WIE IS ER BANG VOOR DE KWANTUMCOMPUTER?

De blockchaintechnologie zal geheel moeten worden herzien

HOE NUTTIG IS DE KWANTUMCOMPUTER? ER IS GOED EN SLECHT NIEUWS, ZEGT ROB VAN DER STAAIJ. HIJ IS GOED VOOR TOEPASSINGEN DIE HET MOETEN HEBBEN VAN VEEL REKENKRACHT, MAAR ER IS SLECHT NIEUWS VOOR DE HUIDIGE ENCRYPTIEALGORITMEN. WIE ZEI OOK ALWEER DAT BLOCKCHAIN INHERENT VEILIG IS? DE HUIDIGE BLOCKCHAIN-TECHNOLOGIE ZAL GEHEEL MOETEN WORDEN HERZIEN.

door Rob van der Staaij beeld Shutterstock

Iedereen die weet wat er in de wereld van de technologie te koop is, heeft er al over gehoord: de kwantumcomputer komt eraan. Maar hoe nuttig of hoe erg is dat? Wat zijn de implicaties ervan? Onheilsprofeten en aanhangers roepen om het hardst dat de kwantumcomputer ons digitale leven op zijn kop zal zetten. Hoe, dat weet niemand nog precies, want de techniek staat nog in de kinderschoenen en de weinige toepassingen zijn nog experimenteel van aard.

Maar dat de kwantumcomputer voor grote veranderingen zal zorgen, is wel zeker. Dit type computer is namelijk in potentie vele malen sneller en krachtiger dan een conventionele computer (zie kader). Dat is goed nieuws en dat is slecht nieuws.

GOED EN SLECHT NIEUWS

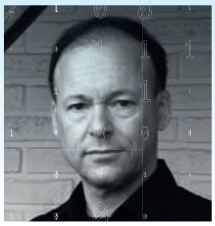
De kwantumcomputer is goed nieuws voor toepassingen die het moeten hebben van veel rekenkracht. Denk aan

NIEUWE ENCRYPTIE-ALGORITMEN

Nieuwe encryptiealgoritmen moeten niet alleen bestand zijn tegen de rekenkracht van de kwantumcomputer, ze moeten ook efficiënt zijn. Encryptiesleutels mogen bijvoorbeeld niet overdreven lang zijn, want dan zou een processor zich erin verslikken. Ook moeten de encryptiesleutels snel genoeg gegenereerd kunnen worden om geschikt te zijn voor realtimetoepassingen.
Onderstaande encryptiealgoritmen zijn veelbelovend (de Engelse termen worden hier gebruikt, omdat het nog ontbreekt aan goede Nederlandse equivalenten).

- Code-based cryptography.
- Supersingular isogeny-based cryptography.
- Lattice-based cryptography.
- Multivariate cryptography.

AUTEUR



ROB VAN DER STAAIJ is oprichter van Stysec (stysec.nl), dat zich richt op advies en trainingen op het gebied van cybersecurity (rstaaij@gmail.com).

kunstmatige intelligentie, het berekenen van klimaatmodellen, het verrichten van metingen in het heelal (waarschijnlijk moet dit meervoud zijn: heelallen) of het analyseren van ingewikkelde scheikundige interacties. Dat laatste is bijvoorbeeld zinvol voor het ontwikkelen van medicijnen. De ontwikkeltijd hiervan kan potentieel worden teruggebracht van tientallen jaren tot enkele weken. Alle reden voor de farmaceutische industrie om zich eens achter de oren te krabben.
De kwantumcomputer is slecht nieuws voor de huidige encryptiealgoritmen. Vooral de bekende asymmetrische encryptiestandaarden, RSA en ECC, zijn kwetsbaar. Die zijn gebaseerd op mathematische principes die voor de conventionele computers van dit moment te complex zijn om te ontwarren, maar waar de kwantumcomputer op een zeker moment korte metten mee zal maken. Het algoritme van Shor is speciaal bedacht om, met behulp van de kwantumcomputer, binnen afzienbare tijd de factoren te ontrafelen van een willekeurig getal, het principe waarop RSA is gebaseerd. De symmetrische encryptiealgoritmen (AES is de belangrijkste) en de hashingalgoritmen (in veel gevallen gebaseerd op SHA-2) zijn eveneens kwetsbaar, maar hier volstaat het waarschijnlijk voorlopig om respectievelijk de sleutellengtes en de hashwaarden te vergroten.

STOOMMACHINE

Hoeveel tijd hebben we nog voordat de gangbare encryptie- en hashingalgoritmen niet meer bruikbaar zijn? Wanneer we het tegenwoordige tempo van de ontwikkeling van de kwantumcomputer in ogenschouw nemen, zal het nog zeker tien jaar duren voordat de asymmetrische encryptiealgoritmen de prullenbak in kunnen. Voor het kraken van een

Het zal nog zeker tien jaar duren

RSA-encryptiesleutel van 2048 bit (de gangbare lengte) heeft een kwantumcomputer volgens de meeste schattingen toch al gauw een capaciteit van enkele duizenden qubits nodig. Daarmee vergeleken is de meest geavanceerde kwantumcomputer van dit moment te vergelijken met een stoommachine.
Maar er zijn meer factoren die eraan bijdragen dat het zo'n vaart nog niet loopt. Kwantumcomputers zijn technisch bijzonder gecompliceerd en nog erg foutgevoelig. Ook zijn er speciale programmeertalen en software voor nodig. Voor het ontwikkelen hiervan is specialistische expertise vereist. Het zal veel tijd vergen die op te bouwen.
Ten slotte is er voor de meeste organisaties voorlopig nog geen businesscase om een kwantumcomputer in te zetten. De kosten hiervan wegen niet op tegen de voordelen, want voor verreweg de meeste toepassingen volstaat conventionele computertechnologie. Dit zal de acceptatie en daarmee de ontwikkeling van commercieel interessante kwantumcomputers remmen.

BLOCKCHAIN

Hoewel we dus nog even respijt hebben, betekent het niet dat er achterovergeleund kan worden. Er is nu al werk aan de winkel. Binnen de meeste organisaties wemelt het van de systemen en de applicaties waarin cryptografie wordt toegepast. Hier volgt een kleine bloemlezing: systemen voor identity- & accessmanagement, PKI-omgevingen, besturingssystemen, VPN-systemen, draadloze netwerken, netwerkcomponenten, systemen voor het ondertekenen van code en data, opslagsystemen, mobiele apparaten, cryptografische API's en instant messaging. Die systemen en applicaties moeten niet alleen allemaal worden geïnventariseerd, vervolgens moet ook worden vastgesteld of en in hoeverre de sleutels en cryptografische mechanismen er hard in zijn gecodeerd. Als dat het geval is, zullen die mechanismen eerst moeten worden losgekoppeld van de rest van de softwarecode om te kunnen worden vervangen. O ja, blockchain is eveneens gebaseerd op cryptografische mechanismen. Wie zei ook

REACTIES EN BIJDRAGEN
Voor reacties en nieuwe bijdragen van IT-experts:
Henk Ester
020-2356415
h.ester@agconnect.nl

WAT IS EEN KWANTUMCOMPUTER?

De werking van de kwantumcomputer is fundamenteel anders dan die van traditionele computertechnologie. Deze laatste is gebaseerd op het verwerken van digitale bits die ofwel een 1 ofwel een 0 als waarde kunnen hebben. De werking van de kwantumcomputer is gebaseerd op de kwantumtoestand van subatomaire deeltjes die bekendstaan als qubits (samengetrokken uit quantumbits). Net als digitale bits vertegenwoordigen qubits informatie. Maar anders dan een traditionele bit kan een qubit gelijktijdig een 1 en een 0 representeren.
Een kwantumcomputer met een capaciteit van drie qubits kan dus tegelijkertijd acht mogelijke combinaties van 1 en 0 opslaan en in één cyclus verwerken: 000, 001, 011, 111, 110, 100, 010, 101. Dat is acht keer zo efficiënt als een conventionele computer met een vergelijkbare capaciteit van drie bits, want die zou voor dezelfde reeks enen en nullen acht opeenvolgende bewerkingen nodig hebben.
Deze eenvoudige rekensom laat ook zien dat de kracht van de kwantumcomputer direct afhankelijk is van het aantal qubits dat deze gelijktijdig aankan. Hoe meer qubits een kwantumcomputer parallel kan verwerken, hoe krachtiger de computer is. IBM biedt inmiddels quantum computing as a service aan met een capaciteit van 20 qubits en heeft al een prototype gereed met een capaciteit van 50 qubits. Recentelijk kondigde Google aan dat het een kwantumchip aan het ontwikkelen is met een capaciteit van 72 qubits.
Overigens wordt het natuurkundige principe waarom een qubit simultaan twee waarden kan hebben nog steeds niet goed begrepen.

alweer dat blockchain inherent veilig is? De huidige blockchaintechnologie zal geheel moeten worden herzien.

WAT TE DOEN?

Wat moeten organisaties doen? Allereerst moeten alle systemen en applicaties worden gelokaliseerd en geïnventariseerd waarin cryptografische mechanismen worden toegepast. Daarnaast moet worden vastgesteld welke algoritmen, sleutellengtes en hashwaarden er in het spel zijn en op welke wijze. Leveranciers, IT-dienstverleners en serviceproviders moeten eveneens worden bevraagd naar hun maatregelen om zich op de komst van de kwantumcomputer voor te bereiden. Nieuwe software moet zo veel mogelijk modulair worden ontwikkeld, zodat cryptografische componenten later gemakkelijker vervangen kunnen worden.
Verder moeten organisaties zich nu al oriënteren op de nieuwe encryptiealgoritmen die volop in ontwikkeling zijn en de belofte in zich hebben opgewassen te zijn tegen de kwantumcomputer (zie kader). In april 2018 heeft het NIST (National Institute of Standards and Technology) de eerste conferentie georganiseerd om nieuwe cryptografische algoritmen te evalueren die bestand zijn tegen de kwantumcomputer.

KWANTUMCRYPTOGRAFIE

Van een geheel andere orde is kwantumcryptografie. In feite gaat het hier niet om cryptografie maar om een bijzondere vorm van distributie. Daarbij wordt gebruikgemaakt van de kwantumeigenschappen van deeltjes – in de praktijk zijn dit meestal fotonen ofwel lichtdeeltjes – om informatie te distribueren op een wijze die niet kan worden verstoord zonder te worden opgemerkt. Hier komt het onzekerheidsprincipe van Heisenberg om de hoek kijken: het gedrag van een subatomair deeltje kan niet worden waargenomen zonder de eigenschappen ervan te veranderen. Dat maakt aftappen van informatie die door middel van kwantumcryptografie wordt gedistribueerd onmogelijk. Om die reden zijn met name overheden en militaire organisaties in de techniek geïnteresseerd. Inlichtingendiensten en hackerscollectieven van buitenlandse mogendheden hebben dan namelijk het nakijken.
Elke vorm van vertrouwelijke informatie, inclusief 'gewone' cryptografische sleutels, kan met behulp van kwantumcryptografie worden verzonden.
Praktische toepassingen van kwantumcryptografie zijn er nog nauwelijks. Er is een speciale infrastructuur voor nodig.
De bestaande IT-infrastructuren zijn ongeschikt voor deze techniek. Waarschijnlijk passen enkele militaire organisaties het al toe.
China heeft in 2016 een satelliet voor kwantumcommunicatie gelanceerd. Sindsdien zijn er enkele succesvolle tests mee uitgevoerd.

STANDAARDEN EN RICHTLIJNEN

Er bestaan diverse richtlijnen en standaarden op het terrein van cryptografie die bruikbaar zijn voor organisaties om zich voor te bereiden op de komst van de kwantumcomputer. Hieronder volgt een overzicht.

- NIST SP (Special Publication) 800-130: aanbevelingen voor het ontwerpen van systemen voor sleutelbeheer.
- NIST SP (Special Publication) 800-131A, revision 1: aanbevelingen voor de transitie van cryptografische algoritmen en sleutellengtes.
- FIPS (Federal Information Processing Standard) Publication 140-2: vereisten voor het ontwerp en de implementatie van cryptografische modules.
- RFC 7696 'Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms': richtlijnen die voorschrijven hoe protocollen kunnen worden gemigreerd van het ene cryptografische algoritme naar het andere.