Veilig communiceren met quantummechanica

We gebruiken tegenwoordig vrijwel dagelijks het internet voor het uitwisselen van persoonlijke informatie, het uitvoeren van banktransacties en het bijhouden van medische gegevens. Het afluisteren van zulke communicatie geeft mogelijkheden tot diefstal en inbreuk op de privacy [1]. Met quantummechanica kan ongemerkt afluisteren fundamenteel onmogelijk worden gemaakt. Het vakgebied quantumcommunicatie onderzoekt hoe dit op grote schaal toepassing kan vinden. Caspar van der Wal

Cryptografie voor internetverkeer

Als we het internet gebruiken voor zaken die geheim moeten blijven voor buitenstaanders gebruiken we een vorm van cryptografie (ook wel encryptie genoemd). Het meest bekende voorbeeld is wellicht een webbrowser die een 'https-protocol' gebruikt in plaats van een gewoon 'http-protocol'. Encryptie maakt communicatie onbegrijpelijk voor een afluisteraar door een mathematische operatie uit te voeren op de informatie (waar je over na kunt denken als een lange rij nullen en enen in digitale representatie) voor het wordt verzonden. De ontvangende partij weet dan hoe dit kan worden terugveranderd in de originele rij nullen en enen.

Een simpel voorbeeld voor zulke encryptie gaat als volgt. Stel dat je de PIN-code van je bankpas wilt versturen aan een partij die je vertrouwt en dat je PIN-code 2360 is. Als jij en de ontvangende partij beiden eenzelfde willekeurig getal beschikbaar hebben waar niemand anders van weet (in dit voorbeeld 3567), dan kun je dit willekeurige getal bij je PIN-code optellen en de som (5927) communiceren. De ontvangende partij trekt hier gewoon 3567 van af en heeft dan de PIN-code. Informatietheoretici kunnen bewijzen dat het onmogelijk is om af te luisteren als dit getal echt willekeurig is en je het maar één keer gebruikt. Het willekeurige getal is dan de *sleutel* (*key*) voor deze cryptografie en alle veilige communicatieprotocollen zijn in essentie een manier om voor een zender en ontvanger een geschikte sleutel beschikbaar te maken. Dit is goed om in gedachten te houden als we hieronder een quantumversie van cryptografie bespreken: het enige wat nodig is, is dat een zender en een ontvanger op afstand van elkaar een zeer groot willekeurig getal produceren dat zij beiden kennen, terwijl niemand anders dat getal te weten kan komen.

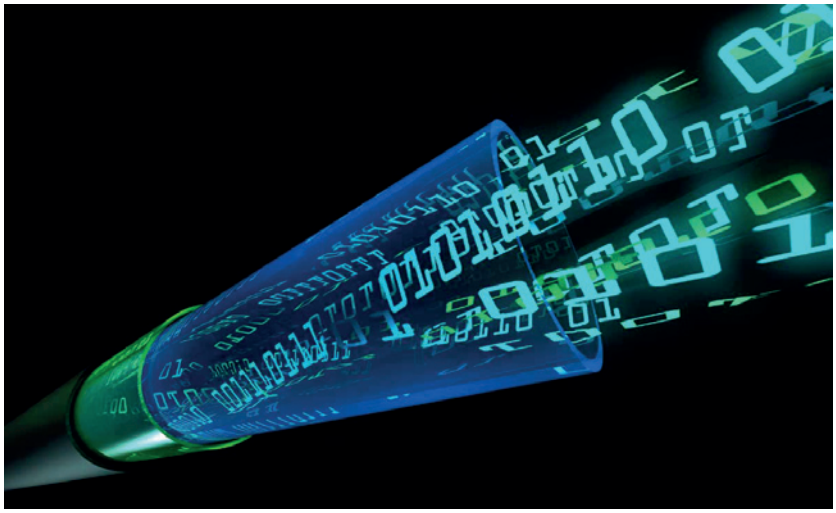
Voor beveiligd internetverkeer gebruiken onze webbrowsers nu vaak een vorm van encryptie die gebaseerd is op het RSA-algoritme voor *public-key* cryptografie (zie ook het artikel van Ronald de Wolf op pagina 183). De sleutel wordt hier gemaakt door in een slimme volgorde een paar getallen uit te wisselen. Dit zijn speciale getallen, die belangrijk zijn voor de wiskunde van het ontbinden van een getal in zijn priemfactoren.

De veiligheid van het algoritme is dan gebaseerd op het (sterke) wiskundige vermoeden dat 9749 x 7753 (vermenigvuldigen van twee priemgetallen) een makkelijk probleem is en het vinden van deze twee priemgetallen als alleen het product gegeven is een moeilijk probleem (in dit geval 75583997 – probeer maar). In de praktijk gebruiken de algoritmen veel grotere getallen. Er is echter (nog) geen wiskundig bewijs dat het vinden van de twee priemfactoren van 75583997 daadwerkelijk veel moeilijker is dan het doen van de vermenigvuldiging 9749 x 7753 en er is dus ook geen wiskundig bewijs dat de encryptiesystemen die we nu op het internet gebruiken veilig zijn. Sterker nog, er is wel geleidelijke (en voor encryptie zorgwekkende) vooruitgang onder wiskundigen die bestuderen hoe je zo efficiënt mogelijk een groot getal kan ontbinden in zijn priemfacto-

Caspar van der Wal (1971) studeerde aan de TU Delft en is daar ook gepromoveerd op onderzoek aan supergeleidende quantumbits. Na een postdoc op Harvard op het gebied van quantumoptica met atoomdampen is hij sinds 2003 verbonden aan het Zernike Institute for Advanced Materials van de Rijksuniversiteit Groningen. Zijn team doet onderzoek aan quantumcoherentie in vastestofdevices.

c.h.van.der.wal@rug.nl

ren (nog afgezien van het feit dat een grote quantumcomputer dit snel zou kunnen doen). Eén van de meest significante recente doorbraken was in 2006 (ook op leuke wijze gerapporteerd in het wetenschapskatern van *NRC Handelsblad* van 11 en 12 februari 2006). Een briljante wiskundige uit China vond toen een manier om veel gebruikte encryptiecodes te kraken in 2^{39} rekenstappen (een dag rekenwerk voor een laptop) in plaats van de 2^{64} rekenstappen die nodig waren voor de snelste methode die tot dan bekend was (ongeveer 2^{25} dagen rekentijd als je het op een laptop wilt doen). Dit is voorlopig opgelost door simpelweg grotere priemgetallen te gebruiken voor encryptie, maar het laat zien dat er behoefte is aan een encryptiemethode die veiliger is.



Artistieke weergave van qubits door een glasvezelkabel.

Quantumcryptografie

Quantummechanica kan hier helpen [2]. Encryptie die gebruik maakt van quantumfysica kan fundamenteel veilig zijn. En terwijl de realisatie van de meeste toepassingsvoorstellen in het vakgebied quantuminformatie nog in de laboratoriumfase zit (met experimentele groepen die misschien over tien jaar een doorbraak kunnen laten zien) werkt quantumcryptografie voor afstanden tot honderd kilometer al echt goed. De *roadmap* voor dit onderzoeksveld in de Europese Unie [3] noemt ook duidelijk dat grootschalige toepassing van quantumcommunicatie een stuk dichterbij is dan quantumcomputing. Sinds het begin van deze eeuw zijn er al enkele (kleine) bedrijven die de apparatuur en diensten verkopen voor quantumcryptografie en het wordt op enkele plaatsen al toegepast voor communicatie tussen banken in *financial districts*. Eén van de meest bekende bedrijven in dit veld is het Zwitserse bedrijf ID Quantique. Zij hebben een interessante website over hun producten en de onderliggende natuurkunde [4].

Quantumcryptografie gebruikt enkele van de meest fundamentele aspecten van quantumfysica om afluisteren bij communicatie onmogelijk te maken. Bij deze zogenaamde quantumcommunicatie moeten de twee partijen (traditioneel Alice en Bob genoemd) quantumtoestanden naar elkaar kunnen sturen. Om dit minder abstract te maken is het goed alvast te noemen dat de fysica die hiervoor veruit het meest geschikt is, bestaat uit optische pulsen die in glasfibers reizen. In mindere mate, maar even serieus, wordt onderzocht hoe het kan worden gerealiseerd met optische pulsen die door de lucht en de ruimte reizen voor quantumcommunicatie via satellieten [2].

Met glasfiber kun je quantumtoestanden versturen door optische pulsen te gebruiken die uit precies één foton bestaan. De quantumtoestand kan dan worden gedragen door de optische polarisatietoestand (quantumsuperpositie) $|\Psi\rangle = \alpha|H\rangle + \beta|V\rangle$ van dit foton, waarbij $|H\rangle$ en $|V\rangle$ de twee orthogonale lineaire polarisatietoestanden zijn, en α en β de waarschijnlijkheidsamplitudes (dit systeem is direct geschikt voor het BB84-voorbeeld uit het artikel van Ronald de Wolf op pagina 183). Een alternatief is om optische pulsen te gebruiken waarbij de quantumtoestand wordt gedragen als een quantumsuperpositie van de toestanden $|0_{fot}\rangle$ (geen puls) en $|1_{fot}\rangle$ (een puls van één foton). Dat is dus een puls die tegelijkertijd uit 0 en 1 foton bestaat. In beide gevallen is er fundamentele veiligheid omdat het onmogelijk is om een onbekende quantumtoestand te meten zonder deze ook te verstoren en voor pulsen met maar één enkel foton kun je maar één meetpoging doen. Hieruit is ook af te leiden dat het onmogelijk is om een kopie te maken van zo'n toestand terwijl het origineel behouden blijft (dit staat bekend als het *no-cloning theorem*).

Laten we communicatie met superposities van toestanden $|0_{fot}\rangle$ en $|1_{fot}\rangle$ verder als voorbeeld nemen. Hiervoor hebben Alice en Bob allebei een identiek quantum-twee-niveausysteem (denk aan een atoom) dat een enkel resonant foton in de toestand $|1_{fot}\rangle$ uitzendt als het van de geëxciteerde toestand $|e\rangle$ naar de grondtoestand $|g\rangle$ gaat en vice versa voor absorptie van zo'n foton. Voor communicatie van een superpositietoestand begint Alice met haar systeem in $|e\rangle$ en Bob met zijn systeem in $|g\rangle$. Alice moet nu haar systeem zo controleren dat de optische puls die eruit komt in gelijke mate de toestand $|0_{fot}\rangle$ en $|1_{fot}\rangle$ bevat (in praktijk is deze controle met lasers te realiseren door gebruik te maken van een derde niveau van het atoom). Het atoom van Alice blijft dan achter in een superpositie van $|g\rangle$ en $|e\rangle$. Als deze puls door een fiber naar Bob vliegt en daar volledig wordt geabsorbeerd door het atoom, zal dit atoom daarna ook in een superpositie van $|g\rangle$ en $|e\rangle$ zijn. Er gelden nu quantumcorrelaties tussen de systemen van Alice en Bob – de twee systemen zijn dan verstrengeld en zitten in een gezamenlijke quantumtoestand in een vorm als $(|e_A\rangle|g_B\rangle + |g_A\rangle|e_B\rangle)/\sqrt{2}$ (de indices geven hier Alice en Bob aan). Quantumverstrengeling is het fenomeen dat vooral bekend is van de Einstein-Podolsky-Rosenparadox (EPR). Als Alice nu meet of haar system in $|g\rangle$ of $|e\rangle$ zit, zal de uitkomst op willekeurige wijze een van de twee antwoorden zijn. Echter, als Bob daarna ook een meting doet zal hij vanwege de quantumcorrelaties met zekerheid het tegenovergestelde van Alice meten. Door dit vaak te herhalen kunnen Alice en Bob dus een lang willekeurig getal opbouwen.

Als een afluisteraar een meting doet aan zo'n optische puls zal dit de EPR-

Cryptografie is belangrijk voor een veilige overdracht van data.

correlaties tussen Alice en Bob verstoren. De afluisteraar kan proberen zijn acties onopgemerkt te houden door pulsen te meten en daarna snel pulsen door te sturen die overeenkomen met zijn meetuitkomst. Toch zal dat de correlaties verstoren, omdat meten aan een superpositietoestand geen volledig inzicht geeft in de toestand voor het meten. Alice en Bob kunnen dus merken dat er afgeluisterd wordt. Ze doen dit door na het versturen van veel toestanden op willekeurige plekken in de reeks een aantal bits aan te wijzen die ze gebruiken voor controle van de correlaties (dit kunnen ze openlijk per telefoon bespreken omdat ze deze bits niet voor de sleutel gaan gebruiken). Als dit aantal controlebits groot is (zeg een aantal N) dan is de kans dat ze niet ontdekken dat de correlaties verstoord zijn $(1/2)^N$ en kan dus exponentieel klein worden gemaakt. Let wel, ze ontdekken dit dus terwijl ze een sleutel proberen te maken, dus voordat de echte boodschap zal worden verzonden. Het echte protocol is overigens één slag complexer dan de beschrijving hier: de veiligheid bewijzen vereist een zogenaamde Belltest van de correlaties. Dit staat bekend als het DLCZ-protocol (de afkorting verwijst naar de vier auteurs van het artikel) [2].

Onderzoek

Quantumcryptografie is dus ideaal voor veilig communiceren. Welk onderzoek vindt nu plaats om dichter bij toepassing op grote schaal te komen? Voor het BB84-protocol zijn al systemen op de markt. Het plaatsen van zo'n systeem is echter nog omslachtig omdat er een directe en zeer stabiele fiberconnectie nodig is zonder tussenversterkers. Door verliezen in de fiber beperkt dit in praktijk de toepassingsafstand ook tot zo'n honderd kilometer. Verder zijn de bronnen voor het maken van pulsen met precies één foton nog verre van ideaal (men gebruikt nu vaak zeer zwakke laserpulsen, er is dan altijd een kleine component met twee fotonen in de puls en de veiligheid is hierdoor niet optimaal). Een bron die gegarandeerd nooit meer dan een enkel foton afgeeft is een enkel los atoom in de geëxciteerde toestand. Echter, een los zwevend atoom laat zich moeilijk controleren en de straling die het afgeeft gaat alle kanten op en laat zich moeilijk efficiënt een fiber insturen. Onderzoek richt zich daarom op vaste-stofdevices, bijvoorbeeld optisch actieve quantumdots of defecten in kristallen. De eerste experimenten waren hier vaak op 4,2 K, maar er worden steeds meer systemen ontdekt die goed werken op kamertemperatuur [5]. Op soortgelijke wijze zijn de detectoren voor de pulsen nog verre van ideaal. De detectie-efficiëntie moet hoog zijn en het garanderen van de veiligheid gaat beter als de detector ook het verschil kan zien tussen een puls met één foton en met twee fotonen [2].

Het mooie van het DLCZ-protocol is dat het wél geschikt is voor afstanden groter dan honderd kilometer: de quantumcorrelaties van opeenvolgende segmenten van honderd kilometer kunnen worden doorgekoppeld. Het is hier echter wel nodig dat de quantumsystemen bij elk begin- en eindpunt behoorlijk lang ongestoord in een quantumsuperpositietoestand kunnen blijven zitten (minstens L/c, waarbij L de communicatieafstand is en c de lichtsnelheid, dit is 10 ms voor $L = 3000$ km). Spintoestanden in vaste stof zijn hier het meest geschikt en recent zijn systemen ontdekt waarbij de quantumtoestanden van spins overtuigend langer leven dan 10 ms – zelfs bij kamertemperatuur [6]. Het team van Ronald Hanson in Delft heeft afgelopen jaar voor het eerst de quantumverstrengeling van spins in twee vaste-stofdevices op afstand aangetoond met defecten in diamant (zie ook *NTvN*, november 2013). Onderzoek in mijn eigen team richt zich erop dergelijke experimenten robuuster te maken, dat kan door met ensembles van defecten te werken in plaats van enkele defecten [7]. Dit vakgebied is dus volop in beweging om een nuttige toepassing van quantuminformatie op grote schaal beschikbaar te maken.

Referenties

1 Seth Lloyd, *Privacy and the Quantum Internet*, *Scientific American* (2009) 80.
2 Zie bijvoorbeeld het recente overzichtsartikel van A. Ekert en R. Renner, *Nature* **507** (2014) 443.
3 http://qurope.eu/content/Roadmap (Version 1.8, February 2013).
4 www.idquantique.com.
5 S. Castelletto , B. C. Johnson, V. Ivády, N. Stavrias, T. Umeda, A. Gali en T. Ohshima, *Nature Materials* **13** (2014) 151.
6 K. Saeedi,S. Simmons, J.Z. Salvail, P. Dluhy, H. Riemann, N.V. Abrosimov, P. Becker, H.-J. Pohl, J.J.L. Morton en M.L.W. Thewalt, *Science* **342** (2013) 830.
7 S. Onur en C. van der Wal, *NTvN* **78-07** (2012) 231.