Publicatie : New Scientist
Datum : 31 dec 2017
cm2 : 1.829
Pagina : 42
Advertentiewaarde : € 6.608,00
Regio : Nederland
Frequentie : 11x per jaar
Oplage : 16.305

Het krachtigste wapen in een cyberoorlog

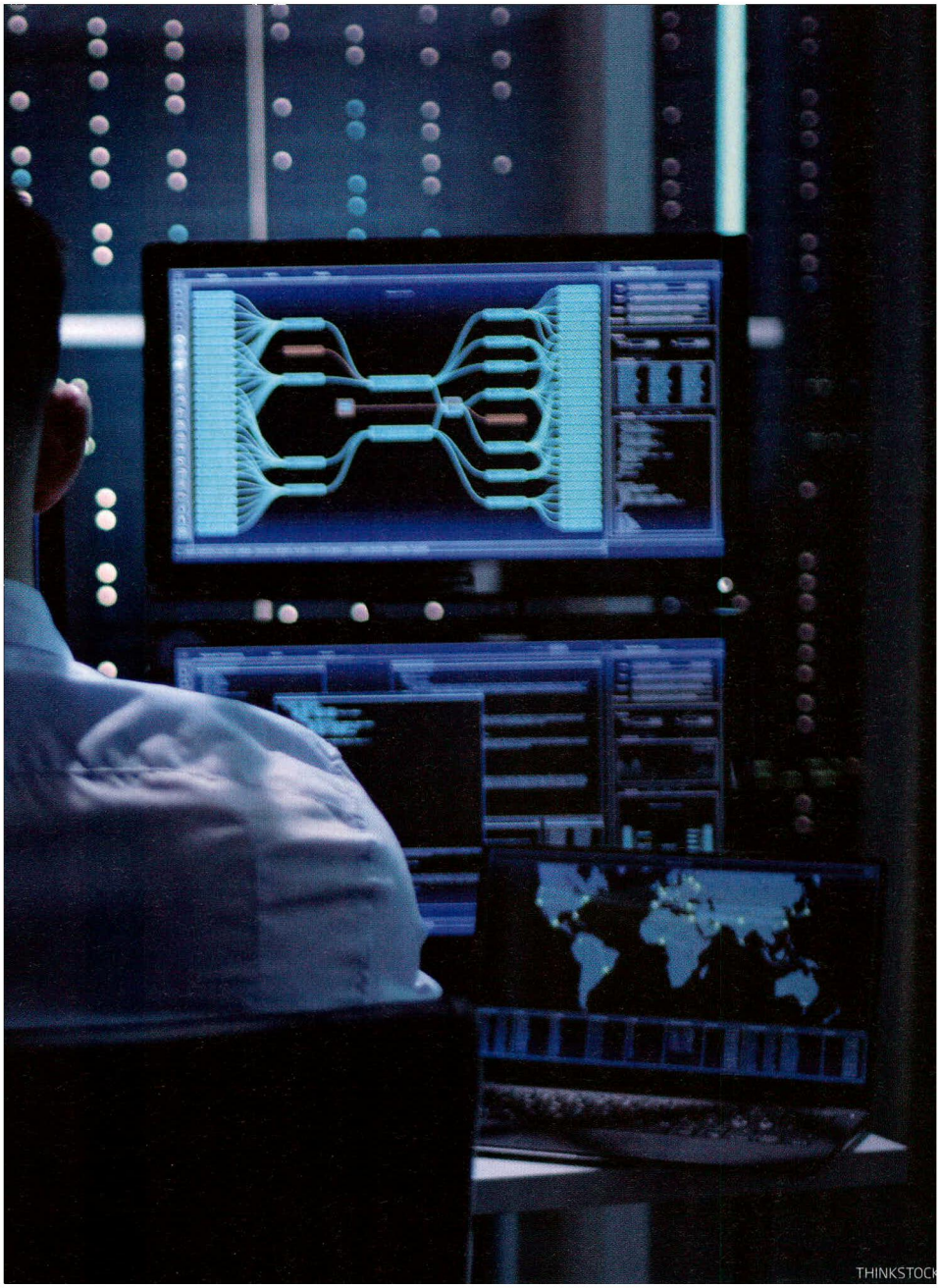
Alle digitale beveiliging is in één klap waardeloos zodra de eerste werkende quantumcomputers verschijnen. Hoe voorkomen we de cryptocalypse?

Door Dorine Schenk

Het is het jaar 2070. Er is een oorlog uitgebroken tussen grootmachten Amerika en Rusland. In het begin merken gewone burgers er weinig van, maar als er geld verdwijnt van Amerikaanse rekeningen, blijven duizenden gezinnen berooid achter. De beveiligingsmethode van de digitale transacties is gekraakt. Er ontstaat paniek. Mensen stormen massaal banken binnen om zo snel mogelijk hun spaargeld veilig te stellen.

Dan beginnen de problemen bij het Amerikaanse leger. Een geheime missie van een onderzeeër wordt ontdekt. Het kan toeval zijn, maar het lijkt alsof de Russen precies weten waar ze moeten zijn. Steeds meer geheime projecten worden gesaboteerd. Ook de beveiligingssystemen van het leger en de geheime diensten zijn gekraakt! Nergens is versleutelde informatie meer veilig. De Russen beschikken over het krachtigste wapen in het digitale tijdperk: een quantumcomputer.

Publicatie : New Scientist
Datum : 31 dec 2017
cm2 : 1.829
Pagina : 42
Advertentiewaarde : € 6.608,00
Regio : Nederland
Frequentie : 11x per jaar
Oplage : 16.305



In werkelijkheid is het nog steeds 2017, maar het geschetste scenario is niet ondenkbaar. In razend tempo zo veel beveiligingssystemen kraken lijkt misschien onmogelijk, maar voor een quantumcomputer is het een peulenschil. Hiermee kun je binnen enkele seconden e-mails, banktransacties en zelfs militaire geheimen achterhalen. Bijna geen enkele vorm van digitale communicatie is veilig voor de supercomputer.

De voorspellingen over wanneer de eerste quantumcomputers in gebruik worden genomen, lopen uiteen van over vijf tot dertig jaar – tot nooit. Maar als ze er komen, kunnen ze quantummechanische trucjes gebruiken om problemen vele malen sneller op te lossen dan mogelijk is met de huidige computers. Voor wetenschappers die hun theoretische modellen willen testen, is dat een zegen, voor de beveiliging van de digitale infrastructuur een vloek. Als deze techniek in verkeerde handen valt kunnen al onze 'gewone' computers razendsnel gekraakt worden. Je e-mails, bestanden en bankgegevens liggen dan op straat.

Een scenario zoals hierboven beschreven, waarbij bijna iedereen nog gebruiktmaakt van gewone computers, maar enkele, wellicht kwaadaardige, instanties in het bezit zijn van een quantumcomputer, staat bekend als de cryptocalypse. Een werkende quantumcomputer die krachtig genoeg is, lijkt nog ver weg, laat staan dat oorlogszuchtige naties of criminelen er een in hun bezit hebben. Maar de risico's zijn groot. Zo groot dat de Amerika veiligheidsdienst NSA, techgigant Google en telecombedrijf KPN al bezig zijn met het beveiligen van gegevens op gewone computers om aanvallen van quantumcriminelen af te kunnen weren. 'Quantumcomputers worden het grootste strategische voordeel sinds kernwapens,' zegt Jaya Baloo, hoofd informatiebeveiliging bij KPN.

'Quantumcomputers worden het grootste strategische voordeel sinds kernwapens'

Ook cryptograaf Leo Ducas van het Centrum Wiskunde & Informatica (CWI) in Amsterdam vindt de mogelijke gevolgen te groot om risico's te nemen. 'Ik weet niet of het ooit zal lukken om een volwaardige quantumcomputer te maken, maar de kans dat het kan gebeuren is genoeg reden om op zoek te gaan naar betere beveiligingsmethoden.' Samen met een internationale groep onderzoekers won Ducas de Internet Defense Prize 2016 voor het ontwikkelen van een nieuw cryptosysteem genaamd NewHope, dat speciaal ontworpen is voor gewone computers om aanvallen van toekomstige quantumcomputers te weerstaan.

Prima priemgetallen

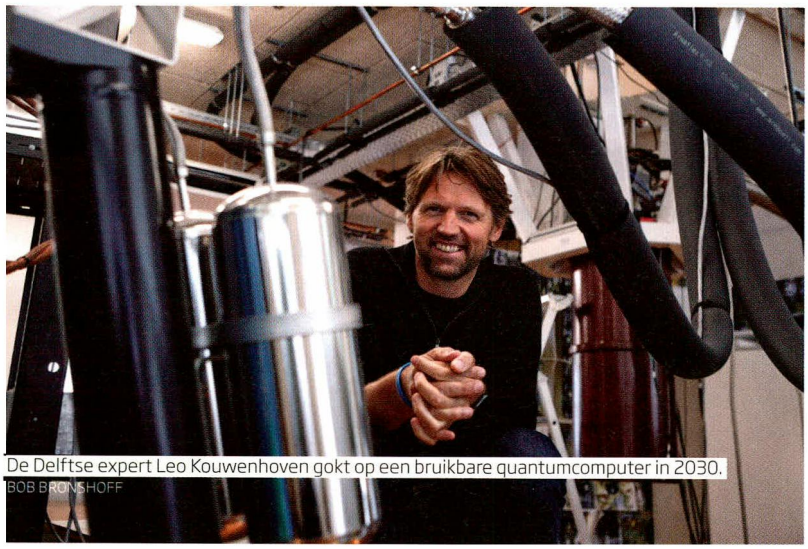
Maar wat maakt de huidige beveiligingssystemen zo kwetsbaar? De huidige digitale communicatiemethoden, zoals e-mailverkeer en banktransacties worden beveiligd door encryptiemethoden die gebaseerd zijn op wiskundige problemen. 'Als je de code kraakt, los je het wiskundige probleem op,' zegt Ducas. Er worden extreem lastige problemen voor gebruikt waar, zover bekend, gewone computers duizenden jaren voor nodig hebben om ze op te lossen. Zo'n code kun je dus niet zomaar kraken door een middagje te puzzelen.

Publicatie : New Scientist
Datum : 31 dec 2017
cm2 : 1.829
Pagina : 42
Advertentiewaarde : € 6.608,00
Regio : Nederland
Frequentie : 11x per jaar
Oplage : 16.305

Hoe lang nog?

Gewone computers rekenen met bits, die een 1 of een 0 zijn. Elke bit bevat dus één eenheid aan informatie (1 of 0, aan of uit). Quantumcomputers rekenen met qubits. Deze blokjes informatie kunnen zowel een 1 als een 0 zijn en alle combinaties daarvan (bijvoorbeeld voor 60 procent 0 en voor 40 procent 1). Omdat één qubit tegelijkertijd een 1 en een 0 kan zijn, is het mogelijk twee berekeningen tegelijkertijd uit te voeren. Met twee qubits kun je vier berekeningen op hetzelfde moment doen en met drie qubit doe je er acht. Hierdoor zijn quantumcomputers ontzettend veel sneller dan de huidige computers in het oplossen van sommige berekeningen (zoals die van RSA-beveiliging). En daar zit het gevaar in. Versleutelingen waar huidige computers miljarden jaren over doen om te kraken, zwichten ineens in enkele seconden.

Hoe ver zijn we eigenlijk met die quantumcomputers? In mei 2017 kondigde computerproducent IBM aan dat ze succesvol een quantumprocessor hebben gebouwd met 17 qubits. Google is aan het testen met 20 en wil aan het eind van het jaar een 49-qubit-processor hebben. Deze minicomputers zijn nog niet krachtig genoeg voor serieuze berekeningen en zullen vooral gebruikt worden voor onderzoek. Omdat qubits kwetsbare onderdelen zijn, is het lastig om een quantumcomputer te bouwen die groot genoeg is om razendsnelle berekeningen uit te kunnen voeren. In de komende jaren wil IBM de 17 qubits uitbreiden naar 50. Dat is een vooruitgang, maar nog lang niet genoeg voor het kraken van serieuze versleutelingen. Het Nederlandse onderzoekscentrum QuSoft in Amsterdam houdt zich bezig met de mogelijkheden van qubits. De onderzoekers kijken welke berekeningen ermee gedaan kunnen worden en ontwikkelen quantumsoftware die kan draaien op quantumcomputers. Een andere uitdaging die overwonnen moet worden, is het herstellen van quantumfouten, die optreden door het gekke quantum-gedrag van qubits. Bij universiteiten en computerbedrijven over de hele wereld wordt gewerkt aan het oplossen van deze obstakels die tussen ons en een werkende quantumcomputer in staan. Een voorbeeld daarvan is het vooruitstrevende QuTech lab in Delft dat samenwerkt met techgigant Microsoft. Voorspellen wanneer het de onderzoekers lukt hun eerste serieuze quantumcomputer bouwen, lijkt lastig. De Delftse expert in quantumcomputers Leo Kouwenhoven gokt op 2030. Maar sceptici zeggen dat de onderzoekers al tien jaar lang 'nog vijftien jaar' roepen. Grote wetenschappelijke doorbraken blijken lastig te voorspellen.



De Delftse expert Leo Kouwenhoven gokt op een bruikbare quantumcomputer in 2030.
BOB BRONSHOFF

Een voorbeeld van een wiskundig encryptiesysteem is RSA. Dit wordt veel gebruikt voor het veilig versturen van gegevens over het internet. Het is vernoemd naar Ron Rivest, Adi Shamir en Leonard Adleman, die de methode voor het eerst beschreven in 1977. Het werkt met zogenaamde priemontbindingen. Om gegevens te beveiligen maak je eerst een sleutel aan. Dit doe je door twee grote priemgetallen te kiezen, bijvoorbeeld 1.319 en 22.511. Vervolgens vermenigvuldig je die met elkaar: 1.319 x 22.511 = 29.692.009. Het achtcijferige getal dat je dan krijgt, is je slot. Hiermee versleutel je je bericht. Degene die het bericht wil bekijken moet het slot openen en heeft daarvoor de geheime sleutel nodig, die bestaat uit de twee gekozen priemgetallen. Iedereen die beschikt over de achtcijferige sleutel kan dus een bericht versleutelen, maar alleen degenen die weten welke priemgetallen eraan ten grondslag liggen weten, kunnen het bericht bekijken.

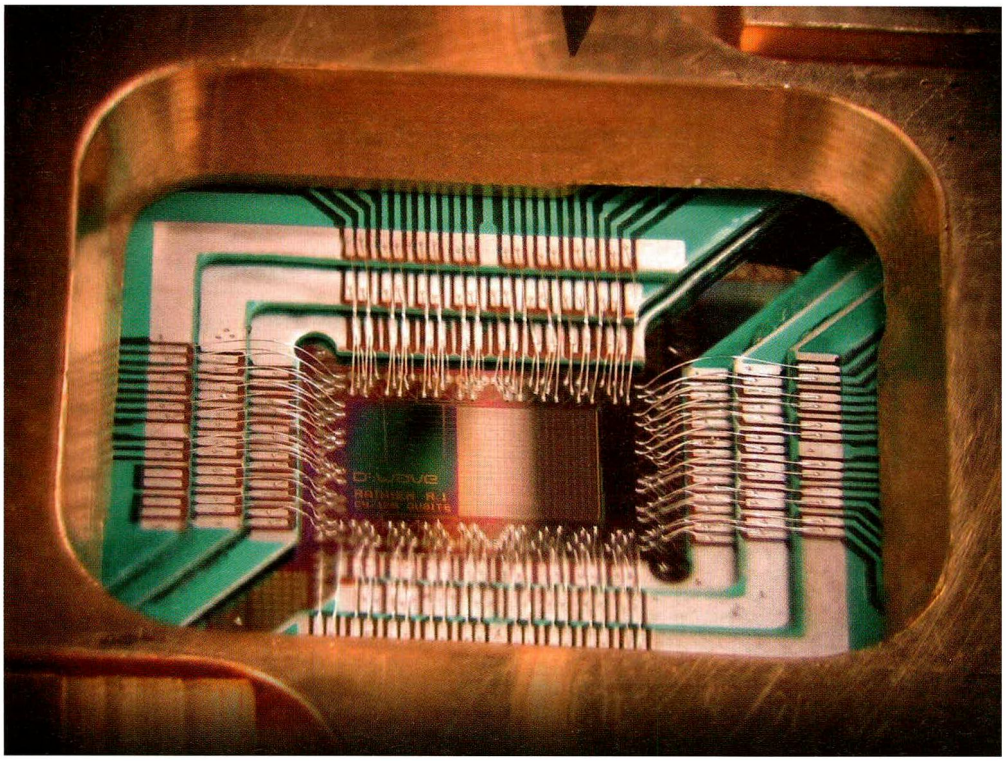
Razendsnel rekenen

Hoe lang het duurt om te achterhalen welke priemgetallen met elkaar vermenigvuldigd zijn om de sleutel te krijgen, is afhankelijk van de lengte van de sleutel. Neem het getal 15. Ze meeste mensen zullen binnen een paar seconden zien dat de priemontbinding daarvan 3 x 5 is. Maar het vinden van de priemontbinding van een getal met 500 cijfers is een stuk lastiger. Met een gewone computer duurt het ongeveer net zo lang als het universum oud is om de priemontbinding te vinden. Het kraken van het RSA-systeem is dus in theorie mogelijk, maar het duurt zo lang, dat het in de praktijk niet lukt, mits de sleutel groot genoeg is. 'De RSA-beveiliging is zelfs door de NSA niet te omzeilen', vertelt hoogleraar wiskunde Bas Edixhoven van de Universiteit Leiden. Maar let op: een quantumcomputer kan dit, in theorie, wel in afzienbare tijd. Het schijnbaar onkraakbare systeem is ineens een lachertje geworden.

Dankzij zogenoemde quantumalgoritmes, die slim gebruikmaken van de rekenkracht van quantumcomputers, kunnen in een razend tempo de priemgetallen gevonden worden waarmee een met RSA versleuteld bericht te openen is.

Het enige wat RSA-beveiliging kan beschermen is het langer maken van de sleutel. Sinds 2014 moeten de sleutels uit meer dan 1024 bits bestaan. En meeste beveili-

Publicatie : New Scientist
Datum : 31 dec 2017
cm2 : 1.829
Pagina : 42
Advertentiewaarde : € 6.608,00
Regio : Nederland
Frequentie : 11x per jaar
Oplage : 16.305



De D-Wave chip met daarin 128 qubits – een enorme doorbraak. Althans: als de claims van de fabrikant kloppen.

gingssystemen gebruiken sleutels van 2048 bits. Dat is voorlopig nog genoeg, zegt Edixhoven. 'Om een RSA-sleutel van meer 1000 bits te kraken, heb je een quantumcomputer met een paar duizend bits nodig.' De komende jaren verwachten experts een processor van hooguit enkele tientallen qubits te kunnen maken (zie kadertekst).

Better safe than sorry

Hoewel we de komende jaren nog niet hoeven te vrezen dat een crimineel met een quantumcomputer onze bankrekening leeg trekt, is er haast geboden. 'Het is mogelijk dat een "grote, boze organisatie" nu al beveiligde data aan het opslaan is en geduldig wacht tot de quantumcomputer er is,' vertelt Baloo. 'Dan kunnen ze in één keer van alle geheimen uit het verleden bekijken.' Als er informatie is die langere tijd geheim moeten blijven, dan is het belangrijk om die zo snel mogelijk te beveiligen.

'Daarom zijn we onder andere bij KPN bezig om het versturen van informatie nog veiliger te maken,' zegt Baloo. Daarvoor gebruiken we drie methoden. Ten eerste worden de sleutels langer gemaakt, zodat de gegevens langer veilig zijn. Vervolgens kan er tussen de plekken waar extreem gevoelige informatie heen en weer gestuurd wordt een glasvezelkabel worden aangelegd die *quantum key distribution* (QKD) mogelijk maakt. Hierbij wordt een quantumsleutel die bestaat uit lichtdeeltjes (fotonen) met bepaalde quantumeigenschappen, verstuurd via de glasvezelkabel. Deze sleutel kan vervolgens gebruikt worden om een versleuteld bestand te openen dat via het internet gestuurd wordt. Bij deze versleutelingsmethode is het meteen zichtbaar als iemand de sleutel heeft onderschept en bekeken. Het bekijken van de quantumeigenschappen verandert namelijk de fotonen van de quantumsleutel, waardoor de ontvanger weet dat hij begluurd wordt. De methode is superveilig, maar vereist het aanleggen van speciale glasvezelverbindingen tussen de contactpersonen. 'Daarom gebruiken we de QKD alleen voor extreem gevoelige informatie,' zegt Baloo. De eerst QKD-verbinding in Nederland is al gelegd; er ligt een glasvezel tussen twee datacentra van KPN in Den Haag en Rotterdam om de methode te testen.

De laatste manier om informatie ook in de toekomst te beveiligen, zonder dat er speciale glasvezelverbindingen nodig zijn, is door nieuwe versleutelmethoden te gebruiken die niet gekraakt kunnen worden door quantumcomputers, genaamd post-quantumcryptografie. 'Ik heb er vertrouwen in dat die methoden gevonden zullen worden; dit is wat mij betreft de toekomstbestendige manier van beveiligen,' zegt Baloo. 'Maar op dit moment kosten de veilige versleutelingsmethoden nog te veel bandbreedte en processorkracht.' De sleutels zijn te groot om praktisch toepasbaar te zijn.

> Onkraakbaar geachte systemen worden ineens een lachertje

Wiskundige redding

Er bestaan wiskundige problemen die ook door een quantumcomputer niet opgelost kunnen worden. Door die om te zetten in versleutelingsmethoden kunnen onze banktransacties voor altijd veilig blijven – of in elk geval totdat iemand een manier vindt om de versleuteling toch te kraken.

Publicatie : New Scientist
Datum : 31 dec 2017
cm2 : 1.829
Pagina : 42
Advertentiewaarde : € 6.608,00
Regio : Nederland
Frequentie : 11x per jaar
Oplage : 16.305

Dat is waar Ducas aan werkt. 'Er zijn verschillende wiskundige problemen die hiervoor gebruikt kunnen worden. Ik werk zelf aan *lattice problems*.' *Lattices* zijn roosters met daarin aangegeven roosterpunten. De wiskundige problemen zijn erop gebaseerd dat het heel erg lastig is om een specifiek roosterpunt te vinden als niemand je de route ernaartoe vertelt (bijvoorbeeld: ga twee roosterpunten omhoog en drie naar rechts). In de wiskunde kun je niet alleen in twee en drie dimensies roosters maken, maar in zoveel je wilt. Als je dan de route wilt beschrijven om bij een geheim roosterpunt te komen, heb je enorme blokken met getallen nodig. Die kunnen in de cryptografie als sleutel dienen. Blokken van 1000 bij 1000 getallen die je op die manier maakt, zijn veilige sleutels, maar ze zijn te groot voor praktisch gebruik. 'Als cryptografen zoeken wij daarom naar slimme trucjes om kleine sleutels te maken, die nog wel zo moeilijk zijn dat ze niet gekraakt kunnen worden', vertelt Ducas.

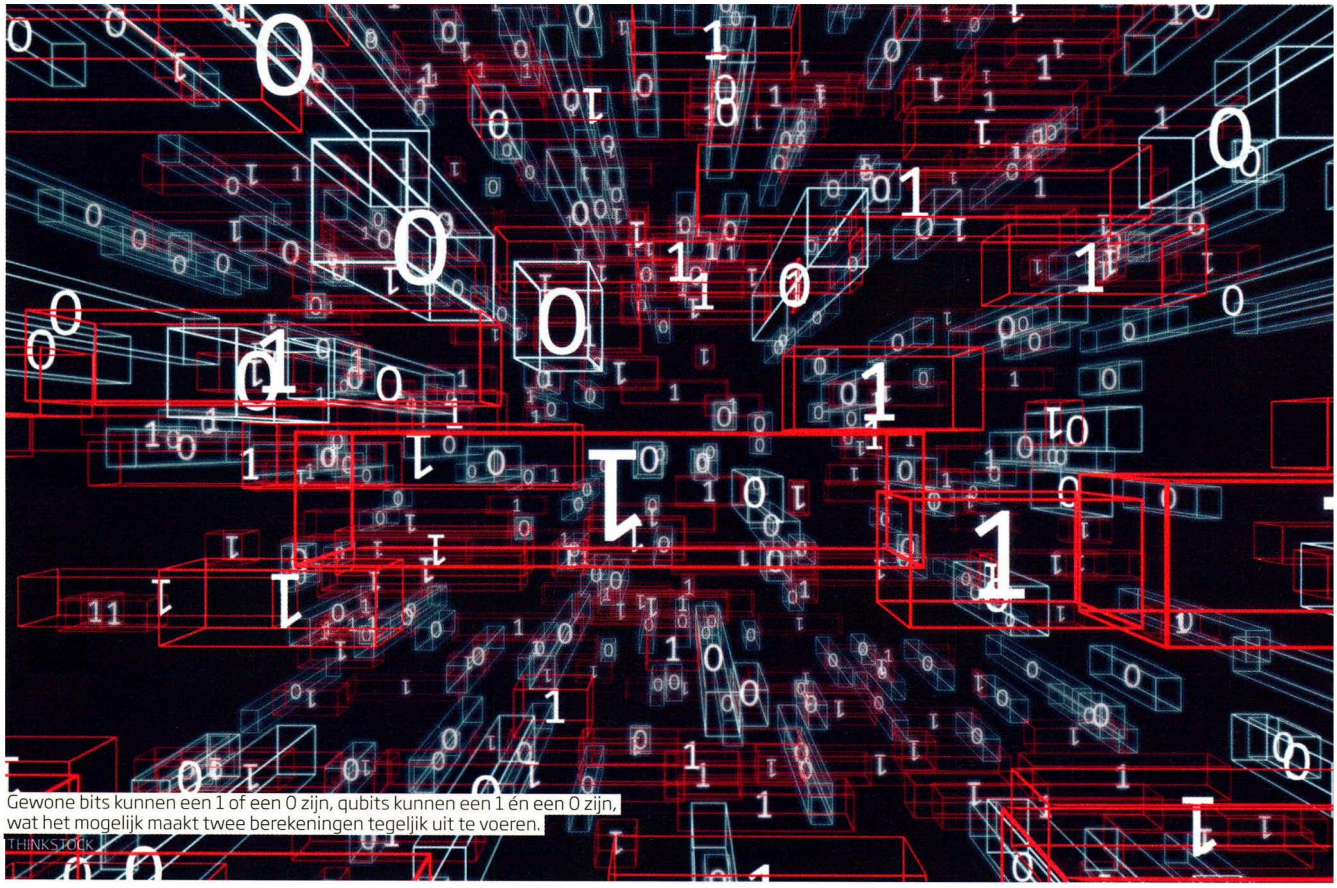
Soms maken ze de sleutels te simpel. 'Eind 2014 kwamen een aantal onderzoekers erachter dat ze te ver waren gegaan. We kraakten hun sleutels.' Het vakgebied kreeg een dreun, maar Ducas geeft niet op. 'We zijn sindsdien voorzichtiger geworden en ik denk nog steeds dat het mogelijk is om met de *lattice problems* veilige en bruikbare versleutelingen te maken.'

Versleutelingen gebaseerd op *lattice problems* zijn nog steeds de meest veelbelovende methode, maar er wordt ook gewerkt aan andere wiskundige problemen die de sleutel kunnen zijn tot veilige transacties. Over de hele wereld wordt door cryptografen gezocht naar wiskundige problemen die ons kunnen behoeden voor een cryptocalypse.

Experts als Ducas en Baloo willen geen enkel risico nemen, ook al is het niet honderd procent zeker dat er ooit een krachtige quantumcomputer komt. Als we onze e-mails en transacties nu al veilig willen stellen, moeten we niet te lang wachten.

'Veilige versleutelingsmethoden kosten op dit moment nog te veel bandbreedte en processorkracht'

Daarom zijn zij en anderen, zoals het Europese project PQCRYPTO, nu al bezig met het ontwikkelen van verschillende beveiligingsmethoden waardoor zelfs een superkrachtige quantumcomputer niet bij onze data kan. Waarschijnlijk lukt het cryptografen om nieuwe versleutelingsmethoden te ontwerpen, gebaseerd op onopgeloste wiskundige problemen. Het kan zomaar gebeuren dat over een paar jaar banken reclame maken met hun 'wiskundig bewezen' en 'quantumcomputerveilige' versleutelingsmethoden. Een grote boze organisatie of criminelen met een quantumcomputer vormen dan geen gevaar. ■



Gewone bits kunnen een 1 of een 0 zijn, qubits kunnen een 1 én een 0 zijn, wat het mogelijk maakt twee berekeningen tegelijk uit te voeren.
THINKSTOCK