Kunnen kwantumcomputers versleuteling kraken?

Huidige encryptiestandaarden zijn met hedendaagse computers niet te kraken. Het proces om zoiets te forceren zou met de nu gangbare rekenkracht miljarden jaren duren. Kunnen kwantumcomputers versleuteling echter wel kunnen omzeilen? We spreken er verschillende experts over.

Phil Zimmermann is een bekende Amerikaanse cryptograaf. Hij ontwierp Pretty Good Privacy, ofwel PGP, een veelgebruikte methode om data over het internet te versleutelen, en te bevestigen dat je ook daadwerkelijk met de juiste persoon aan het praten bent.

PGP maakt gebruik van zogeheten public key cryptography. Hierbij bezit elke gebruiker een publieke sleutel en een private sleutel. Met de publieke sleutel, die openbaar beschikbaar is, versleutel je een boodschap, die alleen te ontcijferen is als je de private sleutel hebt, die geheim is. Alleen de beoogde ontvanger van de boodschap heeft die. Vergelijkbare systemen beveiligen tegenwoordig bijna alles wat we online doen, van onze e-mails en videogesprekken tot online bankieren.

Maar in de komende decennia voldoet dat type beveiliging misschien wel niet meer, en daarmee ook het originele werk van Zimmermann, die in Nederland woont en werkt. De oorzaak? Kwantumcomputers. Deze nieuwe generatie computers is gebaseerd op kwantumfysica, en ze slagen er toevallig in om de meestgebruikte onlineversleuteling te kraken.

Wiskundige problemen

De cryptografie die heel wat van onze dagelijkse communicatie versleutelt en mogelijk maakt, is gebaseerd op complexe wiskunde. Meestal gaat het hier over formules, waarbij het makkelijk is om een zaak in één richting te berekenen, maar niet in de andere.

Eén zo'n techniek is het zogeheten factorisatie-probleem. Hierbij neem je, simpel gezegd, twee priemgetallen die je met elkaar vermenigvuldigt. Maar als je het product daarvan neemt, en de originele priemgetallen probeert te herontdekken, dan is dat enorm moeilijk. Die berekening zou met huidige computers meer tijd in beslag nemen dan het universum oud is.

"Rond zulke wiskundige problemen bouwden we alle populaire public-key-versleutelingen", stelt Zimmermann. Iemand die een private sleutel bezit, kan het probleem dus oplossen, maar zonder die sleutel is het praktisch onmogelijk om de originele boodschap terug te vinden."

Maar nu gaan kwantumcomputers die methoden in de toekomst mogelijk onveilig maken. Via een wiskundige techniek genaamd het Shor's algoritme, dat uitgevonden werd in 1994 door wiskundige Peter Shor, kan een kwantumcomputer het factorisatie-probleem oplossen.

Phil Zimmermann, cryptograaf

"Zo'n computer bestaat misschien al binnen tien tot vijftien jaar", stelt Zimmermann. "Een volwaardige kwantumcomputer kan dit probleem in enkele seconden oplossen. Dat zou desastreus zijn. Het zou militaire en diplomatieke communicatie in gevaar brengen. Als je iets online koopt, zou het niet meer veilig zijn en het bancaire systeem zou in gevaar komen."

Verloren strijd?

Sterker nog, het lijkt erop dat deze strijd al deels verloren is. In theorie zou iemand nu al grote hoeveelheden versleutelde data kunnen verzamelen, om die te ontcijferen zodra hij een kwantumcomputer in handen krijgt. De Chinese overheid ontcijfert zo in de toekomst misschien de communicatie van dissidenten van enkele jaren geleden, of cybercriminelen krijgen een hoop oude wachtwoorden in handen die misschien nog in gebruik zijn.

"Jaren geleden was ik hier niet zo bezorgd over", stelt Zimmermann. "Ik studeerde natuurkunde en kwantumcomputers leken me gewoon te moeilijk om te bouwen. Maar enkele jaren geleden waarschuwde de NSA voor dit soort computers. Je mag denken wat je wilt over hen, maar als ze je waarschuwen voor kwantumcomputers, dan let je op. Nu erkennen cryptografen dat we nieuwe versleutelingsmethoden moeten ontwikkelen."

Overheden raken dus wat bezorgd. Een Amerikaans overheidsagentschap houdt momenteel een wedstrijd om nieuwe cryptografische systemen te vinden die niet kwetsbaar zijn voor kwantumcomputers. En in 2020 kondigde de Nederlandse overheid aan dat ze 23,5 miljoen euro in kwantumtechnologie zou investeren, waaronder in cryptografische systemen.

Fundamentele verschillen

Professor Harry Buhrman, computerwetenschapper aan het Centrum Wiskunde & Informatica en de Universiteit van Amsterdam en directeur van het onderzoekscentrum voor kwantumsoftware QuSoft, herkent hoe kwantumcomputers van theoretisch naar urgent gingen. "Ik werk sinds eind jaren negentig aan kwantumcomputers", zegt Buhrman. "Toen was het nog heel esoterisch. Cryptografen deden nog nonchalant over het potentieel van kwantum, maar sindsdien kwam het uit de schaduw van de obscuriteit en staat het volop in de schijnwerpers."

Prof. Harry Buhrman

Een succesvolle kwantumcomputer zou zo, via onder andere Shor's algoritme, de meestgebruikte cryptografie kunnen breken. Maar hoe doen ze dat? "Dat steunt op drie principes", reageert Buhrman. "Het eerste is het superpositieprincipe, dat zegt dat je meerdere berekeningen tegelijk kunt uitvoeren. Maar op een vreemde manier, want je zit uiteindelijk maar één antwoord."

Kwantumcomputers verschillen namelijk fundamenteel van reguliere computers. De gewone versies doen de ene berekening na de andere, hun kwantumtegenhangers maken echter gebruik van principes uit de kwantumfysica, waar soms weinig intuïtieve verschijnselen optreden die verschillende berekeningen tegelijk mogelijk maken. In de kwantumfyscia is een deeltje soms op twee plekken tegelijk, maar wanneer we het observeren, blijft het maar op één positie over.

"Ten tweede is er het principe van interferentie", vervolgt Buhrman. "Verschillende berekeningen in een kwantumcomputer kunnen elkaar uitdoven of versterken. Vergelijk het met een noise-cancelling koptelefoon, die zelf geluid maakt en daarmee ander lawaai dempt. Een kwantumcomputer kan zo berekeningen die niet het goede antwoord opleveren tegen elkaar laten wegvallen, en de goede resultaten elkaar laten versterken."

"Een derde principe is dat van entanglement, waarbij twee kwantumcomputers zich op een niet-klassieke kwantummanier met elkaar verbinden. Zo los je sneller problemen op met minder communicatie."

Niet per se sneller

Dr. Kaitai Liang

Het gaat er dus niet om dat een kwantumcomputer sneller is dan een gewone computer. Dat zijn ze niet, verduidelijkt Buhrman. "Een kwantumcomputer bezit vooral bepaalde technische eigenschappen, afkomstig uit de kwantumfysica, die nieuwe toepassingen mogelijk maken, zoals het openbreken van onze huidige cryptografie."

Voorlopig blijft dat nog wel theorie, aangezien de ontwikkeling van kwantumcomputers maar langzaam verloopt. "De kwantumcomputer van Google, genaamd Sycamore, heeft bijvoorbeeld maar 53 qubits", stelt dr. Kaitai Liang van de cybersecurity group van de TU Delft.

Waar een gewone computer informatie verwerkt in bits, ofwel een 0 of 1, doet een kwantumcomputer dat in qubits, die tegelijk 0 en 1 kunnen zijn, gebruikmakend van het principe van superpositie. “Als je RSA-230 wilt breken, een veelgebruikte cryptografische methode, dan heb je ongeveer 5800 qubits nodig. Maar in de toekomst wordt dit wel mogelijk.”

Gelukkig gaan een hoop cryptografen en onderzoekers inmiddels de strijd aan om nieuwe, kwantumresistente methoden te ontwikkelen. Zo schreef de National Institute of Standards and Technology (NIST), een agentschap van de Amerikaanse overheid, in 2016 een wedstrijd uit waar cryptografen van overal ter wereld nieuwe methoden konden indienen die wel bestand zijn tegen kwantum. Het doel was om tot een selectie van standaarden te komen die onze computers in de toekomst kunnen beveiligen.

Wedstrijd

Professor Tanja Lange van de TU Eindhoven werkte mee aan drie kandidaatvoorstellen die voortkwamen uit de wedstrijd. “Kwantumcomputers breken niet alle cryptografische systemen open”, aldus Lange. “Nu zoeken we systemen die niet te kraken zijn. Het is eigenlijk een historisch toeval dat de systemen die praktisch het hele internet beveiligen kwetsbaar zijn voor dit type aanvallen. Tegelijk bestaan er cryptografische systemen die hier wel tegen bestand zijn, en nu bepalen we welke daarvan we in de toekomst zullen gebruiken.”

De NIST-competitie is letterlijk een wedstrijd. Cryptografen dienden een hoop voorstellen in, en in verschillende rondes vielen de minder succesvolle kandidaten af, soms omdat andere cryptografen de codes wisten te breken. “De eerste ronde kandidaten ging publiek rond kerstmis 2017, en het was toen leuk om de voorstellen van andere kandidaten te kraken”, lacht Lange. “Eén van mijn doctoraatsstudenten lukte dat al binnen een halfuur. Ik kreeg toen het bericht op de trein naar huis, met de vraag over hoe ze het moesten meedelen aan NIST.”


Prof. Tanje Lange

Een van de opties waar Lange aan meewerkte, bouwt voort op het McEliece-cryptografiesysteem dat onderzoeker Robert McEliece al in 1978 voorstelde. “Toen had je natuurlijk nog geen kwantumcomputers”, stelt Lange.

“Zijn systeem heeft een andere structuur, die een kwantumcomputer niet kan uitbuiten. Het is een conservatievere aanpak in die zin dat het een laag risico kent en veiliger is dan strikt noodzakelijk is. Hier verwachten we geen spannende resultaten, maar het is wel een systeem dat al lang meegaat, en daarom waarschijnlijk betrouwbaarder is."

"Gedurende die hele periode slaagde niemand erin om die oudere methoden publiek te kraken. Het zal niet noodzakelijkerwijs voor alle soort communicatie gebruikt worden, maar als je bijvoorbeeld een gesprek met de advocaten voert van Julian Assange, dan wil je misschien deze methode gebruiken, zodat geheime diensten de communicatie zeker niet kunnen kraken.”

Cryptografie en bandbreedte

Een andere onderzoeker die meedoet aan de wedstrijd is dr. Peter Schwabe, faculteitslid aan het Duitse Max Planck Institute for Security and Privacy en daarnaast hoogleraar aan de Radboud Universiteit. “Eén van de voorstellen waar ik bij betrokken ben, heet Kyber”, vertelt Schwabe.

“Het steunt op een wiskundig probleem dat learning with errors heet. In essentie neem je een random of willekeurig element, dat a heet, een geheim element, dat s heet, en een element van noise, of lawaai, dat e heet. En dan doe je, om het heel simpel te zeggen, a*s+e. Een aanvaller kent a en moet s vinden.”

Dr. Peter Schwabe

Met dit soort wiskunde hopen de cryptografen alvast het internet van de toekomst te beveiligen. Hoewel er nog een aantal obstakels de weg daartoe blokkeert. Zo lopen de nieuwe methoden het risico om meer bandbreedte te verbruiken.

“De prestaties zijn anders dat de systemen die we nu al hebben”, vertelt Schwabe. “Bijna allemaal verbruiken ze meer bandbreedte en data. Voor een webbrowser zal dit niet zo’n groot probleem zijn. Je zult waarschijnlijk een lichte daling zien in prestaties. Maar bij apparaten met een beperkt geheugen kom je wel in de problemen. Denk aan smart cars, de cryptografische sleutels passen niet vanzelfsprekend in het lokale geheugen van die voertuigen.”

De kans is groot dat NIST niet één, maar verschillende systemen zal kiezen om het internet mee te beveiligen. Afhankelijk van de behoeften van de gebruiker, kiest die de beste optie. “We willen zo snel mogelijk een akkoord krijgen over deze standaarden”, aldus Schwabe. “Want zo voorkomen we dat mensen nu al data verzamelen en ze die over tien jaar met een kwantumcomputer ontcijferen. Dat is misschien nu al aan de gang, maar we moeten die mogelijkheid zo snel mogelijk blokkeren.”

Onzekerheid

Tegelijk zit er een onzekerheid in het werk van deze cryptografen. Van de systemen die ze nu voorstellen, is het namelijk niet 100 procent zeker dat ze bestand zullen blijven tegen kwantumcomputers. Het is gewoon de beste gok op basis van onze huidige wiskundige kennis. “Om het overdreven te zeggen: het is alsof je een kip slacht en dan met de ingewanden voorspelt of het systeem echt veilig is”, vertelt Lange.

“We doen ons best om tijdens het ontwerpen alle mogelijkheden te bekijken en daarna proberen cryptografen zoveel mogelijk om de voorgestelde systemen te breken. Maar we weten nooit helemaal zeker dat we echt alle opties bekeken. Een systeem dat ouder is, dat dus langer overleefde zonder dat iemand het kraakte, boezemt natuurlijk meer vertrouwen in. Maar er bestaat de mogelijkheid dat over enkele jaren een slim iemand voorbijkomt en iets ziet dat iedereen tot nu toe gemist heeft.”

Dit is iets waar Harry Buhrman ook voor waarschuwt. “We weten niet of er voor andere types cryptografie ook een kwantumalgoritme bestaat”, stelt hij. “In zekere zin blijft het een soort gok. Misschien is er een algoritme dat we nog niet kennen, dat nieuwe cryptografische systemen oplost.”

Voorlopig is dit een risico waarmee we moeten leren leven, maar in de toekomst lossen kwantumcomputers dit probleem gedeeltelijk zelf op. “Met kwantummechanica kun je ook cryptografische systemen bouwen”, stelt Buhrman. “Hier gebruik je in plaats van gewone computers en communicatie, kwantumcommunicatie. De partijen sturen qubits naar elkaar en in die wereld zijn bepaalde zaken wel aantoonbaar veilig. Het maken van een gezamenlijke geheime sleutel kun je op die manier veilig doen. Dit geldt niet voor alle cryptografie, maar hier kun je wel aantonen dat het absoluut veilig is.”

Dat klinkt dus erg goed, maar de technologie is er nog niet klaar voor. “Het grote nadeel is dat we geen kwantumcommunicatie bezitten”, stelt Buhrman. “We werken nu erg hard om kwantumnetwerken te bouwen. Maar dat loopt ver achter op het gewone internet. Op dit moment vormt dit geen oplossing. Het duurt ook nog wel even voor we dit kunnen, ik schat minstens tien jaar. De zaken die uit de NIST-competitie komen, kun je daarentegen nu implementeren, alhoewel we niet 100 procent zullen weten of ze veilig zijn.”

In de praktijk

Drs. ir. Maran van Heesch

Maar zodra de nieuwe standaarden er zijn, moeten die nog in de praktijk gebracht worden. Een groot deel van de cryptografie van het internet zal dus een update moeten krijgen; geen makkelijke uitdaging.

Drs. ir. Maran van Heesch van TNO werkt aan dat vraagstuk. “Binnen anderhalf jaar verwachten we de eerste standaarden van NIST, hoewel er daarna mogelijk nog extra rondes komen”, aldus van Heesch. “Maar als je die standaarden hebt, moet je die ook goed implementeren. Dat is een grote uitdaging. Voor bedrijven gaat dit niet alleen over de post-kwantumcryptografie; het vormt een heel bedrijfsproces waar ze door moeten."

"Ze moeten verkennen wat er intern gebeurt en onder andere kijken waar de cryptografie zit in al hun systemen. Ze moeten daar vaststellen waar ze zelf actie moeten nemen of wachten op de acties van anderen. Daarna komt pas de post-kwantumcryptografie."

Een heel aantal bedrijven, waarvan een deel IT-systemen gebruikt die decennia oud zijn, zal de cryptografie moeten aanpassen. Daarom vindt van Heesch het belangrijk dat er nu al actie komt. “We mogen niet wachten tot de standaarden er zijn”, stelt ze. “Er zijn heel wat acties die je nu al kunt ondernemen. Het zal nog even duren voordat de standaarden goed geïmplementeerd zijn, maar dat neemt niet weg dat we dit nu al moeten voorbereiden.”