



PROCESSOR MAAKT GEBRUIK VAN SUPERPOSITIE

SCHRÖDINGERS PC

Na decennia van dromen lijkt de revolutionaire kwantumcomputer over vijf à tien jaar echt realiteit te worden. De eerste werkende kwantumchips zijn inmiddels bruikbaar. Zowel aan de hardware- als aan de softwarekant moeten onderzoekers echter nog veel werk verzetten. Beide partijen hopen dat de ander het werk eenvoudiger maakt. 'We zijn op zoek naar een *killer app*.'

tekst Marc Seijlhouwer MSc



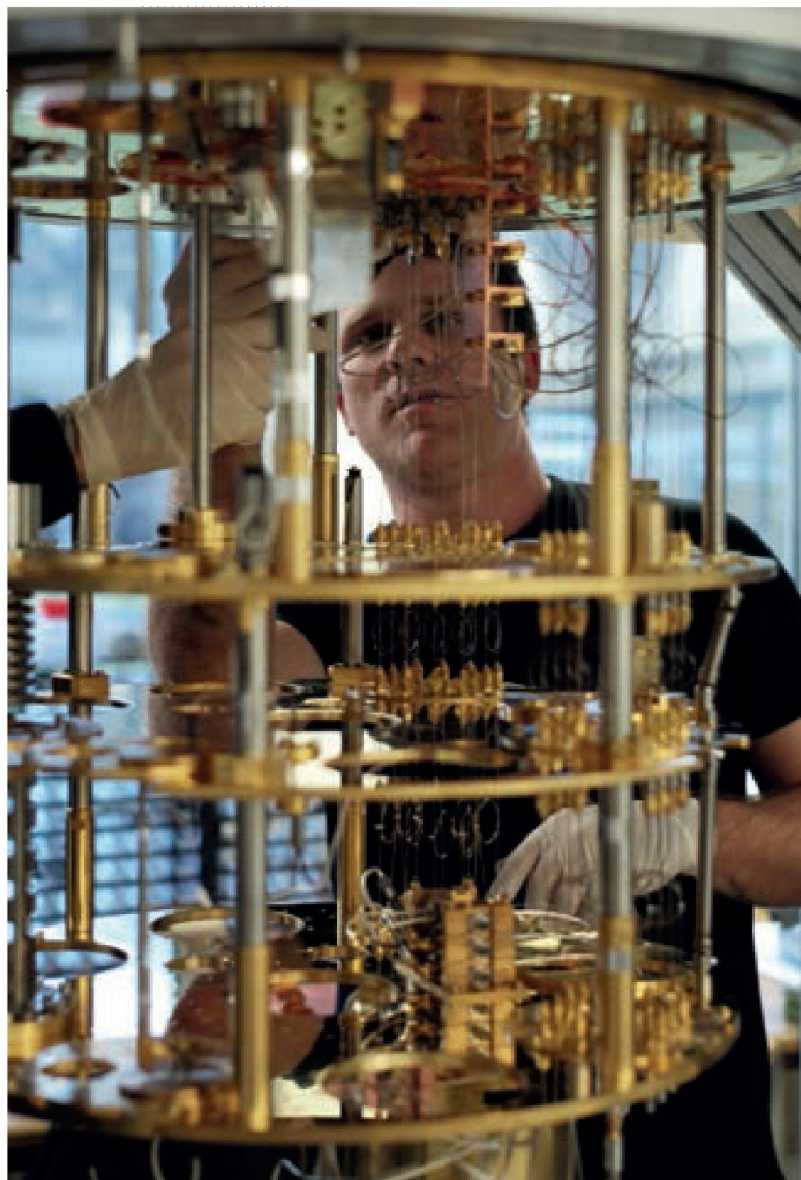


Een van de koelers in het Delftse kwantuminstituut QuTech. In dit geval is de omhulzing verwijderd om de binnenkant te tonen. Helemaal onderaan hangt de kwantumchip, waar de temperatuur maar een paar milligraden boven het absolute nulpunt is.

foto quitech/tu delft



IBM-onderzoeker Andreas Fuhrer bij een koeltoren in zijn werklaboratorium in Zürich, waar hij de werking van supergeleidende kwantumchips bekijkt.



De wereld maakt zich zorgen. Bankiers, veiligheidsdiensten, overheden en techbedrijven volgen met zweet op het voorhoofd de opmars van de kwantumcomputer. Iets dat een paar jaar terug nog een onhaalbare droom leek, ontwikkelt zich plotseling zo rap dat er maatregelen nodig zijn ter beveiliging. Want zo'n speciale computer, die gebruikmaakt van kwantumfenomenen als verstrengeling en superpositie, betekent het einde van de cryptografie zoals we die nu gebruiken. En daarmee van de tot nog toe ijzersterke beveiliging van bankgegevens en overheidsgeheimen.

Het is een van de grote beloftes van de kwantumcomputer sinds de Amerikaanse wiskundige Peter Shor in de jaren negentig een algoritme bedacht voor de kwantumcomputer waarmee elk getal, hoe groot ook, eenvoudig is te ontbinden. Dat is namelijk ook het geraamte waarop de moderne cryptografie stoelt. Ook kan zo'n kwantumcomputer dankzij de grote rekenkracht simulaties draaien van de meest complexe processen. Hele ecosystemen, planeten of zelfs universa met daarin miljoenen variabelen zijn met een kwantumcomputer na te bootsen. Net als de wisselwerking tussen een medicijn en een eiwit, wat medicijnonderzoek goedkoper zou maken.

Lange tijd was de kwantumcomputer een theoretisch apparaat, iets waarvan kwantumwetenschappers dachten dat het moeilijk zou zijn die ooit echt te maken. Je moet er immers individuele kwantumdeeltjes voor kunnen bouwen en manipuleren – en niet een paar, maar vele duizenden of zelfs miljoenen.

Maar na de ontdekking van Shor werden de kwantumingenieurs wakker. Zij gingen koortsachtig op zoek naar een manier om de kwantumcomputer werkelijkheid te maken. Ze sleutelden en experimenteerden en creëerden zo de qubit, het fundament van de kwantumcomputer. Een qubit – een samentrekking van de Engelse woorden 'quantum' en 'bit' – is een kwantumdeeltje in een computer. Net als een bit in een gewone pc kan het de waarde 0 of 1 hebben. Bijzonder is echter dat er dankzij de kwantumeigenschappen een spectrum aan andere opties is: de superposities tussen 0 en 1. Superpositie is het fenomeen dat een deeltje zich

in twee toestanden tegelijk bevindt, bekend van Schrödingers gedachte-experiment met een kat in een doos die tegelijkertijd levend en dood is. Pas als je de doos opent, weet je het antwoord. Met een qubit gaat het net zo: als hij in superpositie staat, kan hij tegelijkertijd 0 en 1 zijn. Pas bij uitlezen vervalt de bit naar óf 0 óf 1, met een bepaalde kans.

Koelkast

Dat klinkt onpraktisch voor een computer, waarvan je juist zekerheid wilt hebben en constant hetzelfde antwoord. Bovendien merk je, op het moment dat je het resultaat van een berekening wilt bekijken, niets van de superpositie: je ziet alleen een reeks van nulletjes en een-tjes. Maar slimme software maakt het mogelijk om de resultaten van een kwantumberekening te bekijken mét de superpositie. Dat kan met zogenoemde interferentie, waarbij de resultaten als het ware worden ontward. Het interpreteren van een kwantumberekening is een lastig uit te leggen proces dat een totaal nieuwe manier van programmeren vereist.

Voor de bouwers van kwantumcomputers is het programmeren echter een zorg voor later. Nu zit het fysieke deel van de kwantumcomputer in de lift. Op een kwantumcongres in het kader van het Nederlands EU-voorzitterschap zegde de Europese Commissie een

ELEKTRONENEILAND

Hoe maak je een kwantumchip? Prof.dr.ir. Lieven Vandersypen van de TU Delft doet dat met halfgeleiders, die ook in vrijwel alle consumentenelektronica zitten. Het is een veelbelovende methode, juist door de ervaring die de industrie heeft met het materiaal.

Om een qubit te maken brengt Vandersypen een zeer specifiek patroon van draadjes aan op een halfgeleidend substraat. In het midden van het substraat ontstaat zo een eilandje, omringd door de draden. Hij zet de draadjes onder spanning, waardoor de elektronen op de halfgeleider één voor één wegspringen uit het eilandje. Uiteindelijk blijft er één geïsoleerd elektron over. Door dat elektron te manipuleren met verschillende magneetvelden zet Vandersypen het precies in de gewenste spintoestand.

Het kwantumeffect komt van de spin van het elektron. Kortgezegd kan deze spin omhoog staan (dan stelt hij een 0 voor), omlaag (een 1), of in een willekeurige andere richting ertussenin. Die laatste optie is de superpositie-

toestand van het elektron. Als een gebruiker van een kwantumchip het resultaat van een berekening wil weten, kijkt hij naar de spin van het elektron. Die is te achterhalen door te kijken hoe het elektron, onder invloed van zijn omgeving, van en op het eilandje springt.

Het is een ingewikkeld proces, dat bovendien lastig is te controleren doordat het deeltje zo klein is. Mede daardoor loopt de techniek nu achter op de andere populaire methode om een qubit te maken, met supergeleidende chips (zie kader 'Zichtbare supergeleiders'). Vandersypen denkt echter dat dat zal veranderen. 'Dankzij de ervaring uit de halfgeleiderindustrie kan deze methode snel groot worden. Zeker omdat we het manipuleren van enkele elektronen steeds beter in de vingers krijgen. Nu moeten we elke qubit nog apart inregelen, wat veel werk is. Maar we werken aan manieren om dat te automatiseren. Zo stroomlijnen we het gebruik van een halfgeleidende kwantumchip.'

miljard euro subsidie toe aan onderzoek naar de kwantumcomputer. Elke spreker, van beleidsmaker tot gerenommeerd onderzoeker, noemde vijf tot tien jaar als kritische grens: dan is er een kwantumcomputer die de huidige supercomputers voorbijstreeft.

Dat optimisme is begrijpelijk als je op de TU Delft komt. In het laboratorium van QuTech, nog eventjes gevestigd in het ouderwetse natuurkundegebouw van de universiteit, hangt de nieuwste van de nieuwste apparatuur. Acht langgerekte pilaren hebben aan de bovenkant een enorme hoeveelheid kabels, die naar de verdieping erboven leiden. 'Die pilaren dienen puur voor koeling', vertelt prof.dr.ir. Lieven Vandersypen, leider van het naar hem vernoemde lab. 'Hier aan de onderkant zit de chip waar het echt om gaat.' De pilaar is een hightech koelkast,

'Wij zien weinig fundamentele problemen met de ontwikkeling van een supergeleidende variant'

die in staat is om de piepkleine chip aan de onderkant tot ongekend lage temperaturen te koelen: minder dan één graad boven het absolute nulpunt.

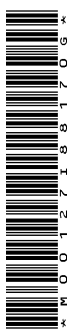
Die temperatuur is nodig om de chip te laten werken. Er zijn veel methoden om een kwantumchip te maken en Vandersypen onderzoekt er één van: de halfgeleiderchip (zie kader 'Elektroneneiland'). Hij gebruikt een halfgeleidend substraat, zoals galliumarseen of silicium. Daarop isoleert hij één elektron, dat vervolgens met magneetvelden in superpositie is te brengen. Om dat elektron op zijn plek te houden moet de chip echter wel ijs- en ijskoud zijn.

Collega dr. Leo DiCarlo kijkt naar een compleet andere methode, namelijk naar supergeleidende chips (zie kader 'Zichtbare supergeleiders'). 'Groot voordeel is dat onze chips micrometers groot zijn, in plaats van een paar nanometer. Dat maakt het tastbaarder.' Temperatuur is bij hem echter net zo belangrijk, want een supergeleider is alleen supergeleidend bij extreem lage temperaturen – ook DiCarlo's chips hangen dus aan de onderkant van de koelingspilaren.

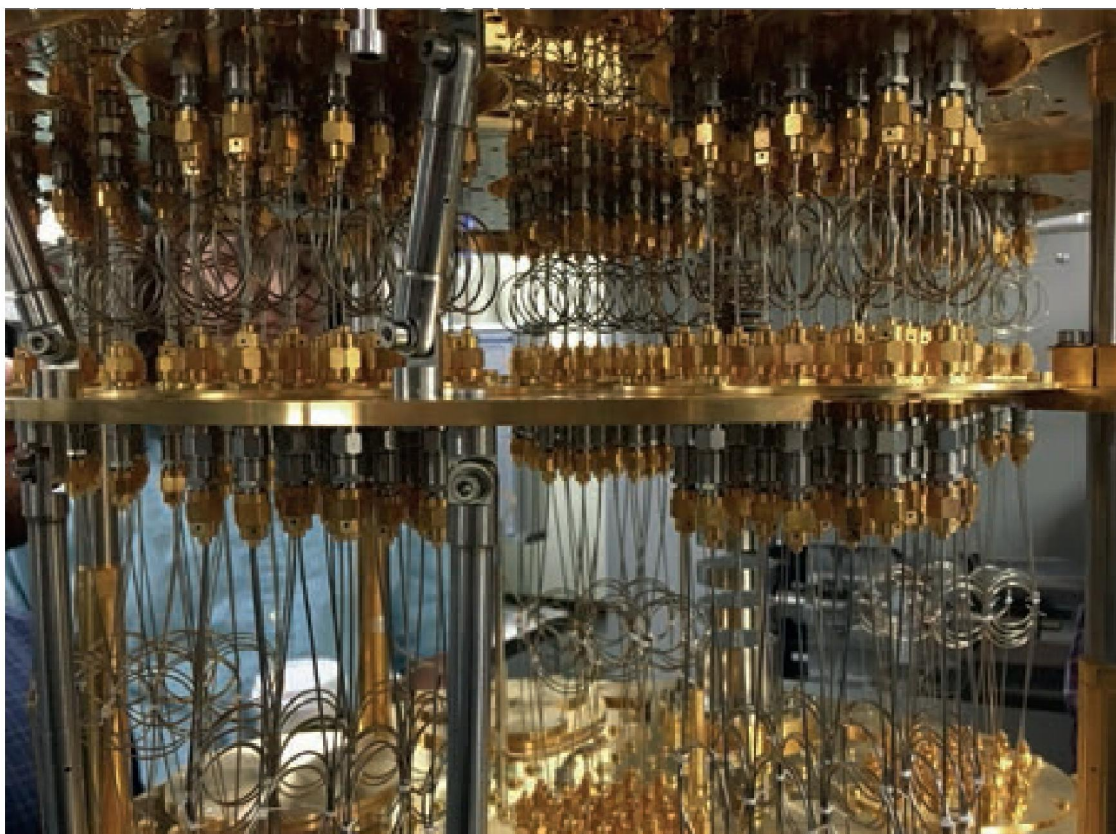
Beide onderzoekers werken al jaren aan de kwantumchip en ze zien de grote sprongen die de afgelopen jaren zijn genomen. Vandersypen: 'Er is nu veel momentum, dat klopt inderdaad.' De EU-investering, maar ook de interesse van de industrie versnellen de ontwikkeling nog eens. Chipmaker Intel werkt sinds een paar maanden samen met het QuTech-lab. 'Intel gaat ons helpen om zuiverdere chips te maken, zodat we betere resultaten krijgen', aldus Vandersypen. En IBM, concurrent van Intel, lanceerde twee maanden terug een website waar wetenschappers via de cloud een kwantumalgoritme kunnen uploaden, dat IBM vervolgens uitvoert op hun supergeleidende 5 qubit-chip.

Vervuiling

Vandersypen ziet twee redenen waarom de kwantumcomputer plotseling zo populair is. 'Ten eerste, en dit geldt vooral voor de halfgeleiders, wordt de overstap gemaakt van het substraat galliumarseen naar silicium. Met dit materiaal heeft de chipindustrie ontzettend veel ervaring, waar-



Programmeercommando's voor de vijf qubit-kwantumchip van IBM in de Verenigde Staten komen vanuit de cloud binnen, en worden vertaald naar een serie microgolven, die vervolgens via deze draden bij de chip komen.



door de qubit makkelijker wordt te maken. Maar wellicht nog belangrijker is dat silicium het superpositieproces minder vervuult.' Vandersypen verwijst naar een vervelend probleem in de kwantumwereld: omdat alles om enkele deeltjes draait, wordt de superpositie snel verpest. In het geval van galliumarseen hebben de atomen in het substraat bijvoorbeeld allemaal een klein beetje spin, een fundamentele eigenschap van deeltjes. Die spin beïnvloedt de draairichting van het ene elektron dat als qubit dient, waardoor het langzaam zijn evenwicht kwijtraakt en uit de superpositie schiet. 'Toen we begonnen met het maken van halfgeleidende qubits, was galliumarseen een geschikt materiaal, iedereen gebruikte dat. Vooral omdat het schone halfgeleiders oplevert, met weinig defecten en atomen die netjes op een rijtje liggen. Dat is, naast de spininvloed van de atomen, ook van onschatbaar belang voor stabiliteit.'

Een substraat van silicium is te purificeren, zodat de atomen geen spin meer hebben. Dat is een grote stap naar meer stabiliteit van het ene elektron. 'Dit verhoogt de stabiliteit met een factor 100 tot zelfs 10 000, afhankelijk van hoe puur je het silicium maakt. Nadeel is dat silicium dan weer eerder defecten kent door een minder schoon atoomrooster. Intel kan helpen om de

chips nog puurder te maken. Daarnaast wordt het waarschijnlijk mogelijk om de chip net zo defectloos te krijgen als bij galliumarseen, zodat het oorspronkelijke probleem met silicium wegvalt. Intel weet hoe je een schone siliciumchip maakt, en daar kunnen wij veel aan hebben.'

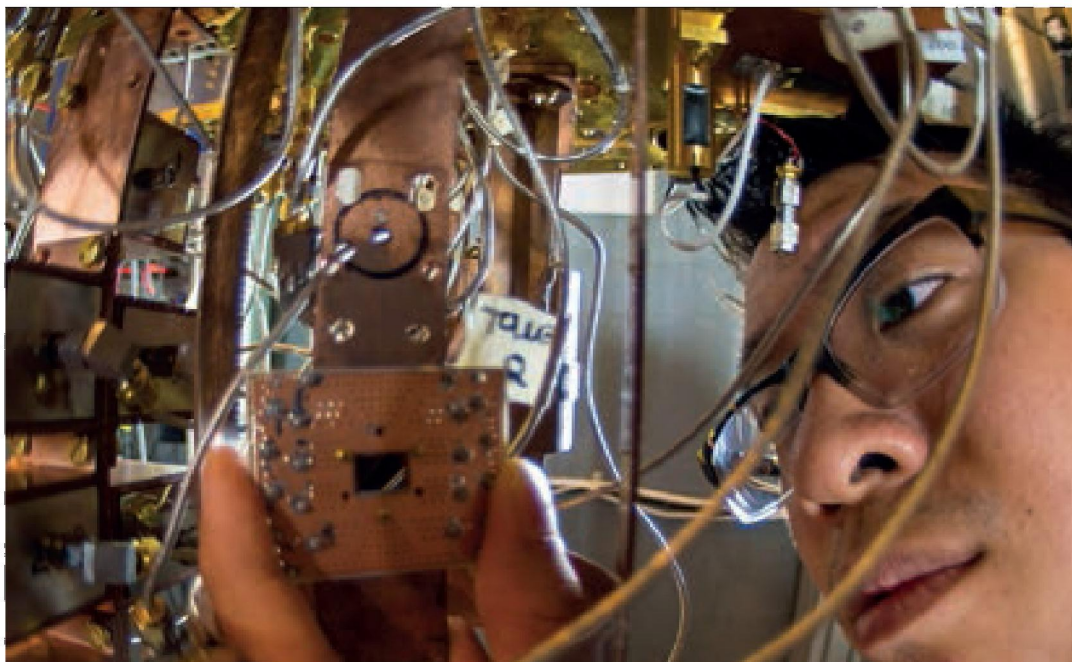
Ook DiCarlo rekent voor het maken van zijn supergeleiders op Intel. 'De circuits die wij bouwen zijn telkens een klein beetje anders. Daardoor krijgen onze qubits een karakter, een ogenschijnlijk onvoorspelbaar eigen willetje. Door ze netter te produceren hopen we die persoonlijkheid minder grillig te maken.'

Foutcorrectie

De tweede reden voor de toename in populariteit van de kwantumcomputer is dat de kwantumchip minder foutcorrectie nodig heeft dan eerst werd aangenomen. Die foutcorrectie is een belangrijk en fundamenteel onderdeel van de kwantumcomputer, waar de bouwers een oplossing voor moeten vinden.

De fouten ontstaan door een proces dat decoherentie heet. Een kwantumdeeltje kan namelijk maar korte tijd in superpositie blijven, voordat het onherroepelijk terugvalt naar een evenwichtspositie, een 0 of 1 dus. Vanaf dat moment is het deeltje nutteloos voor kwantumberekeningen. Dat heeft tot gevolg dat een gebruiker van de kwantumcomputer maar een beperkte tijd heeft om berekeningen uit te voeren. Daarna zullen steeds meer qubits decoherent raken en ontstaan er steeds meer fouten.

Om die fouten te corrigeren moet er voldoende redundantie worden ingebouwd in een kwantumcomputer. Daarmee zijn de fouten eruit te halen, maar dat werkt alleen als de computer sneller fouten



Jerry Chow, architect van de vijf qubit-kwantumchip van IBM, bij zijn creatie.

verwijderd dan dat ze ontstaan. 'Voorheen lag die grens bij één fout op tienduizend operaties. Het was verdraaid lastig om chips te maken met zo weinig fouten', zegt Vandersypen. 'Dankzij het werk van theoretici weten we nu echter dat die grens bij één fout op honderd operaties ligt.' DiCarlo vult aan: 'En dat is iets wat eigenlijk al lange tijd haalbaar was. Daarmee werd een werkende kwantumcomputer plotseling veel realistischer.' Die tolerantiesprong kwam doordat kwantumwetenschappers het model voor een kwantumcomputer doorrekenden en manieren vonden om de werking van die computer te verbeteren. Onder die werking valt onder meer hoe de computer commando's verwerkt en waar signalen heen gaan. Met die verbeteringen liep de computer soepeler, nog voordat hij bestond, en dat maakt het geheel toleranter voor fouten.

Inmiddels is de kwantumwereld zo ver dat de eerste werkende kwantumchips bruikbaar zijn. Google investeerde in het werk van

prof.dr. John Martinis, die een supergeleidende chip met negen qubits maakte. IBM kwam met een eerste, voor het publiek zichtbare resultaat in de vorm van een chip met vijf qubits, via de cloud programmeerbaar. In het IBM-lab in het Amerikaanse Yorktown draait deze supergeleidende chip in een huls waar het 14 mK (-273,13 °C) is. Via een notenbalkachtige interface kan iedereen programmeeropdrachten geven, die vervolgens door een kamer vol apparatuur wordt vertaald in microgolven, de 'taal' van de supergeleidende kwantumchips.

Het is voor IBM het begin van de weg naar een kwantumcomputer met vijftig tot honderd

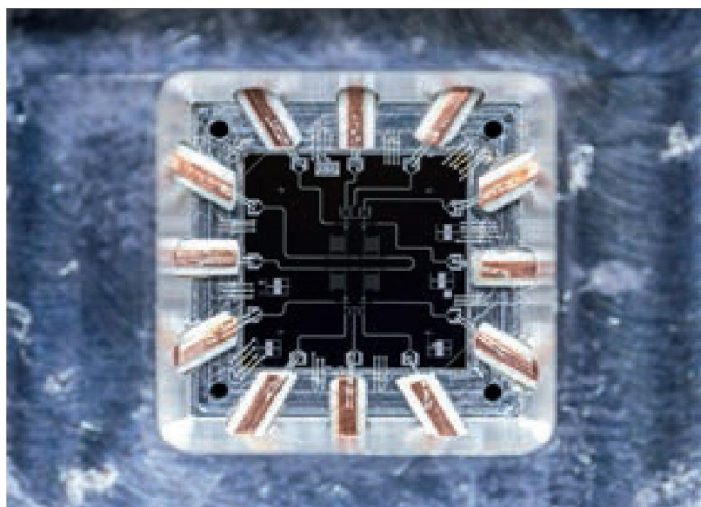
ZICHTBARE SUPERGELEIDERS

Dr. Leo DiCarlo van de TU Delft is expert op het gebied van supergeleidende kwantumchips. Hij begon ooit als onderzoeker van halfgeleiders, maar maakte de overstap toen hij de potentie van supergeleiders zag. 'Bovendien zijn mijn chips een paar micrometer groot. Je bouwt echt iets, een circuit dat je kunt zien.'

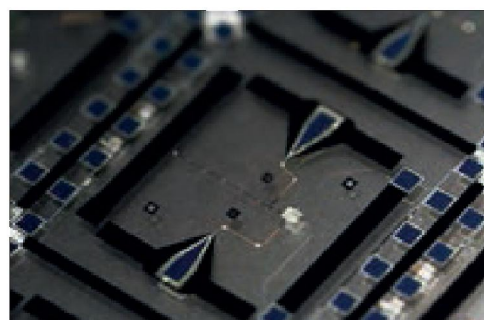
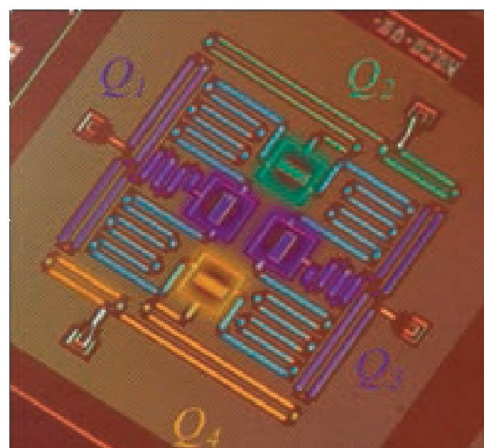
Die circuits beginnen zoals alle supergeleidende circuits: met een substraat, ook hier vaak van silicium, en een supergeleidend materiaal erop. Met een zogenoemde Josephson-junctie, een soort sandwich met vulling van aluminiumoxide, ontstaat een apparaat dat zich precies zo gedraagt als een atoom. Als je het geheel afkoelt, ontstaat een energiespectrum, met verschillende discrete energieniveaus. DiCarlo kan de chip met behulp van micro-

golven naar bepaalde, specifieke energieniveaus brengen, of juist tussen twee niveaus in laten zweven. Dat laatste is een alternatieve vorm van superpositie, die is te gebruiken om mee te rekenen.

Op dit moment gaat de ontwikkeling van supergeleidende chips harder dan die van halfgeleiders. Toen de kwantumchip net in opkomst was, waren de grotere supergeleiders makkelijker te produceren. Supergeleidende kwantumchips zijn er nu al met tien qubits, terwijl halfgeleiders op slechts een paar qubits zitten. DiCarlo is bezig met een chip van zeven-tien qubits. 'De schaalbaarheid is wel lastig. Het verbinden van verschillende supergeleidende qubits bleek bijvoorbeeld niet makkelijk. Maar we vinden wel mogelijke oplossingen die het productieproces beter schaalbaar maken.'



Verschiede supergeleidende chips van dichtbij, door de jaren heen. De chips zijn afkomstig van het door Google gesteunde lab van John Martinis en het Quantum Research Lab van IBM.



qubits. Dr. Andreas Fuhrer, onderzoeker bij het IBM-lab in Zürich en betrokken bij het kwantumproject: 'Wij zien weinig fundamentele problemen bij de ontwikkeling van een supergeleidende kwantumcomputer. De techniek is goed schaalbaar. Over vijf à tien jaar moet die computer er zijn.'

Dat zou een mijlpaal betekenen voor de kwantummechanica. Een kwantumcomputer heeft namelijk meer rekenkracht dan de beste supercomputer, in ieder geval voor sommige specifieke problemen, zoals het simuleren van atomen. Dat een kwantumcomputer dat al met enkele tientallen bits kan, terwijl supercomputers miljarden transistors nodig hebben, komt door de superpositie. Daardoor is het mogelijk om tegelijkertijd een groot aantal inputs te gebruiken. Door de superpositie heeft elke bit immers twee opties tegelijkertijd, in plaats van één. De hoeveelheid informatie die in de computer past, neemt dan snel toe: bij twee qubits heb je vier opties (00, 01, 10 en 11), bij drie qubits heb je er al acht, en zo groeit het verder.

'Dat betekent niet dat we met vijftig qubits klaar zijn', benadrukt Fuhrer. 'Het is nog geen universele kwantumcomputer, de echte droom van het vakgebied. Om cryptografie-algoritmen te breken zijn alsnog miljoenen qubits nodig.' Vandersypen en DiCarlo beamen dat: 'Vijftig qubits is een mijlpaal, maar het is nog lang niet genoeg. Mede doordat je veel qubits nodig hebt voor de foutencorrectie, heb je veel meer qubits nodig.'

Toch is er volgens Fuhrer ook met vijftig qubits al veel te doen. 'Vooral op simulatiegebied zijn er

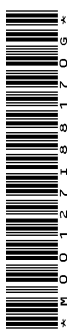
interessante opties. Nu zijn kwantumprocessen, zoals het samenspel tussen twee atomen, vaak slecht begrepen, omdat het simuleren van kwantumprocessen ontzettend veel rekenkracht kost. Maar met een kwantumcomputer zitten die processen als het ware in de computer gebakken. Dat maakt het simuleren makkelijker en levert een schat aan wetenschappelijke inzichten op.'

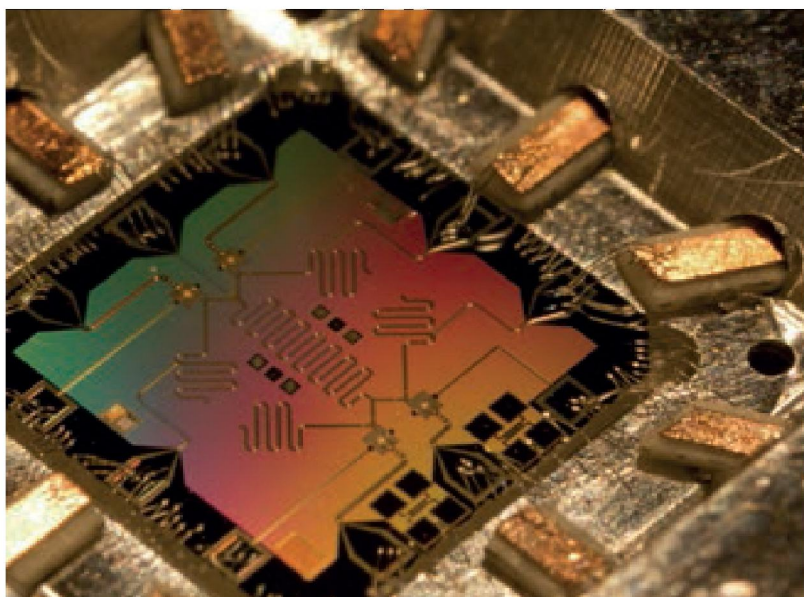
Vandersypen denkt ook dat er met vijftig qubits al een en ander mogelijk is. 'Daarnaast heb ik ook goede hoop op verbeteringen aan de algoritmekant van de kwantumcomputer. Als slimme softwareprogrammeurs manieren vinden om grootse dingen te doen met minder qubits, is dat voor ons natuurlijk een zegen.'

Killer app

Daarmee kaart Vandersypen een ander belangrijk onderdeel van kwantumcomputers aan: de software. Zonder algoritmen en programma's is een kwantumcomputer immers niets meer dan een duur, maar nutteloos stuk hightech. En wachten tot de computer er is om software te ontwikkelen is geen optie, denkt prof.dr. Harry Buhrman, hoogleraar bij de Universiteit van Amsterdam en het Centrum Wiskunde & Informatica (CWI). Hij richtte in december het instituut QuSoft op, dat voor kwantumsoftware moet doen wat QuTech in Delft doet voor de hardware. 'We zijn op zoek naar een killer app voor de 50 qubit-computers die er over twee, drie jaar komen.' Zo'n app, een programma of toepassing die het nut van de kwantumcomputer in één klap duidelijk maakt, blijkt lastig te vinden.

Het is opvallend dat kwantumsoftware nog niet zo ver is. Het idee van de kwantumcomputer kreeg immers aandacht doordat wiskundige Shor een mogelijk baanbrekend algoritme bedacht. Zijn algoritme





liet zien dat met een krachtige kwantumcomputer de factorisatie van priemgetallen plotseling snel is te doen. Dat zou de veelgebruikte traditionele cryptografie, die onder meer dienstdoet als wereldwijde internetbeveiliging, in één klap waardeloos maken.

Dat algoritme vereist echter nog steeds een krachtige kwantumcomputer die er niet in de nabije toekomst zal komen. Dus kijkt Buhrman met zijn snel groeiende team softwareontwikkelaars naar andere toepassingen. 'Er moeten dingen kunnen met een kleine kwantumcomputer. Zelfs met vijftig bits heb je iets wat krachtiger is dan de huidige supercomputers.' Maar wat het is, dat weten ze nog niet. Het vinden van een nuttig algoritme vereist veel uitproberen. 'We kijken of we bestaande klassieke algoritmen kunnen ombouwen en experimenteren wat met simulaties van een paar qubits. Zo hopen we op goede ideeën te komen.'

VEILIGE VERSTRENGELING

Het Delftse kwantuminstituut QuTech bouwt niet alleen computers, maar werkt ook aan een kwantuminternet. Daarbij speelt de verstrengeling van deeltjes een sleutelrol. Nadat het team van prof.dr. Ronald Hanson aan de TU Delft vorig jaar onomstotelijk het bestaan van dit vreemde verschijnsel aantoonde, willen onderzoekers het nu toepassen in een netwerk tussen een aantal Nederlandse steden.

Een kwantuminternet gebruikt verstrengelde deeltjes voor veilige communicatie. Door twee deeltjes te verstrengelen en beide communicerende partijen één deeltje te geven weten ze zeker dat ze met elkaar hebben te maken. Een luistervink die vervolgens communicatie wil onderscheppen, heeft geen kans. Zodra hij het verstrengelde deeltje bekijkt, verandert het immers, waardoor de beoogde ontvanger ziet dat er iets mis is.

In de praktijk betekent dit dat tussen steden als Den Haag, Rotterdam en Delft via glasvezelkabels verstrengelde deeltjes zullen lopen. Het is voorlopig nog puur bedoeld voor onderzoek.

Programmeren voor kwantumcomputers is echter minstens zo lastig als het bouwen van de chips. 'Het grootste probleem is dat je maar lastig een 'goed' antwoord uit een berekening krijgt. Immers, het moment dat je de resultaten van een berekening meet, klapte de superpositie in elkaar en zie je maar één ding.'

Architectuur

Het is niet het enige probleem. Omdat de werking van een kwantumcomputer zo anders is dan van gewone pc's, moet elk aspect van de computerkunde worden herzien. 'De architectuur van een systeem, de manier waarop je een hogere programmeertaal vertaalt naar dingen waar de hardware fysiek iets mee kan, moet ook uitgedokterd en verfijnd worden.' Toch denkt Buhrman dat er genoeg voorbeelden zijn van potentiële algoritmen die gaan werken. Bovendien zal de softwareontwikkeling in een stroomversnelling komen als de computer er eenmaal is. Ondertussen hopen Vandersypen en zijn collega's juist dat de softwarebouwers manieren vinden om het aantal benodigde bits te verlagen. Zo hopen beide partijen dat de ander hun werk eenvoudiger maakt.

Buhrman sluit zich, ondanks de hordes qua softwareontwikkeling, aan bij het optimisme van Fuhrer van IBM en Vandersypen en DiCarlo van de TU Delft: binnen een paar jaar komt de 50 qubit-editie van de kwantumcomputer pc er. De schaalbaarheid is er, de technologie is goed genoeg begrepen, en onderzoekers worden alleen maar beter in het op grotere schaal produceren van qubits.

Rest alleen de vraag of eenieder met beveiligde informatie zich al zorgen moet maken. Volgens Buhrman komt het wel goed, mits er hard wordt gewerkt. 'RSA, het meest gebruikte encryptieprotocol, is inderdaad kwetsbaar. Maar er zijn andere versleutelingen die, voor zover we nu kunnen zien, wél bestand zijn tegen de rekenkracht van een kwantumcomputer. Maar er is nog verder onderzoek nodig voordat die bruikbaar zijn, en dat kan te laat zijn voor gegevens die kwaadwillenden nu, versleuteld en al, reeds kapen. Als de kwantumcomputer er is, kunnen ze die gegevens kraken. Er moet nog een hoop gebeuren voordat we een kwantumveilige bruikbare encryptie hebben. Maar er is wel hoop.' |