January 2021
Smals Research

Smals
ICT for society

Kwantumcomputers & cryptografie

Kwantumcomputers, hun impact op moderne cryptografie en de zoektocht naar kwantumresistentie

Kristof Verslype, PhD

Inhoud

Voornaamste bevindingen

Dit rapport bevat vier hoofdstukken. Voor elk van die hoofdstukken worden hieronder de voornaamste bevindingen gegeven.

Kwantum- Vs. klassieke computer

Terwijl klassieke computers gebaseerd zijn op Newtoniaanse – zeg maar de klassieke – fysica, zijn kwantumcomputers gebaseerd op principes uit de kwantumfysica, met name *superpositie* en *verstrengeling*. De kleinste reken- en informatieenheid is de *qubit*.

Berekeningen gebeuren op fundamenteel andere wijze dan bij klassieke computers. Klassieke programmeertalen volstaan bijgevolg niet.

Er is een beperkte, maar zeer interessante, categorie van problemen waar kwantumcomputers in excelleren. Daaronder problemen die moeilijk moeten blijven om moderne cryptografie veilig te houden.

Kwantum (niet) in de praktijk

Vandaag is er geen enkel probleem dat een kwantumcomputer kan oplossen dat een klassieke computer niet kan oplossen. Het is discutabel of kwantumcomputers vandaag sneller zijn dan klassieke computers voor ten minste één probleem dat in de praktijk nutteloos mag zijn.

Kwantumcomputers zijn ontzettend moeilijk te bouwen. Onder de uitdagingen vinden we isolatie – qubits zijn immers enorm gevoelig voor interferentie van buitenaf –, foutencorrectie – fouten zullen nooit helemaal vermeden kunnen worden –, en schaalbaarheid. Ook de topologie (layout) van de processor van een kwantumcomputer levert uitdagingen op.

De huidige generatie universele kwantumcomputers, gebouwd door onder meer *Google*, *IBM* en *Rigetti*, bevatten een paar tiental qubits. Daarnaast zijn er de *D-Wave* kwantumcomputers gebaseerd op een ander principe uit de kwantumfysica. Deze machines zijn makkelijker te bouwen en bevatten vandaag een paar duizend qubits. Het is evenwel onduidelijk of deze machines daarmee krachtiger zijn dan universele kwantumcomputers met een paar tiental qubits.

Het aantal qubits is sowieso geen goede maatstaf voor de kracht van een kwantumcomputer. Er zijn nog tal van andere aspecten die daarop een sterke impact hebben.

De crypto-apocalypse?

Het *algoritme van Grover* zou een voldoende krachtige kwantumcomputer in staat stellen om de veiligheid van symmetrische cryptografie en cryptografische hashfuncties te verminderen. Het volstaat om de lengte van de symmetrische sleutel te verdubbelen en de uitvoerlengte van cryptografische hashfuncties met 50% ter verhogen om eenzelfde veiligheidsniveau te behouden als in een wereld zonder krachtige kwantumcomputers.

Het *algoritme van Shor* stelt een kwantumcomputer in staat om de huidige generatie publieke sleutelcryptografie onveilig te maken.

Om het algoritme van Shor of het algoritme van Grover een bedreiging te laten vormen voor de moderne cryptografie, is een kwantumcomputer met miljoenen (fysieke) qubits vereist.

Kwantumresistente cryptografie

Het NIST heeft een procedure lopen met als doel te komen tot kwantumresistente standaarden voor publieke sleutelcryptografie. Er zijn twee luiken: een luik *digitale handtekeningen* en een luik *encryptie en key*

exchange. Verwacht wordt dat in 2021-2022 de procedure afgerond zal worden.

Men verwacht het meest van *lattice-based cryptografie*. De NSA heeft zijn vertrouwen hierin reeds uitgesproken.

Er is geen imminente dreiging. Daarom bevelen we aan de NIST procedure af te wachten en pas daarna te overwegen om geleidelijk naar de nieuwe standaarden te migreren.

Voorwoord

"*Vertel eens*," vroeg Wittgenstein aan een vriend, "*waarom zegt men altijd dat het normaal was dat de mens aannam dat de zon rond de aarde draaide in plaats van dat de aarde rond haar as draaide?*" Zijn vriend antwoordde: "*Wel, het is toch duidelijk dat het lijkt alsof de zon rond de aarde draait.*" Wittgenstein antwoordde: "*Wel, hoe zou het eruit hebben gezien indien het leek alsof de aarde rond haar as draaide?*"

De Oostenrijkse filosoof Ludwig Wittgenstein (1989-1951) is ongetwijfeld één van de meest invloedrijke filosofen uit de moderne geschiedenis. Bovenstaande dialoog geeft perfect aan waarom we niet steeds mogen vertrouwen op intuïtie. Intuïtie is namelijk een onbewuste extrapolatie van wat we reeds kennen, en van daaruit komen mensen vaak tot foute conclusies, die dan uitgedrukt worden in bewoordingen zoals "*Het is natuurlijk*", "*Het is logisch*" en *"Het kan toch niet anders*". Intuïtie is helaas enkel waardevol bij het evalueren van situaties die gelijkaardig zijn aan deze waar we reeds in het verleden mee geconfronteerd werden.

Voor de meeste stervelingen is het atomaire en subatomaire niveau echter een totaal ongekende wereld, met een logica die lichtjaren ver lijkt te staan van wat we als mens rondom ons ervaren. Kwantumfysica is de wetenschappelijke discipline die die wereld van het atomaire en subatomaire tracht de doorgronden. Het is een wereld die weinig ruimte laat voor intuïtie, met dus weinig referentiepunten uit onze vertrouwde wereld. Dat maakt kwantumfysica een erg moeilijk te doorgronden domein.

Niettemin zou het wel eens een nooit geziene aardbeving kunnen veroorzaken in de moderne cryptografie. Op basis van principes uit de kwantumfysica kunnen immers – vandaag nog enkel in theorie – computers gebouwd worden die naar verluidt de fundamenten van de moderne cryptografie zullen ondermijnen en vervolgens genadeloos zullen opblazen.

In onze hedendaagse samenleving is deze cryptografie echter cruciaal, onder meer voor allerlei financiële transacties, het beveiligen van uw medische gegevens en het beschermen van de nationale belangen.

Het tijdperk van de kwantumcomputers lijkt nochtans snel dichterbij te komen. In de populaire media lezen we geregeld schreeuwerige titels. Bedrijven claimen revolutionaire doorbraken. Grootmachten investeren miljarden waardoor het zelfs wat doet denken aan een nieuwe wapenwedloop.

Bij bedrijven en overheidsinstellingen groeit samen met de onduidelijkheid ook de ongerustheid. Hoogtijd dus om wat klaarheid te brengen in deze complexe problematiek.

Dit rapport is een herwerking van een vierdelige artikelenreeks die in de loop van 2020 verschenen is op www.smalsresearch.be en tracht op een toegankelijke manier inzicht verschaffen in deze complexe wereld.

Het rapport is onderverdeeld in vier hoofdstukken die afzonderlijk gelezen kunnen worden, elk met een eigen conclusie. Het eerste hoofdstuk legt de achterliggende principes van kwantumcomputers uit. Het tweede hoofdstuk schijnt een licht op de huidige stand van zaken in kwantumcomputerland. Het derde hoofdstuk behandelt de dreiging van kwantumcomputers voor de hedendaagse cryptografie. Het vierde hoofdstuk, ten slotte, bespreekt de zoektocht naar kwantumresistente cryptografie, dus cryptografie die zelfs door een krachtige kwantumcomputer niet gekraakt kan worden.

Ik wens u alvast veel leesplezier!

Kristof Verslype
Cryptograaf bij Smals Research

Kwantum- Vs. klassieke computer

Dit hoofdstuk gaat eerst in op de limieten van de klassieke computer en vervolgens op de soms weinig intuïtieve eigenschappen van kwantumcomputers. Daarna bespreken we hoe met kwantumcomputers gerekend kan worden en hoe krachtig die berekeningen kunnen zijn.

De limieten van de klassieke computer

De wet van Moore – eigenlijk een extrapolatie – stelt dat om de zoveel tijd het aantal transistors op een chip verdubbelt. Oorspronkelijk was dit om de 12 maand, maar het is ondertussen afgevlakt naar 24 maand. Velen nemen aan dat ze rond 2025 zal ophouden. Krachtigere klassieke computers bouwen wordt meer en meer een uitdaging.

Evolutionair gezien lijkt de opkomst van kwantumcomputers dan ook logisch. Klassieke computers zijn gebaseerd op Newtoniaanse – dus de klassieke – fysica. Men bouwt daarbij steeds kleinere circuits. Vandaag zijn ze nog nauwelijks enkele nanometers. Als je maar voldoende inzoomt kom je op den duur onvermijdelijk op atomair en subatomair niveau en dus in een wereld waar de kwantummechanische wetten spelen. De kwantumfysica is krachtiger dan de Newtoniaanse en bijgevolg lijkt het dat ook kwantumcomputers – in theorie althans – krachtiger zijn dan de Newtoniaanse.

Eigenschappen van kwantumcomputers

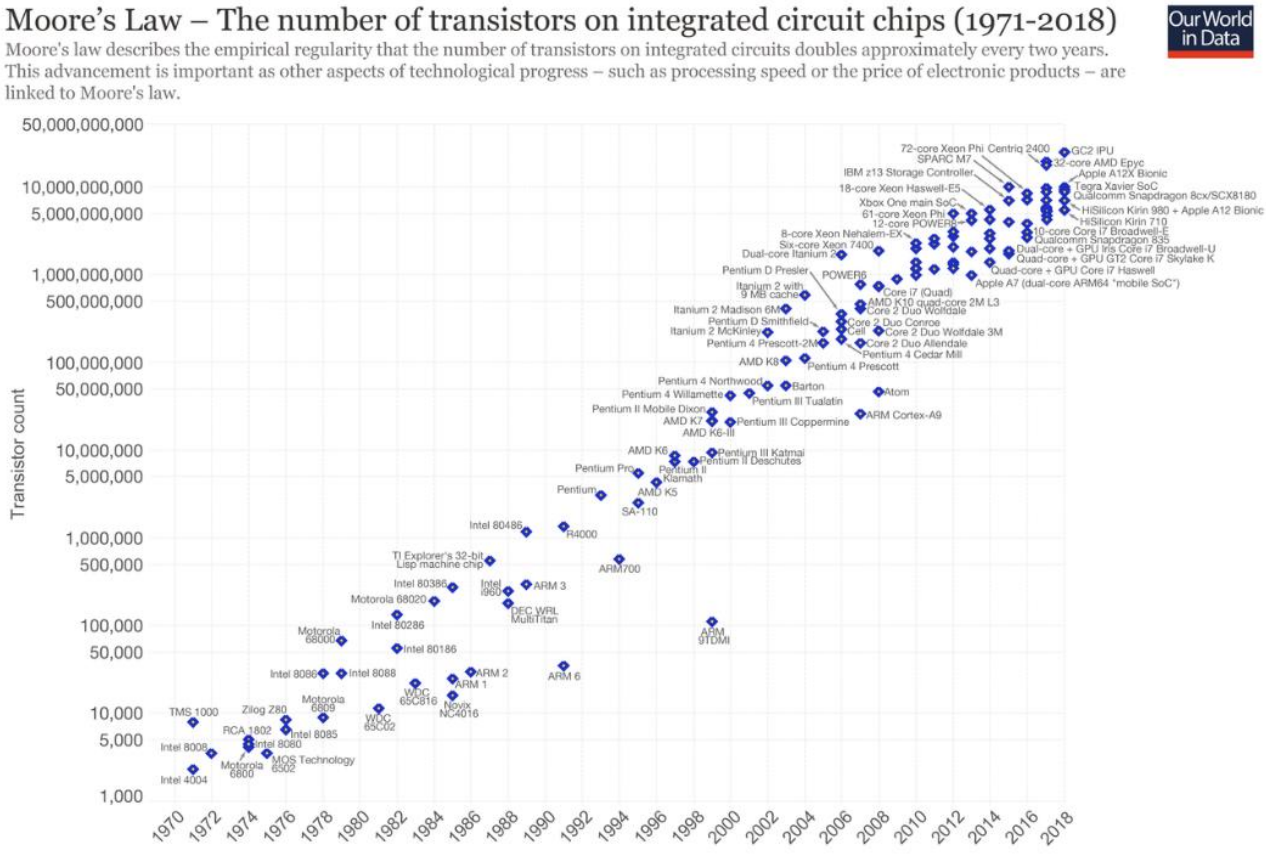
Klassieke computers hebben als kleinste informatie- en verwerkingseenheid de bit, die ofwel de waarde 0 ofwel de waarde 1 heeft. Bij kwantumcomputers is de kleinste informatie- en verwerkingseenheid de *qubit* (quantum bit), wat een klein deeltje is, zoals een foton of elektron, en waar dus de kwantummechanische effecten ten volle spelen en ook benut worden.

Volgens kwantummechanica gedragen kleine deeltjes, zoals elektronen, ionen en fotonen, zich als golven (en vice versa), waarmee bedoeld wordt dat hun toestand – snelheid, positie, spin, polarisatie – 'uitgesmeerd' is over de verschillende mogelijke toestanden en daarbij geen specifiek karakter kent. Pas bij het meten neemt deze golf één concrete toestand aan. Een elektron, bijvoorbeeld, krijgt bij het meten één concrete spin (rotatie om zijn as). Men zegt dat de golffunctie bij het meten ineenstort.

Dat brengt ons bij de eerste eigenschap van qubits: de *superpositie*. De waarde van een qubit is onbepaald tot op het moment van de meting, wat met een bepaalde waarschijnlijkheid 0 als resultaat geeft, en met een bepaalde waarschijnlijkheid[1] 1. Vaak wordt gesteld dat een qubit de waardes 0 en 1 tegelijkertijd heeft, maar een dergelijke formulering maakt de zaken nodeloos complex en mystiek. Pas bij de meting neemt de qubit dus een concrete waarde aan (0 of 1). We zeggen dat de qubit bij de meting ineenstort, aangezien haar toestand niet langer een superpositie (het mogelijke) is maar één concrete waarde (het feitelijke). Het uitlezen van een qubit verstoort dus haar toestand.

Door het probabilistisch karakter zal het meten van verschillende qubits in dezelfde toestand (dus met dezelfde waarschijnlijkheidsdistributie) niet steeds hetzelfde resultaat geven. Volgens de Kopenhaagse de meest populaire – interpretatie van de kwantummechanica is de uitkomst van een meting volledig ondeterministisch en dus – i.t.t. tot de Newtoniaanse fysica – niet aan de hand van andere

[1] In de kwantumfysica spreekt met niet over waarschijnlijkheden, maar over amplitudes, die elk beschreven worden a.d.h.v. een complex getal.



FIGUUR 1. DE WET VAN MOORE IN DE PRAKTIJK

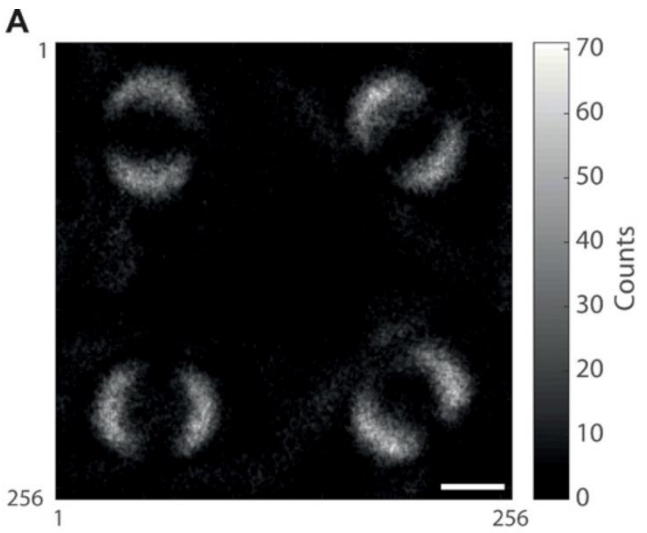
factoren te verklaren. Voor Einstein was dit problematisch, wat wordt weergegeven door het populaire, door hem meerdere malen herhaalde citaat "*Jedenfalls bin ich überzeugt, daß der nicht würfelt.*" ("*Ik ben er in elk geval van overtuigd dat Hij [God] niet dobbelt.*")

Een tweede kwantumeigenschap is de *verstrengeling* (entanglement), wat wil zeggen dat er een correlatie bestaat tussen de metingen van twee of meerdere verwante deeltjes, waarbij de fysieke afstand tussen de deeltjes er niet toe doet. Als twee qubits verstrengeld zijn met een gelijke superpositie dan weten we dat beide qubits bij lezing dezelfde waarde zullen teruggeven. We hoeven dus maar één qubit te lezen om te weten wat het resultaat zou zijn bij lezing van de andere qubit.

Dit lijkt in tegenspraak met wat eerder gezegd is, namelijk dat de uitkomst van een meting volledig ondeterministisch is. Experimenteel werd echter reeds met hoge waarschijnlijkheid aangetoond dat de correlatie niet te verklaren is aan de hand van lokale variabelen en dat er dus hoogstwaarschijnlijk een soort connectie tussen de deeltjes is, onafhankelijk van hun afstand. Dit is tegenintuïtief en strijdig met de Newtoniaanse fysica, waarbij afstand wel degelijk een cruciale rol speelt bij de invloed die objecten op elkaar uitoefenen. Zelfs Einstein had het er moeilijk mee en noemde dit vreemde verschijnsel spottend "*spukhafte Fernwirkung*" ("*spookachtige werking op afstand*"). Voorlopig moeten we dit, gegeven de ondertussen sterke experimentele bevestiging, aanvaarden als meest waarschijnlijke hypothese.

Rekenen met kwantumcomputers

Berekeningen met klassieke bits gebeuren op het laagste niveau met behulp van logische poorten, zoals de NOT, AND en OR poort. Het manipuleren van één, twee of een beperkt aantal qubits gebeurt daarentegen met behulp van kwantum logische poorten (die beschreven worden door matrixoperaties met complexe getallen). De *Pauli-X* poort in de kwantumwereld komt



FIGUUR 2. DE EERSTE FOTO'S OOIT VAN KWANTUMVERSTRENGELING (2019) [1].

bijvoorbeeld overeen met de NOT poort bij klassieke computers. Na het toepassen van de Pauli-X poort op een qubit verwisselen de waarschijnlijkheden (meer correct, de amplitudes) om 0 en 1 te meten. Daarnaast zijn er nog vele andere poorten, zoals de *Hadamard* poort die gebruikt wordt om (sets van) qubits te initialiseren. Een toegankelijke intro tot het manipuleren van qubits met behulp van kwantum logische poorten is de *Hello Quantum* app van IBM, die zowel voor iOS als Android beschikbaar is. Het wordt gepresenteerd als een spelletje waarbij je puzzels moet oplossen om naar een hoger niveau te gaan.

Kwantumalgoritmes zijn dus gebouwd op een totaal andere logica dan die voor klassieke computers. Ze vereisen dan ook specifieke assembleertalen, programmeertalen en ontwikkelomgevingen (Software development kits). Enkele kwantum assembleertalen zijn *Quil* en *OpenQASM*. Voorbeelden van kwantum programmeertalen zijn *Quantum Computation Language (QCL), Q#* en *Q language*. Bestaande ontwikkelomgevingen zijn o.a. *Qiskit, ProjectQ* en *Forest* en zijn vandaag vaak gebaseerd op bestaande programmeertalen zoals *Python*.

De populaire perceptie dat de kwantumcomputer in alles de klassieke computer zal verslaan is trouwens fout. Voor het overweldigende deel van computerberekeningen bieden kwantumcomputers geen performantiewinsten ten opzichte van klassieke computers [2]. Het is een populaire misvatting dat

FIGUUR 3. IBMS HELLO QUANTUM APP. MANIPULEER TWEE VERSTRENGELDE QUBITS M.B.V. PAULI-X POORTEN!

kwantumcomputers alle problemen zullen kunnen oplossen die moeilijk (of zelfs onmogelijk) zijn voor klassieke computers.

Er is weliswaar een beperkte, maar zeer interessante, categorie van problemen waar kwantumcomputers in excelleren. Daaronder vinden we problemen die moeilijk zijn voor klassieke computers en sowieso moeilijk moeten blijven om de moderne cryptografie veilig te houden. Anders gezegd zullen voldoende krachtige kwantumcomputers een groot deel van de moderne cryptografie kunnen kraken of op zijn minst verzwakken. Dit verklaart meteen ook grotendeels de investeringen van grootmachten zoals China en de VS in de technologie [3]. De beveiligde communicatie van de tegenstander kraken is altijd al zeer interessant geweest en heeft in de Tweede Wereldoorlog trouwens niet enkel geleid tot een cruciale wending, maar ook tot de ontwikkeling van de klassieke computer.

Verder wordt ook naar kwantumcomputers gekeken voor optimalisatieproblemen, simulaties en machine learning, maar dit valt buiten de scope van dit rapport.

Kwantumcomputers zijn bovendien probabilistisch en geven dus enkel met hoge waarschijnlijkheid correcte resultaten.

Conclusie

Samengevat maken kwantumcomputers gebruik van weinig intuïtieve kwantummechanische effecten zoals superpositie en verstrengeling. Daarmee steunt het op fundamenteel andere – en krachtigere – principes dan klassieke computers.

Toch blijft er nog veel onduidelijkheid over het potentieel. Koen Bertels, een Belgische professor aan de TU Delft en hoofd van het Quantum Computer Architectures Lab aan diezelfde universiteit stelde recent: "*Hoeveel keer sneller [kwantumcomputers zullen zijn] is echter nog koffiedik kijken. Misschien 10 keer, misschien 100 keer. Sommigen hebben het zelfs over 100 miljoen keer sneller*." [4]

Het grote voordeel dat een krachtige klassieke computer vandaag geniet ten opzichte van een krachtige kwantumcomputer is dat hij effectief bestaat. Maar dat kan natuurlijk ooit veranderen. Bereiden we ons dan toch alvast niet best voor op een tijdperk? De volgende hoofdstukken gaan hier dieper op in.

Kwantum (niet) in de praktijk

Dit hoofdstuk gaat in op de huidige stand van zaken in kwantumcomputerland en schijnt een licht op vragen zoals: "*Hoe ver staan we met de bouw van kwantumcomputers?*", "*Hoe moeilijk is het bouwen ervan?*" en "*Zullen ze binnen 10 jaar klassieke computers op vele fronten ingehaald hebben?*" .

Quantum supremacy

Quantum computing wordt momenteel erg gehypet. Niet alleen liggen de verwachtingen erg hoog maar ook de terminologie is misleidend, meer bepaald de term *quantum supremacy* (kwantumsuperioriteit) die een veel zwakkere inhoud heeft dan wat de term op zich doet vermoeden. De term werd in 2012 voorgesteld door John Preskill [5]. Het doel van quantum supremacy is aantonen dat een kwantumcomputer een probleem kan oplossen dat een klassieke computer in de praktijk niet kan, onafhankelijk van het nut van deze oefening. Het oplossen van exact één, in de praktijk nutteloos probleem, volstaat bijgevolg om quantum supremacy te bereiken. Het luidt dus allerminst het einde in van de klassieke computer. Preskill schreef in 2019 zelf dat de term niet ideaal is, niet alleen omdat het de hype versterkt, maar ook omwille van de sterke ideologische lading van het woord '*supremacy*' [6].

Google claimde eind 2019 in het natuurwetenschappelijk tijdschrift *Nature* quantum supremacy door middel van hun *Sycamore* kwantumcomputer, die 53 werkende qubits bevatte [7]. De claim had weliswaar betrekking op een in de praktijk nutteloos probleem, met name het genereren van willekeurige gekozen getallen volgens een zeer specifieke distributie die makkelijk is voor een kwantumcomputer maar moeilijk voor een klassieke computer, gezien die laatste daarvoor complexe simulaties moet doen. Hun kwantumcomputer kon dit in 200 seconden, daar waar een klassieke computer, aldus Google, 10 000 jaar nodig zou hebben.

IBM sprak de claim al snel tegen en stelde dat een klassieke computer dit, conservatief geschat, in 2,5 dagen zou kunnen en bovendien met een veel hogere nauwkeurigheid [8]. Ook Koen Bertels, een Belgische professor aan de TU Delft en hoofd van het *Quantum Computer Architectures Lab* aan diezelfde universiteit, is duidelijk [4]: "*De recente claim van Google, waarbij ze beweerden dat hun kwantumcomputer een complexe berekening véél sneller kon uitvoeren dan de krachtigste supercomputers die we momenteel hebben, is simpelweg niet waar.*" Ondanks de sterke prestatie van Google is hun claim van quantum supremacy betwistbaar. Toch is dit wellicht slechts een kwestie van tijd voor dit werkelijk het geval zal zijn.

Hoogstens – en ook dit is betwistbaar – is *quantum advantage* bereikt, waarmee doorgaans bedoeld wordt dat een kwantumcomputer een – al dan niet nuttig – probleem sneller kan oplossen dan een traditionele computer. Reeds in 1994 werd daartoe het probleem van Simon bedacht, wat volstrekt nutteloos is, maar, net zoals het Sycamore experiment, op zo'n wijze geconstrueerd was om een kwantumcomputer een maximaal voordeel te geven ten opzichte van een klassieke computer. Tot op heden is quantum advantage hier nog niet aangetoond.

Waar staan we vandaag? IBM claimt een kwantumcomputer met 53 qubits, Googles Sycamore heeft er 54 (waarvan eentje niet werkte tijdens hun fameuze experiment). Google claimde reeds in 2018 met hun Bristlecone een 72 qubit computer [9]. Toch mag niet enkel gekeken worden naar het aantal qubits. Ruis en foutenmarges op verschillende vlakken, het niveau van verstrengeling tussen de qubits, de eigenschappen van de ondersteunde kwantum logische poorten zijn voorbeelden van aspecten die bijdragen aan de uiteindelijke kracht van de machine. IBM gebruikt daarom de term *quantum volume* om aan te geven hoe krachtig een kwantumcomputer werkelijk is [10]. Helaas worden doorgaans maar weinig technische details prijsgegeven over kwantumcomputers, waardoor een eerlijke, objectieve vergelijking moeilijk is.

Het bedrijf D-Wave verkoopt zogenoemde Adiabatische kwantumcomputers, waarbij hun krachtigste model 5000 qubits bevat. De kostprijs is onbekend, maar het prijskaartje van hun vorige model met 2048 qubits was zo'n 15 miljoen dollar. Het aantal qubits van deze

FIGUUR 4. TWEE D-WAVE KWANTUMCOMPUTERS

machines lijkt enorm vergeleken met de kwantumcomputers van o.a. IBM en Google. Het is echter gebaseerd op een ander paradigma uit de kwantummechanica - de Adiabatische stelling - waarbij veel minder verstrengeling vereist is. Testen door onder meer NASA, Google en ETH Zurich hebben niet kunnen aantonen dat de huidige generatie D-wave machines quantum advantage hebben, wat zoals eerder reeds aangegeven, betekent dat er een – al dan niet nuttig - probleem is waarvoor ze sneller zijn dan klassieke computers. Sommigen betwijfelen zelfs of dat ooit het geval zal zijn. De D-Wave machine werd in de markt gezet voor optimalisatievraagstukken en niet voor het kraken van moderne cryptografie. Toch zijn dergelijke kwantumcomputers in theorie equivalent met de universele kwantumcomputers, zoals die van Google en IBM [11]. Weliswaar zal een D-Wave steeds meer qubits nodig hebben dan een even krachtige universele kwantumcomputer.

Een kwantum-computer bouwen

Het bouwen van een kwantumcomputer is enorm complex. Dit om verschillende redenen, waaronder isolatie, foutencorrectie en schaalbaarheid.

Laat ons eerst kijken naar de *isolatie*. Qubits zijn kleine deeltjes zoals elektronen (met spin) of fotonen (met een polarisatie). Die deeltjes zijn enorm gevoelig voor interferentie van buitenaf en moeten dus aan temperaturen dicht tegen het absolute nulpunt (-273,15° C) bewaard worden, afgeschermd van onder meer trillingen, licht en magnetische straling. Deze isolatie maakt het moeilijk om de qubits te controleren, te manipuleren en te lezen. Eén van de vele uitdagingen voor kwantumcomputers is het voldoende lang coherent houden van zijn toestand. De probabiliteiten – of correcter, de amplitudes – om 0 of 1 te meten kunnen immers verstoord worden alsook de verstrengeling tussen qubits. Men spreekt over de decoherence time om aan te geven hoe lang qubits in een coherente kwantumtoestand blijven. In het geval van supergeleidende circuits, zoals in Googles Sycamore, situeert die *decoherence time* zich in de grootteorde van tienden of honderdsten van een microseconde [12]. Er is de voorbij jaren veel vooruitgang geboekt om qubits beter af te schermen, maar desondanks zullen fouten allicht nooit helemaal vermeden kunnen worden. Hoogstens misschien ergens in de verre toekomst, voorbij onze huidige horizon. Radioactieve straling blijft bijvoorbeeld aanwezig, zelfs op het absolute nulpunt.

Daarom lijkt *foutencorrectie* noodzakelijk, waarbij meerdere fysieke qubits samen één logische qubit vormen. De fysieke qubits mogen tot op zekere hoogte fouten bevatten zonder dat het de waarde van de logische qubit die ze samen vormen impacteert. Die foutencorrectie is theoretisch mogelijk, hoewel het nog als onmogelijk beschouwd werd in de jaren ‘80 en ’90 van de vorige eeuw. Zo kunnen vijf fysieke qubits vereist zijn om één logische qubit te bekomen [13]. Dit zal uiteraard stijgen indien de onderliggende qubits meer onderheving zijn aan fouten. Sowieso kan foutencorrectie enkel toegepast worden indien de qubits voldoende lange tijd in een coherente toestand blijven, wat op zich al een enorme uitdaging is.

Kwantumfoutencorrectie is een actief, maar vandaag wel een puur theoretisch onderzoeksdomein. We zitten zelfs nog niet in de fase van de experimenten. De huidige generatie kwantumcomputers maken er bijgevolg geen gebruik van (en kunnen dat ook niet [14]). Toch lijkt het op termijn een noodzakelijkheid. Niettemin betwijfelen sommigen of foutencorrectie überhaupt wel in de praktijk mogelijk is. Eén van hen, niet de minste, is professor fysica *Mikhail Dyakonov* aan de Université Montpellier. Eind 2018 schreef hij [15]: “*How many physical qubits would be required for each logical qubit? No one really knows, but estimates typically range from about 1,000 to 100,000.*”

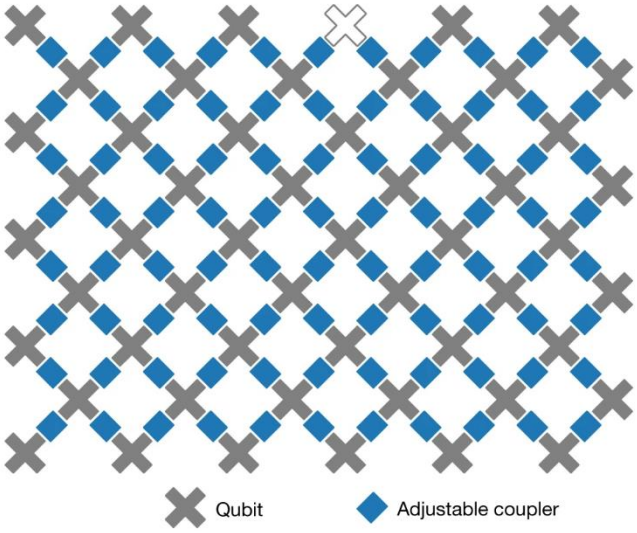
Dit brengt ons bij een andere uitdaging waar Dyakonov op ingaat: *schaalbaarheid.* De toestand van een traditionele computer met N bits wordt beschreven aan de hand van N bits. De toestand van een traditionele computer met 1000 bits wordt dus beschreven door 1000 bits, ofwel ongeveer 300 decimale cijfers. De toestand van een kwantumcomputer met N verstrengelde qubits wordt beschreven door 2^N complexe getallen (ofwel 2^{N+1} reële getallen). Voor een kwantumcomputer met 1000 qubits betekent dit dus 2^{1000} (ongeveer 10^{300}) complexe getallen.

Het werken met een kwantumcomputer houdt in dat de qubits, beschreven a.d.h.v. complexe getallen, gemanipuleerd worden met behulp van de kwantum logische poorten die op hun beurt beschreven worden aan de hand van - soms erg grote - matrices met complexe getallen (zie hoofdstuk 1). Het is voor uw auteur vooralsnog onduidelijk hoe dit praktisch realiseerbaar zou kunnen zijn voor een kwantumcomputer met voldoende qubits om enigszins nuttig te zijn. Dyakanov: "*A useful quantum computer needs to process a set of continuous parameters that is larger than the number of subatomic particles in the observable universe.*" Vergeet niet dat de foutencorrectie van daarnet dit verder doet exploderen.

De complexiteit van kwantumcomputers stijgt dus exponentieel met het aantal qubits. Anders gezegd: één qubit erbij verdubbelt de complexiteit van de kwantumcomputer. Dit is anders bij klassieke computers. Daar stijgt de complexiteit lineair, wat betekent dat de complexiteit pas verdubbelt als ook het aantal bits verdubbelt.

Dit zijn maar drie van de uitdagingen. De huidige generatie kwantumcomputers op basis van supergeleidende circuits, zoals die van IBM en Google, hebben nog andere ernstige beperkingen. Bij een klassieke computer kun je bijvoorbeeld berekeningen doen op twee (of meer) waardes in het RAM geheugen, onafhankelijk van hun relatieve posities in het RAM geheugen. Ze hoeven dus niet aangrenzend te zijn. Kwantumcomputers op basis van supergeleidende circuits laten enkel operaties (door middel van poorten) toe op individuele qubits en op qubits die aan elkaar grenzen. Zoals figuur 5 toont, grenst een qubit in de Sycamore machine ten hoogste aan vier andere qubits.

Volgt u nog? Samengevat zijn de uitdagingen enorm en lijken ze voor sommigen zelfs simpelweg



FIGUUR 5. DE 54 QUBITS IN DE SYCAMORE KWANTUMCOMPUTER VAN GOOGLE. EÉN BIT BOVENAAN WAS ECHTER DEFECT OP HET MOMENT VAN DE TESTEN. TEVENS DOET DE FIGUUR - MISSCHIEN NIET GEHEEL TOEVALLIG - DIENST ALS OPTISCHE ILLUSIE. (BRON: NATURE)

onoverkomelijk. Sowieso is het interessant om te zien hoe de horizon van wat als mogelijk beschouwd wordt steeds opschuift. Foutencorrectie werd niet zo heel lang geleden zelfs puur theoretisch als onmogelijk beschouwd. Een nieuwe, inventieve benadering kan plots heel wat deuren doen opengaan. Toch is de realiteit vandaag dat de kwantumcomputer nog maar in zijn kinderschoenen staat en dat het enorme middelen zal vergen om die te ontgroeien.

Conclusie

Het idee van de kwantumcomputer dateert reeds van 1980 is daarmee ondertussen 40 jaar oud. Voorlopig zijn er experimenten door onder meer Google, IBM en Intel die getuigen van de enorme vooruitgang in het veld. Anderzijds zien we ook dat de luide claims toch wat in perspectief geplaatst dienen te worden en dat kwantumcomputers nog in hun kinderschoenen staan, al zijn er diverse beloftevolle initiatieven.

In de toekomst kijken is sowieso onmogelijk en er is dan ook niemand die met zekerheid kan zeggen of een nuttige kwantumcomputer ooit praktisch mogelijk zal zijn, laat staan wanneer. De meest optimistische schattingen gaan uit van vijf tot tien jaar, de meer voorzichtige plaatsen de horizon tussen 20 en 30 jaar in

de toekomst. Ten slotte is er nog een minderheid die stelt dat het sowieso niet binnen voorzienbare toekomst zal zijn.

Een nuttige kwantumcomputer betekent overigens niet per se dat die ook onmiddellijk in staat zal zijn alle moderne cryptografie te breken. Wat exact de gevaren zijn van kwantumcomputers op de moderne cryptografie maakt het onderwerp uit van het volgende hoofdstuk.

De crypto-apocalypse?

Welke impact zullen kwantumcomputers hebben op onze moderne cryptografie, die levensnoodzakelijk is in onze samenleving? Dit hoofdstuk bespreekt de impact op symmetrische encryptie, op cryptografische hashfuncties en op publieke sleutelcryptografie.

Symmetrische encryptie

Bij symmetrische encryptie gebeurt encryptie en decryptie met dezelfde sleutel (zie figuur 6). *AES* (Advanced Encryption Standard) is vandaag de wereldwijde standaard, die ongeveer 20 jaar geleden ontwikkeld werd aan de KU Leuven. Vandaag biedt een AES-sleutel die 256 bits lang is (AES-256) een veiligheid van 256 bits, wat wil zeggen dat er $2^{256} \approx 10^{77}$ (een 1 gevolgd door 77 nullen) mogelijke sleutels zijn. De efficiëntste aanval doet niet veel beter dan het één na één testen van alle mogelijke sleutels, tot de juiste gevonden is. Doordat de zoekruimte zo enorm groot is, is dit gewoon onbegonnen werk en zijn de kansen op succes verwaarloosbaar.

In 1996 stelde *Lov Grover* echter een kwantumalgoritme (Grover's algorithm) voor dat de zoekruimte om de inverse te berekenen van een blackbox functie verkleint van N tot $\sqrt{N}$, waarbij N het aantal mogelijke inputs (de zoekruimte) is. In het geval van symmetrische vercijfering bestaat die blackbox uit niet alleen het vercijferalgoritme, maar ook de symmetrische sleutel.

Het algoritme van Grover biedt daarmee een kwadratische versnelling voor het vinden van symmetrische sleutels. De zoekruimte van een AES-256 sleutel verkleint immers van $2^{256} \approx 10^{77}$ tot $\sqrt{2^{256}} = 2^{128} \approx 10^{38}$ (een 1 gevolgd door 38 nullen). Om een zelfde veiligheidsniveau als vandaag te behouden in een tijdperk met krachtige kwantumcomputers, volstaat het dus om de sleutellengte te verdubbelen. Dat valt al bij al goed mee.

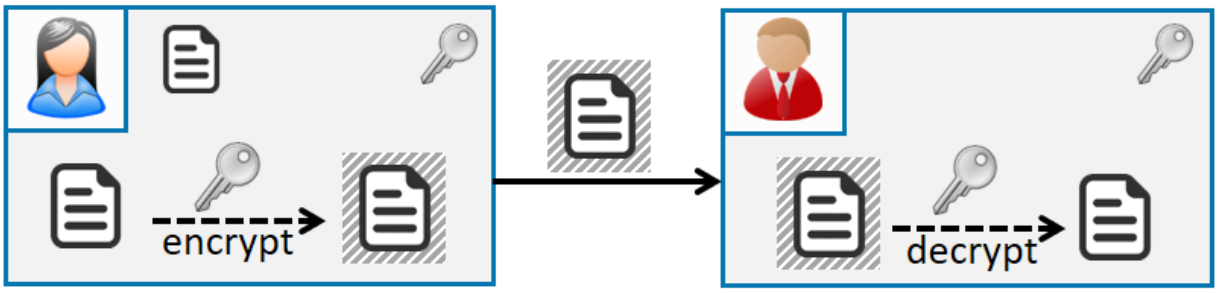
Onderzoekers berekenden in 2016 dat voor AES sleutels van 128, 192 en 256 bits respectievelijk 2953, 4449 en 6681 logische qubits vereist zijn voor het uitvoeren van het algoritme van Grover [18]. (Zie hoofdstuk 2 voor het onderscheid tussen logische en fysieke qubits.)

Het algoritme van Grover steunt op de aanname dat er reeds een orakel bestaat - een grote kwantum logische poort (zie hoofdstuk 1) - dat meermaals toegepast wordt op de N (logische) qubits samen. Dit orakel is in feite een (kwantum)representatie van de blackbox. In werkelijkheid zal dit orakel afgeleid moeten worden uit de (klassieke) blackbox functie. Het is voor uw nederige auteur vooralsnog onduidelijk hoe deze voorbereidende stap sneller dan lineair uitgevoerd kan worden. Dit is nochtans een conditio sine qua non om kwantumcomputers zelfs nog maar in theorie een bedreiging te laten vormen voor symmetrische cryptografie.

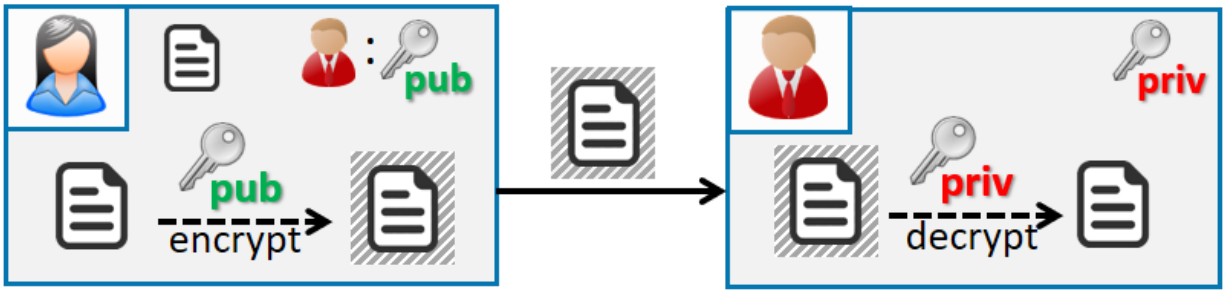
Samengevat vormt het algoritme van Grover vandaag slechts op papier en onder een zware assumptie een bedreiging voor symmetrische encryptie. Het werd tot op heden nog niet op een kwantumcomputer uitgevoerd, zelfs niet met erg korte sleutels. Indien die bedreiging zich ooit zou concretiseren, kunnen we daar bovendien mee omgaan door de sleutellengte te verdubbelen.

Cryptografische hashfuncties

Cryptografische hashfuncties laten toe een unieke fingerprint te berekenen van data, zonder dat die fingerprint informatie prijsgeeft over die data zelf. Het is een cryptowerkpaard dat in de praktijk enorm vaak gebruikt wordt, bijvoorbeeld bij het plaatsen van digitale handtekeningen en bij het bouwen van blockchains. De output van eenzelfde hashfunctie (dus de fingerprint) heeft daarbij een vaste lengte, onafhankelijk van de grootte van de input.



FIGUUR 7. ENCRYPTIE EN DECRYPTIE M.B.V. EENZELFDE, GEDEELDE SYMMETRISCHE SLEUTEL



FIGUUR 6. ENCRYPTIE MET EEN PUBLIEKE SLEUTEL EN DECRYPTIE MET DE CORRESPONDERENDE PRIVATE SLEUTEL

Wanneer voor een cryptografische hashfunctie twee inputs gevonden worden die dezelfde output genereren, kan de cryptografische hashfunctie niet langer als veilig beschouwd worden. Voor de SHA1 hashfunctie – nog steeds in gebruik op vele eID kaarten – werd een dergelijke collision in 2017 gevonden [19]. Dit alles heeft niets te maken met kwantumcomputers, maar toont wel aan hoe strikt men is voor cryptografische hashfuncties (en cryptografie in het algemeen), gezien het vaak een kwestie van tijd is voor een aanval die er op het eerste zicht misschien nogal onschuldig uitziet verder verfijnd wordt. Dat gebeurde dan ook in 2019 met een publicatie die een krachtigere en praktischere aanval beschrijft [20].

Een hashfunctie met een output van 256 bits heeft een veiligheid van 128 bits door de *verjaardagenparadox*[2], mits de aanvaller beschikt over voldoende schijfruimte om 2^{128} hashwaarden te bewaren. Vandaag is zo'n aanval onhaalbaar.

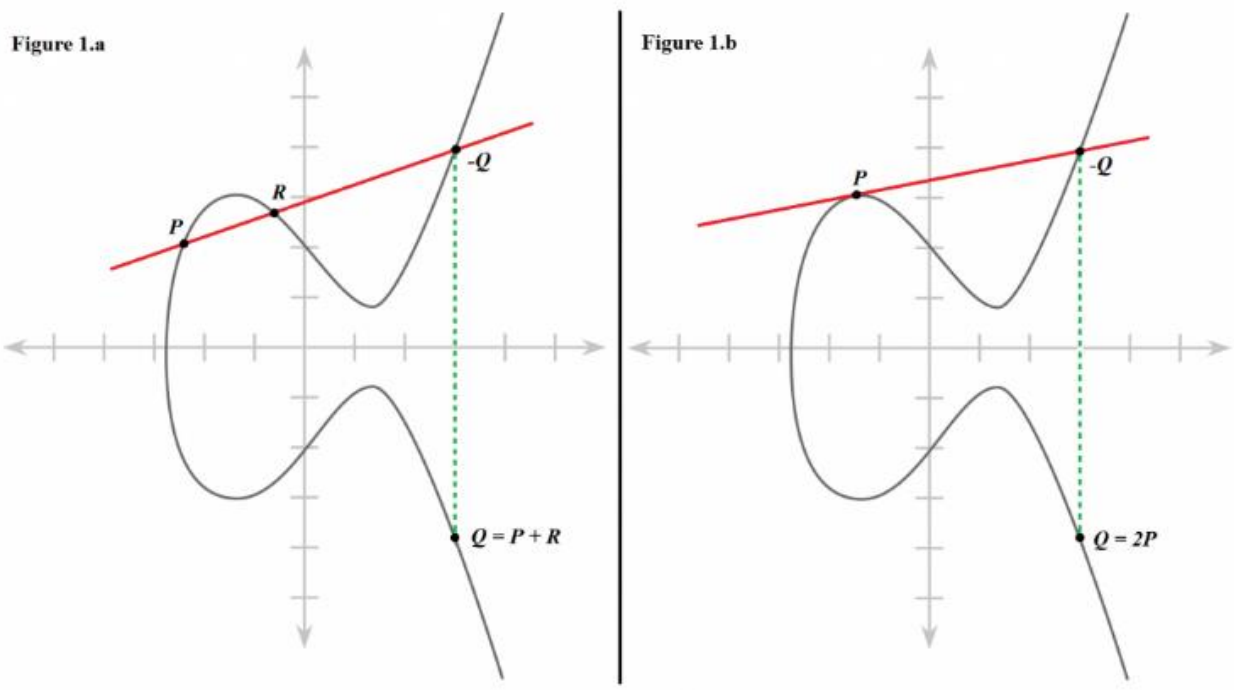
Door het algoritme van Grover te combineren met deze paradox daalt de veiligheid van een 256 bit hashfunctie van 128 naar 85 bit ($\sqrt[3]{2^{256}} \approx 285 \approx 10^{26}$) en wordt de aanval in dit geval dus een kleine 9000 miljard keer makkelijker. Meer algemeen zakt het veiligheidsniveau uitgedrukt in bits met één derde. Voor dit alles zijn trouwens evenveel logische of fysieke qubits vereist als in de vorige sectie. Er zijn dus 6681 logische qubits vereist om SHA-256 te verzwakken. Ook hier blijft de aanname van het bestaan van het kwantumorakel.

Samengevat zitten we met dezelfde uitdagingen als in de vorige sectie en vormen kwantumcomputers vandaag ook hier slechts op papier een bedreiging. Verder volstaat het om de lengte van de uitvoer met de helft te verhogen om een zelfde veiligheidsniveau als vandaag te behouden in een tijdperk met krachtige kwantumcomputers. Ook hier valt best mee te leven.

Publieke sleutelcryptografie

De grootste dreiging vanuit kwantumcomputers situeert zich in de publieke sleutelcryptografie. Bij publieke sleutelcryptografie wordt gebruik gemaakt van een sleutelpaar: een publieke sleutel die in principe door iedereen gekend mag zijn en een private sleutel die

[2] Verjaardagenparadox: De kans dat er in een kamer met 23 willekeurig gekozen mensen er twee zijn met eenzelfde verjaardag, bedraagt meer dan 50%. Die 23 ligt dichter bij de vierkantswortel van 365 dan bij 365.



FIGUUR 8. OPTELLING VAN PUNTEN OP ELLIPTISCHE KROMMEN IN HET REËLE VLAK

slechts door één entiteit gekend hoort te zijn. Dit wordt onder meer gebruikt voor digitale handtekeningen, authenticatie, het opzetten van veilige kanalen en vaak ook voor vercijfering (zie figuur 7).

In 1994 vond *Peter Shor* een kwantumalgoritme dat in staat is om efficiënt een getal te factoriseren, wat wil zeggen het ontbinden in zijn priemfactoren [21]. Het getal 175 is bijvoorbeeld (uniek) te ontbinden in 5 * 5 * 7. Voor klassieke computers is er daarvoor nog geen efficiënt algoritme gekend.

Hedendaagse publieke sleutelcryptografie, meer bepaald *RSA*, is net gebaseerd op de veronderstelling dat dit probleem moeilijk is en blijft. Meer specifiek steunt RSA op de assumptie dat het onhaalbaar is om uit een groot getal dat het product is van twee half zo grote priemgetallen, opnieuw die priemgetallen te vinden. Cryptografie gebaseerd op RSA zou dus gekraakt kunnen worden door een voldoende krachtige kwantumcomputer. Cryptografie gebaseerd op RSA wordt vandaag nog intensief gebruikt. Onder meer uw Belgische elektronische identiteitskaart maakt er gebruik van, zowel voor digitale handtekeningen als voor authenticatie.

Het RSA algoritme werd voor het eerst publiekelijk voorgesteld in de jaren '70. Ondertussen wordt meer en meer, vooral sinds de eeuwwisseling, gemigreerd naar cryptografie gebaseerd op *elliptische krommen* (zie figuur 8 voor een elliptische kromme in het reële vlak) omwille van de hogere efficiëntie en kortere sleutels. Punten op een dergelijke kromme kunnen opgeteld worden, wat resulteert in een nieuw punt op de kromme. Een punt *P* kan ook *n* keer (*n* is een natuurlijk getal) met zichzelf opgeteld worden: $P' = n \cdot P$. Cryptografie gebaseerd op elliptische krommen veronderstelt dat er geen efficiënt algoritme bestaat om uit *P* en *P'* de waarde n te vinden. Deze veronderstelling heet het *elliptic curve discrete logarithm problem*, of kortweg *ECDLP*. Dit lijkt een totaal ander probleem dan dat waarop RSA steunt, maar toch zijn ze niet zo verschillend en kan het algoritme van Shor ook cryptografie gebaseerd op elliptische krommen breken.

De ironie wil dat door de kortere sleutellengte de modernere cryptografie gebaseerd op ECDLP met minder krachtige kwantumcomputers te kraken is dan oudere cryptografie gebaseerd op RSA. Er zijn bijvoorbeeld 1300 tot 1600 logische qubits nodig om een 224 bit EC sleutel te kraken [22]. Dit biedt een gelijkaardige veiligheid als een 2048 bit RSA sleutel, dat pas gekraakt kan worden door een kwantumcomputer

met 4096 qubits. Let wel, het gaat hier over logische qubits.

In 2019, zeer recent dus, hebben wetenschappers in detail berekend hoeveel fysieke qubits er nodig zijn om een 2048 bit RSA (publieke) sleutel te kraken: **Een kwantumcomputer met 20 miljoen fysieke qubits zou 8 uur moeten rekenen** [23]. Dit resultaat werd mogelijk gemaakt door verschillende optimalisaties aan het Shor algoritme. Schattingen uit 2012 gingen nog uit van 1 miljard fysieke qubits [24]. Het is dus niet onwaarschijnlijk dat er in de toekomst benaderingen gevonden zullen worden die minder dan 20 miljoen qubits zullen vereisen.

Flash back naar vandaag. De krachtigste universele kwantumcomputer vandaag heeft 72 fysieke qubits en het grootste getal dat een kwantumcomputer met behulp van het algoritme van Shor heeft kunnen factoriseren is 21 en dateert van 2012 [25].

Ondertussen bestaan er naast het algoritme van Shor ook andere kwantumalgoritmes om getallen te factoriseren. Daarbij wordt het factorisatieprobleem omgevormd naar een optimalisatieprobleem. Dat is waar de adiabatische kwantumcomputers van D-Wave goed in zijn. Ze zijn makkelijker te bouwen maar zijn sowieso minder krachtig dan universele kwantumcomputers met evenveel qubits. Onderzoekers slaagden er in 2017 in om het getal 291311 te factoriseren in 523 en 557 op een D-Wave 2X machine met ruim 1000 (fysieke) qubits [26a]. Echter, deze methode is vooral sterk wanneer de twee priemfactoren in hun binaire voorstelling slechts weinig verschillen. In het geval van 523 en 557 is de binaire voorstelling 1000**0**01**01**1 en 1000**1**01**10**1 die inderdaad in slechts drie bits van elkaar verschillen. Eind 2019 zou het getal 1 099 551 473 989 door een kwantumcomputer gefactoriseerd zijn in 1 048 589 en 1 048 601 [26b]. Binair verschillen deze twee priemgetallen getallen maar twee bits. Dergelijke methodes laten dus enkel toe om zeer specifiek gekozen getallen ("*stunt-numbers*") te factoriseren, terwijl men in de cryptografie de priemfactoren steeds willekeurig kiest. Om aan deze kwantumdreiging te kunnen weerstaan, hoeven we bij de sleutelgeneratie hoogstens bijkomend te testen of de twee priemfactoren in hun binaire vorm toevallig niet te hard op elkaar lijken.

Ter vergelijking: klassieke computers slaagden er in februari 2020 in, na maanden rekenen, om het in 1991 gepubliceerde getal *RSA-250* te factoriseren [27]. Dit getal bestaat uit 250 decimalen (821 bits) en wordt hieronder weergegeven.

2140324650240744961264423072839333563008614
7151447550177977549208814180234471401366433
4551909580467961099285187247091458768739626
1921557363047454770520805119056493106687691
5900197594056934574522305893259766974716817
3806936489469987157849497593749793 7.

Laat ons eerlijk zijn: dit is een gigantisch verschil met 21 of zelfs de stunt numbers die door de huidige generatie kwantumcomputers gefactoriseerd werden.

Conclusie

Symmetrische encryptie en cryptografische hashfuncties zijn beter bestand tegen kwantumcomputers dan de hedendaagse publieke sleutelencryptie. Een voldoende krachtige kwantumcomputer kan in een korte tijd een RSA of EC sleutel kraken, terwijl de lengte van AES sleutels en hash uitvoer gewoon verhoogd moeten worden (maal 2 en maal 1,5 respectievelijk) om een zelfde veiligheid te behouden eens we het kwantumtijdperk binnentreden.

Gegeven dat vandaag de krachtigste universele kwantumcomputer 72 fysieke qubits bevat en gegeven de exponentiële complexiteitstoename van kwantumcomputers met het aantal qubits, lijkt de bedreiging van de moderne cryptografie door kwantumcomputers toch wat verderaf te zijn dat wat veelal wordt aangenomen.

Toch blijft het onmogelijk te voorspellen wat de toestand binnen een aantal decennia zal zijn, terwijl gegevens die vandaag met behulp van cryptografie beschermd worden (at rest of in transit), dan nog steeds gevoelig kunnen zijn. In ons vierde en laatste hoofdstuk leest u gelukkig welke stappen er ondernomen worden om onze gegevens en communicatie veilig te houden in geval men er ooit in slaagt krachtige kwantumcomputers te bouwen. Want, zo redeneert men bij zaken die men moeilijk kan inschatten, *better safe than sorry*.

Kwantumresistente cryptografie

Op termijn kunnen krachtige kwantumcomputers een bedreiging vormen voor de moderne publieke sleutelcryptografie. Dit vierde en laatste deel bespreekt hoe we ons daartegen kunnen wapenen met behulp van kwantumresistente cryptografie.

Publieke sleutelcryptografie is steeds gebouwd op veronderstellingen. De huidige generatie publieke sleutelcryptografie steunt op wiskundige problemen waarvan men veronderstelt dat een computer ze niet op een efficiënte wijze kan oplossen. Momenteel is publieke sleutelcryptografie grotendeels gebouwd op ofwel het RSA probleem, ofwel het discrete logaritme probleem voor elliptische krommen (ECDLP). Deze wiskundige problemen zijn inderdaad moeilijk voor een klassieke computer, maar een voldoende krachtige kwantumcomputer kan ze helaas een pak efficiënter oplossen.

Daarom heeft het Amerikaanse NIST, National Institute of Standards and Technology, momenteel een standaardisatieprocedure voor kwantumresistente cryptografische algoritmes lopen [29]. Dergelijke algoritmes steunen op problemen die ook voor een krachtige kwantumcomputer moeilijk zijn. Ze maken zelf geen gebruik van kwantumcomputers en kunnen dus uitgevoerd worden op klassieke computers. De standaardisatieprocedure van het NIST bestaat uit twee luiken: *Public-key Encryption and Key-establishment Algorithms* enerzijds en *Digital Signature Algorithms* anderzijds. De procedure loopt over meerdere jaren en de tweede ronde werd onlangs voltooid.

Verschillende principes

Er zijn een aantal principes waarop kwantumresistente cryptografie gebouwd kan worden. We besparen u de wiskundige details, maar geven toch een kort overzicht van de drie principes die het vaakst gebruikt werden door de ingestuurde NIST kandidaat-algoritmes.

Lattice-based cryptografie is de meest beloftevolle groep. De meeste NIST inzendingen zijn op het principe van lattices (roosters, traliewerken) gebaseerd. Het laat zowel vercijfer- als handtekeningschema's toe. *NTRUEncrypt* is het gekendste encryptiealgoritme dat op dit principe steunt. Het werd ontwikkeld en gepatenteerd in 1996 [30]. In 2017 werd het in het publieke domein geplaatst. Ondertussen wordt het ondersteund door onder meer de populaire crypto-library *Bouncy Castle*. De sleutels zijn langer dan de hedendaagse cryptografie gebaseerd op ECDLP, maar wel doorgaans korter dan RSA sleutels. Een belangrijke eigenschap is dat het computationeel efficiënter [31] is dan zowel ECDLP als RSA, wat natuurlijk zeer interessant is. Bovendien heeft lattice-based cryptografie eigenschappen die interessante mogelijkheden bieden voor geavanceerde cryptografie, waaronder homomorfe encryptie en functionele encryptie. Niet oninteressant is dat in 1999 ook *NTRUSign* voorgesteld werd, het broertje van NTRUENcrypt voor digitale handtekeningen. Dat bleek helaas al snel, in 2000, onveilig te zijn. Niettemin zijn er ondertussen meerdere andere voorstellen voor digitale handtekeningen gebaseerd op dit principe.

Code-based cryptografie vormt de tweede grootste groep in de lijst van NIST inzendingen. Het oudste algoritme in deze groep werd door *Robert McEliece* reeds in 1978 voorgesteld en is daarmee één van de oudste algoritmes voor publieke sleutelencryptie, bijna even oud als RSA. Deze groep heeft de reputatie enorm grote publieke sleutels te vereisen, waardoor het de facto onbruikbaar zou worden. Voor het algoritme van McEliece was dit inderdaad het geval: Er worden publieke sleutels tot 8,4MB aanbevolen. Toch zijn er ondertussen modernere code-based voorstellen, waarbij de publieke sleutel slechts enkele kilobytes groot is voor het hoogste veiligheidsniveau (256 bit security) [32]. Dit is weliswaar nog steeds meer dan bij zowel RSA als EC (elliptische krommen) voor hetzelfde veiligheidsniveau. Tijdens de tweede ronde vielen een aantal code-based voorstellen af door de ontdekking van nieuwe aanvallen.

Multivariate cryptografie is de derde grootste groep in de lijst van NIST inzendingen. Opnieuw werden zowel vercijfer- als handtekeningschema's gebaseerd op dit principe ingezonden. Het principe werd voor het eerst

voorgesteld in 1988 [33], maar in 1995 bleek dit eerste voorstel onveilig te zijn [34]. Ondertussen zijn er tal van andere multivariate cryptografische schema's voorgesteld. Eentje ervan is *LUOV* [35], de NIST inzending van de KU Leuven voor het luik digitale handtekeningen. Voor het hoogste veiligheidsniveau - 256 bit security - bedraagt de lengte van de publieke en private LUOV-sleutel respectievelijk 82.0 KB en 32 bytes. Een handtekening is 440 bytes lang. Met andere woorden heeft LUOV grote publieke sleutels, maar wel kleine digitale handtekeningen, die weliswaar nog steeds langer zijn dan digitale handtekeningen gebaseerd op ECDLP. Helaas overleefde LUOV de tweede NIST selectieronde niet doordat ondertussen nieuwe aanvallen gevonden waren, onder meer tegen LUOV. Die LUOV zwakheden zijn misschien wel te verhelpen, maar volgens het NIST toont het wel aan dat de innovatie in LUOV ten opzichte van reeds bestaande algoritmes nog te nieuw is om het tot standaard te verheffen.

Samengevat heeft het NIST de moeilijke opdracht om een keuze te maken uit een hele set van kandidaten met erg uiteenlopende eigenschappen, gebaseerd op uiteenlopende principes en aannames. Dit alles in een context waarbij er geregeld nieuwe zwakheden ontdekt worden.

Standaardisatie

Het NIST heeft, zoals reeds vermeld, een standaardisatieproject voor kwantumresistente cryptografie lopen, bestaande uit twee luiken: *Public-key Encryption and Key-establishment Algorithms* enerzijds en *Digital Signature Algorithms* anderzijds. In december 2016 publiceerde het NIST een call for proposals, waarop tot eind november 2017 gereageerd kon worden. Er werden 82 kandidaat-algoritmes ingezonden, waarvan er 69 weerhouden werden. Na de eerste ronde waren er 26 overblijvers: 17 voor Public-key Encryption and Key-establishment Algorithms en 9 voor Digital Signature Algorithms.

De tweede ronde werd afgerond op 22 juli 2020, waarbij de zeven finalisten bekend gemaakt werden, alsook de acht alternatieve voorstellen [36]. Onder de vier finalisten voor het eerste luik (encryptie en key-establishment) vinden we o.a. *CRYSTALS-KYBER* van IBM en *SABER* van de KU Leuven. Bij de finalisten voor digitale handtekeningen vinden we opnieuw een IBM inzending, genaamd *CRYSTALS-DILITHIUM*. De KU Leuven inzending, LUOV, werd, zoals reeds vermeld, niet weerhouden wegens te prematuur.

Er wordt verwacht dat de derde ronde 12 tot 18 maand zal duren, wat hopelijk zal resulteren in nieuwe standaarden. Vijf van de zeven finalisten zijn lattice-based, en dus gebaseerd op (ruwweg) hetzelfde wiskundige principe. Bovendien valt niet uit te sluiten dat er alsnog fundamentele zwakheden ontdekt zullen worden na de NIST standaardisatie. Daarom zal er nog een vierde ronde komen om na te gaan of er ook uit de acht alternatieve kandidaten gestandaardiseerd kan worden om zo over alternatieven, gebaseerd op andere principes, te beschikken mocht dit ooit nodig zijn.

De inzendingen kunnen, net zoals de huidige generatie algoritmes voor publieke sleutelcryptografie, gewoon op klassieke computers uitgevoerd worden. Na de publicatie van de nieuwe NIST standaarden moeten de gekozen algoritmes geïntegreerd worden in bestaande cryptografische library's zoals *OpenSSL*, *libssh* en *BouncyCastle*. Pas daarna kunnen de kwantumresistente algoritmes gebruikt worden in – bestaande of nieuwe – toepassingen in productie. Er bestaan weliswaar reeds libraries met kwantumresistente cryptografische algoritmes. In de eerste plaatst denken we dan aan het *Open Quantum Safe (OQS)* project [37], dat een implementatie bevat van - op het moment van schrijven op één na - alle NIST finalisten. OQS stelt duidelijk dat deze implementaties momenteel enkel dienen voor prototyping en het evalueren van de algoritmes, gezien we momenteel nog onvoldoende vertrouwen kunnen hebben in deze algoritmes. Het is inderdaad mogelijk dat sommige van deze algoritmes alsnog fouten bevatten en minder veilig zijn dan aanvankelijk aangenomen, mogelijks ook ten aanzien van klassieke computers.

De NIST standaardisatieprocedure voor kwantumresistente cryptografie is erg complex door de noodzakelijke rigoureuze analyse van elk van de kandidaat-algoritmes. Omdat die procedure meerdere jaren in beslag neemt, is het NIST een eenvoudigere en snellere standaardisatieprocedure gestart om een meer dringende nood aan kwantumresistente digitale handtekeningen te ledigen. Het gaat daarbij om twee hash-based signature schemes, die weliswaar

kwantumresistent zijn, maar wel twee belangrijke nadelen hebben: Met één sleutel kan maar een beperkt aantal digitale handtekeningen geplaatst worden en er moet samen met de private sleutel een tellertje bijgehouden worden dat bij elke handtekening verhoogd wordt. Deze schema's zijn dus niet geschikt voor algemeen gebruik. Een draft van de nieuwe NIST standaard is sinds 19 december 2019 beschikbaar [38].

NSA

Het *IAD* is de defensieve tak van de Amerikaanse inlichtingendienst *NSA* (National Security Agency). Voorlopig ondersteunt het IAD nog in haar *CNSA* (Commercial National Security Algorithm) suite zowel RSA als EC (elliptische krommen) voor het beschermen van informatie tot op het allerhoogste niveau – Top secret –, mits voldoende lange sleutels uiteraard. Toch bereidt ze zich voor om op termijn cryptografie gebaseerd op het RSA probleem of op het ECDLP te vervangen door kwantumresistente cryptografie. Reeds in 2015 formuleerde ze het als volgt [39]:

> "*IAD will initiate a transition to quantum resistant algorithms in the not too distant future. […] For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition.* […] *Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, which has made it clear that elliptic curve cryptography is not the long term solution many once hoped it would be. Thus, we have been obligated to update our strategy."*

De NSA neemt de mogelijkheid dat op termijn een vreemde mogendheid over een voldoende krachtige kwantumcomputer beschikt dus serieus. Op zijn minst acht ze het risico daarop te groot om er niet op te anticiperen. Ze schrijft zelfs dat kwantumresistente cryptografie essentieel is voor de verdediging van de Verenigde Staten.

Kort na de bekendmaking van de zeven NIST finalisten sprak de NSA haar vertrouwen uit in lattice-based cryptografie voor algemene toepassingen en hash-based signatures voor bepaalde niche toepassingen [40].

Hardware ondersteuning

Een HSM (Hardware Security Module) is hardware die toelaat cryptografische operaties uit te voeren met behulp van een sleutels die door die HSM zelf beschermd worden en in principe die HSM nooit verlaten. Navraag leert dat de meeste aanbieders van HSMs de NIST standaardisatieprocedure afwachten. Bemerk wel dat HSMs veelal de mogelijkheid ondersteunen om code van cryptografische algoritmes in te laden, waardoor – mits wat meer werk – toch reeds kwantumresistente cryptografie op HSM's mogelijk wordt. Het bedrijf *Ultimaco* profileert zich nog het meeste rond kwantumresistente cryptografie [41].

Conclusie

Zoals we in hoofdstuk 2 reeds aangaven, is het bouwen van een voldoende krachtige kwantumcomputer die effectief een bedreiging vormt voor de huidige publieke sleutelcryptografie gigantisch complex, misschien zelfs onmogelijk. Of en wanneer een dergelijke computer zal gerealiseerd worden blijft giswerk. Niemand heeft een glazen bol en een doorbraak of nieuw inzicht kan de verwachtingen sterk veranderen in zowel de ene als de andere richting. Dit neemt echter niet weg dat nog heel wat hordes genomen moeten worden.

We zien dan ook geen imminente dreiging. We raden ten eerste aan om de NIST standaardisatieprocedure af te wachten vooraleer over te schakelen naar het gebruik van kwantumresistente cryptografie in productieomgevingen. Ten tweede raden we aan om grote kosten om te migreren naar kwantumresisente cryptografie te vermijden en eerder te opteren voor een geleidelijk migratieproces. Het migreren impliceert immers niet alleen een update van de software, maar ook eventueel hardware (zoals HSMs), het vervangen van alle publieke sleutels en certificaten, enz. Kwantumresistente cryptografie kan zelfs efficiënter zijn

dan de huidige cryptografie, wat op zich al een interessante driver kan zijn om langzaam aan te migreren.

Sowieso is het noodzakelijk een goed overzicht te hebben van welke cryptografie waar toegepast wordt om welke data te beschermen. Voor gegevens die meerdere decennia erg gevoelig blijven kan migratie een hogere prioriteit krijgen. Ook dienen systemen voldoende flexibel gebouwd te worden opdat ze relatief vlot aangepast kunnen worden om overweg te kunnen met nieuwe cryptografische bouwblokken. Dit heet *crypto agility* en is sowieso een best practice, los van een eventuele kwantumdreiging.

Referenties

[1] Fiona Macdonald. *Scientists Just Unveiled The First-Ever Photo of Quantum Entanglement*, Science Alert, 13 juli 2019. https://www.sciencealert.com/scientists-just-unveiled-the-first-ever-photo-of-quantum-entanglement

[2] Yuri Ozhigov, *Quantum Computers Speed Up Classical with Probability Zero*, arXiv.org, 24 maart 1998, https://arxiv.org/abs/quant-ph/9803064

[3] Smriti Srivastava, *Top 10 Countries Leading In Quantum Computing Technology*, Analytics Insight, 14 december 2019, https://www.analyticsinsight.net/top-10-countries-leading-quantum-computing-technology/

[4] Hetty Helsmoortel, Wim De Maeseneer, *Vlaamse topwetenschappers blikken vooruit: Staat er in 2030 een kwantumcomputer in onze woonkamer?*, VRT Nieuws, 5 januari 2020, https://www.vrt.be/vrtnws/nl/2019/12/24/vlaamse-topwetenschappers-blikken-vooruit-naar-2030-kwantumcomp/

[5] Preskill J. Quantum computing and the entanglement frontier. arXiv preprint arXiv:1203.5813. 2012 Mar 26.

[6] John Preskill. *Why I Called It 'Quantum Supremacy'*. Quanta Magazine, 2 oktober 2019. https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/

[7] Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R, Biswas R, Boixo S, Brandao FG, Buell DA, Burkett B. Quantum supremacy using a programmable superconducting processor. Nature. 2019 Oct;574(7779):505-10. https://www.nature.com/articles/s41586-019-1666-5

[8] Edwin Pednault, John Gunnels, Dmitri Maslov, Jay Gambetta. *On "Quantum Supremacy"*, IBM, 21 oktober 2019. https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

[9] Julian Kelly. *A Preview of Bristlecone, Google's New Quantum Processor*. Google AI Blog, 15 maart 2018. https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html

[10] Jerry Chow, Jay Gambetta. *Quantum Takes Flight: Moving from Laboratory Demonstrations to Building Systems.* IBM Research Blog, 8 januari 2020. https://www.ibm.com/blogs/research/2020/01/quantum-volume-32/

[11] Albash T, Lidar DA. Adiabatic quantum computation. Reviews of Modern Physics. 2018 Jan 29;90(1):015002.

[12] Jonathan Hui, *Quantum Supremacy — Google Sycamore Processor.* 24 oktober 2019. Medium. https://medium.com/@jonathan_hui/quantum-supremacy-google-sycamore-processor-6f30073a17fa

[13] Laflamme R, Miquel C, Paz JP, Zurek WH. Perfect quantum error correcting code. Physical Review Letters. 1996 Jul 1;77(1):198.

[14] DiVincenzo DP. The physical implementation of quantum computation. Fortschritte der Physik: Progress of Physics. 2000 Sep;48(9-11):771-83.

[15] Mikhail Dyakonov. *The Case Against Quantum Computing.* IEEE Spectrum. 15 november 2018. https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing

[17] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. InProceedings 35th annual symposium on foundations of computer science 1994 Nov 20 (pp. 124-134). Ieee.

[18] Grassl M, Langenberg B, Roetteler M, Steinwandt R. Applying Grover's algorithm to AES: quantum resource estimates. InPost-Quantum Cryptography 2016 Feb 24 (pp. 29-43). Springer, Cham.

[19] Stevens M, Bursztein E, Karpman P, Albertini A, Markov Y. The first collision for full SHA-1. InAnnual International Cryptology Conference 2017 Aug 20 (pp. 570-596). Springer, Cham.

[20] Leurent G, Peyrin T. From collisions to chosen-prefix collisions application to full SHA-1. InAnnual International Conference on the Theory and

Applications of Cryptographic Techniques 2019 May 19 (pp. 527-555). Springer, Cham.

[21] Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review. 1999;41(2):303-32.

[22] Proos J, Zalka C. Shor's discrete logarithm quantum algorithm for elliptic curves. arXiv preprint quant-ph/0301141. 2003 Jan 25.

[23] Gidney C, Ekerå M. How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits. arXiv preprint arXiv:1905.09749. 2019 May 23.

[24] Fowler AG, Mariantoni M, Martinis JM, Cleland AN. Surface codes: Towards practical large-scale quantum computation. Physical Review A. 2012 Sep 18;86(3):032324.

[25] Martin-Lopez E, Laing A, Lawson T, Alvarez R, Zhou XQ, O'brien JL. Experimental realization of Shor's quantum factoring algorithm using qubit recycling. Nature photonics. 2012 Nov;6(11):773-6.

[26a] Li Z, Dattani NS, Chen X, Liu X, Wang H, Tanburn R, Chen H, Peng X, Du J. High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311. arXiv preprint arXiv:1706.08061. 2017 Jun 25.

[26b] L. Crane. *Quantum computer sets new record for finding prime number factors.* 13 december 2019. NewScientist. https://www.newscientist.com/article/2227387-quantum-computer-sets-new-record-for-finding-prime-number-factors

[27] Paul Zimmermann. *Factorization of RSA-250*. cado-nfs-discuss (Mailing list). 28 februari 2020 https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html

[28] Barker E, Roginsky A. Transitioning the use of cryptographic algorithms and key lengths. National Institute of Standards and Technology; 2018 Jul 19.

[29] NIST. Post-Quantum Cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography

[30] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, *Public key cryptosystem method and apparatus*, 1997, https://patents.google.com/patent/US6081597

[31] The NTRU Project, https://tbuktu.github.io/ntru/

[32] Aragon N, Barreto P, Bettaieb S, Bidoux L, Blazy O, Deneuville JC, Gaborit P, Gueron S, Guneysu T, Melchor CA, Misoczki R. : bit flipping key encapsulation.

[33] Matsumoto T, Imai H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In Workshop on the Theory and Application of of Cryptographic Techniques 1988 May 25 (pp. 419-453). Springer, Berlin, Heidelberg.

[34] Patarin J. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. InAnnual International Cryptology Conference 1995 Aug 27 (pp. 248-261). Springer, Berlin, Heidelberg.

[35] Beullens W, Szepieniec A, Vercauteren F, Preneel B. LUOV: Signature scheme proposal for NIST PQC project.

[36] Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Kelsey J, Liu YK, Miller C, Moody D, Peralta R, Perlner R. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NIST, Tech. Rep., July. 2020 Jul 22. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf

[37] Open Quantum Safe. https://openquantumsafe.org/

[38] Cooper D, Apon D, Dang Q, Davidson M, Dworkin M, Miller C. Recommendation for stateful hash-based signature schemes. National Institute of Standards and Technology; 2019 Dec 11.

https://csrc.nist.gov/publications/detail/sp/800-208/draft

[39] NSA – CSS. Commercial National Security Algorithm Suite. 19 augustus 2015. https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm

[40] NSA – CSS. Post-Quantum Cybersecurity Resources, https://www.nsa.gov/what-we-do/cybersecurity/post-quantum-cybersecurity-resources/

[41] Utimaco. Blogposts met tag « post-quantum ». https://content.hsm.utimaco.com/blog/tag/post-quantum

Bronnen afbeeldingen

- Coverafbeelding. Equilibrium door Rob Oo (Flickr), gepubliceerd onder creative commons. https://www.flickr.com/photos/105105658@N03/30235805927/
- **Wet van Moore.** Max Roser – Transistor count. https://ourworldindata.org/uploads/2019/05/Transistor-Count-over-time-to-2018.png
- **D-Wave 2000Q Quantum Computer**.D-Wave Systems. https://www.dwavesys.com/press-releases/d-wave%C2%A0announces%C2%A0d-wave-2000q-quantum-computer-and-first-system-order
- **Layout Sycamore processor.** Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R, Biswas R, Boixo S, Brandao FG, Buell DA, Burkett B. Quantum supremacy using a programmable superconducting processor. Nature. 2019 Oct;574(7779):505-10. https://www.nature.com/articles/s41586-019-1666-5
- **Elliptische krommen.** A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/a-and-b-show-elliptic-curve-addition-and-doubling-respectively-In-Elliptic-addition_fig2_300079947 [accessed 18 Nov, 2020]
- **Hello Quantum.** Hello Quantum: The Making of a Seriously Fun Quantum Game. https://www.ibm.com/blogs/research/2018/07/hello-quantum/
- **Kwantumverstregneling**. Fiona Macdonald. Scientists Just Unveiled The First-Ever Photo of Quantum Entanglement, Science Alert, 13 juli 2019. https://www.sciencealert.com/scientists-just-unveiled-the-first-ever-photo-of-quantum-entanglement

Kristof Verslype is toegepaste cryptograaf bij Smals Research. Hij behaalde een doctoraat in de ingenieurswetenschappen aan de KU Leuven. Hij wordt regelmatig gevraagd als spreker of consulent.

kristof.verslype@smals.be
+32(0)2 7875376
www.smals.be
www.smalsresearch.be

Over Smals en Smals Research

Smals realiseert innovatieve ICT-projecten en diensten voor werk, gezin en gezondheid voor instellingen uit de sociale zekerheid en de gezondheidszorg in België en biedt hen een breed gamma ICT-diensten aan.

Met haar eigen team van hoogopgeleide onderzoekers investeert Smals in onderzoek en ontwikkeling over verschillende technologische domeinen heen, die zorgvuldig geselecteerd worden in overleg met de klanten-leden. Speciale aandacht gaat uit naar het in gebruik laten nemen van de door het team voorgestelde technologieën en concepten. Meer informatie over de onderzoekers en hun publicaties is te vinden op www.smalsresearch.be.