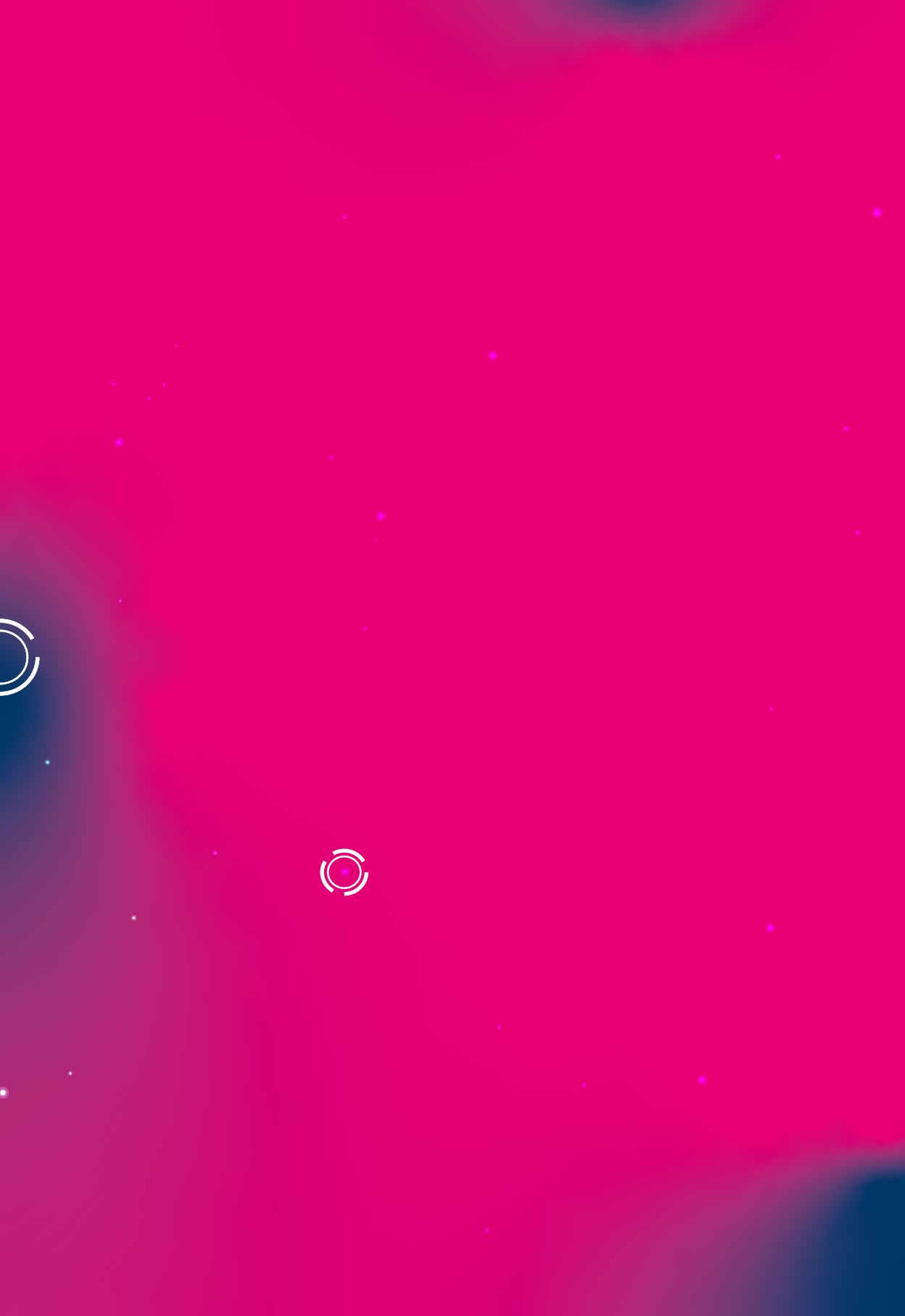
Trillingen, versnelling of objecten (in de grond, lucht of onder water) kunnen nauwkeuriger worden waargenomen. Ook de tijd of zwaartekracht kan veel beter worden gemeten, waardoor onze GPS -systemen nauwkeuriger kunnen worden, en precieze positiebepaling zelfs mogelijk wordt op plekken waar geen satellietsignaal ontvangen kan worden (bijvoorbeeld ondergronds, of in een onderzeeër diep in de zee).

Quantum internet

Het quantuminternet maakt het mogelijk quantuminformatie tussen quantumcomputers uit te wisselen, met behoud van de quantum-eigenschappen. De basis voor het quantuminternet is verstrengeling: twee met elkaar verstrengelde deeltjes gedragen zich als één enkel deeltje, ook als ze ver uit elkaar zijn. Het quantuminternet benut dit verschijnsel *(NWO, 2019)*.

De ontwikkeling van dit internet is in een experimenteel stadium. KPN verwacht binnen enkele jaren de eerste werkende quantuminternet-backbone beschikbaar te hebben *(Computable, 2019)*. De functionaliteit is nog erg beperkt. Met het quantuminternet kunnen quantumcomputers en quantumsensoren samenwerken en verbonden worden.

Quantuminternet speelt ook een belangrijke rol bij beveiliging: het is door de verstrengeling van qubits weliswaar mogelijk om quantuminformatie verzonden via het quantuminternet af te luisteren *(NWO, 2019)*, maar dat wordt opgemerkt omdat er daardoor fouten ontstaan in de overdracht.



Thema:
Informatieveiligheid en cryptografie

Cryptografie is altijd een betrouwbare bouwsteen geweest voor het afschermen van informatie en het weren van onbevoegden (vertrouwelijkheid). Het is nodig om zeker te stellen dat partijen daadwerkelijk communiceren met wie ze willen communiceren, en informatie ook echt afkomstig is van een bepaalde partij (authenticiteit), en voor het garanderen van een onveranderde boodschap (integriteit). Cryptografie zit verborgen achter bijna alles wat we digitaal doen. Zo vormt het bijvoorbeeld een integraal onderdeel van internetstandaarden als TLS/SSL, van digitale handtekeningen en van methoden voor het betrouwbaar opslaan van data in de cloud.

Quantumalgoritmen

De berekeningen welke noodzakelijk zijn om versleuteling te verbreken zijn dermate complex dat zelfs de snelste computers ter wereld hier jarenlang over doen. We zijn de afgelopen decennia al gewend geraakt aan het feit dat met de komst van snellere processoren allerlei versleutelingsmethoden 'gekraakt' en daarmee onveilig worden.[8] Met de komst van de quantumcomputer raakt dit proces van het onveilig worden van veilige versleutelingsmethoden in een stroomversnelling.

Peter W. Shor heeft in 1994 een algoritme gepresenteerd voor quantumcomputers, waardoor de meest gebruikte protocollen in de familie van versleutelingsmethoden (asymmetrische encryptie) niet meer veilig zijn. Asymmetrische encryptie is de bouwsteen voor efficiënte sleuteluitwisseling en digitale handtekeningen.[9] Met een quantumcomputer die krachtig genoeg is kan een aanvaller de sleutel bemachtigen die gebruikt wordt om de daadwerkelijke berichten mee te vercijferen, om deze vervolgens dus te kunnen ontcijferen. Ook kan een aanvaller de rechtsgeldigheid van digitaal getekende en gemarkeerde documenten en bestanden compromitteren, waardoor bijvoorbeeld de betrouwbaarheid van softwarepatches afneemt en er veiligheidsinbreuken kunnen ontstaan.

Het is nog niet mogelijk een goede inschatting te geven wanneer quantumcomputers krachtig genoeg zijn om encryptie te breken. Schattingen lopen uiteen van 2025 tot 2040. Een aandachtspunt vormt het 'store now decrypt later'-scenario: kwaadwillenden die nu versleutelde informatie opslaan, met als doel de encryptie te verbreken als quantumcomputers krachtig genoeg zijn.

In hun voorlichting en publicaties wijzen organisaties als het Nationaal Cyber Security Centrum *(AIVD, 2019)* en de Algemene Inlichtingen- en Veiligheidsdienst erop dat organisaties en bedrijven in Nederland zelf verantwoordelijk zijn voor hun digitale beveiliging *(NCTV, 2019)*. Dat betekent dat elke organisatie moet begrijpen wat de impact is van de quantumdreiging op zijn (core)business of activiteiten. Om vertrouwen te kunnen houden in onze digitale handelingen worden er cryptosystemen ontworpen die 'quantum-safe' zijn.

Ook al zal het nog wel even duren voordat quantumcomputers krachtig genoeg zijn om deze protocollen te kraken, toch is het belangrijk nu al na te denken over oplossingen. Wiskundigen hebben dit probleem gelukkig al even geleden voorzien en inmiddels zijn ook encryptie-methoden beschikbaar die de rekenkracht van de quantumcomputer wel kunnen weerstaan.

Quantumcryptografie

Quantumcryptografie is gebaseerd op natuurkundige verschijnselen en vereist het gebruik van quantumapparatuur. Het meest bekende quantumcryptografische protocol is Quantum Key Distributie (QKD), waarmee twee gebruikers gezamenlijk via een quantumlink (een point-to-point quantumnetwerk) een sleutel genereren, welke vervolgens gebruikt wordt om gegevens te versleutelen op de huidige manier. Op dit moment is het erg moeilijk om op een volledig veilige manier encryptie- en decryptiesleutels uit te wisselen: altijd kan er iemand zijn die de sleutels in handen krijgt. Bij QKD wordt opgemerkt wanneer iemand anders de quantuminformatie heeft bekeken: uit de analyse achteraf blijkt dan dat er veel meer fouten in de sleutel zitten dan verwacht.[10]

Post-quantumcryptografie

Post-quantumcryptografie wordt gebaseerd op wiskundige problemen waarvoor (nog) geen quantumalgoritmes bestaan die deze kunnen kraken. Een misverstand dat vaak optreedt, is dat post-quantumcryptografie gebruik maakt van quantumtechnologie. Dat is niet zo: het is een vervanging van de huidige cryptografie, die werkt op klassieke computers. De uitdaging zit hem daarbij niet alleen in de nieuwe manier van versleutelen, maar ook in de praktische uitwerking daarvan.
In internationaal verband werken experts op het gebied van post-quantumcrypto samen aan de standaardisatie van deze technieken. Verwacht wordt dat de eerste post-quantumcryptosystemen binnen enkele jaren gestandaardiseerd zullen worden door het National Institute of Standards and Technology (NIST) in de Verenigde Staten.

Crypto-agility

Organisaties zullen meer en meer rekening moeten houden met het feit dat cryptografische methoden die nu nog veilig zijn, bij het toenemen van rekenkracht of door het ontdekken van kwetsbaarheden onveilig kunnen worden. Crypto-agility betekent dat bedrijven hun gebruikte cryptografiemethoden gemakkelijk kunnen aanpassen, wanneer dat nodig is. Dit kan bijvoorbeeld door hiervoor dwingend aandacht te vragen bij huidige IT-leveranciers. Samenwerking met publieke en private partijen die een rol spelen in het veilig en stabiel houden van het internet is belangrijk: denk bijvoorbeeld aan internet.nl.

Meer lezen

https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/data-sharing/quantum/

De financiële sector over de toekomst van encryptie: https://www.betaalvereniging.nl/actueel/achtergrondinformatie/in-het-kort/kwantumcomputers-in-het-kort/

Factsheet postquantum cryptografie van het nationaal cybersecurity center: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-postkwantumcryptografie

Crypto-agility: stelt een informatiesysteem in staat om zonder significante veranderingen in de infrastructuur te switchen naar een andere vorm van encryptie: https://en.wikipedia.org/wiki/Crypto_agility

Voor het testen van de veiligheid van de encryptie van uw internet-verbinding, mail- en webservers hebben overheid en bedrijfsleven internet.nl ingericht.

Thema:
Ethische, juridische en sociaal-maatschappelijke aspecten

De ontwikkeling van quantumtechnologie heeft niet alleen een technologische of economische impact, maar het heeft ook een ethische, juridische en sociale kant. Deze wordt samengevat met de term ELSA: *ethical, legal and societal aspects*.

Maatschappelijke vraagstukken

Voor de ontwikkeling en maatschappelijke acceptatie van quantumtechnologie zijn deze aspecten van groot belang. Net als iedere andere revolutionaire technologie roept quantumtechnologie vragen op. In de media verschijnen bijvoorbeeld geregeld artikelen over privacy en veiligheid. Het draait dan om de vraag wat er gebeurt wanneer er op termijn universele quantumcomputers zijn die bestaande encryptiesleutels kunnen breken. Dit is zeker een belangrijk maatschappelijk vraagstuk, waar al oplossingen voor worden ontwikkeld in het kader van post-quantumcryptografie, maar het is niet het enige

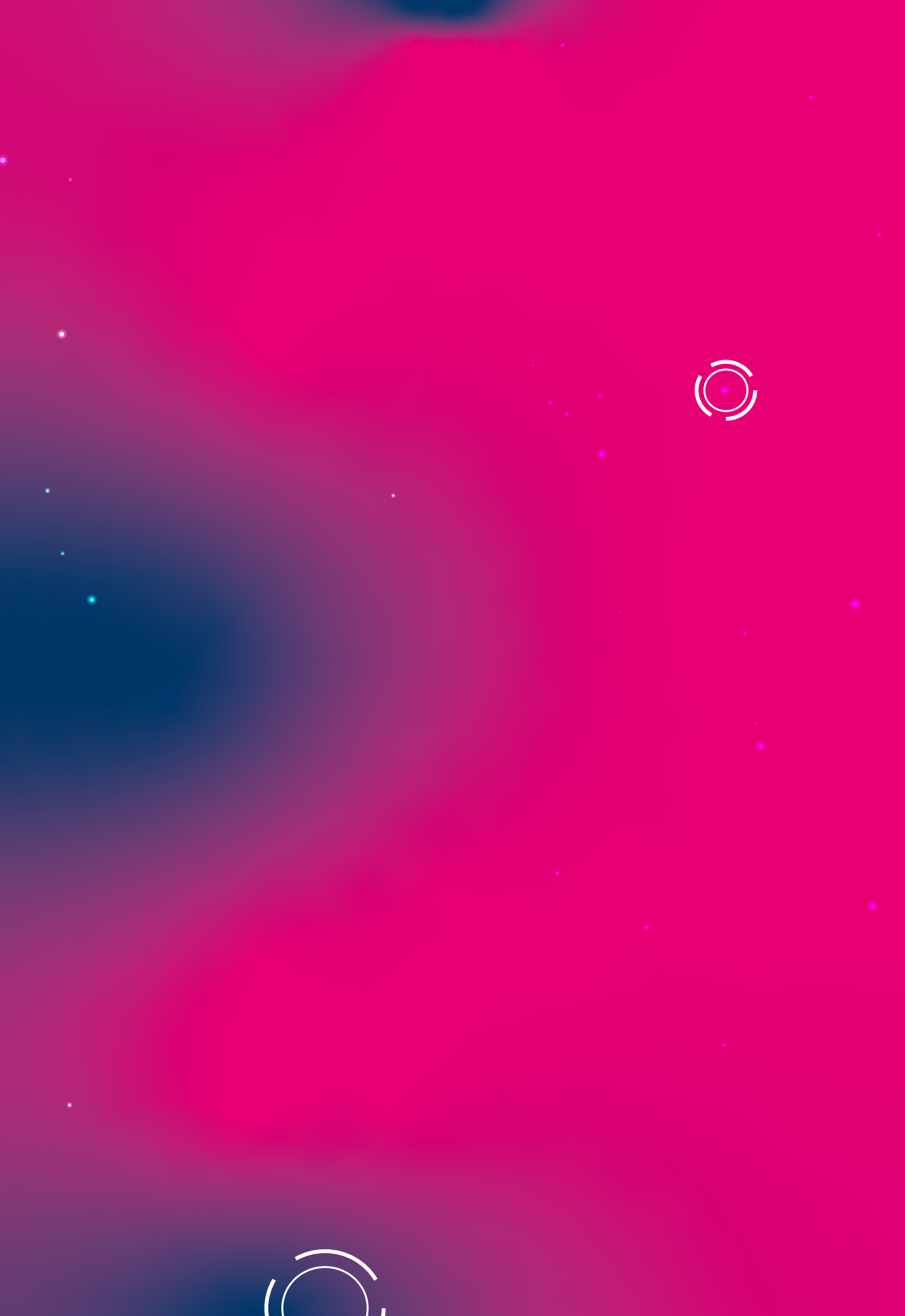
vraagstuk. Zo kan quantumtechnologie mogelijk ook leiden tot een grotere economische ongelijkheid (tussen have's en have not's), criminele netwerken die niet meer afgeluisterd kunnen worden ('is dat gewenst?') of drastisch veranderende geopolitieke verhoudingen (economisch, maar ook militair). Quantumtechnologie wordt daarom algemeen beschouwd als een strategisch zeer belangrijke asset; door landen, maar ook door bedrijven. Ook de rol van quantumcomputers in de ontwikkeling van artificial intelligence kan vragen oproepen.

Maatschappelijke dialoog

Al deze vragen vereisen antwoorden, nieuwe of aangepaste wetgeving, nieuwe businessmodellen en allerlei andere maatregelen. De Nationale Agenda Quantumtechnologie, die door een kernteam van Nederlandse universiteiten, instituten en bedrijven[11] is opgesteld en op 16 september 2019. is aangeboden aan de Nederlandse overheid, roept op tot het starten van een maatschappelijke dialoog over quantumtechnologie, waarin precies dit type vragen aan de orde komt. Het doel van deze dialoog is niet om allerlei doemscenario's te identificeren, maar juist om antwoorden te vinden en kansen te onderkennen. De technologie zelf is namelijk niet goed of slecht, maar de manier waarop we ermee omgaan bepaalt vaak hoe het uitwerkt. In de nationale dialoog staat dat besef centraal; deze beoogt brede acceptatie van de technologie te versnellen en alle betrokkenen in de maatschappij mee te nemen in de ontwikkelingen.

Meer lezen

ELSA staat niet voor niets volop in de belangstelling. Zo heeft het Quantum Vision Team van de TU Delft onlangs een magazine over de impact van quantuminternet gepubliceerd (https://www.tudelft.nl/2019/tu-delft/tu-delft-lanceert-publicatie-over-de-impact-van-quantuminternet/) en heeft het Quantum Software Consortium een Legal & Societal Sounding Board ingesteld dat de ELSA-aspecten onderzoekt van de verwerking van quantuminformatie (http://www.quantumsc.nl/ABOUT-QSC2/Legal-Societal-Board/). Over de Nationale Agenda Quantumtechnologie kunt u meer lezen op de websites van de betrokken organisaties, zoals TNO, NWO, QuTech, QuSoft en QT/e (https://qutech.nl/national-agenda-on-quantum-technology-the-netherlands-as-an-international-centre-for-quantum-technology/).



Thema:
De toppositie van Nederland

Hoewel de ontwikkeling van quantumcomputers, quantumnetwerken en quantumsensoren nog maar relatief kortgeleden gestart is, huisvest Nederland verschillende internationaal vooraanstaande organisaties en samenwerkingsverbanden die actief zijn op deze onderwerpen. Zij werken aan doorontwikkeling van de technologie enerzijds en aan het daadwerkelijk realiseren van use cases en toepassingsmogelijkheden anderzijds.

Internationale toppositie

Nederlandse universiteiten en kennisinstellingen hebben een vooraanstaande positie in een aantal wereldwijde ontwikkelingen van quantumtechnologie. Ze zijn koploper op het gebied van qubits, quantuminternet, quantumalgoritmes en post-quantumcryptografie. Uit een studie van Elsevier blijkt dat de citatie-impact van Nederlandse publicaties op het gebied van quantumcommunicatie, quantumcomputing

en encryptietechnologieën met scores tussen de 1,6 en 2,1 ver boven het wereldwijde gemiddelde van 1,0 ligt *(Elsevier Research Intelligence, 2018)*. Ook Europees gezien behoort Nederland tot de absolute top. Dit is een stevig bewijs dat er in ons land kwalitatief hoogwaardig onderzoek wordt gedaan. We zijn bovendien sterk in systems engineering en in het combineren van diverse technologieën tot werkende systemen; cruciaal voor innovatie.

Gespecialiseerde onderzoekscentra

De ruggengraat van dit unieke kennis- en innovatielandschap wordt gevormd door drie gespecialiseerde onderzoekscentra:

- Het Delftse QuTech, door de overheid aangemerkt als 'Nationaal Icoon' in 2014, is het gezamenlijke kennisinstituut van de TU Delft en TNO. Wereldwijd heeft QuTech een unieke positie. Dit wordt bevestigd door de excellente scores en bewoordingen in het internationale evaluatierapport dat onlangs werd gepubliceerd onder leiding van de in dit vakgebied gerenommeerde prof. dr. Robbert Dijkgraaf, directeur en hoogleraar van het 'Institute for Advanced Study', Princeton.
- QuSoft is het samenwerkingsverband van CWI, Universiteit van Amsterdam en de Vrije Universiteit en richt zich op het ontwikkelen en testen van nieuwe protocollen, algoritmes en toepassingen voor quantumcomputers.
- QT/e is het 'Center for Quantum Materials and Technology Eindhoven'. Hier werken de faculteiten Technische Natuurkunde, Wiskunde & Informatica en Electrotechniek van de TU/e samen aan bijvoorbeeld quantumsimulatoren, waarmee simulatie van complexe materialen en moleculen mogelijk wordt.

Daarnaast zijn de universiteiten van Leiden, Nijmegen, Utrecht, Twente en Groningen en de onderzoekinstituten TNO en AMOLF zeer actief op het gebied van quantumtechnologie. Onderling wordt nauw samengewerkt aan onderzoek en innovatie, waarbij ook nationale en internationale bedrijven zijn aangehaakt, zoals Microsoft, Intel, ABN AMRO, KPN, Delft Circuits, Qblox, Bosch en Shell. Een mooi voorbeeld hiervan vormt het Microsoft Quantum Lab, dat Koning Willem-Alexander in februari 2019

heeft geopend op de campus van de TU Delft. Wereldwijd zijn bedrijven als Intel, Google, Microsoft, IBM, Baidu, Ababa en Tencent bezig de eerste stabiele quantumcomputer te maken.

Nationale Agenda Quantumtechnologie

De positie als voortrekker en pionier wil Nederland behouden en verder versterken. Zoals Silicon Valley de aanjager en het middelpunt is geworden voor de halfgeleiderindustrie en haar toepassingen, zo streeft Nederland ernaar dat te worden voor quantumtechnologie. Deze ambitie wordt uitgesproken in de Nationale Agenda Quantumtechnologie, die op 16 september 2019 is gelanceerd: Nederland wil internationaal gidsland zijn voor quantumtechnologie en haar leidende positie behouden en uitbouwen. Deze nieuwe technologie moet high-tech industrie aantrekken en fungeren als banenmotor. Nederland wil een magneet zijn voor topwetenschappers en quantum engineers, en bovendien wil Nederland richting geven aan nieuwe quantumregelgeving en -ethiek. Langjarig onderzoek wordt in gang gezet. Een nationale dialoog over maatschappelijke en ethische vragen wordt gestart door ECP en partners. Met de Nationale Agenda profileert Nederland zich als een internationale quantumdelta, met de ambitie zich te ontwikkelen tot een bruisend quantumecosysteem dat een Europese en zelfs mondiale functie heeft. De Nationale Agenda Quantumtechnologie vat alle ambities samen in vier doelen:

- Verbinden van partijen in Nederland, samenwerken aan gezamenlijke doelen en uitdagingen;
- Versnellen van de economische impact van quantumtechnologie voor Nederland;
- Bijdragen aan de maatschappelijke opgaven van de overheid;
- Nederland positioneren als internationaal kennis- en innovatieknooppunt voor quantumtechnologie.

De agenda definieert vier actielijnen, en overkoepelend bovendien drie ambitieuze katalysatorprogramma's of KAT-programma's om de technologie versneld naar de markt en maatschappij te brengen via 'demonstrator'-faciliteiten. Deze KAT-programma's zijn:

- KAT-1 | Quantum Computing and Simulation;
- KAT-2 | Nationaal Quantum Netwerk;
- KAT-3 | Quantum Sensing Applicaties.

Deze KAT-programma's moeten de technologie tastbaar maken en eindgebruikers en onderzoekers ruimte bieden om ervaring op te doen met het gebruik ervan. Een nationaal loket zorgt ervoor dat iedereen die iets met de technologie wil, weet waar hij of zij terecht kan.

Meer lezen

De agenda is te vinden op: https://qutech.nl/national-agenda-on-quantum-technology-the-netherlands-as-an-international-centre-for-quantum-technology/ Toelichting is te vinden op de sites van de deelnemende instituten.

Toepassingsgebieden

In dit hoofdstuk komen concrete voorbeelden van toepassingen van quantumtechnologie aan de orde. Het hoofdstuk bevat ook verwijzingen naar bronnen waar u meer informatie kunt vinden.

Quantumcomputing

Deze paragraaf gaat in op de toepassingen van quantumcomputing en quantumsimulatie.

De ontwikkelingen naar een volwaardige quantumcomputer zijn in volle gang: in 2014 deed de eerste 9-qubits quantumcomputer berekeningen (in Santa Barbara). De eerste quantumcomputer die de 50-qubitgrens doorbreekt en die voor het eerst berekeningen kan uitvoeren die met de klassieke computer niet meer uitvoerbaar zijn, lijkt bij het verschijnen van deze publicatie gerealiseerd *(Sciencenews, 2019) (NRC, 2019)*

(Qusoft, 2019). NRC *(2019)* noemt in zijn berichtgeving dat voor het eerst een quantumcomputer (53 quantumbits) in 200 seconden een taak uitvoerde die op een supercomputer tienduizend jaar zou kosten. Verschillende partijen zitten elkaar vlak op de hielen in de race naar de eerste computer die krachtiger is dan de huidige supercomputers: met name Google en IBM.

De ontwikkelingen gaan snel, de verwachtingen zijn hooggespannen, maar wat zijn de toepassingsgebieden die binnen afzienbare termijn in het verschiet liggen? In deze publicatie gaan we nader in op vier van die mogelijke toepassingsgebieden:

- **Quantumchemie:** het op schaal kunnen analyseren en simuleren van fysisch-chemische processen. Het accuraat en snel simuleren van moleculen biedt enorme mogelijkheden, van nieuwe materialen tot gepersonaliseerde medicijnen en nog veel meer;
- **Optimalisatievraagstukken:** het parallel en in realtime kunnen uitvoeren van complexe, exponentieel schalende berekeningen om sneller tot betere (benaderingen van) uitkomsten te komen, met verstrekkende toepassingen in bijvoorbeeld de logistiek, het financiële systeem;
- **Machine learning:** het door vergaande parallellisatie veel sneller tot diepe inzichten kunnen komen die nu verborgen liggen in de enorme hoeveelheden ongestructureerde (en gestructureerde) data die we als maatschappij produceren;
- **Security:** het versleutelen, beschermen en transporteren van data op manieren die de beste supercomputers overstijgen. Dit onderwerp wordt geadresseerd in het thema 'Informatieveiligheid en cryptografie' aan het begin van deze publicatie.

Chemie

Voor de simulatie van chemische processen en materialen is veel rekenkracht nodig. Omdat het aantal moleculen dat interacties kan aangaan zo groot is, ontstaan al snel een enorm aantal mogelijke toestanden. Een klein verschil in zo'n toestand kan al veel uitmaken voor het betreffende materiaal en zijn chemische eigenschappen. De enorme hoeveelheid toestanden is met traditionele computers niet te berekenen. Aangezien quantumcomputers juist gebruik maken van dezelfde

quantumeffecten die aanwezig zijn in moleculen, kunnen deze computers in principe beter omgaan met de grote hoeveelheid en verscheidenheid aan toestanden. Dit maakt een quantumcomputer uitermate geschikt voor het uitvoeren van dit soort simulaties.

Als dergelijke simulaties mogelijk worden, heeft dat impact op verschillende industrieën. Zo zou het de ontwikkeling van efficiëntere batterijen mogelijk kunnen maken en kan het de ontwikkeling van nieuwe medicijnen versnellen, om maar even twee willekeurige voorbeelden te noemen.

De eerste quantumcomputers die op kleine schaal deze berekeningen kunnen uitvoeren, zijn nu al beschikbaar. Verwachting is dat de ontwikkeling van krachtiger computers snel zal gaan.

Bedrijven die zich richten op materialen, chemische stoffen of medicijnen doen er daarom verstandig aan op korte termijn de mogelijkheden van quantumcomputers te verkennen.

Met krachtiger (en minder foutgevoelige) quantumcomputers kunnen op termijn mogelijk ook de interacties tussen stoffen in het menselijk lichaam worden gesimuleerd, waardoor medicijnen op maat gemaakt kunnen worden. Verder kunnen zogenaamde metamaterialen gesimuleerd worden: materialen met eigenschappen die we niet kennen van de natuurlijke materialen en stoffen *(de Ingenieur, 2019)*: denk aan onzichtbare materialen, nog scherpere lenzen, materiaal dat geluid en licht op nieuwe manieren absorbeert of transformeert. Metamaterialen kunnen voor grote veranderingen zorgen op allerlei vlakken, van de auto-industrie (nieuwe frames) tot in de energiesector (kamertemperatuur-supergeleiders of veel efficiëntere zonnepanelen).

De vernieuwingen die dit met zich meebrengt voor de gezondheidszorg, energiesector en het materiaalonderzoek zullen doorwerken naar vele andere sectoren.

Een additionele reden om nu al toepassingsmogelijkheden te onderzoeken van quantumtechnologie, is dat de manier van denken en de algoritmen die worden ontwikkeld in dit vakgebied ook kunnen zorgen voor beter begrip van problemen die met klassieke computers worden berekend.

Optimalisatie

De rekenkracht van quantumcomputers kan naar verwachting gebruikt worden om complexe optimalisatievraagstukken beter te benaderen. Een paar voorbeelden van dergelijke vraagstukken, in verschillende sectoren:

- **In de financiële sector** kan rekenkracht gebruikt worden voor beter portfoliobeheer: het maken van keuzes in welke aandelen te investeren.
- **In de logistiek** kunnen het spoor- en wegennet beter worden benut door de rekenkracht in te zetten voor het in korte tijd berekenen van de effecten van het her-routeren van grote aantallen auto's of treinen.
- **In de retail:** winkeliers willen zo min mogelijk nee-verkopen en stemmen daar hun voorraad op af. De huidige algoritmen en computers kunnen dat niet realtime, waardoor winkels niet direct kunnen reageren op plotselinge gebeurtenissen. Dat geldt ook voor het aanvullen van de schappen: het beter en sneller verwerken van informatie over de individuele producten in de schappen en de klanten die deze kopen, kan bijdragen aan beter voorraadbeheer, beter gevulde schappen, en uiteindelijk minder verspilling van producten. Ook het voorspellen van het aantal bezoekers en wat ze gaan kopen is met de rekenkracht van de huidige computers niet nauwkeurig mogelijk: de modellen zijn nu, noodgedwongen, zeer beperkt en onnauwkeurig.

De hamvraag is wanneer quantumcomputers op deze optimalisatie-vraagstukken ingezet kunnen worden. De verwachting is dat de ontwikkeling van quantumalgoritmes die op enig moment operationeel toegepast kunnen worden in allerlei sectoren, nu al moet plaatsvinden: van retailers tot banken en van energieproviders tot overheidsinstanties. Parallel daaraan wordt gewerkt aan de ontwikkeling van technologie. De opbouw van nieuwe kennis in een 'quantumecosysteem van overheden, bedrijven en kennisinstituten' zal gelijke tred moeten houden met de ontwikkeling van de technologie.

Machine learning

De hoeveelheid data in de wereld neemt exponentieel toe. Zo ook onze mogelijkheden om deze data toe te passen. Bijvoorbeeld door het zoeken, vinden en leren van patronen in data. Denk aan hoe tech-platformen de volgorde van zoekresultaten bepalen voor specifieke gebruikers op specifieke momenten en hoe zij bijpassende advertenties tonen op een pagina. Ook kan op basis van data-analyse bepaald worden wat de volgende zet in een schaakspel is, wat de kans is dat een kredietnemer in betalingsproblemen komt en wat geleerd kan worden uit de eindeloze hoeveelheid mailtjes die binnenkomen bij de klantenservice.

Kenmerkend voor machine learning is dat wanneer de hoeveelheid data toeneemt, het aantal variabelen of dimensies (dat nodig is om patronen in deze data te beschrijven) exponentieel toeneemt. Het aantal variabelen groeit veel sneller dan de hoeveelheid data. Hierdoor worden computermodellen alsmaar complexer. Deep Learning helpt ons goed op weg om deze uitdaging het hoofd te bieden, via brute rekenkracht. Dat is hard nodig, omdat de huidige rekenmodellen zo complex zijn dat ze niet meer te bevatten zijn voor een mens. Door de verder toenemende hoeveelheid data zullen computermodellen in de nabije toekomst nóg complexer worden.

Quantumalgoritmes zijn één van de mogelijke volgende stappen. De tijd die het kost voor een quantumalgoritme om (sommige [12]) problemen op te lossen, groeit niet exponentieel, maar lineair met de toename van de hoeveelheid data (zie het kader 'rekenkracht' aan het begin van deze publicatie. Quantumalgoritmes zijn daardoor (in theorie althans) gemakkelijker te schalen tot hoger dimensionale problemen. Een voorbeeld hiervan is Grover's algoritme dat zoekt naar de beste match in ongestructureerde data. Grover's algoritme is kwadratisch sneller dan klassieke algoritmes en is daardoor in staat meer data door te nemen in dezelfde tijd – wat tot een beter resultaat leidt.

Het aantal onderzoeks- en toepassingsgebieden van quantumtechnologie in machine learning is groot en kent vele specialisaties, van power-gridoptimalisatie tot ziekteherkenning. Ook wordt er druk geëxperimenteerd

met hybride leeralgorithmes, waarbij intensieve vraagstukken door quantumcomputers worden uitgerekend en traditionele computers het 'eenvoudiger werk' doen.

Quantum sensing

De quantumverschijnselen kunnen ook gebruikt worden voor sensing: het nauwkeuriger registreren van signalen. Wereldwijd wordt onderzoek gedaan naar toepassingsmogelijkheden.

Radar en quantum technologie

Quantumradar maakt gebruik van verstrengelde quantumdeeltjes. Daarmee zouden stealth vliegtuigen en raketten mogelijk kunnen worden ontdekt. China en Canada zijn landen die flink investeren in de ontwikkeling van quantum-radarsystemen.

Meer informatie over een Canadees Defensie project: https://uwaterloo.ca/stories/quantum-radar-will-expose-stealth-aircraft.

In de South China Morning Post staat een onderzoek naar quantumradar: http://www.scmp.com/news/china/society/article/2121479/could-ghost-imaging-spy-satellite-be-game-changer-chinese.

Bodemonderzoek en quantum technologie

Quantumgravitatiesensoren kunnen net als andere gravitatiesensoren ingezet worden voor bodemonderzoek, bijvoorbeeld voor de detectie van grondwater, mijnen en tunnels. Op dit moment worden quantumgravitatiesensoren doorontwikkeld, zodat deze compacter en goedkoper geproduceerd kunnen worden.

Er zijn meerdere initiatieven op dit gebied. Een van deze initiatieven is het Europese project iSense. (https://www.isense-gravimeter.eu/119.html#c198). Ook zijn er al commerciële quantumgravimeters te koop (https://www.muquans.com/index.php/products/aqg).

Quantum GPS

Quantumtechnologie maakt GPS op verschillende manieren beter. Met quantumtechnologie zijn betere atoomklokken mogelijk, waardoor GPS of andere satellietgebaseerde systemen in staat zijn om de positie nauwkeuriger te bepalen.

Ook locatiebepaling zonder GPS zal nauwkeuriger worden: quantumaccelerometers en quantumgyroscopen spelen daarbij een belangrijke rol. Voertuigen als schepen, vliegtuigen en raketten maken gebruik van sensoren om op basis van de eigen snelheid en richting de actuele positie te bepalen: maar de huidige methoden zijn niet genoeg om als enige locatiebron te gebruiken. Met deze quantumsensoren belooft locatiebepaling zonder GPS nauwkeuriger te worden. Als deze quantumsensoren doorontwikkeld worden kunnen ze toepasbaar worden in kleinere voertuigen zoals auto's, en uiteindelijk misschien zelfs in de mobiele telefoon.

Voor meer informatie: *(TU-Delft, the Quantum vision team, 2019b)*.

Beeldvorming ('imaging')

Quantumverschijnselen kunnen gebruikt worden om de kwaliteit van beeldmateriaal te verbeteren. Een voorbeeld is het maken van MRI-scans: het kost veel rekenkracht en tijd om te bepalen wat de herkomst is van een foton dat is teruggekaatst door een bepaald weefsel. Met verstrengelde fotonen kan de herkomst van een teruggekaatste foton veel sneller worden bepaald en een scan sneller en beter worden uitgevoerd *(Economist, 2019b)*.

Quantuminternet

Toepassing

Via het quantuminternet kunnen quantumcomputers informatie uitwisselen met behoud van quantumeigenschappen.

Het Quantuminternet dat in ontwikkeling is bij QuTech en KPN *(TU-Delft, Quantum Internet, 2019a)* kan straks quantuminformatie bewijsbaar veilig transporteren door een netwerk van knooppunten heen. Om bewijsbaar veilig data uit te kunnen wisselen, wisselt het netwerk verstrengelde qubits uit met tussenliggende knooppunten. Dit knooppunt wisselt weer verstrengelde qubits uit met het volgende knooppunt zodat er uiteindelijk van begin tot eind een verstrengeling ontstaat. Dit wordt nu de basis waarop het netwerk bruikbaar wordt.

Als iemand inbreuk maakt op de verbinding, dan wordt dat zichtbaar: het aantal fouten in de overgedragen informatie is dan veel hoger.

De relatief korte afstand maakt de directe uitwisseling van qubits mogelijk van begin- naar eindpunt. Voor grotere netwerken zijn er quantumrepeaters: deze zijn echter nog in ontwikkeling. *(TU-Delft, Quantum Internet, 2019a)*.

De praktijk

QuTech en KPN werken samen aan het realiseren van een quantuminternet. *(TU-Delft, Quantum Internet, 2019a)*. Er is nog heel veel nodig om quantuminternet werkend te krijgen, zoals de installatie van knooppunten die bestaan uit quantumcomputers van enkele qubits. In een aantal jaren tijd breidt het netwerk zich uit tot vier locaties. Er is wetenschappelijk nog veel te ontdekken om dit mechanisme betrouwbaar te gebruiken.

Toepassingsgebieden

Op korte termijn is Quantum Key Distribution de belangrijkste toepassing van quantuminternet: het afspreken van geheime sleutels om informatie te versleutelen (zie in deze verkenning het thema 'Informatieveiligheid en cryptografie').

Om grotere afstanden te overbruggen wordt geëxperimenteerd met Quantum Key Distribution en een satelliet[13]. De reikwijdte kan dan doorschalen naar pan-Europees niveau. Geschat wordt dat hier tussen de vijf en tien jaar aan ontwikkeling nodig is, om zo'n satelliet in een baan om de aarde te brengen. De ontwikkelingen om een quantuminternet gebaseerd op de verstrengeling tussen qubits te maken, heeft naar schatting nog zeker tien jaar nodig. Deze methode heeft wetenschappelijke doorbraken nodig om verder te komen en de weg naar industriële toepasbaarheid moet nog beginnen.

Op den duur zal quantuminternet ook gebruikt kunnen worden om quantumcomputers samen te laten werken, omdat de quantumeigenschappen van de informatie met quantuminternet niet verloren gaat.

De IRTF (Internet Research Task Force) is bezig met het verkennen van de benodigde standaardisering van de protocollen die rond quantuminternet van belang kunnen zijn (IRTF, QIRG).

Meer lezen

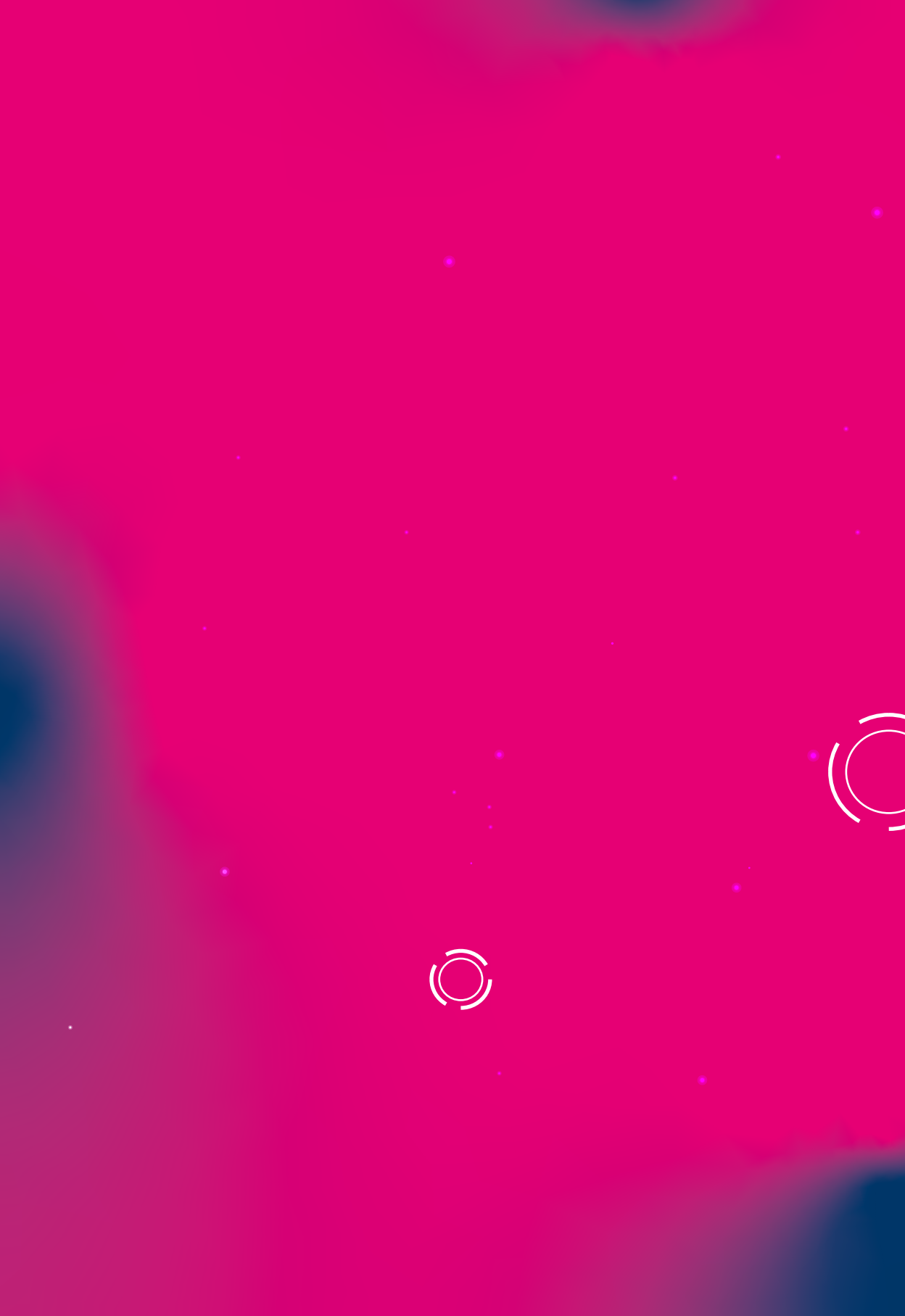
The Engineering of Software-Defined Quantum Key Distribution Networks, A. Aguado, V. López, D. López, M. Peev, A.Poppe, A. Pastor, J. Folgueira and V. Martín. IEEE Communications Magazine, Future Internet: Architectures and Protocols issue, 2019.

Quantum Internet Research Group (QIRG): https://datatracker.ietf.org/rg/qirg/about/.

Over Quantum Key Distribution: zie in deze verkenning het hoofdstukje ‘informatieveiligheid en cryptografie'.

Over een samenwerking tussen TNO, QuTech en de financiële wereld rond dit thema: https://www.tno.nl/en/about-tno/news/2019/6/quantum-technology-makes-secure-internet-banking-future-proof-abnamro-qutech-and-tno-space-in-collaboration/

Over Quantum Key Distribution: zie in deze verkenning het hoofdstukje ‘informatieveiligheid en cryptografie'.



Aanbevelingen

Aanbevelingen informatieveiligheid en cryptografie

Deze aanbevelingen zijn voor organisaties voor wie informatieveiligheid belangrijk is. Lees meer in: 'Thema: Informatieveiligheid en cryptografie' op pagina 17.

Aanbeveling 1

Onderzoek nu alvast de gevolgen van quantum voor informatieveiligheid. Een goede eerste stap is te onderzoeken of in de huidige organisatie digitale risico's gemitigeerd zijn door het toepassen van cryptografie. Als dat het geval is, dan is de volgende vraag hoe lang die informatie beschermd moet blijven. Hoe langer de beschermingstermijn, hoe

urgenter het wordt om in het licht van quantumtechnologie een mitigatieplan op te stellen. In de praktijk zullen veel organisaties gebruik maken van cryptografie en dus een onderbouwd antwoord moeten formuleren op de risico's die deze technologie met zich meebrengt. Voor het uitwerken van een mitigatieplan of het vaststellen van de urgentie is adequate informatievoorziening en voorlichting noodzakelijk.

Aanbeveling 2

Ga werken aan crypto-agility, ofwel: het verhogen van de flexibiliteit waarmee de gebruikte cryptografiemethode aangepast kan worden. Dit kan bijvoorbeeld door hiervoor dwingend aandacht te vragen bij huidige IT-leveranciers. Samenwerking met publieke en private partijen die een rol spelen in het veilig en stabiel houden van het internet is belangrijk: denk bijvoorbeeld aan internet.nl

Aanbevelingen ethiek, juridische en sociaal-maatschappelijke aspecten van quantum

Deze aanbevelingen zijn voor overheid, wetenschap en techniek-aanbieders. Lees meer in: 'Thema: Ethische, juridische en sociaal-maatschappelijke aspecten' op pagina 23.

Aanbeveling 3.

Faciliteer het voeren van een vruchtbare en goede maatschappelijke dialoog. Alleen door rond quantumtechnologie steeds hype van realiteit te scheiden, partijen te duiden en te verbinden én de balans te bewaken tussen mogelijkheden, ethiek en rechtsbescherming rondom data-gebruik en encryptie, zullen we meer en meer de vruchten gaan plukken van deze disruptieve technologie. Echter, om deze dialoog goed te kunnen voeren is voorlichting, kennis en onderwijs noodzakelijk.

Aanbevelingen quantum voor de Nederlandse economie

Deze aanbevelingen zijn voor overheid, wetenschap en technologie-bedrijven. Lees meer in: 'Thema: de toppositie van Nederland' op pagina 27.

Aanbeveling 4

Zorg voor brede kennisdeling en bewustwording. Kennisdeling is noodzakelijk, om organisaties, branches, bedrijven, MKB, ZZP'ers, onderwijsinstellingen en de samenleving als geheel voor te bereiden op de veranderingen die zich zullen voltrekken als gevolg van quantumtechnologie.

Aanbeveling 5

Richt één informatiepunt op waar Nederlandse bedrijven en organisaties terecht kunnen. Het is belangrijk dat bedrijven en organisaties adequate (en betrouwbare) informatie kunnen krijgen. Geef dit informatiepunt twee taken:

- het monitoren van de ontwikkeling en realisatie van quantumcomputers én het monitoren van de praktische toepasbaarheid van quantumalgoritmes die een risico vormen voor de informatieveiligheid;
- en deze informatie op een begrijpelijke manier beschikbaar maken voor Nederlandse organisaties.

Aanbeveling 6

Zorg voor de ontwikkeling van een ecosysteem van partijen en disciplines die nodig zijn om quantumtechnologie te ontwikkelen en toe te passen.

De ontwikkeling van quantumtechnologie is alleen mogelijk met gebruikmaking van andere technologieën in andere domeinen. Daarnaast is er nog een lange weg te gaan met betrekking tot het toepassen van de technologie. Quantumtechnologie vereist dat deeltjes op microniveau worden gemanipuleerd en bewerkt. Daarvoor is apparatuur nodig: om de lage temperaturen te bereiken die nodig zijn, maar ook veel hard- en

software om die processen te controleren. Daarnaast is hard- en software nodig voor de besturing en uitlezing van qubits. Het bedenken van nuttige toepassingen en implementeren daarvan is weer een andere discipline. Op al die terreinen moet nog een grote slag gemaakt worden. Daarom is het van belang dat er een 'ecosysteem' komt van overheden, bedrijven, kennisinstituten en maatschappelijke organisaties die elkaar weten te vinden en die elkaar versterken vanuit een gedeeld en gezamenlijk belang.

Aanbeveling 7

Zorg voor aansluiting bij en samenwerking tussen lopende programma's en initiatieven. Omdat voor quantumtechnologie ook de inzet en ontwikkeling van andere technologieën nodig is, die vaak op dezelfde plek ontstaan (denk aan universiteiten, kennisinstellingen en bedrijfsleven die bijvoorbeeld al bezig zijn met big data, artificial intelligence en blockchaintechnologie), dienen kansen voor synergie en versnelling te worden onderzocht.

Daarnaast is het cruciaal dat in Nederland kennis en vaardigheden omtrent quantumtechnologie worden ontwikkeld. Fundamentele en toegepaste wetenschap spelen hierin een belangrijk rol. Dit is het fundament onder nieuwe producten, diensten en toepassingen. Het onderwijs dient hierop in te spelen, zodat Nederland zijn koppositie kan vasthouden.


Verwijzingen

Aggarwal, R., Sharma, H., & Gupta, D. (2011). Analysis of Various Attacks over BB84 Quantum Key Distribution Protoco. International Journal of computer Applications, vol. 20 - no. 8 - 0975-8887. Opgeroepen op 09 30, 2019, van https://pdfs.semanticscholar.org/2000/99146ddfb8c2de14fb5698f0290d70d912c0.pdf

AIVD. (2019, 09 11). Bereid u voor op de komst van de quantum computer. Opgehaald van aivd.nl: https://www.aivd.nl/documenten/publicaties/2015/04/15/bereid-u-voor-op-de-komst-van-de-quantum-computer

Computable. (2019, 09 11). Ciso Jaya Baloo verruilt kpn voor avast. Opgehaald van computable: https://www.computable.nl/artikel/nieuws/security/6704822/250449/ciso-jaya-baloo-verruilt-kpn-voor-avast.html

de Ingenieur. (2019, 09 30). Bouwmethode voor metamaterialen. Opgehaald van deingenieur.nl: https://www.deingenieur.nl/artikel/bouwmethode-voor-metamaterialen

Economist. (2019a, 09 11). Quantum technology beginning to come on its own. Opgehaald van economist.com: https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own

Economist. (2019b, 09 11). Quantum Technology is beginning to come on its own. Opgehaald van economist.com: https://www.economist.com/news/essays/21717782-quantum-technology-beginning-come-its-own

Elsevier Research Intelligence. (2018, 06 01). Kwanitatieve analyse van onderzoek en innovatie in sleuteltechnologieën in Nederland. Opgehaald van Rijksoverheid.nl: https://www.rijksoverheid.nl/documenten/rapporten/2018/06/01/kwantitatieve-analyse-van-onderzoek-en-innovatie-in-sleuteltechnologieen-in-nederland

Emerce. (2019, 09 23). Nederland internationaal centrum quantumtechnologie. Opgehaald van emerce: https://www.emerce.nl/wire/nederland-internationaal-centrum-quantumtechnologie

NCTV. (2019, 09 11). Nationale veiligheidsstrategie. Opgehaald van NCTV.NL: https://www.nctv.nl/organisatie/nationale_veiligheid/nvs/index.aspx

NRC. (2019, 09 30). Klus van 10000 jaar in 200 seconden. Opgehaald van nrc.nl: https://www.nrc.nl/nieuws/2019/09/26/klus-van-10000-jaar-in-200-seconden-a3974728

NWO. (2019, 09 11). Quantummechanica voor een nieuw internet. Opgehaald van NWO: https://www.nwo.nl/onderzoek-en-resultaten/programmas/nwo/spinozapremie/interview-ronald-hanson-2019.html

Qusoft. (2019, 09 11). Software. Opgehaald van qusoft.org: http://www.qusoft.org/software/

QuTech. (2019, 09 23). National Agenda on Quantum Technology. Opgehaald van Qutech.nl: https://qutech.nl/national-agenda-on-quantum-technology-the-netherlands-as-an-international-centre-for-quantum-technology/

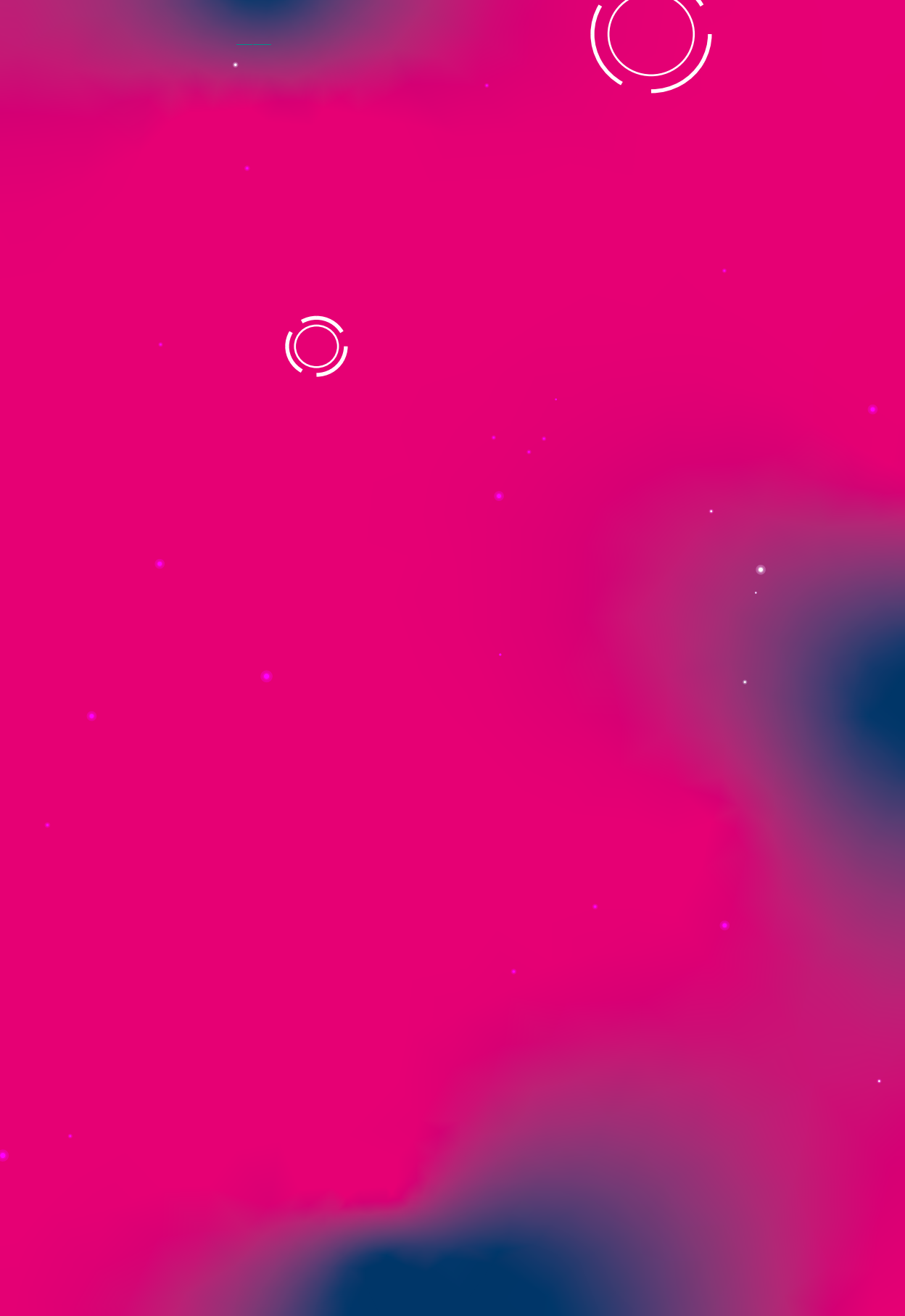
Sciencenews. (2019, `09 30). Rumors hint that google has accomplished quantum supremacy. Opgehaald van sciencenewslorg: https://www.sciencenews.org/article/rumors-hint-that-google-has-accomplished-quantum-supremacy;

TNO. (2019, 09 11). Quantumtechnologie. Opgehaald van TNO: https://www.tno.nl/nl/aandachtsgebieden/industrie/expertisegroepen/quantumtechnologie/

TU-Delft, Quantum Internet. (2019a, 09 11). KPN en Qutech slaan handen ineen om quantum internet te realiseren. Opgehaald van tudelft.nl: https://www.tudelft.nl/2019/tu-delft/kpn-en-qutech-slaan-handen-ineen-om-quantum-internet-te-realiseren/

TU-Delft, the Quantum vision team. (2019b, 09 11). Quantum magazine june 2019. Opgehaald van TU-Delft.nl: https://issuu.com/tudelft-mediasolutions/docs/quantum_magazine_june_2019

Tweakers. (2019, 09 11). De race naar een quantumcomputer. Opgehaald van tweakers.net: https://tweakers.net/reviews/5981/all/de-race-naar-een-quantumcomputer-wint-google-ibm-of-microsoft.html



Noten

1 De wetten op microniveau gelden ook op macroniveau, maar op macroniveau zijn effecten goed genoeg te beschrijven met klassieke mechanica. De wetten op macroniveau zijn limieten van de wetten op microniveau.

2 Vaak wordt gesproken over superpositie als de situatie waarin een deeltje "twee waarden tegelijkertijd heeft". Correcte formulering is dat het deeltje "in superpositie is van twee toestanden".

3 Er gelden op microniveau geen andere wetten dan op macroniveau. De wetten op microniveau gelden ook op macroniveau, maar op macroniveau zijn effecten goed genoeg te beschrijven met klassieke mechanica. De wetten op macroniveau zijn limieten van de wetten op microniveau.

4 Bij spin-qubits gaat het bijvoorbeeld over een linksdraaiende spin of een rechtsdraaiende spin. Bij supergeleidende qubits gaat het over de richting van de stroom. Bij quantum dots gaat het over de aanwezigheid van een elektron of niet. NV-centers werken met behulp van aangeslagen deeltjes welke de verschillende toestanden aangeven.

5 Correcter geformuleerd: bevindt zich in superpositie van twee toestanden.

6 Deze bewerkingen kunnen alleen plaatsvinden als data zich in een quantumtoestand bevinden: een dataset met nullen en enen, geschikt voor de klassieke computer, volstaat niet.

7 Er wordt onderzoek gedaan naar materialen die supergeleidend zijn bij kamertemperatuur: theoretisch gezien zou quantum computing dan ook mogelijk zijn bij kamertemperatuur.

8 Op internet.nl staat een testmethode om te testen of een computer onveilige versleutelingsmethoden ondersteunt.

9 De komst van de quantumcomputer heeft ook impact op symmetrische cryptografie. Door Grover's quantumalgoritme te gebruiken kan je deze cryptografie sneller breken. De impact is echter minder groot dan de impact van Shor's quantum algoritme op asymmetrische encryptie, omdat het risico gemitigeerd kan worden door de lengte van de gebruikte sleutels te verdubbelen. Op dit moment wordt niet verwacht dat deze encryptie vervangen hoeft te worden.

10 Quantum Key Distribution en de veiligheid van bepaalde methoden is onderwerp van onderzoek. Het BB84 schema (uit 1984) dat een vorm van QKD implementeert kan bijvoorbeeld op verschillende manieren succesvol worden aangevallen. (Aggarwal, Sharma, & Gupta, 2011)

11 TNO, QuTech, QuSoft, QT/e, NWO, Lorentz Instituut, AMS-IX, Techleap.nl en Microsoft

12 Niet ieder qauntumalgoritme is in staat een exponentiële groei van de rekentijd met de toename van de hoeveelheid data te reduceren tot een lineaire toename.

13 China en Oostenrijk hebben dit al gedaan, zie bv: https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/. De snelheid was echter heel laag.

Met medewerking van:

Capgemini IBM kpn Microsoft

Ministerie van Economische Zaken en Klimaat SIDN LABS TNO innovation for life TU Delft


Het essay 'Verkenning quantumtechnologie' is een initiatief van TNO en ECP | Platform voor de InformatieSamenleving, een onafhankelijk en neutraal platform waar overheid, wetenschap, bedrijfsleven, onderwijs en maatschappelijke organisaties publiek-privaat samenwerken aan en kennis uitwisselen over een verantwoorde vormgeving van onze digitaliserende samenleving. De inhoud van het essay is, in samenwerking met TNO, ECP deelnemers en leden van de ECP-werkgroep Quantum, tot stand gekomen om denk- en gespreksstof aan te bieden ter voorbereiding op een gezamenlijke toekomst met quantumtechnologie.

De digitale versie van het essay kunt u vinden op: https://ecp.nl/publicatie/essay-verkenning-quantumtechnologie/

www.ecp.nl

Met medewerking van: