

INNOVATIE & STRATEGIE

Laat Nederlands succes
kwantumcomputer geen toeval zijn

VOL GAS OP ONTWIKKELING

SOFTWARE KWANTUMCOMPUTER

SOFTWARE ONTWIKKELEN VOOR EEN COMPUTERARCHITECTUUR DIE NOG NIET BESTAAT, LIJKT ONZINNIG. TOCH IS DAT PRECIES WAT HET NEDERLANDSE QUSOFT NU AL TWEE JAAR DOET. STERKER NOG, DE FOUNDING FATHERS, WAARVAN HARRY BUHRMAN ER EEN IS, WERKEN AL SINDS EIND JAREN NEGENTIG AAN DE FUNDAMENTEN VAN KWANTUMCOMPUTERSOFTWARE.

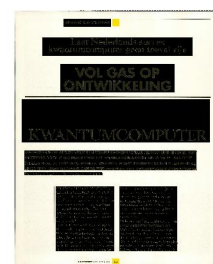
door Thijs Doorenbosch beeld De Beeldredactie/Peter Strelitski

BUHRMAN HAALT ONMIDDELIJK ZIJN GELIJK IN DE GESCHIEDENIS: "Vergeet niet dat alle navigatiesoftware gebaseerd is op een algoritme van Edsger Dijkstra dat hij in de jaren vijftig op het toenmalige CWI heeft ontworpen, lang voordat de computerarchitectuur bestond waar de software nu op draait."

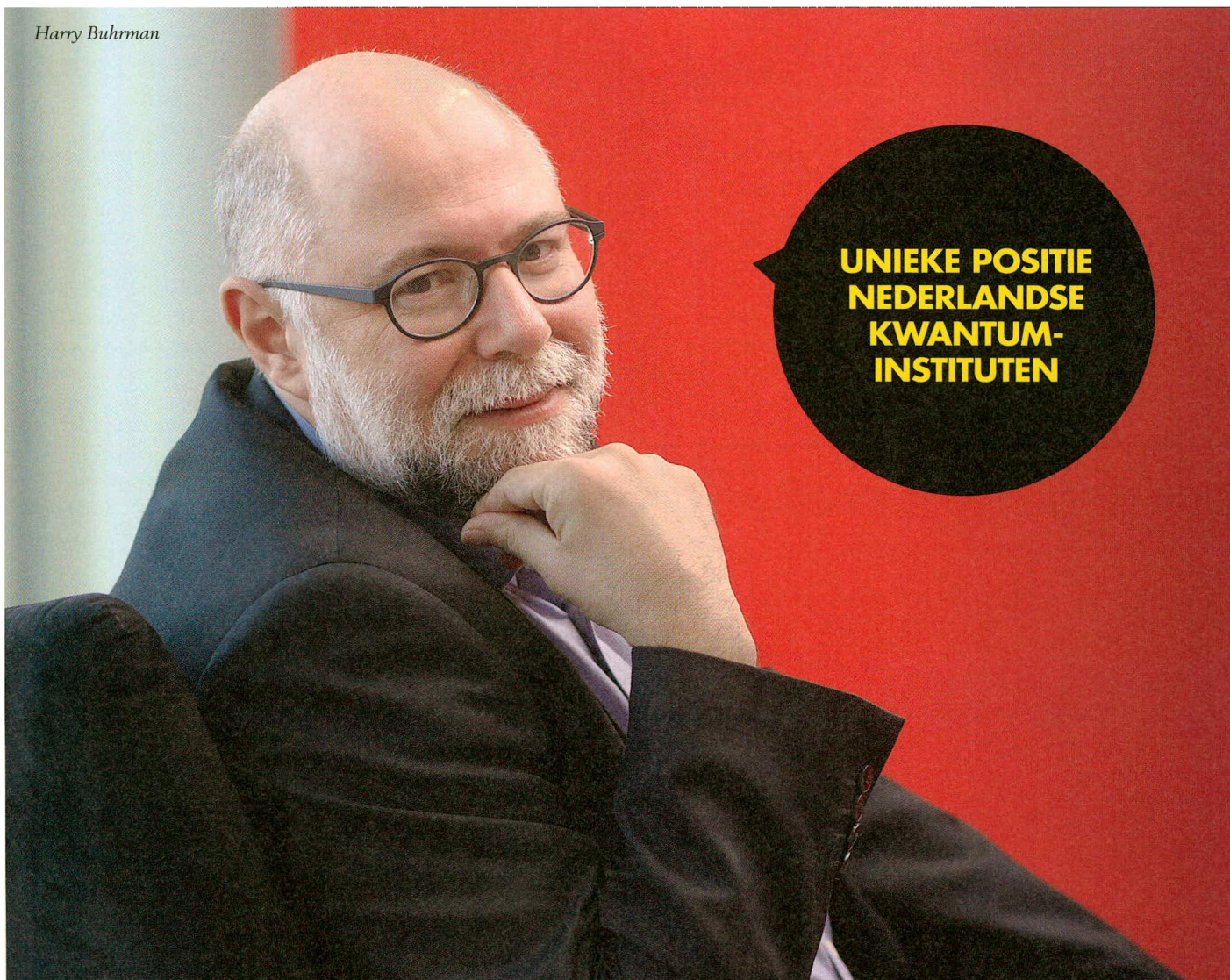
Daarom is het ook nu erg belangrijk al theoretisch bezig te zijn met wat straks kan met de kwantumcomputer. Ook de Cloud Security Alliance hamerde daar onlangs nog op vanuit een andere invalshoek. Het kraken van de huidige encryptietoepassingen is naar verwachting bin-

nen tien tot vijftien jaar een fluitje van een cent voor de kwantumcomputer. Nieuwe encryptie ontwikkelen kost echter minstens zoveel tijd, leert de geschiedenis. Gelukkig biedt de kwantumcomputer ook weer mogelijkheden om nieuwe vormen van encryptie te ontwikkelen.

Nederland heeft een unieke positie in de kwantumsoftwareontwikkeling, met QuSoft in Amsterdam dat toonaangevend werk verricht, en leidend is; niet alleen in Europa maar in de hele wereld. "Het is zaak die voorsprong te behouden, maar dat zal niet vanzelf gaan", stelt Buhrman. "In Amerika en China wordt



Harry Buhrman



TEGENINTUÏTIEF

Aan de basis van de kwantumcomputer ligt de kwantumfysica, de revolutie in de natuurkunde die zich begin 20e eeuw voltrok met werk van Planck, Einstein, Heisenberg en Bohr. Het bleek dat de wereld op atomair niveau zich heel anders gedraagt dan de wereld op macroscopisch niveau waar wij dagelijks mee te maken hebben. Inmiddels bestaat door de inspanningen van veel theoretisch natuurkundigen een heel goed wiskundig model van die subatomaire natuurkunde. Dat model

voorspelt tot nu toe perfect hoe de wereld zich gedraagt. Het probleem is dat alle vergelijkingen mank gaan wanneer wordt geprobeerd de eigenschappen die bij die subatomaire wereld horen, duidelijk te maken met zaken uit de macrowereld die we kennen. Neem het voorbeeld dat wanneer je naar een bekertje koffie kijkt en er gebeurt verder niets. Dan heeft dat kijken geen invloed op de toestand van het bekertje. Maar wanneer je kijkt naar de superpositie van een kwantum-

deeltje in deze superpositie, raakt deze status verstoord. Dat maakt het geheel contra-intuïtief en veel aspecten van de kwantumcomputer moeilijk begrijpbaar. De theoretisch fysicus Richard Feynman maakte daarom wel het statement 'Shut up and calculate'. Probeer niet met eindeloze discussies aan te tonen of het wel een superpositie is en hoe het eruitziet. Ga gewoon met die rekenmodellen aan de slag, want dat vertelt je alles. Het wiskundig model klopt.

“Shut up
and
calculate”

heel veel geïnvesteerd in de ontwikkeling van kwantumcomputerhardware. Maar ook daar groeit de belangstelling voor software. “Dat is niet vreemd”, zegt hij. Want de les uit de huidige generatie computers is wel dat met software veel meer geld valt te verdienen dan met hardware. “Software ontsluit door de inbreng van creativiteit de kracht die zit in de hardware. De software is dus duur en de hardware kun je bij wijze van spreken als commodity bij de supermarkt kopen.”

ZO PROGRAMMEER JE EEN KWANTUMCOMPUTER

Het ontwikkelen van software voor kwantumsystemen is erg lastig, benadrukt de Amsterdamse hoogleraar Harry Buhrman. “Het is een groot misverstand dat kwantumcomputers veel sneller rekenen dan klassieke computers. Ze rekenen op een andere manier waardoor je bij sommige problemen sneller bij het antwoord komt.” Daarom is het programmeren ook zo anders. Het basisblok van de klassieke computer is de bit die de waarde 0 of 1 kan hebben. De basis voor de kwantumcomputer is de kwantumbit die tegelijkertijd 0 én 1 kan zijn. Dit noem je de superpositie van twee toestanden. Maar met twee qubits heb je een superpositie tussen vier toestanden, bij drie gaat het al om acht en zo gaat dat exponentieel verder. Buhrman: “Het mooie is dat je met de kwantumcomputer op al die superposities een berekening kunt uitvoeren. Dus in de tijd dat je met een klassieke supercomputer een berekening uitvoert, kun je met een kwantumcomputer van 300 qubits 2 tot de macht 300 berekeningen uitvoeren. Dat zijn dus meer berekeningen dan het aantal moleculen in het heelal.”

Maar er is wel een probleempje: Hoe krijg je het antwoord uit de kwantumcomputer? “Zodra je gaat kijken naar de waarde van de qubits, is alles weg en zie je slechts de uitkomst van een van die berekeningen. Daar hadden we die kwantumcomputer niet voor nodig”, grapt Buhrman. “Gelukkig hebben we nog een tweede aspect uit de kwantumfysica en dat is de interferentie. Daarbij moet je je zoiets voorstellen als geluidsgolven die elkaar kunnen uitdoven zoals in een noise cancelling headphone. Een deeltje dat in superpositie is, kan met zichzelf interfereren waardoor sommige berekeningen tegen elkaar wegvallen en andere elkaar versterken. Ik maak wel de vergelijking met een componist. Die zorgt ervoor dat de geluidsgolven zo met elkaar interfereren dat er mooie muziek ontstaat. Zo zorgt de kwantumcomputerprogrammeur dat de superposities zo met elkaar interfereren dat je nuttige informatie krijgt. Het geeft aan dat we anders moeten nadenken over hoe je een kwantumcomputer programmeert dan dat we gewend zijn met een klassieke computer.”

LAAT NEDERLANDS SUCCES GEEN TOEVAL ZIJN

De unieke positie van Nederlandse kwantuminstellingen – kwantumhardware-instituut QuTech in Delft en kwantumsoftware-instituut QuSoft in Amsterdam – brengt Buhrman wel op een dilemma. Wetenschappers zijn geneigd hun resultaten open te delen, maar hij vraagt zich af of Europa toch niet enigszins beschermend te werk moet gaan om te voorkomen dat ook deze voorsprong naar andere werelddelen verdwijnt. “Het is puur toeval dat Edsger Dijkstra een Nederlander was en jaren later het Nederlands bedrijf TomTom furore maakte met navigatiesoftware. Laten we nou zorgen dat dat met kwantumsoftware dit keer geen toeval is.”

GEEN EENVOUDIGE CONTROLE BOVEN 50 QUBITS

De onderzoekers werken aan verschillende lagen van de software stack, die zich ongetwijfeld ook gaat ontwikkelen voor de kwantumcomputer. Het gaat dus om high-end toepassingen die pas mogelijk zijn wanneer er kwantumcomputers bestaan met vele qubits, zoals kwantumcryptografie en het simuleren van elektronen die rond een atoomkern spinnen. Maar ze onderzoeken ook hoe je kwantumcomputers kunt controleren. De uitkomsten van een systeem van enkele qubits zijn nog te verifiëren met een klassieke computer, maar wanneer je kunt gaan rekenen met 50 qubits of meer, valt die controlemogelijkheid weg. Dan is de vraag hoe je weet of de uitkomst juist is. Nadenken over wat je met kwantumbits kunt doen zonder het daadwerkelijk uit te voeren, is daarom heel zinvol. Daarom is het ook goed dat hardware en software los van elkaar worden ontwikkeld, vindt Buhrman. “De ontwikkelingen in hardware verlopen op een ander tempo dan die in de software. Je komt los van elkaar op mogelijkheden en beperkingen waar je wellicht in nauwe samenwerking niet op zou zijn gestuit. Het is wel belangrijk veel overleg te hebben om de wensen en mogelijkheden te bespreken.” 