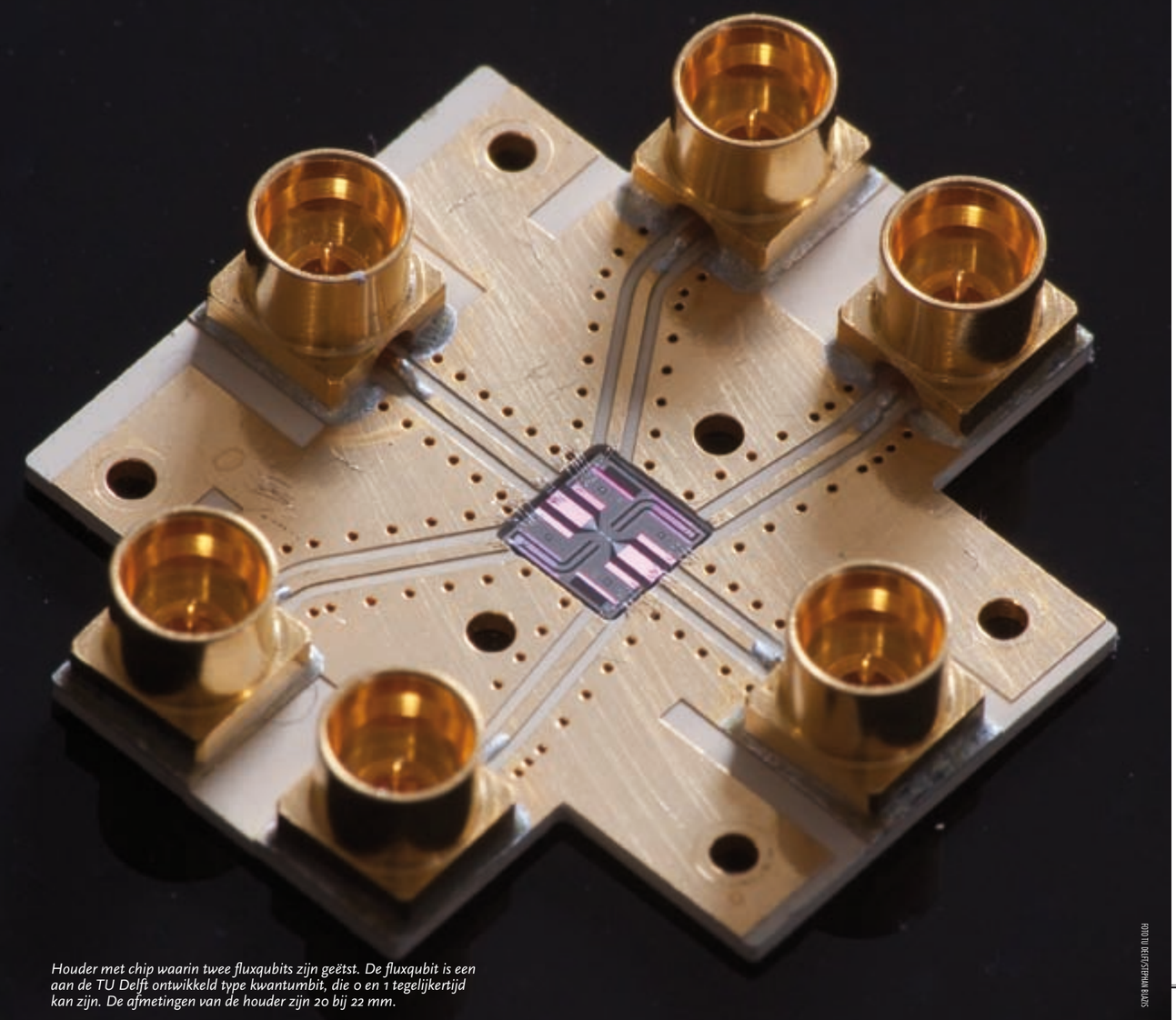
Onbreekbare codekraker

Temmen van de fluxqubit



Houder met chip waarin twee fluxqubits zijn geëtst. De fluxqubit is een aan de TU Delft ontwikkeld type kwantumbit, die 0 en 1 tegelijkertijd kan zijn. De afmetingen van de houder zijn 20 bij 22 mm.

FOTO TU DELFT/SIMON BLEIJS

TEKST DRS. TIMO KÖNNEN

Rekenen met kwantummechanische trucs gaat zo vlug dat het de duurste conventionele supercomputer op een slak laat lijken. De beveiliging van internet zou onder dit kwantumgeweld onmiddellijk bezwijken. Maar sinds David Deutsch in 1985 liet zien dat het kon, een kwantumcomputer laten rekenen, zijn er nog maar een paar toepassingen ontdekt. En de onderdelen van zo'n computer zijn tere kruidjes-roer-mij-niet, waardoor het bouwen van het apparaat een zaak van lange adem is gebleken.

De toch al zo geplaagde bankensector moet rekening houden met een nieuw soort probleem op de dag dat er kwantumcomputers in de winkels staan: de beveiliging voor telebankieren is dan op slag waardeloos geworden. Die systemen baseren hun veiligheid op de moeite die de bestaande computers hebben om de delers van een groot getal te vinden, en dat is nu net het soort opgave waar een kwantumcomputer wel raad mee weet. Binnen een minuut kraakt hij een getal van driehonderd cijfers, waar een gewone 'klassieke' computer aan honderd jaar rekentijd nog niet genoeg heeft. Voeg nog een paar cijfers toe en er ontstaat een getal dat geen enkele klassieke computer ooit aan zal kunnen, hoe veel sneller de chipfabrikanten hun producten ook nog zullen maken. De kwantumcomputer, die zo heet omdat hij rekent met behulp van kwantummechanische trucs, kraakt dat getal in een paar minuten. Dat zijn vaststaande feiten, want hoe een kwantumcomputer moet werken, is allang precies bekend. De verwezenlijking verloopt alleen wel wat moeizaam. De kwantumcomputer is nog altijd een foetus, en de dokters maken zich zorgen over zijn trage groei.

Het oorspronkelijke idee voor het nieuwe apparaat kwam in 1981 van de Amerikaanse natuurkundige en Nobelprijswinnaar Richard Feynman. Hij kwam op dat idee door het probleem waar onderzoekers tegen aan lopen als ze computers willen onderzoeken met computers. Het allerkleinste onderdeel van onze computer is een van de miljoenen transistoren op een chip. De stroompjes die daar doorheen lopen, zijn zo klein dat de elektronen zich vaak als golven gedragen in plaats van als afzonderlijke ladingdeeltjes. Die tweeslachtigheid is een typisch kwantummechanisch verschijnsel.

Wie op dit kwantumniveau in een computer wil afdalen, heeft een onderzoekscomputer nodig die op eveneens bijna-kwantumniveau kan werken, anders heeft die heel veel rekenstappen nodig en wordt de uitkomst nogal slordig. Daar begint de computerkat zich in zijn eigen staart te bijten. Feynman realiseerde zich dat het gereedschap fijner moet zijn dan het verschijnsel dat het wil vastpakken. Dat kon alleen maar een computer zijn die zélf een kwantumsysteem is. Zo'n computer is zo te programmeren dat hij materiaal in kwestie imiteert, en de uitkomst komt er dan haast vanzelf uitrollen.

David Deutsch, een theoretisch natuurkundige in Oxford, vroeg zich vervolgens af wat er met die computer nog meer zou kunnen. Waren er soms nog andere dingen die sneller konden? Hij stelde in 1985 een theorie op die precies beschreef wat op een kwantumcomputer mogelijk was. Ook gaf hij als eerste een voorbeeld van een berekening die op een kwantumcomputer inderdaad in minder stappen kon: zo'n computer kon in één stap bepalen of twee bits identiek waren (beide 0 of beide 1). Een klassieke computer heeft daar minimaal twee stappen voor nodig, want hij moet het ene bit eerst gelezen hebben om het met het andere te kunnen vergelijken. Het bewijs was geleverd, al was dit nog wel een erg simpel voorbeeld, waar niemand veel aan had. De bits van Deutsch' kwantumcomputer bestonden uit golven, die elkaar versterk-

BOUTU BREET

Een logische poort bestaande uit twee fluxqubits (links en rechts op de afbeelding), gemaakt met een atomic force microscoop.

ten als beide bits identiek waren, en elkaar uitdoofden als dat niet zo was. Interferentie tussen golven is altijd hét gereedschap van de kwantumprogrammeur gebleven.

Bijna tien jaar bleef het stil, terwijl kleine groepjes onderzoekers kauwden op manieren om de kwantumcomputer iets interessanters te laten doen. In 1994 kwam de doorbraak. De Amerikaanse wiskundige Peter Shor van AT&T Bell Laboratories werkte een methode uit om snel de delers (priemfactoren) van een getal te vinden, wat de kwantumcomputer in principe tot een bedreiging voor allerlei elektronische beveiligingssystemen maakt. Het leidde tot veel opschudding. Niet dat de wereld nu zat te wachten op het waardeloos worden van zulke systemen, waaronder beveiligde internet- en telebankierverbindingen, maar de hoop op andere doorbraken leek gerechtvaardigd. Er kwamen fondsen beschikbaar voor onderzoekers die wilden proberen een kwantumcomputer te bouwen. En twee jaar later vond de Indiase Amerikaan Lov Grover een algoritme met een aanzienlijk breder toepassingsgebied: een methode om in een ongeordende lijst snel een object te vinden. Grote databases zouden daar in bijna griezelig korte tijd mee zijn te doorzoeken. De kwantumcomputer als *supercrawler*!

Grote databases zijn in bijna griezelig korte tijd te doorzoeken

Maar daarna werd het weer stiller op het gebied van de rekenmethoden. ‘Het werken met interferentie maakt het lastig om goede algoritmen te bedenken’, verklaart prof.dr. Harry Buhrman, hoofd van de themagroep Quantum Computing van het Centrum voor Wiskunde en Informatica (CWI) en hoogleraar aan de Universiteit van Amsterdam. ‘Bovendien is de kwantumcomputer van nature nu eenmaal een apparaat met een beperkt toepassingsgebied. Van verreweg de meeste problemen kun je bewijzen dat hij ze niet sneller kan oplossen dan een gewone computer.’ Niettemin beloofden de al bekende toepassingen genoeg om het doen van verder onderzoek te rechtvaardigen. Wat het bouwen van de computer betreft ging het – en gaat het – in feite alleen nog om het allerkleinste onderdeel: de kwantumbit of qubit. De bits waar een klassieke computer mee rekent, zijn meestal condensatoren die twee spanningen kunnen hebben: de ene spanning staat voor ‘0’ en de andere voor ‘1’. Die twee mogelijkheden sluiten elkaar uit. De qubit is een variant op de bit die tegelijk 0 en 1 kan zijn. Aan het Kavli-instituut voor Nanowetenschap van de TU Delft maakt de groep Kwantumtransport bijvoorbeeld fluxqubits op een chip in de vorm van kleine circuits van supergeleidend metaal, waarin een stroompje van elektronen rondloopt. Rechtsom is 1, linksom is 0. De elektronen, een paar miljard stuks, maken bij elkaar 0,5 µA. Het voorvoegsel ‘flux’ verwijst naar het magnetisch veld dat zo’n rondlopende stroom opwekt, en dat wordt gebruikt om die stroom te meten. In de kwantummechanica is het mogelijk het stroompje in beide richtingen tegelijk te laten lopen, zodat de qubit zowel 0 als 1 is. ‘Het is dus niet zo dat de helft van de elektronen linksom gaat en de andere helft rechtsom’, waarschuwt prof.dr.ir. Hans Mooij, de oprichter van de onderzoeksgroep. ‘Elk elektron gaat in beide richtingen tegelijk. Het is in een superpositie van de twee bewegingsrichtingen.’ Deze spookachtige toestand is mogelijk doordat het elektron zich meer als een golf dan als een deeltje gedraagt. Een golf kan zijn opgebouwd uit twee ‘deelgolven’, die in tegengestelde richting reizen. Pas wanneer er een meting aan het stroompje wordt gedaan, is de qubit gedwongen te kiezen tussen ‘linksom’ en ‘rechtsom’: alle elektronen gaan zich weer als deeltjes gedragen en er komt alsnog een 0 óf een 1 uit de bus.

Dat het elektron tegelijkertijd linksom en rechtsom beweegt, is goed voorstelbaar door het circuit te beschouwen als een slotgracht met water. Als daar een bootje in plonst, dan rolt een golf zowel linksom als rechtsom. Maar als het bootje gaat varen, moet het kiezen tussen linksom en rechtsom. Golf en bootje zijn manifestaties van hetzelfde verschijnsel: energie. Zo kan een elektron zich ook manifesteren als golf en als deeltje.

In Delft kunnen ze de golftoestand nu, vijftien jaar na Shors doorbraak, nog niet langer dan 3 µs laten bestaan, en meer dan twee qubits tegelijk aansturen lukt ook nog niet. Dat moet veel langer en meer worden om met grote aantallen qubits berekeningen te kunnen doen.

WISSELWERKING

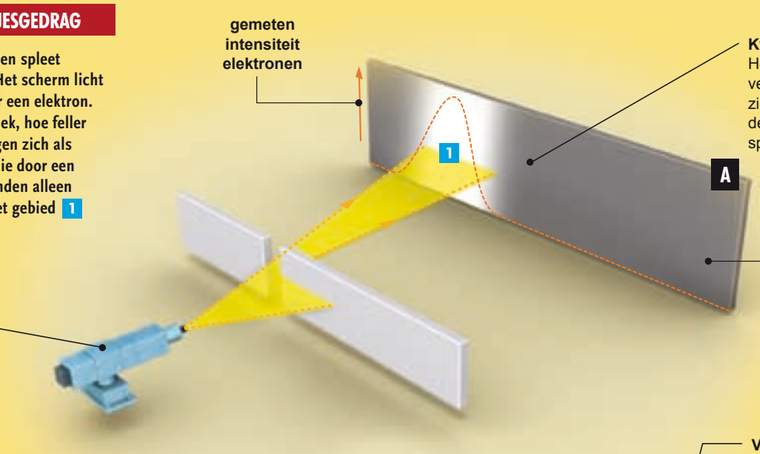
Dat de vooruitgang zo langzaam is, komt vooral doordat qubits extreem gevoelig zijn voor invloeden van buitenaf. Als ze ook maar een beetje met hun omgeving in wisselwerking treden, wordt hun superpositie (gelijktijdig voorkomen) vernietigd. Het is alsof de omgeving zegt: ‘Hoe zit dat nu met dat stroompje, draait het rechtsom of linksom?’ De elektronen moeten dan kiezen, ze gaan zich als deeltjes gedragen en weg is de kwantumeigenschap. Deze decoherentie is analoog aan wat er in het tweespletenexperiment (zie illustratie op pagina 21) gebeurt op het moment dat er detectoren bij de spleten worden geplaatst. Als één qubit uitvalt, is dat nog niet meteen een ramp: 1 op de 10 000 qubits mag tijdens een berekening aan decoherentie ten prooi vallen, zo toonde Shor in 1996 aan. De verstoorde qubits kunnen dan nog worden gecorrigeerd. Om die correctie mogelijk te maken moet het aantal qubits wel minimaal vijf keer zo groot worden. En dat maakt het weer moeilijker een computer te bouwen die groot genoeg is voor praktische doeleinden.

‘Het is een voortdurende strijd tegen decoherentie’, zegt Mooij. ‘Aan de ene kant wil je een qubit zo veel mogelijk loskoppelen van zijn omgeving, maar aan de andere kant wil je hem toch kunnen aansturen en uitlezen.’ Het aansturen

ELEKTRONEN ZIJN PUNTDEELTJES EN GOLVEN

A ENKELE SPLEET: DEELTJESGEDRAG

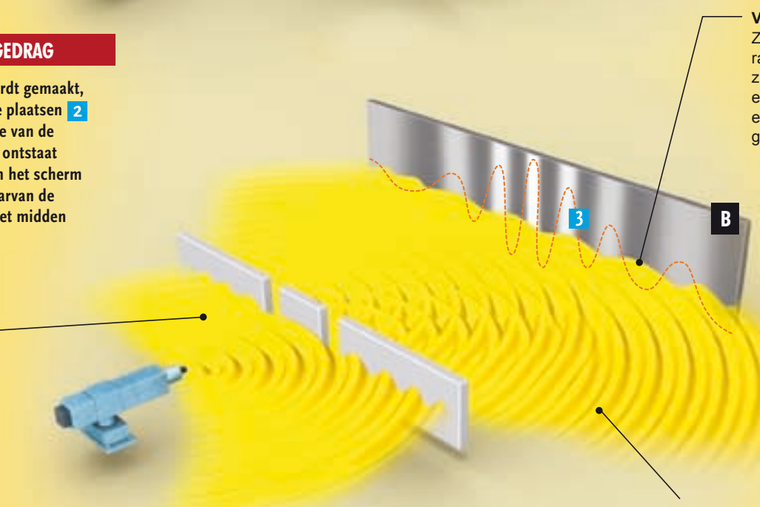
Een elektronenbron vuurt via een spleet elektronen af op een scherm. Het scherm licht op als het wordt getroffen door een elektron. Hoe meer elektronen op één plek, hoe feller het licht. De elektronen gedragen zich als deeltjes, alsof het kogels zijn die door een pistool zijn afgevuurd. Er belanden alleen elektronen op het scherm in het gebied 1 achter de open spleet.



Kwantumgedrag
Het is een typisch kwantumverschijnsel dat het elektron zich bij een enkele spleet als deeltje gedraagt en bij meer spleten (zie B) als golf.

B TWEE SPLETEN: GOLFGEDRAG

Als er een tweede spleet bij wordt gemaakt, is te verwachten dat er op twee plaatsen 2 op het scherm, in het verlengde van de spleten, elektronen inslaan. Er ontstaat echter over de hele breedte van het scherm een patroon van pieken 3 waarvan de intensiteit vermindert vanuit het midden naar buiten.



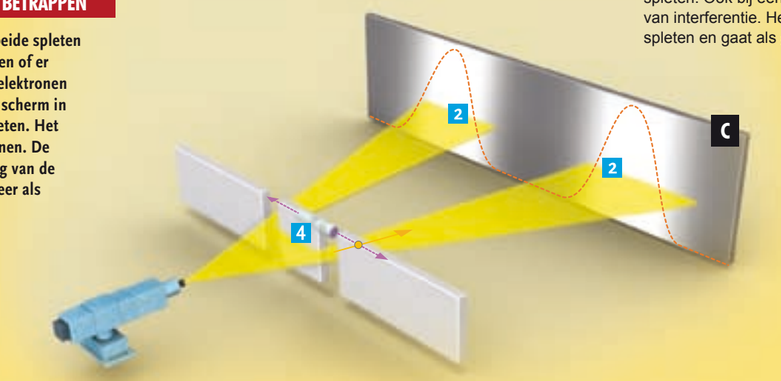
Van golf naar deeltje
Zodra de golf het scherm raakt, manifesteert het elektron zich weer als een deeltje met een exacte positie. Het ‘kiest’ een plaats in een van de witte gebieden.

Interferentie
Het piekenpatroon wordt verklaarbaar door aan te nemen dat een elektron zich gedraagt als een golf. Bij de twee spleten ontstaan twee nieuwe golven die elkaar versterken of uitdoven.

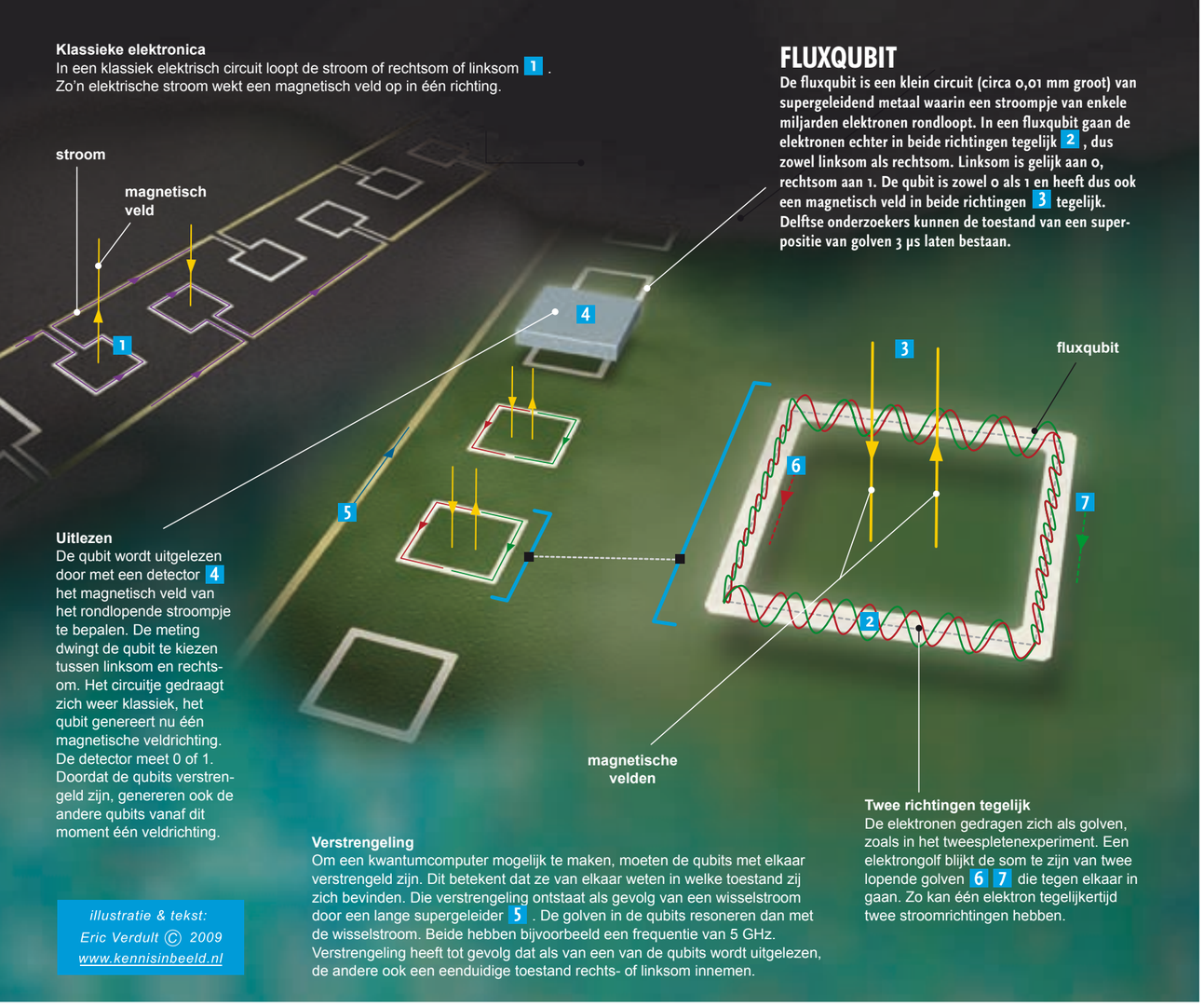
Elektron gaat door beide spleten
Zelfs als de bron maar één elektron afvuurt, belandt het elektron ergens op de volle breedte van het scherm en niet alleen achter de spleten. Ook bij één elektron is er dus sprake van interferentie. Het elektron ‘ziet’ beide spleten en gaat als golf door beide tegelijk.

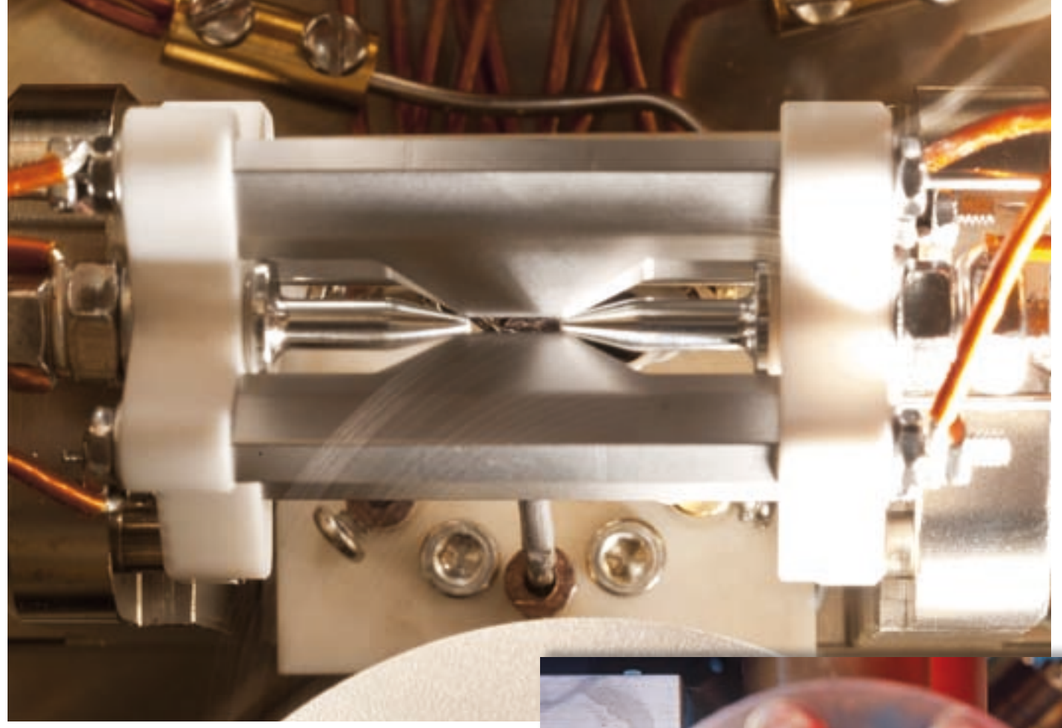
C GOLFGEDRAG NIET TE BETRAPPEN

De onderzoekers plaatsen bij beide spleten een detector 4 die moet meten of er een elektron voorbij komt. De elektronen belanden nu alleen nog op het scherm in de gebiedjes 2 achter de spleten. Het interferentiepatroon is verdwenen. De meting verstoort het golfgedrag van de elektronen waardoor ze zich weer als deeltjes gaan gedragen.



Detectoren 4
Elk elektron wordt door slechts een van de twee detectoren geregistreerd, nooit door allebei.





Ionenval uit Innsbruck. Calciumionen worden met magnetische en elektrostatische velden opgesloten in het kleine gebied in het midden. Manipulatie van de qubitionen gebeurt met laserlicht. De lengte van het metalen gedeelte bedraagt 3 cm. De inzet toont de ionenval in vacuümopstelling.

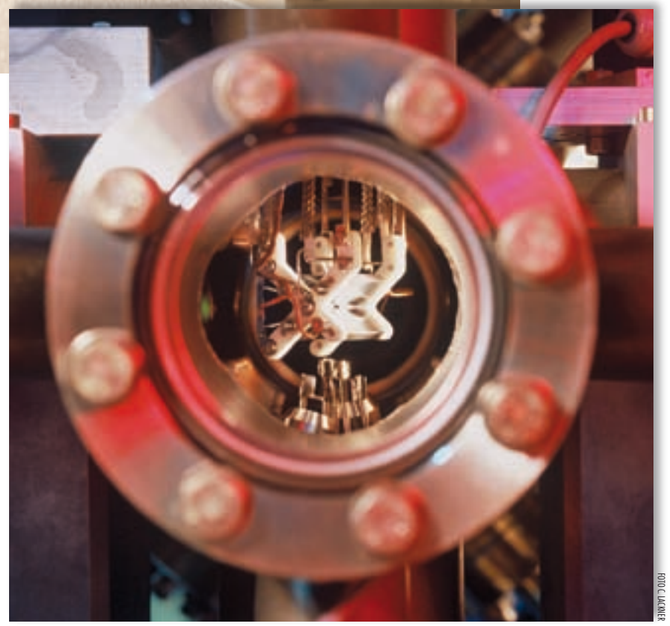


FOTO CHRISTIAN

De metingen gebeuren meestal door de magnetische flux van het rondlopende stroompje te bepalen. Dat vindt plaats met een zogeheten SQUID (Superconducting Quantum Interference Device), een zeer gevoelig detectortje dat in de chip is ingebouwd.

THERMISCHE RUIS

Voor het aansturen, het uitlezen en ook de toevoer van elektronen moeten er allerlei metalen nanodraadjes door een chip lopen. Dat zijn allemaal mogelijke beïnvloeders van de qubit, en dus ongewilde bronnen van storing en decoherentie. 'De stroompjes die we toevoeren, komen uiteindelijk van apparaten op kamertemperatuur. Ze zitten dus vol met thermische ruis', legt Mooij uit. Om daar iets aan te doen, koelen de onderzoekers de stroom in een aantal stappen af en gebruiken daarbij telkens een filter dat een deel van de ruis tegenhoudt. Dan nog zijn er allerlei kunstgrepen in het ontwerp van de chips nodig; zo moeten de draden elkaar bijvoorbeeld zo min mogelijk kruisen om wederzijdse beïnvloeding te voorkomen. 'De problemen zijn analoog aan die in de gewone halfgeleidertechniek, alleen is een qubit nog veel gevoeliger', zegt Mooij, die het concept van de fluxqubit tien jaar geleden samen met collega's van het Amerikaanse Massachusetts Institute of Technology (MIT) bedacht. De onderzoekers maken hun chips dan ook nog steeds zelf. 'Ik ben er meer dan 60 % van mijn tijd aan kwijt', schat promovendus ir. Pieter de Groot.

De Delftenaren hebben inmiddels complete beheersing over afzonderlijke qubits. Ze zijn in staat de fase van de rondlopende golven in te stellen, waardoor een qubit is te gebruiken als logische poort, een van de bouwstenen die een computer gebruikt om bewerkingen te doen. Ook kunnen ze speciale 'voorzichtige' metingen aan de magnetische flux doen, die een qubit wel dwingen te kiezen tussen 0 en 1, maar daarbij de golftoestand intact laten. Het mengsel van elektrongolven die linksom en rechtsom reizen, verandert dus in golven die allemaal dezelfde richting hebben, zonder dat de elektronen zich gebeurt met magnetische krachten. Een fluxqubit, zelf enkele honderdsten van een millimeter groot, zit op een chip van een paar millimeter. Die chip staat in het midden van een spoel die erbij vergeleken reusachtig groot is: een kleine decimeter in doorsnede. Het geheel bevindt zich in vacuüm en wordt op een temperatuur van 50 mK gehouden, om thermische ruis in de chip zo veel mogelijk te beperken. Door de spoel onder stroom te zetten kunnen de onderzoekers de qubit een vlak en constant magnetisch veld aanbieden. Door magnetische inductie wekt dit in de qubit een secondair stroompje van elektrongolven op, en omdat het om een supergeleider gaat, blijft het stroompje lopen wanneer de spoel weer wordt uitgeschakeld. De qubit is dan in zijn grondtoestand, die ook bijvoorbeeld 'linksom' of '0' is te noemen.

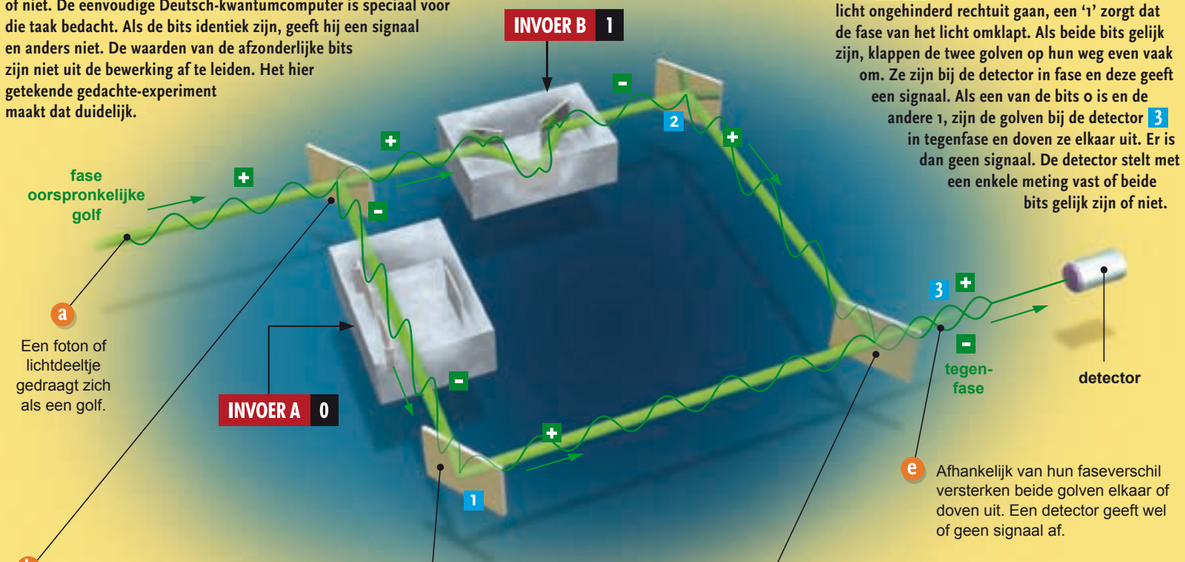
Dat is nog niet goed genoeg voor kwantumberekeningen: daarvoor moet de qubit immers 0 en 1 tegelijk zijn. Om dat te bereiken moeten de onderzoekers de qubit nog wat verder manipuleren. De spoel is daar een te grof middel voor. 'Het gebeurt met behulp van minuscule metaaldraden die in de chip zelf zitten', legt Mooij uit. Zeer snelle elektrische pulsen die daar doorheen worden gestuurd, bijvoorbeeld met een frequentie van 5 GHz, voeren energie naar de elektrongolven in de qubit. Het gevolg is dat ze steeds meer een superpositie worden van de grondtoestandgolf en een golf van hogere energie die de andere kant op loopt, de aangeslagen toestand ('rechtsom' of '1'). De frequentie van de pulsen is precies gelijk is aan die van de aangeslagen golf. Telkens als een golfpiek passeert, krijgt die een extra zetje mee van een nieuwe puls. Met elk nieuwe puls wordt de aldus aangeslagen golf wat krachtiger: zijn golfhoogte of amplitude neemt toe, terwijl die van de grondtoestand steeds verder krimpt. Volgens de wetten van de kwantummechanica betekent dit dat de kans om bij een meting een 1 te krijgen ook steeds groter wordt, en de kans op een 0 kleiner. Mooij, enthousiast: 'Op deze manier kunnen we precies bepalen hoe onze superposities gemengd zijn. Als we op het juiste moment stoppen, is het 50 % kans op 0 en 50 % kans op 1. Maar we kunnen het ook zo regelen dat het bijvoorbeeld 80 % kans op 0 is en 20 % op 1.' Tijdens een echte kwantumberekening kunnen zulke metingen overigens achterwege blijven: het is dan juist mogelijk de superpositie van golven te laten voortbestaan, zodat de qubit een beetje 0 en een beetje 1 blijft.

als deeltjes gaan gedragen. Dat is bijzonder, omdat bijna alle metingen aan kwantumsystemen, en zeker de standaard fluxmeting met een SQUID, in de woorden van Mooij 'verschrikkelijk destructief' zijn voor het golfgedrag. 'Een SQUID is net als een qubit een metalen supergeleidend circuit, waar zich een stroompje van elektronen in golfvorm doorheen kan bewegen', legt hij uit. 'Dat stroompje laat je steeds sterker worden. Op een gegeven moment kan het metaal dat niet meer aan, het verliest zijn supergeleidende eigenschappen en de stroom wordt een 'klassieke' stroom van elektrondeeltjes. Het punt waarop dat gebeurt, hangt af van de flux waaraan de SQUID blootstaat.' De waarde van die flux is dan ook af te leiden uit de kritische stroomsterkte. Maar de omschakeling naar klassiek

WAARDEN VAN BITS BEPALEN

Om te bepalen of twee bits (0 of 1) gelijk zijn of niet, moet een klassieke computer de waarden eerst kennen om ze te kunnen vergelijken. Hiervoor zijn dus meerdere handelingen nodig. Een kwantumcomputer kan de interferentie tussen golven gebruiken om in één bewerking vast te stellen of de bits identiek zijn of niet. De eenvoudige Deutsch-kwantumcomputer is speciaal voor die taak bedacht. Als de bits identiek zijn, geeft hij een signaal en anders niet. De waarden van de afzonderlijke bits zijn niet uit de bewerking af te leiden. Het hier getekende gedachte-experiment maakt dat duidelijk.

In de kwantumcomputer worden in twee 'schakelaars' A B twee bits ingevoerd. Een '0' laat het licht ongehinderd rechtuit gaan, een '1' zorgt dat de fase van het licht omklapt. Als beide bits gelijk zijn, klappen de twee golven op hun weg even vaak om. Ze zijn bij de detector in fase en deze geeft een signaal. Als een van de bits 0 is en de andere 1, zijn de golven bij de detector 3 in tegenfase en doven ze elkaar uit. Er is dan geen signaal. De detector stelt met een enkele meting vast of beide bits gelijk zijn of niet.



gedrag creëert een geweldige bron van storing vlakbij de qubit, die daardoor onmiddellijk uit zijn eigen kwantumtoestand wordt gestoten.

De 'voorzichtige' meting maakt eveneens gebruik van een SQUID, maar de bepaling van de kritische stroomsterkte gaat indirect, zonder een overgang naar klassiek gedrag op te wekken. 'We schakelen een condensator parallel aan het SQUID-circuit', legt Mooij uit. 'Daarmee kunnen we de frequentie van de elektrongolven in de SQUID verschuiven.' Uit de manier waarop de stroomsterkte daarop reageert, kunnen de onderzoekers vervolgens de kritische stroomsterkte afleiden en dus de magnetische flux, zonder dat de qubit er last van heeft. 'Met deze metingen hebben we een belangrijke voorspelling van de kwantummechanica bevestigd', benadrukt Mooij. 'Als we direct daarna opnieuw de uitslag meten, heeft die dezelfde uitkomst.'

Om een kwantumcomputer mogelijk te maken, moeten de qubits nauw met elkaar in verbinding staan. Die verstrengeling wordt bereikt door de qubits op een chip zo dicht bij elkaar te zetten dat ze direct elkaars elektromagnetische krachtveld voelen. De eerste stap in die richting, twee fluxqubits samen op een chip, is al enkele jaren geleden gezet. De Groot is een van degenen die werken aan het verder verbeteren van dit type chip. Met twee verstrengelde fluxqubits heeft de Delftse groep ook al een *controlled not*-poort gemaakt, een logische poort die de waarde van een bit omkeert (0 wordt 1 en 1 wordt 0) wanneer een andere bit 1 is. Daarmee zijn alle ingrediënten voor een werkende kwantumcomputer aanwezig. Informatici hebben namelijk bewezen dat zo'n computer met behulp van de twee genoemde typen poorten alle soorten berekeningen kan uitvoeren. 'Het blijft erg lastig om meer dan twee qubits te verstrengelen', zegt Mooij. Een chip met verscheidene qubits dicht tegen elkaar aan krijgt namelijk al gauw een ingewikkelde bedrading, met te veel kruisende lijnen die decoherentie veroorzaken. Om dat te vermijden werkt zijn groep aan een soort telefoonlijn waarover de qubits met elkaar kunnen 'praten'. Dit is een lange dunne supergeleider, waar het kwantummechanisch equivalent van een wisselstroom doorheen loopt. Een qubit in de buurt van die geleider raakt met het ding verstrengeld als zijn eigen golven resoneren met de wisselstroom. Koppeling en ontkoppeling kunnen dan worden bewerkstelligd door de frequentie van een van de twee aan te passen. 'Koppelen met één qubit lukt al', zegt Mooij.

Experimentatoren als Mooij graven als het ware het begin van een tunnel, die weer boven de grond moet komen op de plaats waar theoretici als Buhrman hun eigen begin aan het maken zijn. Die laatsten zoeken naar nieuwe manieren om met kwantumcomputers dingen uit te rekenen, maar dat is erg lastig. Het meeste is nog bereikt door de bestaande methoden zo veel mogelijk uit te melken. Zo borduurde het algoritme van Shor voort op het voorbeeldalgoritme van Deutsch. Ook de methode van Grover heeft als inspiratiebron voor allerlei nieuwe rekenschema's gediend. De meeste daarvan hebben echter nogal esoterische wiskundige doeleinden. Buhrman: 'We boeken vooruitgang, al moet ik toegeven dat het minder spectaculair is dan wat Shor en Grover deden. Maar zulke *blockbusters* komen in de toekomst wel weer.'

Een collega van Mooij in Delft is de Vlaming prof.dr.ir. Lieven Vandersypen. Rond 2000 was hij bij IBM Almaden in Californië betrokken bij de bouw van de eerste functionerende kwantumcomputer, die met zeven qubits werkte. Dat was net genoeg om met het algoritme van Shor een klein getal te factoriseren. 15 = 3 x 5, kwam er uit de berekeningen rollen. Geen wereldschokkend resultaat, maar wel een bewijs dat het kon. Hoe kan het dat Mooij en zijn medewerkers nu met moeite twee qubits koppelen, als IBM het in 2000 al met zeven qubits deed? Vandersypen: 'De techniek die we toen gebruikten, kernspinresonantie, was een doodlopende weg. Dat wisten we al toen we eraan begonnen, maar het was interessant omdat we er snel een werkende computer mee konden maken.' Kernspinresonantie is dezelfde techniek die MRI-scanners in ziekenhuizen gebruiken – een groot voordeel, omdat de onderzoekers konden profiteren van veel bestaande ervaring. De computer is bij deze aanpak een molecuul in een vloeistof, de qubits zijn de atomen. De atomen kunnen linksom of rechtsom om hun as draaien (de kernspin); de ene richting staat voor 0 en de andere voor 1 – en superposities staan voor beide richtingen tegelijk. 'Opschalen naar meer qubits is bij deze techniek haast niet mogelijk', legt Vandersypen uit. 'Niet alleen omdat je dan enorm grote moleculen zou moeten maken, maar meer nog omdat het meetsignaal met elke extra qubit de helft zwakker wordt.'

In een ionenval van het National Institute for Standards and Technology in het Amerikaanse Colorado, zijn vier berylliumionen betrapt in het gebied tussen de oranje elektroden. De verticale afstand tussen de elektroden is 0,2 mm.

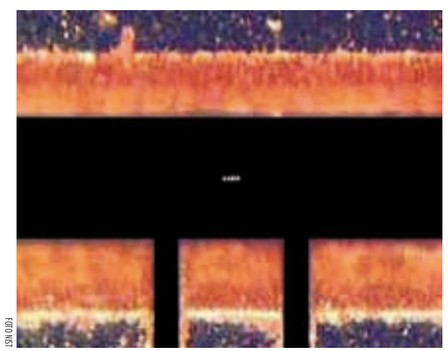


FOTO NIST

IONENVAL

Wie met qubits snel succes boekt, komt ook snel aan de grenzen van zijn mogelijkheden, lijkt het wel. Het gaat in elk geval ook op voor de techniek die op dit moment het meest ver is, de ionenvallen. Daarbij worden calciumionen (calciumatomen met een elektrische lading) opgesloten in een elektromagnetisch krachtveld. Ze kunnen dan twee energieniveaus hebben, die als 0 en 1 worden gebruikt. Hoewel er al verstrengelingen van acht qubits op naam van deze techniek staan en decoherentie veel minder snel optreedt, is het volgens Mooij een open vraag of de techniek de fluxqubits gaat verslaan. 'De fluxqubits bestaan minder lang, maar wij hebben in die tijd meer vooruitgang geboekt. Bovendien maken zij, onder wie de mensen van de Universität Innsbruck, hun ionenvallen nog altijd uit losse onderdeeltjes. Als ze verder willen opschalen, zullen ze net als wij chips moeten gaan maken. Dan moeten ze een grote stap terug doen, want dat hebben ze niet in de vingers.'

Met ionenvallen en fluxqubits zijn twee van de drie meest belovende technieken genoemd. Vandersypen werkt tegenwoordig aan de derde: de kwantumdots. Daarbij gaat het net als bij de fluxqubits om elektronen, maar hier is het er per qubit maar één. De groep van Vandersypen prikt ze met behulp van elektrische krachten vast in een 'stip' binnenin een chip – vandaar de term kwantumdot. Zo'n gevangen elektron blijft om zijn eigen as tollen (spin); de twee draairichtingen vormen de 0 en 1 van de qubit. 'Er is veel uitwisseling tussen Vandersypens groep en die van ons', vertelt Mooij. 'We werken immers met dezelfde materialen, kleine metaal- en halfgeleidersystemen.'

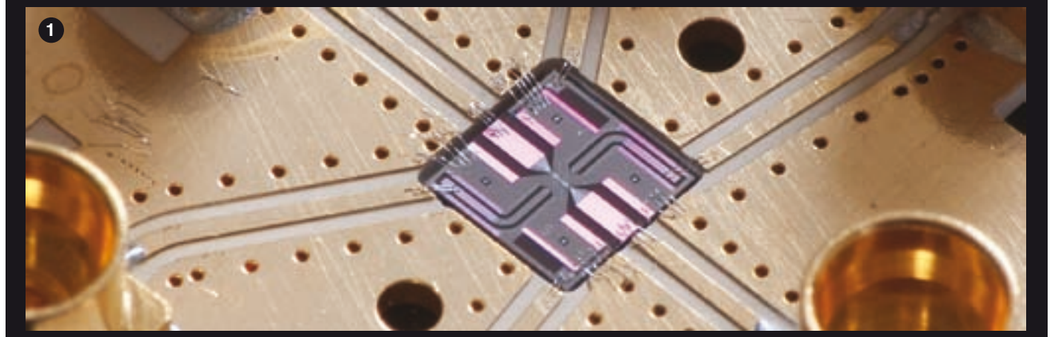
Ook voor Vandersypen is decoherentie het sleutelbegrip. 'Een gevangen elektron overlapt met ongeveer een miljoen atomen galliumarsenide, die zelf allemaal een zwakke kernspin hebben', legt hij uit. 'De fluctuaties daarin beïnvloeden de spin van het elektron, waardoor we na ongeveer 1 µs decoherentie krijgen. Intussen zijn wij en andere groepen erin geslaagd om die fluctuaties sterk te onderdrukken, zodat er minder decoherentie optreedt. Dat doen we door de kernspins mee te laten dansen op een wisselend uitwendig magneetveld.' Mocht dat uiteindelijk toch niet voldoende helpen, dan overweegt Vandersypen de overstap naar een kernspinloos materiaal, zoals grafeen of silicium. Maar dan moet zijn groep dat materiaal eerst weer in de vingers krijgen.

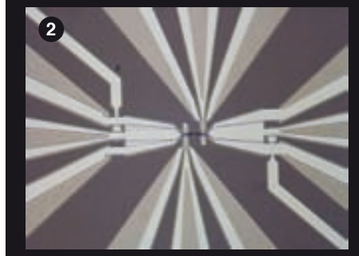
Het is hard ploeteren. Een kwantumcomputer met de duizenden bits die nodig zijn voor zinvolle toepassingen van de algoritmes van Shor en Grover, lijkt nog heel ver weg. Komt dat apparaat er eigenlijk wel ooit? 'Het komt er, als we het echt willen', antwoordt Vandersypen. Mooij is op het eerste gezicht minder optimistisch: 'Die algoritmen staan zo ver af van wat we hier doen. En dan de extra bits voor de foutencorrectie... Er zijn duizenden bits nodig, Mijn hemel!' Toch is hij ervan overtuigd dat er over een jaar of dertig kwantumcomputers van een of andere soort zullen werken. 'Alleen zullen de eerste toepassingen uit de hardware voortkomen. Het begrip van de kwantumwereld staat eigenlijk nog maar in de kinderschoenen. Wij kunnen nu echt kwantumsystemen op maat maken. We kunnen ze engineeren, we kunnen écht onderzoeken hoe ze zich gedragen. Daar zullen nieuwe dingen uit voortkomen die we ons nu niet kunnen voorstellen.' Zeker valt te voorspellen, zeggen zowel Mooij als anderen, dat kwantumcomputers hun nut zullen bewijzen bij het simuleren van andere kwantumsystemen, het oorspronkelijke idee van Feynman. Al vanaf het zeer haalbare aantal van dertig à vijftig qubits zijn ze in staat de klassieke rekenmonsters op dat gebied te verslaan. Daarvan zal onder meer de wereld van de vastestoffysica, met inbegrip van de fabrikanten van chips, profiteren. Bijvoorbeeld om de steeds verder geminiaturiseerde chips voor klassieke computers door te rekenen op kwantumeffecten.

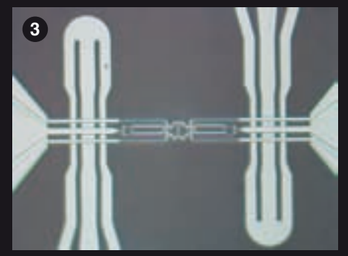
De visie van Buhrman is niet eens zo anders, al hoopt hij de algoritmen van Shor en Grover ooit echt aan het werk te zien. 'Het is als een steen waaraan je beitelt om het binnenste bloot te leggen', zegt hij. 'Je weet niet zeker of je daar ooit komt, maar de splinters die je losmaakt zijn zelf waardevol.' De worsteling met de algoritmen leidt tot een beter begrip van de kwantumwereld. Daar komt bij dat het nut van sommige resultaten die wereld overstijgt. Zo kon een stelling uit de 'klassieke' informatica jarenlang niet bewezen worden. De groep van Buhrman vertaalde hem in een stelling over de kwantumcomputer, en kon hem toen wel bewijzen. Het bewijs vertaalden ze vervolgens terug naar de klassieke computer.

Een fundamenteel resultaat van de groep is verder een wiskundige methode om aan te tonen dat een kwantumcomputer een gegeven probleem niet sneller kan oplossen dan een klassieke computer. Informatici wisten al dat dit voor verreweg de meeste problemen gold, maar het is prettig om het van een specifieke opgave te weten voordat wordt geprobeerd er een kwantumalgoritme voor te schrijven.

Zo hebben de onderzoekers laten zien dat de vraag of het aantal enen in een rij bits even of oneven is, door de kwan-







Op vier schalen, van groot naar klein, het nieuwste Delftse ontwerp van twee verstrengelde fluxqubits op een chip, gemaakt door ir. Pieter de Groot. Op foto 1 de chip, van 3,6 bij 3,6 mm, in zijn houder. De metaaldraadjes verbinden de onderdelen van de chip elektrisch met de buitenwereld.
Foto 2 is een uitvergroting van het middelste deel van de chip, ongeveer 1 mm breed, gemaakt met een optische microscoop. Van boven en onder komen twee aansluitdraden voor de 'antennes' waarmee de onderzoekers de toestand van de qubits kunnen manipuleren. De draden voor het signaal van de detectoren komen van links en rechts. De twee witte vlakken links en rechts van het midden zijn condensatoren die bij de detectoren horen. De qubits zelf bevinden zich, onzichtbaar klein, tussen de twee antennes.
Foto 3 is een verdere uitvergroting van het middendeel, breedte 0,11 mm. Op deze optische opname zijn de qubits zichtbaar: de twee tegen elkaar aan liggende gebiedjes in het midden zijn de uiteinden ervan. Het grootste deel van elke qubit ligt verborgen onder een rechthoekige structuur, de magneetveldetector. Dit is een zogeheten SQUID (Superconducting Quantum Interference Device), een zeer gevoelig apparaat dat in de chip is meegebakken.
Foto 4 is gemaakt met een elektronenmicroscoop. Links en rechts de uiteinden van de SQUIDS. De 'schaduwen' van de onderdelen zijn achtergebleven resten van het productieproces. Het is goed te zien dat een qubitcircuit een aantal kleine onderbrekingen bevat, zogeheten Josephson-juncties, die dienen om het golfgedrag van de elektronen af te dwingen.

tumcomputer niet wezenlijk sneller kan worden beantwoord. 'Zo'n bewijs kan je een hoop werk besparen. En omgekeerd, als het je niet lukt het bewijs te leveren, is dat een sterke aanwijzing dat het wel sneller kan', zegt Buhrman. Ten slotte is er de kwantumcommunicatie. 'We hebben manieren gevonden om ervoor te zorgen dat twee kwantumcomputers die samen aan een probleem rekenen, minder gegevens hoeven uit te wisselen dan twee klassieke computers.' Het idee is dat de kwantumalgoritmen die op beide computers draaien, ook in elkaars geheugen kunnen kijken. Ze kunnen bijvoorbeeld met 'Grover' snel elkaars database doorzoeken. De communicatie tussen klassieke computers kan daar ook weer efficiënter van worden, door ze via een kwantumextensie met elkaar te laten praten.

Zulke hybride systemen zullen waarschijnlijk de toekomst van de kwantumcomputer worden. Ze zijn namelijk ook veel beter in het corrigeren van foute qubits dan een losse kwantumcomputer. 'Dat ontmoedigende getal van maximaal 1 op de 10 000 fouten zingt nog steeds rond, maar het klopt allang niet meer', zegt Buhrman. 'Door kwantumberekeningen en -correctie af te wisselen met klassieke controlestappen kunnen we de fouttolerantie tot een paar procent opvoeren.' Dat moet een hoopgevend geluid zijn voor de ploeteraars in Delft en de rest van de wereld, die beetje bij beetje hun qubits stabieler proberen te maken.

Wanneer de kwantumcomputer er komt, wat zal dan zijn belangrijkste toepassing zijn? Buhrman reageert met een tegenvraag: 'Wat is de belangrijkste toepassing van de bestaande computers? Gamen? Tekstverwerking? Als je dat had gezegd tegen de bedenkers van de klassieke computer, hadden ze je vreemd aangekeken. Het is haast niet te voorspellen. Misschien wordt het simulatie, misschien Grovers algoritme, maar waarschijnlijk wordt het iets dat we ons nu niet kunnen voorstellen.' De toekomst van de kwantumcomputer is blijkbaar nog in een superpositie van mogelijkheden. Maar superposities mogen dan wat moeilijk te vatten zijn, dat het mogelijkheden biedt, staat vast. ●

INTERNETBRONNEN

www.ns.tudelft.nl/qt
De Delftse Quantum Transport Group, met uitleg over het onderzoek.

www.quantumoptics.at
De Quantum Optics and Spectroscopy Group van de Universität Innsbruck. De link Research leidt naar uitleg, met fraaie foto's.

www.cwi.nl/nl/quantumcomputers
Beschrijving van het onderzoek van de themagroep Quantum Computing van het CWI.

www.scottaaronson.com/blog/?p=208
Wetenschapsblog van de Amerikaanse informaticus Scott Aaronson met een gedetailleerde uitleg van Shors algoritme. Onder www.scottaaronson.com/democritus zijn de teksten van Aaronsons college 'Quantum Computing Since Democritus' aan de University of Waterloo te vinden.