

KWANTUMCOMPUTERS

Daar komt de kwantumprogrammatuur!

Supersoftware in wording

In onderzoek naar de kwantumcomputer wordt veel geld en tijd gestoken. Maar de software die voor deze machines nodig is, krijgt veel minder aandacht. Vreemd eigenlijk, want zonder software kun je niet veel met zo'n computer.

TEKST: ANOUSHKA BUSCH

De kwantumcomputer wordt de supercomputer van de toekomst. Over vijftien jaar hebben die zoveel rekenkracht dat ze vraagstukken kunnen oplossen die nu nog onoplosbaar zijn, zo voorstellen deskundigen. Ook zullen ze veel versleutelde bestanden kunnen kraken. Denk aan gecodeerde berichten van veiligheidsdiensten, maar ook de creditcardgegevens die we via het internet sturen.

We moeten dan natuurlijk wel software voor de kwantumcomputers hebben. En tot nu toe is die er niet. Maar als het aan wiskundige en informaticus Harry Buhrman van het CWI en de Universiteit van Amsterdam ligt, zal dat niet lang meer duren.

Geen nullen of enen

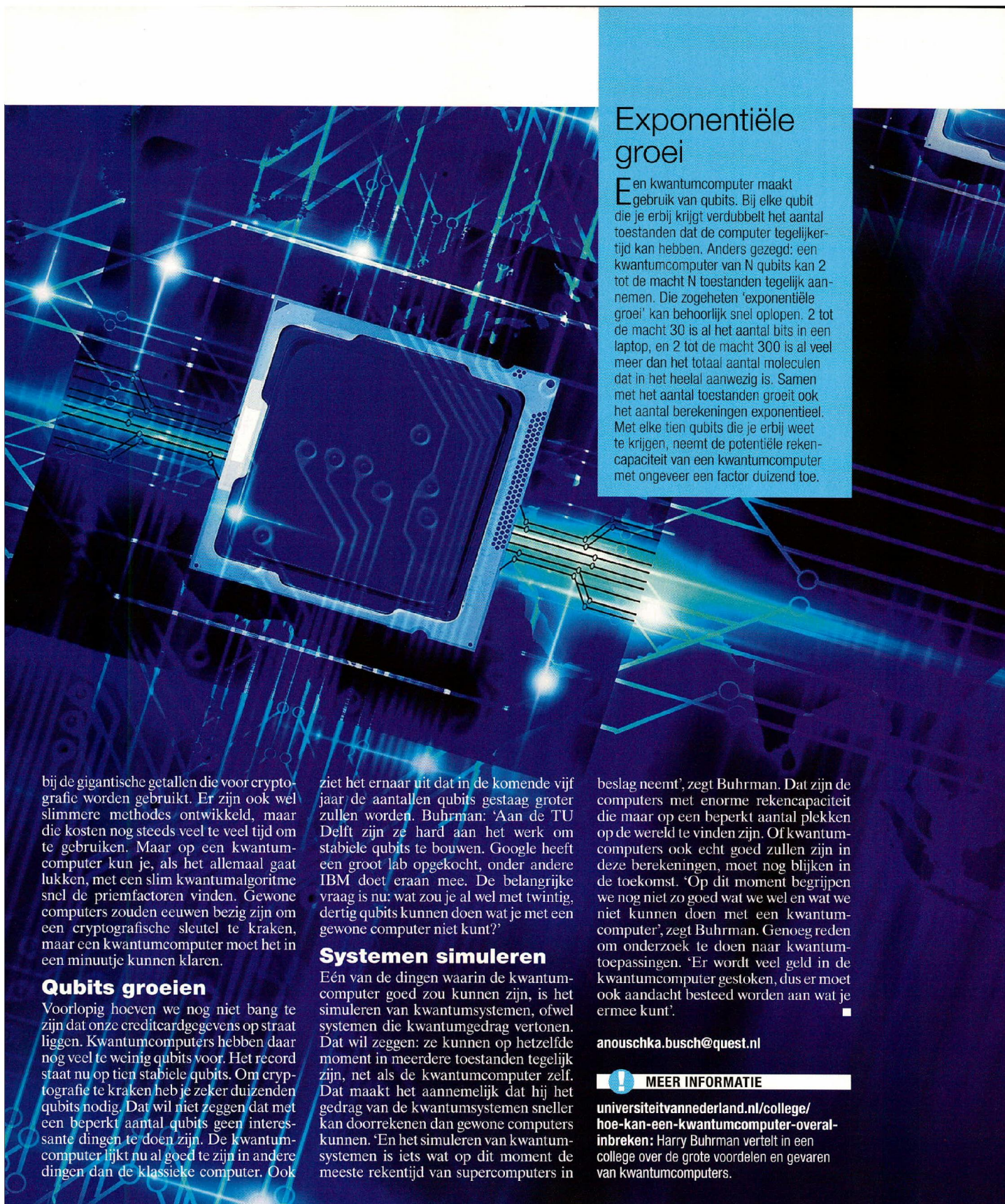
Is de normale standaardprogrammatuur niet op kwantumcomputers te gebruiken? Helaas niet. De voornaamste reden: de

rekenen eenheden van deze computer zijn helemaal anders dan die van een gewone computer. 'In een klassieke computer wordt informatie opgeslagen in de vorm van nullen en enen', legt Buhrman uit. 'Kwantumcomputers werken met qubits, bits die in 'superpositie' verkeren.' Dat wil zeggen dat ze tegelijkertijd zowel een nul als een één kunnen zijn. Dat heeft een groot voordeel: door alle verschillende mogelijke combinaties van nullen en enen kunnen ze in heel veel toestanden tegelijk zijn en kun je er heel veel berekeningen tegelijk mee uitvoeren (zie het kader 'Exponentiële groei'). Maar helaas heeft dat ook een groot nadeel. Bits in superpositie hebben namelijk de irritante eigenschap dat zodra je ernaar kijkt, het weer 'gewone' bits worden. Als je de uitkomst van je berekeningen wilt bekijken, dan zie je daardoor niet heel veel gelijktijdige berekeningen, maar slechts één willekeurige. En dat is waar kwantumprogrammeurs een slimme oplossing voor moeten vinden. Hun software moet

ervoor gaan zorgen dat van al die gelijktijdige berekeningen alleen diegene overblijft waarvan je het antwoord wilt weten.

Code gekraakt

Kwantumsoftwaremakers staan voor de opgave om toepassingen te vinden die aansluiten bij de gekke eigenschappen van het kwantumrekenen. Wat voor toepassingen dat zouden zijn? Een voorbeeld is het ontbinden van een getal in priemfactoren. Dat is het principe waarop een groot deel van onze cryptografie (het versleutelen van bestanden) berust. Hierbij wil je voor een getal de priemgetallen vinden die, als je ze vermenigvuldigt, als uitkomst dat getal geven. Bij 15 zouden dat bijvoorbeeld 3 en 5 zijn, want $3 \times 5 = 15$. Een manier die we daarvoor hebben, is om alle mogelijkheden een voor een uit te proberen. Is het getal deelbaar door 2? Door 3 dan? Net zo lang tot een getal gevonden is waardoor het wel deelbaar is. Dat kost je enorm veel tijd op een gewone computer, zeker



Exponentiële groei

Een kwantumcomputer maakt gebruik van qubits. Bij elke qubit die je erbij krijgt verdubbelt het aantal toestanden dat de computer tegelijkertijd kan hebben. Anders gezegd: een kwantumcomputer van N qubits kan 2 tot de macht N toestanden tegelijk aan-nemen. Die zogeheten 'exponentiële groei' kan behoorlijk snel oplopen. 2 tot de macht 30 is al het aantal bits in een laptop, en 2 tot de macht 300 is al veel meer dan het totaal aantal moleculen dat in het heelal aanwezig is. Samen met het aantal toestanden groeit ook het aantal berekeningen exponentieel. Met elke tien qubits die je erbij weet te krijgen, neemt de potentiële reken-capaciteit van een kwantumcomputer met ongeveer een factor duizend toe.

bij de gigantische getallen die voor cryptografie worden gebruikt. Er zijn ook wel slimmere methodes ontwikkeld, maar die kosten nog steeds veel te veel tijd om te gebruiken. Maar op een kwantum-computer kun je, als het allemaal gaat lukken, met een slim kwantumalgoritme snel de priemfactoren vinden. Gewone computers zouden eeuwen bezig zijn om een cryptografische sleutel te kraken, maar een kwantumcomputer moet het in een minuutje kunnen klaren.

Qubits groeien

Voorlopig hoeven we nog niet bang te zijn dat onze creditcardgegevens op straat liggen. Kwantumcomputers hebben daar nog veel te weinig qubits voor. Het record staat nu op tien stabiele qubits. Om cryptografie te kraken heb je zeker duizenden qubits nodig. Dat wil niet zeggen dat met een beperkt aantal qubits geen interes-sante dingen te doen zijn. De kwantum-computer lijkt nu al goed te zijn in andere dingen dan de klassieke computer. Ook

ziet het ernaar uit dat in de komende vijf jaar de aantallen qubits gestaag groter zullen worden. Buhrman: 'Aan de TU Delft zijn ze hard aan het werk om stabiele qubits te bouwen. Google heeft een groot lab opgekocht, onder andere IBM doet eraan mee. De belangrijke vraag is nu: wat zou je al wel met twintig, dertig qubits kunnen doen wat je met een gewone computer niet kunt?'

Systemen simuleren

Eén van de dingen waarin de kwantum-computer goed zou kunnen zijn, is het simuleren van kwantumsystemen, ofwel systemen die kwantumgedrag vertonen. Dat wil zeggen: ze kunnen op hetzelfde moment in meerdere toestanden tegelijk zijn, net als de kwantumcomputer zelf. Dat maakt het aannemelijk dat hij het gedrag van de kwantumsystemen sneller kan doorrekenen dan gewone computers kunnen. 'En het simuleren van kwantum-systemen is iets wat op dit moment de meeste rekentijd van supercomputers in

beslag neemt', zegt Buhrman. Dat zijn de computers met enorme reken-capaciteit die maar op een beperkt aantal plekken op de wereld te vinden zijn. Of kwantum-computers ook echt goed zullen zijn in deze berekeningen, moet nog blijken in de toekomst. 'Op dit moment begrijpen we nog niet zo goed wat we wel en wat we niet kunnen doen met een kwantum-computer', zegt Buhrman. Genoeg reden om onderzoek te doen naar kwantum-toepassingen. 'Er wordt veel geld in de kwantumcomputer gestoken, dus er moet ook aandacht besteed worden aan wat je ermee kunt'.

anouschka.busch@quest.nl

MEER INFORMATIE

universiteitvannederland.nl/college/hoe-kan-een-quantumcomputer-overal-inbreken: Harry Buhrman vertelt in een college over de grote voordelen en gevaren van kwantumcomputers.