

techniek

Met qubits kraak je straks elke code

tekst Joep Engels (Trouw)

beeld TU Delft Hanson Lab

Zijn roem snelt de quantumcomputer vooruit. Voorlopig wordt de rekenmachine van de toekomst nog met gemak verslagen door een willekeurige scholier, maar zijn potentie is enorm. En daar houden sommigen nu al rekening mee.

Een ambassade die geheime informatie verstuurt, moet voorkomen dat de code wordt gekraakt, zegt Harry Buhrman, groepsleider aan het Centrum Wiskunde & Informatica en hoogleraar computerwetenschappen aan de Universiteit van Amsterdam. „Nu niet, maar ook niet over twintig jaar. Het is goed denkbaar dat de quantumcomputer er tegen die tijd is. Het kraken van de huidige codes is dan een fluitje van een cent. Daarom slaan veel inlichtingendiensten de nu nog onkraakbare informatie op. „Store now, decrypt later”, is het motto.”

De NSA, de Amerikaanse geheime dienst, raadde daarom afgelopen zomer de ambassades aan om over te stappen op „quantum-veilige cryptografie”, op codes die ook voor een quantumcomputer veilig zijn. „Wat dat zou kunnen zijn, wordt een van de pijlers van ons centrum”, zegt Buhrman. Hij is een van de directeuren van QuSoft, een onderzoekscentrum voor quantumsoftware dat afgelopen donderdag werd opgericht.

Quantumsoftware? Het is zo’n probleem waar je als leek niet bij stilstaat. Begin jaren tachtig bedacht Richard Feynman dat je de quantumfysica kon gebruiken om een supercomputer te bouwen en sinds de jaren negentig werken fysici aan onderdelen voor zo’n apparaat. Onderzoekers van de TU Delft hebben zich ten doel gesteld

om er vóór 2020 eentje gebouwd te hebben.

Rekencapaciteit

Zoals gezegd, een rekenmachine met een enorme potentie. Waar een gewone computer werkt met bits (0 of 1), rekent de quantumcomputer met qubits, die 0 en 1 tegelijk kunnen zijn. Superpositie, heet dat in quantumtermen. En omdat bij iedere extra qubit het aantal mogelijke toestanden in de superpositie verdubbelt, is de rekencapaciteit van deze computer al snel uitzonderlijk groot. Een quantumcomputer met 300 qubits beschikt over meer rekeneenheden dan er atomen in het heelal zijn.

De enorme rekenkracht komt niet bij ieder probleem van pas. De quantumcomputer zal zijn waarde vooral bewijzen bij vraagstukken die hij kan opsplitsen in delen die hij parallel kan behandelen. Het kraken van codes bijvoorbeeld. Die zijn vaak versleuteld als het product van twee grote getallen – meer dan duizend cijfers. De krachtigste klassieke computer zou er miljoenen jaren aan kwijt zijn om die twee getallen te vinden, maar een quantumcomputer heeft de klus zo geklaard. Hij zou ook goed zijn in het nabootsen van natuurlijke processen. Het weer bijvoorbeeld, of de dynamiek van een lichaamsscel.

Maar ja, hoe laat je die qubits voor jou werken? Hoe krijg je ze aan het rekenen zonder dat ze hun quantumfysische eigenschappen verliezen? Want in dat geval zou ook hun rekenvermogen verdampen. Het wetenschapsblad *American Scientist* vroeg zich dat een jaar geleden ook al af. Een redacteur stelde zich voor hoe hij in 2024 zijn quantumcomputer zou aanzetten, hoe met een zacht gezoem de minuscule quantumprocessor tot leven zou komen, en hoe hij.... „Tja, hoe zou ik een computerprogramma schrijven? Is er een quantumtaal? Kan ik vertrouwen op de bekende algoritmes?”

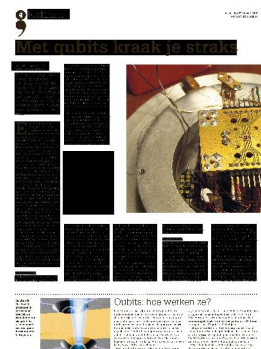
Wat hij over quantumprogram-

ma’s leest, gaat meestal als volgt: breng de qubits in hun beginstand, voer een reeks operaties uit en meet de eindtoestand van de qubits. „Dat klinkt niet als een computerprogramma, dat lijkt meer op een natuurkundig experiment.”

Proefopstelling

Maar dat is niet helemaal eerlijk. Ook een klassieke computer werkt op het meest basale niveau als was het een proefopstelling uit de natuurkunde. Het is niet meer dan een complexe structuur van transistoren en andere elektronische elementen waar elektrische stroompjes doorheen gaan. Zo’n transistor staat open of dicht, en dat is – op een hoger niveau – te lezen als 1 of 0. Ook logische elementen zoals AND of NOT zijn een interpretatie van stroompjes en spanningen. De programmeertaal is weer een laag hoger. En als iemand op een app’je wat intoetst, wordt dat in een aantal stappen vertaald naar dat allerlaagste niveau: de stroompjes mogen dóór of niet.

Dat gaat in een quantumcomputer niet anders, zegt Buhrman. De transistoren hebben plaatsgemaakt voor quantumeenheden, zoals lichtdeeltjes of kleine stroomkringetjes – als ze maar als qubits kunnen fungeren en dus twee standen kunnen hebben. En er zijn operatoren waarmee je de qubits kunt bewerken: je kunt ze in superpositie brengen of je draait ze in een andere stand (een qubit is vaak een soort magneetje). „Vraag me niet hoe dat precies werkt”, zegt Buhrman. „Het blijft



quantumfysica. Maar op een wat hoger niveau kom je op een programmeertaal uit die hetzelfde werkt als de klassieke. Je kunt er zelfs meer mee.”

Het onderzoek hiernaar is één van de pijlers van het nieuwe instituut QuSoft. Andere wetenschappers van het centrum richten zich meer op de betrouwbaarheid van de rekenkunsten. Buhrman: „Het mooie van de quantumcomputer is dat je met een kleine hoeveelheid qubits al astronomisch veel berekeningen kunt uitvoeren. Dat klinkt prachtig, maar daar zit ook een probleem: hoe kies je uit die brij de berekening waar je op uit was?”

Het antwoord heet interferentie, zegt hij. Al die vreemde quantumprocessen zijn in beginsel golfbewegingen, en golven hebben de eigenschap dat ze elkaar kunnen uitdoven of versterken. Gooi twee stenen in een vijver en zie wat er gebeurt als de golfjes elkaar kruisen. „Koptelefoons die omgevingsgeluiden wegfilteren, maken ook gebruik van uitdoving door interferentie. Op vergelijkbare wijze zeven wij uit die brij van de quantumcomputer het gezochte antwoord.”

Puzzelen

Maar hoe weet je dan of dat ook het goede antwoord is? Doorgaans is dat niet zo moeilijk: de controle achteraf is vaak eenvoudiger dan de zoektocht zelf. Het is bijvoorbeeld nog wel even puzzelen voordat je ontdekt dat 2701 te schrijven is als het product van 37 en 73 (en niet anders). Maar de controle is zo gedaan. Buhrman: „De problemen ontstaan als je de quantumcomputer processen laat doorrekenen die de kracht van een gewone computer te boven gaan. Wat gebeurt er in chemische processen, wat gebeurt er als je een aantal chemicaliën bijeenbrengt? Dat soort simulaties moet een van de toepas-

singen van de quantumcomputer worden, maar de uitkomsten zijn niet een-twee-drie te verifiëren.

Een derde poot van het centrum richt zich op de vraag hoe snel de ontwikkelingen gaan. Met 300 qubits mag de quantumcomputer dan groter dan het heelal zijn, het record staat vooralsnog op negen qubits. Delft wil over vijf jaar een computer van 50 qubits hebben. Dan ben je in principe de klassieke computer voorbij. Onze vraag is: wat kun je met bijvoorbeeld 30 qubits?”

Dat is meer dan alleen een tussensstation. De astronomische reken Capaciteiten haalt de quantumcomputer alleen op papier. In de praktijk zullen er ook qubits nodig zijn ter controle. Buhrman spreekt in dit verband van ‘vuile’ en ‘schone’ qubits. Niet onbelangrijk: geheime diensten of banken willen weten wanneer hun codes in gevaar komen.

Dat is voorlopig nog hét toekomstperspectief van de quantumcomputer: de superpositie maakt het mogelijk veel berekeningen tegelijk uit te voeren en daarmee is hij superieur aan de klassieke computer.

Kraakpotentie

Superieur bij specifieke problemen althans, zoals het kraken van codes waarmee geheime boodschappen zijn versleuteld. Buhrman: „In de eerste plaats gaat het ons om de vraag hoe je de quantumcomputer moet programmeren zodat hij zijn kraakpotentie waarmaakt. Maar het gaat ons ook om de vraag hoe je codes quantumveilig kunt maken.” Hij haalt twee transparante vellen tevoorschijn waarop, schijnbaar willekeurig, zwarte blokjes zijn ingetekend. Aan geen van de twee vellen is iets bijzonders te zien, maar legt hij ze op elkaar, dan komt er een figuur tevoorschijn.

„Het ene vel is de sleutel, het andere de boodschap. Zonder sleutel kun je de boodschap niet lezen.”

Zoiets kun je ook voor quantumsystemen doen. „Voordat ik jou een boodschap stuur, zend ik je eerst een quantumsleutel. Als iemand die sleutel onderschept, verstoort hij onherroepelijk de superpositie. Jij kunt dus controleren of de sleutel ongezien is overgekomen. Is dat het geval, dan kan ik je veilig de boodschap sturen.”

Eigenlijk, zegt hij, bevinden we ons in dezelfde situatie als in de begintijd van de computer, de jaren veertig. De tijd waarin Thomas Watson, de baas van IBM, de legendarische uitspraak deed dat de wereld genoeg zou hebben aan vijf computers.

Buhrman: „Opnieuw is de software de bottleneck. We weten van sommige problemen dat de quantumcomputer ze aan zou kunnen, maar we hebben nog geen idee waar nog meer toepassingen liggen. We werken nog slechts met pen en papier, we hebben nog geen apparaat waarmee we kunnen spelen. Als dat er is, kunnen we echt aan de gang.”

„Eigenlijk bevinden we ons in dezelfde situatie als in de begintijd van de computer, de jaren veertig”

