Het quantuminternet

Over quantumcomputers hebben we het op deze site al vaker gehad. Maar wie “computer” zegt, denkt ook direct “internet”. Komt er in de toekomst ook een quantuminternet? En wat hebben we daaraan? Gastauteur Jonas Helsen, promovendus bij QuTech aan de TU Delft, beantwoordt deze vragen.

Afbeelding 1. Een quantuminternet?Via je toetsenbord verbindt het internet je met de hele wereld. Maar hoe wordt dat als we binnenkort met quantumcomputers gaan werken? Afbeelding: frankieleon.

“L”, “O”. Dit waren de twee letters die de toekomst inluidden. Om half elf, op 29 oktober 1969, stuurde promovendus Charley Kline, in een laboratorium in de universiteit van Californië in Los Angeles, dit korte berichtje via zijn computer naar een verbonden computer

in Stanford, zo'n 500 kilometer verderop. De intentie was om het woord 'LOGIN' te versturen, maar het systeem crashte halverwege. Desalniettemin zou dit systeem, ARPANET, snel uitgroeien tot het eerste volwaardige computernetwerk. ARPANET kan gezien worden als de eerste voorvader van het huidige internet, dat miljarden computers verbindt en misschien wel de spil van de moderne tijd is.

Terwijl Charley Kline zijn eerste letters de geschiedenis in stuurde, werkte aan andere kant van het Amerikaanse continent, aan de Columbia-universiteit in New York, Stephen Wiesner aan zijn ideeën. Wiesner was een fysicus die, als een van de weinigen in die tijd, geïnteresseerd was in de informatie-theoretische aspecten van quantummechanica. Ergens aan het einde van de jaren 60 kwam hij op het idee van 'quantum money': quantumgeld. Hij had het idee om 'bankbiljetten' te maken op basis van de eigenschappen van quantummechanische toestanden, meer specifiek het zogeheten no-cloningprincipe. Hiermee kon hij, in theorie, bankbriefjes maken die onmogelijk te vervalsen waren. Wiesner was zijn tijd ver vooruit en hij slaagde er initieel niet in zijn ideeën te publiceren. Gelukkig voor de wetenschap deelde hij die ideeën wel met zijn vriend Charles Bennett. Deze Bennet zou ongeveer 15 jaar later de eerste B in het onder quantumcryptografen wereldberoemde *BB84-protocol* zijn.

Dit protocol, dat Bennett in 1984 samen met Gilles Brassard ontwikkelde, gebruikt de eigenschappen van quantummechanische toestanden om cryptografische 'sleutels' te creëren die onmogelijk te stelen zijn. Deze sleutels kunnen bijvoorbeeld gebruikt worden om berichten zodanig te coderen dat ze alleen gelezen kunnen worden door anderen die ook de sleutel in hun bezit hebben. Dit quantummechanische 'sleutelverdelingsprotocol' is een van de belangrijkste ontdekkingen van de moderne cryptografie. Het enige probleem met dit protocol is het feit dat om een sleutel te verdelen tussen twee partijen deze partijen niet alleen de mogelijkheid moeten hebben om quantummechanische toestanden te creëren en uit te meten, maar ook om ze te versturen over lange afstanden. Deze noodzaak was de eerste motivatie voor het bouwen van een netwerk dat ook quantuminformatie kan verwerken: een *quantuminternet*.

Video: het BB84-protocol.Met het BB84-protocol kunnen boodschappen overgebracht worden zonder dat

iemand onderweg die boodschappen kan afluisteren.

Quantuminternet, wat is dat?

Het internet kan gezien worden als een grote verzameling computers die informatie uitwisselen. In beginsel bestaat deze informatie uit lange reeksen bits: nullen en enen. Een quantuminternet is precies hetzelfde, maar in plaats van uit computers bestaat het netwerk uit quantumcomputers en de informatie die deze quantumcomputers uitwisselen bestaat niet uit bits maar uit quantumbits of *qubits*. Meer informatie over wat deze qubits precies zijn en hoe quantumcomputers precies werken kan je vinden in de driedelige serie over quantumcomputers die Joris Kattemölle voor deze site schreef.

Het uitwisselen van qubits zorgt ervoor dat op een quantuminternet dingen mogelijk zijn die volstrekt onmogelijk zijn op een ‘klassiek’ (niet-quantum-) internet. Het bekendste voorbeeld hiervan is het al genoemde BB84 sleutelverdelingsprotocol. De wetten van de natuur zelf (in de vorm van het onzekerheidsprincipe van Heisenberg en het no-cloningprincipe) zorgen ervoor dat de sleutels geproduceerd door dit protocol niet te lezen zijn door een afluisterende partij. Hierdoor wordt wel eens gezegd dat het quantuminternet onhackbaar is. Maar er zijn natuurlijk nog andere dingen waar een quantuminternet goed voor is. Ideeën daarover zijn zo uiteenlopend als het verbeteren van de synchronisatie van atoomklokken – uiteindelijk ook quantummechanische objecten – of het kunstmatig vergroten van de capaciteit van telescopen via de verstrengeling van lichtdeeltjes die invallen op verschillende telescopen, tot meer esoterische taken zoals het verdelen van geheime informatie tussen verschillende partijen zodat het geheim alleen ontdekt kan worden als alle partijen samenwerken zonder dat een enkele partij (of kleine groep partijen) op zichzelf het geheim te weten kan komen.

Maar waarschijnlijk het belangrijkste voordeel van een quantuminternet is een zogenaamde ‘quantum cloud’. Binnen enkele tientallen jaren zullen we waarschijnlijk volwaardige quantumcomputers hebben. Helaas zullen deze computers in eerste instantie ongetwijfeld enorm groot en moeilijk te onderhouden zijn. Dit betekent dat er een wereld zal ontstaan waar een klein aantal spelers zich specialiseert in het aanbieden van quantumberekeningen ‘in de cloud’. Mensen met behoefte aan quantumberekeningen sturen dan instructies naar deze cloud, die vervolgens de instructies uitvoert en de resultaten terugstuurt. De opmerkzame lezer zal nu denken: ”Maar wacht even? Waarom heb je hier een

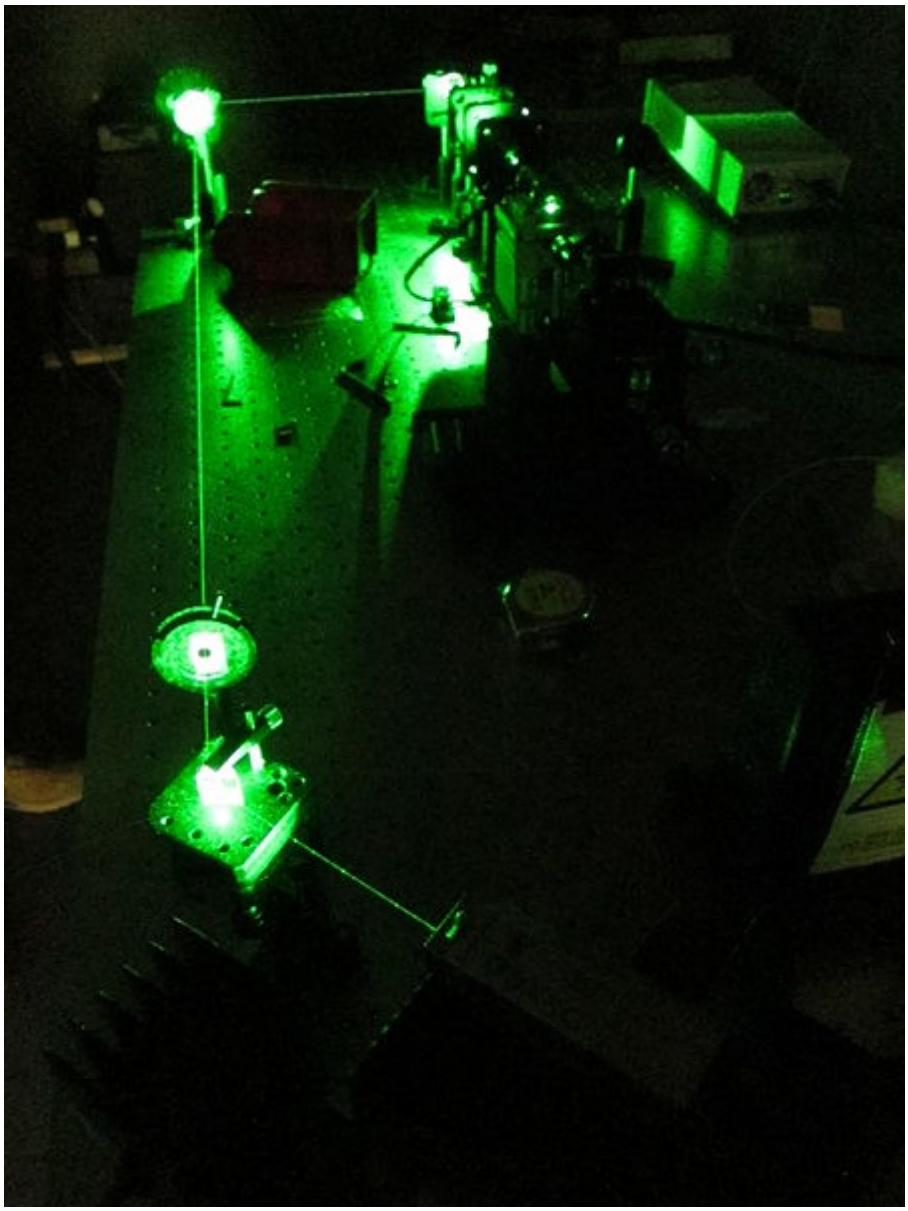
quantuminternet voor nodig? Zowel de instructies als de resultaten bestaan toch uit gewone, niet-quantuminformatie?" Dit is natuurlijk waar! Maar het wordt een stuk interessanter als de opdrachtgever niet alleen zijn of haar berekeningen wil laten uitvoeren maar er ook zeker van wil zijn dat (1) de berekeningen correct zijn uitgevoerd en (2) de data waarop de berekeningen gebaseerd zijn onzichtbaar zijn voor de beheerder van de quantumcloud. Dit laatste is bijvoorbeeld belangrijk voor grote bedrijven die absoluut zeker willen zijn dat de simulaties van hun nieuwste uitvindingen geheim blijven.

Als je een quantumberekening wil laten uitvoeren met deze voorwaarden van correctheid en geheimhouding, ben in het land van 'verifiable blind quantum computation' aangekomen. Dit soort geheime berekeningen is mogelijk, en zelfs vrij efficiënt. Maar je hebt er wel een quantuminternet voor nodig! De reden hiervoor is dat de protocollen voor 'verifiable blind quantum computation' alleen werken als de klant ook een quantumcomputer heeft. Deze quantumcomputer hoeft niet groot te zijn: een tiental qubits zou volstaan. Vanuit deze kleine quantumcomputer kan de klant dan kleine beetjes quantuminformatie uitwisselen met de grotere quantumcomputer in de cloud. Het hele proces is nogal ingewikkeld, dus dat zullen we hier niet in detail bespreken (zie bijvoorbeeld hier voor meer informatie), maar aan het einde ervan zou de klant het resultaat van zijn of haar berekeningen in handen hebben terwijl de computer in de cloud niets geleerd heeft over de data van de klant. De computer in de cloud kan natuurlijk proberen vals te spelen en de data te stelen, maar met wat slimmigheden die uiteindelijk gebaseerd zijn op het quantum-money systeem van Wiesner kan de klant dit soort valsspelerij altijd ontdekken.

Quantuminternet: wie maakt het?

Qubits manipuleren en opslaan is niet eenvoudig. Quantumtoestanden zijn zeer breekbaar en elke interactie met de buitenwereld zorgt voor een verlies aan informatie. Dit is een probleem als je een quantumcomputer wilt bouwen maar het is dubbel een probleem als je een quantuminternet wilt bouwen, waar de quantumtoestanden niet alleen opgeslagen moeten worden maar ook verstuurd over lange afstanden. Bij QuTech aan de TU Delft wordt aan een prototype van een quantuminternet gewerkt. Het plan is om in 2020 een quantumnetwerk op te bouwen dat vier steden in Nederland verbindt; Delft, Den Haag, Leiden en Amsterdam. Op dit netwerk kunnen dan applicaties zoals sleutelverdeling en 'blind verified quantum computing' getest worden. In dit netwerk zouden de qubits gevormd

worden door zogenaamde ‘nitrogen-vacancy centres’ of *NV-centra*. Deze qubits worden gemaakt door stikstofatomen te introduceren in een geordende structuur van koolstofatomen – beter bekend als diamant. Eenmaal geïntroduceerd in de structuur, neemt het stikstofatoom de plaats in van een koolstofatoom in het ‘raderwerk’ van de diamant. Een stikstofatoom heeft echter vijf valentie-elektronen waarmee het bindingen met andere atomen kan maken, terwijl de omliggende koolstofatomen maar vier valentie-elektronen hebben. Dit betekent dat het stikstofatoom een ongebonden elektron heeft dat vastzit in de diamantstructuur.



Afbeelding 2. Een optische tafel.Op optische tafels zoals deze wordt, onder meer bij QuTech in Delft, onderzoek gedaan naar NV-centra. Foto: Giorgio Brida.

Dit ongebonden elektron blijkt een perfecte qubit te vormen. Het mooie aan NV-centra als qubits is dat ze zeer sterk reageren op licht in het zichtbare spectrum. Dit betekent dat we standaard-lasers kunnen gebruiken om de qubit aan te sturen. Daarbovenop kan de qubit ook zijn quantumtoestand overdragen aan een lichtdeeltje of foton. Dit betekent dat de quantuminformatie in een NV-centrum kan worden verstuurd in de vorm van licht. Dit is nuttig, want na 50 jaar ervaring met optische telecommunicatie zijn ingenieurs erg goed geworden in het overbrengen van lichtdeeltjes over glasvezelkabels. Deze glasvezelkabels bevinden zich nu al overal in de grond waar ze informatie dragen voor het reguliere internet. Dit betekent dat er voor een quantuminternet met NV-centra geen nieuwe kabels gelegd moeten worden!

Er zijn natuurlijk nog veel moeilijkheden die overwonnen moeten worden voor het quantuminternet in Nederland echt van de grond komt. Een groot probleem is dat de glasvezelkabels in de grond geoptimaliseerd zijn om infrarood licht te transporteren. Het licht dat wordt uitgezonden door NV-centra is echter niet infrarood maar eerder groen, met ongeveer de helft van de optimale golflengte. Dit betekent dat de golflengte van de NV-fotonen moet worden omgezet naar infrarood. Dit moet echter gebeuren zonder de quantuminformatie te verliezen! Dat is geen eenvoudig proces. Daarbovenop verliezen glasvezelkabels, zelfs op een optimale golflengte, een bepaalde hoeveelheid fotonen per kilometer kabel. Dit verliesproces zorgt ervoor dat na een bepaald aantal kilometers de informatie in de kabel volledig verdwijnt. Dit proces is er natuurlijk ook voor de fotonen die klassieke informatie (voor het gewone internet) vervoeren. Hier wordt dit probleem opgelost door het gebruik van versterkers, speciale apparatuur die het klassieke signaal elke paar kilometer versterken zodat het zeer lange afstanden kan afleggen zonder aan kracht te verliezen. Een gelijksoortig systeem is echter onmogelijk voor quantuminformatie, juist vanwege het al eerder genoemde no-cloning principe. Dit betekent, ironisch genoeg, dat een van de eigenschappen die quantuminformatie zo nuttig maakt, er ook voor zorgt dat die informatie enorm moeilijk te transporteren is. Een oplossing voor dit probleem is de zogenaamde ‘quantumherhaler’; een apparaat dat gebruikmaakt van verstrengeling en het quantumteleportatieprotocol om het no-cloningprincipe te omzeilen en quantum communicatie mogelijk te maken over lange afstanden. Zo zie je maar, voor elk

quantumprobleem, is er een quantumoplossing.