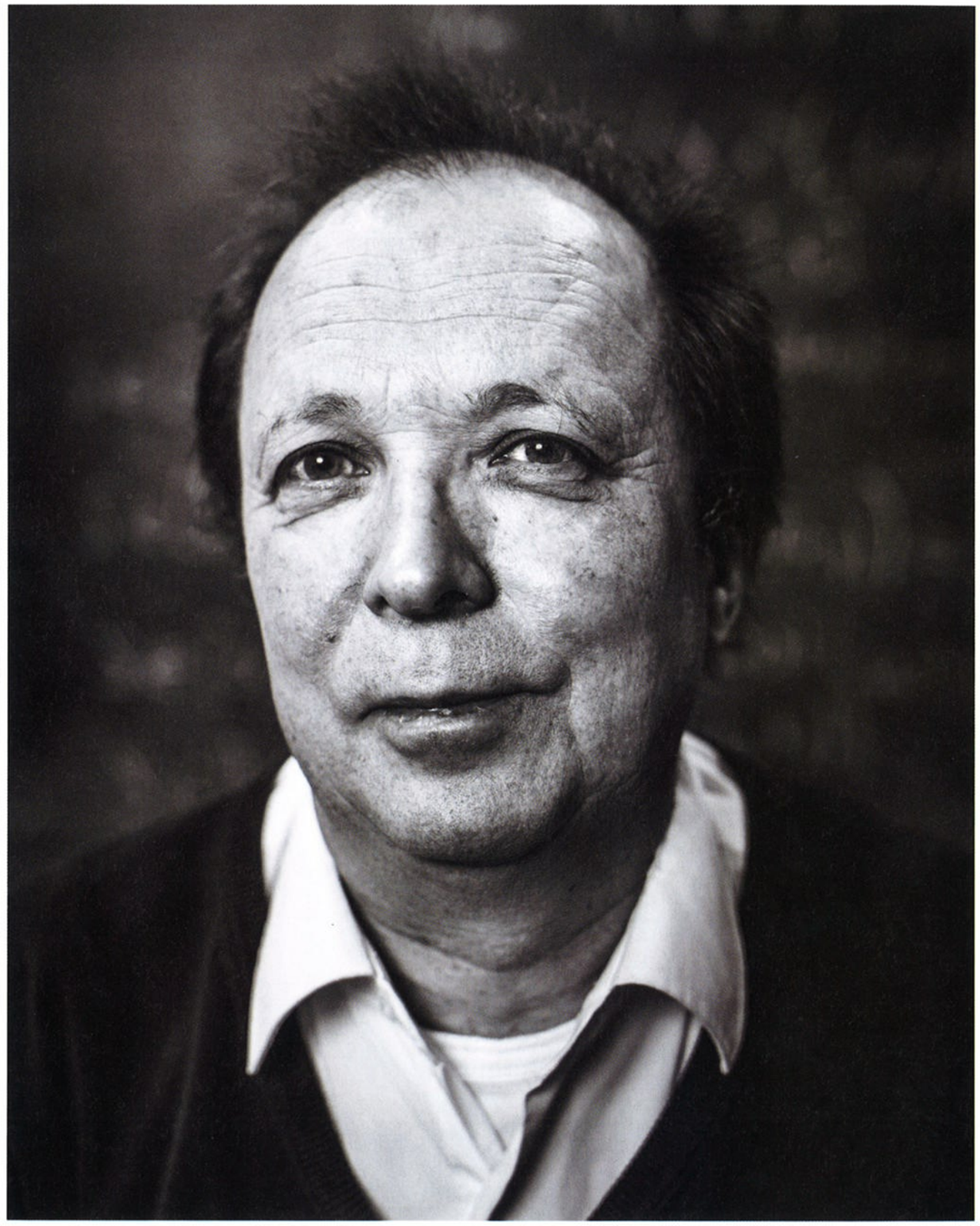

‘Ook een quantumcomputer voorspelt niet feilloos het weer’

De verwachtingen rond de quantumcomputer zijn hoog. Té hoog, zegt wiskundige Bas Edixhoven. ‘Het lijkt me heel sterk dat je het complete weersysteem met een quantumcomputer kunt simuleren.’

Door Jean-Paul Keulen

In de media – en ja, zeker ook in *New Scientist* – verschijnen geregeld verhalen waarin de quantumcomputer wordt neergezet als een enorme stap voorwaarts voor de mensheid. Wiskundige Bas Edixhoven (Universiteit Leiden) ziet het met lede ogen aan. Volgens hem wekken de betrokken wetenschappers geregeld verkeerde verwachtingen en moeten we maar afwachten of de grote beloften van nu worden ingelost.

De capaciteiten van quantumcomputers worden te rooskleurig afgeschilderd?
‘Sowieso wordt vaak gezegd dat de quantumcomputer alles sneller kan doen wat een klassieke computer kan, maar het is helemaal niet bekend of dat zo is. We weten alleen dat er een paar specifieke problemen zijn die een quantumcomputer veel beter kan oplossen dan een klassieke computer. Ook worden er soms toepassingen genoemd die niet geloofwaardig zijn. Zo zei natuurkundige Leo Kouwenhoven in oktober 2015 in *New Scientist* dat een quantumcomputer het complete weersysteem van de aarde kan simuleren en 100 procent accurate voorspellingen kan leveren. Dat lijkt mij heel sterk.’

Waarom kan dat dan niet?
‘Zo’n quantumcomputer moet zijn gegevens ook ergens hebben staan. Hoeveel qubits [de bits waar een quantumcomputer mee werkt, red.] denk je nodig te hebben voor alle informatie over het weer? Dat is niet realistisch. IBM heeft nu een quantumcomputer met enkele tientallen qubits; dat is nog niets in vergelijking met wat je voor zo’n weersimulatie nodig hebt.’

Verder wordt vaak gezegd dat de quantumcomputer al onze beveiligde gegevens kan kraken.
‘Dat klopt voor de nu bestaande protocollen voor cryptografie, die gebruikmaken van het vermenigvuldigen van grote priemgetallen. Maar dan kun je niet zeggen dat quantumcomputer álle cryptografie kan breken. Er zijn hoogstwaarschijnlijk alternatieve vormen van cryptografie met een klassieke computer die wel veilig zijn voor de quantumcomputer.’

Quantumcryptografie wordt opgevoerd als hét alternatief voor de manier waarop we nu gegevens beveiligen.
‘Ja, daarbij zouden we allemaal aan een soort quantuminternet hangen om op die manier onze transacties veilig te laten verlopen. Maar voordat we die methode kunnen toepassen op alles wat we nu met een klassieke computer doen, moet er nog heel veel gebeuren. Het is dan een stuk eenvoudiger om de klassieke methodes quantumveilig te maken.’

Stel dat we straks gegevens wél kunnen beveiligen door middel van quantumcryptografie, is dat dan niet een veel fundamentelere manier van beveiligen dan welke klassieke methode dan ook?
‘Als wiskundige zeg ik: er is op dat gebied nog nooit iets heel sterks bewezen. We weten bijvoorbeeld niet eens of onze huidige protocollen wel veilig zijn als je de quantumcomputer buiten beschouwing laat. Misschien kan het ontbinden van getallen in priemfactoren nog veel sneller dan met de beste methodes van nu – en dan zou een klassieke computer onze huidige beveiligingen ook kunnen kraken. Maar natuurkundigen bewijzen nooit iets zoals een wiskundige dat doet. Die doen alleen maar proefjes, die een bepaald model kunnen ondersteunen of tegenspreken. Dat zie je ook bij quantumcryptografie. Natuurkundigen zeggen dan: het is bewezen vanuit de wetten van de quantummechanica dat die cryptografie niet te breken is. Maar zo’n ‘bewijs’ is gebaseerd op aannames vanuit een bepaald model. En het is maar de vraag in hoeverre je ervan uit mag gaan dat zo’n model klopt.’

> ‘Vergelijk het met energie uit kernfusie. Hoeveel geld is daarin gestoken en hoe ver zijn we nu?’

Grote bedrijven als Microsoft, Google en IBM investeren wel.
‘Het doet denken aan Shell dat miljoenen investeert in duurzame energie. Dat lijkt heel wat, totdat je bedenkt dat het totale budget van zo’n bedrijf miljarden bedraagt. Pas als Shell meer dan de helft van zijn kapitaal inzet op duurzame energie betekent het wat. Hetzelfde geldt voor Google en IBM. Als de quantumcomputer voor hen echt van het hoogste belang zou zijn, zouden ze álles erin stoppen – en dat doen ze niet.’

Toch lijken er grote stappen richting de quantumcomputer te worden gezet.
‘Ik moet het allemaal nog zien gebeuren. Vergelijk het met iets wat al veel langer speelt: energie uit kernfusie. Hoe is het daarmee gegaan? Hoeveel geld is daarin gestoken en hoe ver zijn we daar nu mee? Als wetenschappers weer eens beloven ‘over zoveel jaar hebben we dit-en-dit gerealiseerd’, zet die datum dan eens in je agenda zodat je te zijner tijd kunt kijken of ze die belofte ook zijn nagekomen.’ ■