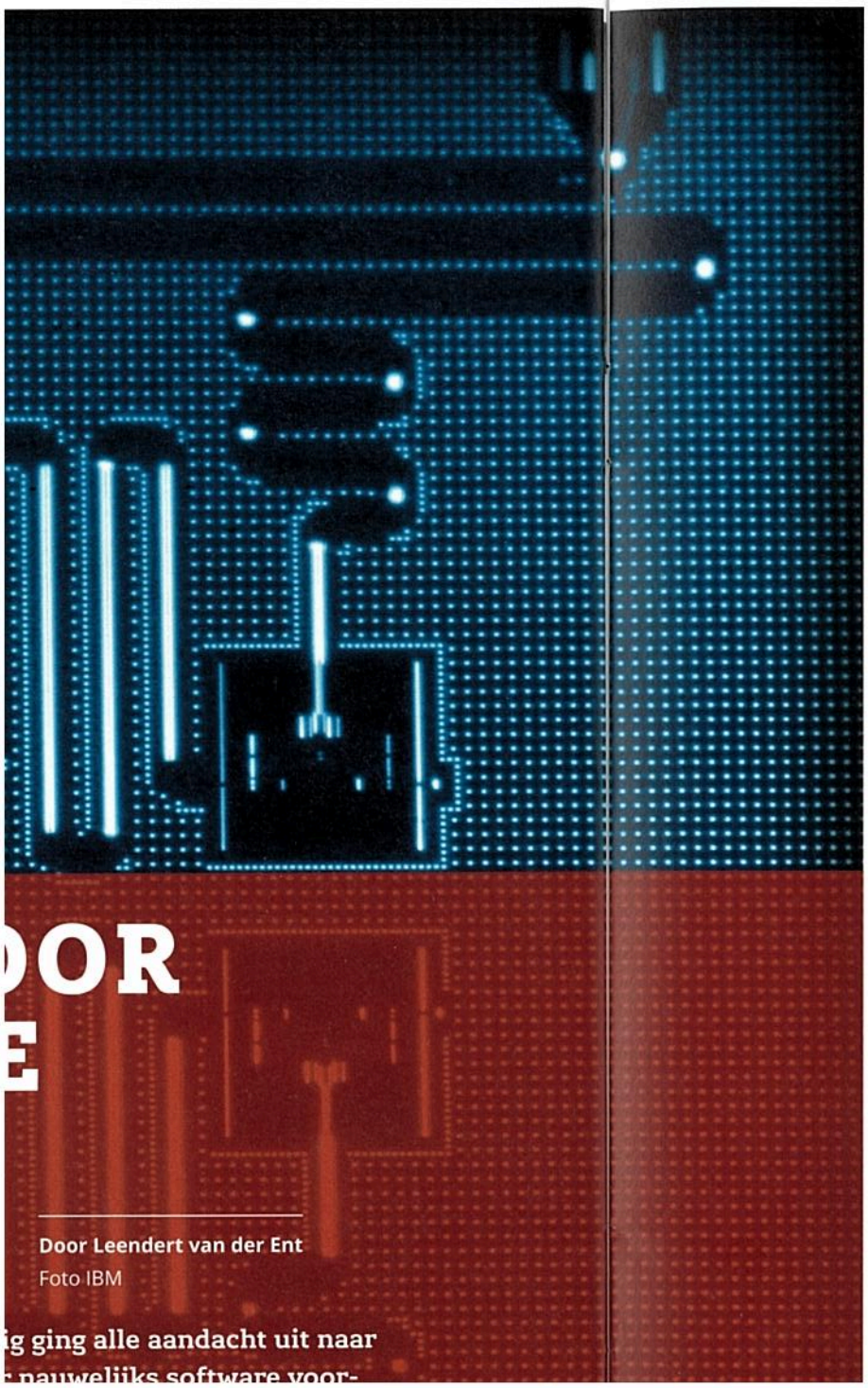
SOFTWARE VOOR TOEKOMSTIGE COMPUTERS EN INTERNET

Door Leendert van der Ent
Foto IBM

Tijdens de ontwikkeling van de computer in de jaren zestig ging alle aandacht uit naar de hardware. Toen die computer er eenmaal was, bleek er nauwelijks software voorhanden om erop te draaien. Harry Buhrman vindt dat het voor de quantumcomputer anders moet. Met de 18,8 miljoen euro aan Zwaartekrachtsubsidie die hij onlangs ontving, gaat zijn instituut QuSoft samen met het CWI, de Universiteit Leiden, QuTech, de Technische Universiteit Delft, de Universiteit van Amsterdam en de Vrije Universiteit software ontwikkelen voor quantumcomputers en quantumnetwerken.



OOR
E

Door Leendert van der Ent
Foto IBM

ig ging alle aandacht uit naar
t nauwelijks software voor-

Eenvoudig uitleggen hoe een quantumcomputer werkt is onmogelijk, maar een belangrijk uitgangspunt is wel te geven. Dat is de tegen-intuïtieve mogelijkheid dat een deeltje zich in twee toestanden tegelijk kan bevinden. Bij de huidige computers is een bit één of nul. De bits werken alle stappen in een berekening na elkaar af. Quantumbits (qubits) kunnen tegelijk één en nul zijn. Door deze zogeheten superpositie bekijken ze beide mogelijkheden tegelijk. Koppel je meer qubits aan elkaar, dan gaat het aantal toestanden waarin de qubits zich tegelijkertijd kunnen bevinden exponentieel omhoog.

Harry Buhrman, directeur van QuSoft, faculteitshoogleraar aan de Universiteit van Amsterdam en groepsleider bij het Centrum Wiskunde & Informatica: 'De belofte is duizelingwekkend. Als je met driehonderd qubits tegelijk kunt rekenen, krijg je al meer mogelijkheden dan het aantal moleculen in het heelal. Daarmee lijkt het dat je zo'n beetje alle oplossingen voor berekenbare problemen kunt vinden.'

Maar let op het woordje lijkt, want het idee dat je met een quantumcomputer alle berekeningsproblemen versneld kunt oplossen, is niet waar. Buhrman: 'Op het moment dat je er naar gaat kijken, is een deeltje niet in twee toestanden tegelijk, maar in één van beide met een kansverdeling wat de exacte toestand betreft. Door ernaar te kijken maak je de superpositie stuk en vernietig je feitelijk alle uitkomsten op één na. Als je een experiment herhaalt, zal de uitkomst dan ook niet steeds hetzelfde zijn, wat natuurlijk nogal vervelend is.'

Quantumalgoritmen

Om dit probleem op te lossen, is software nodig. 'Vergelijk het met de werking van een ruisonderdrukkende hoofdtelefoon die met antigeluid ongewenste geluidsgolven wegfiltert en gewenste versterkt. Datzelfde doen quantumalgoritmen. Door middel van interferentie op de superpositie kun je de gewenste berekeningen

'Als je met driehonderd qubits tegelijk kunt rekenen, krijg je al meer mogelijkheden dan het aantal moleculen in het heelal'

deels een mysterie. Waarschijnlijk zal de quantumcomputer goed zijn in het simuleren van quantummechanische systemen met moleculen en elektronen met toepassingen binnen de materiaalkunde, bijvoorbeeld gericht op toepassingen van hogetemperatuursupergeleiding.'

Duidelijk is in elk geval al wel dat de quantumcomputer een kei zal zijn in het factoriseren van getallen: het ontbinden van een getal in priemfactoren. Buhrman: 'Dat is niet alleen maar goed nieuws. Daarmee kun je namelijk veel van de huidige encryptiemethodieken kraken. Nu al slaan geheime diensten gecodeerde berichten op om ze te kunnen kraken als de quantumcomputer klaar is. Een belangrijke software-opgave is dan ook om nieuwe beveiligingen te ontwikkelen die ook de quantumcomputer niet kan kraken.'

Zwaartekrachtconsortium

Afgelopen mei maakten het ministerie van Onderwijs, Cultuur en Wetenschap en NWO bekend welke zes onderzoeksteams elk 18,8 miljoen euro uit het Zwaartekrachtprogramma zouden krijgen voor de uitvoering van hun onderzoeksvoorstellen.
Het Quantum Software Consortium is een van de gehonoreerde teams, en betreft een samenwerking tussen informatici, wiskundigen en natuurkundigen. De financieringsaanvraag is gedaan door Harry Buhrman (CWI, Universiteit van Amsterdam, QuSoft), Dirk Bouwmeester (Universiteit Leiden), Ronald Cramer (Universiteit Leiden, CWI), Ronald Hanson (QuTech, TUDelft), Stephanie Wehner (QuTech, TUDelft) en Ronald de Wolf (CWI, Universiteit van Amsterdam).
Het consortium gaat software ontwikkelen voor