Publicatie : AG Connect
Datum : 31 okt 2018
cm2 : 1.129
Pagina : 70
Advertentiewaarde : € 14.900,00
Regio : Nederland
Frequentie : 10x per jaar
Oplage : 4.346

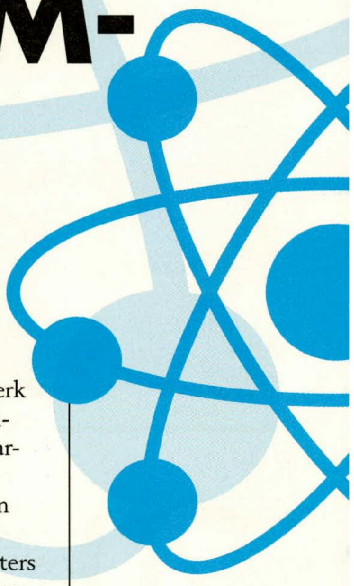
IT-STUDIES

HOE KUN JE EEN KWANTUMCOMPUTER VEILIG LATEN REKENEN OP GEVOELIGE GEGEVENS, ALS DEZE KWANTUMCOMPUTER ERGENS ANDERS STAAT? OP DIT MOMENT WORDEN ER CRYPTOGRAFISCHE TECHNIEKEN ONDERZOCHT DIE STRAKS DE 'KWANTUMCLOUD' VEILIG ZULLEN MAKEN.

door door Florian Speelman beeld Shutterstock

Deze cryptografische technieken kunnen de kwantumcloud veiliger maken

VEILIG REKENEN MET EEN KWANTUM-COMPUTER



DE KWANTUMCOMPUTER WAS LANGE TIJD SLECHTS EEN THEORETISCHE MOGELIJKHEID, MAAR DE AFGELOPEN JAREN BOEKEN ACADEMISCHE ONDERZOEKSGROEPEN, WAARONDER QUTECH IN DELFT, KWANTUMSTART-UPS EN GROTE TECHBEDRIJVEN, ZOALS GOOGLE, IBM, INTEL EN MICROSOFT, GROTE VOORUITGANG IN DE TECHNISCHE IMPLEMENTATIE. Het aantal beschikbare werkende qubits zit nu rond de 50, maar dat getal groeit geleidelijk. Het is een grote uitdaging om een werkende kwantumcomputer te bouwen. De huidige kwantumsystemen die als basis zullen dienen, moeten zeer sterk gekoeld en geïsoleerd van de buitenwereld zijn. Het is daarom heel waarschijnlijk dat de eerste kwantumcomputers in handen zullen zijn van universiteiten, overheden en grote bedrijven – net als de eerste computers die in het midden van de vorige eeuw gemakkelijk een hele kamer in beslag namen, in groot contrast met de rekenkracht die wij inmiddels in onze broekzak hebben. Dat betekent ook dat de gebruikers van deze kwantumservers hun gegevens moeten opsturen naar deze servers, en hier zit ook potentieel gevoelige informatie bij. Hoe kunnen gebruikers van deze kwantumcomputers

Publicatie : AG Connect
Datum : 31 okt 2018
cm2 : 1.129
Pagina : 70
Advertentiewaarde : € 14.900,00
Regio : Nederland
Frequentie : 10x per jaar
Oplage : 4.346

zeker weten dat hun gegevens veilig zijn, en dat de kwantumcomputers werken zoals beloofd?

FULLY HOMOMORPHIC ENCRYPTION

Voor gewone computers zijn er diverse technieken die achter de schermen kunnen helpen om servers veilig te laten rekenen op data. Een van de nieuwste en krachtigste daarvan is fully homomorphic encryption (FHE). Voor het veilig bewaren van gegevens zijn er veilige encryptiemethoden, maar het is (bijna per definitie) moeilijk om iets nuttigs te doen met deze versleutelde gegevens: voor de server zien ze er namelijk uit als willekeurige ruis. FHE-encryptieschema's zijn methoden die het tóch toelaten om te rekenen op die gegevens: de gebruiker versleutelt, stuurt de versleutelde data naar de server, en na het uitvoeren van de berekening heeft de server nu de versleutelde uitkomst van de berekening in handen om terug te sturen, zonder dat de onversleutelde data ooit zichtbaar was. De wiskundige trucs die hiervoor nodig zijn, zijn overigens niet gratis in rekentijd: de eerste implementatie van FHE uit 2009 was 100 triljoen keer langzamer dan onversleuteld rekenen, al hebben moderne implementaties dat verbeterd tot vertraging van een factor duizend. Onder andere de Amerikaanse defensie, via IARPA, heeft kort geleden 1 miljoen dollar geïnvesteerd in verbeteringen van FHE. Naar verwachting zullen gevoelige cloudberekeningen van de toekomst gebruik kunnen maken van deze nieuwe technieken. Ook voor decentrale berekeningen op de blockchain zijn deze ontwikkelingen belangrijk.

HOMOMORPHIC ENCRYPTION VOOR KWANTUMCOMPUTERS

Het was een tijd lang een open vraag of het ook mogelijk is om fully homomorphic encryption voor kwantumcomputers te bouwen (QFHE).[1] Een recente doorbraak kwam onder andere van onderzoekers van het QuSoft-instituut voor kwantumsoftware in Amsterdam.[2] Het schema vraagt de cliënt de gegevens te versleutelen met een kwantumcode, in combinatie met hulp-kwantumgegevens. Vervolgens is er door een server te rekenen op deze data. Een nadeel is wel dat er een klassieke FHE-encryptie bij nodig is, in parallel met de kwantumberekening, wat dus altijd voor een vertraging zal zorgen. Ook zijn de benodigde hulp-kwantumsleutels relatief groot, wat ervoor zorgt dat dit schema pas echt goed kan werken als er genoeg kwantumgeheugen bestaat om de hulpsleutels te vervoeren.

Latere verbeteringen[4 5] zorgen ervoor dat de versleuteling niet meer kwantum hoeft te zijn, en dus geheel uitgevoerd kan worden door een gewone computer. Maar de hoeveelheid werk die de kwantumserver moet verzetten, is alsnog een stuk groter dan dat van de onversleutelde berekening.

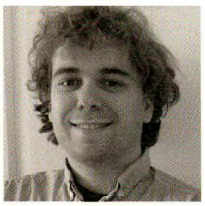
DE WISKUNDIGE TRUCS DIE NODIG ZIJN, ZIJN OVERIGENS NIET GRATIS IN REKENTIJD

Vooralsnog zijn dit type schema's dus vooral een academische doorbraak, al wel met de belofte voor toepassingen op de langere termijn.

BLIND QUANTUM COMPUTATION

De ontwikkelingen van kwantum-FHE zijn theoretisch erg interessant, en geven een oplossing bij veel mogelijke scenario's, maar omdat voorlopig elke qubit zal tellen, zijn deze schema's voorlopig nog niet praktisch toepasbaar. Er zijn ook andere schema's bedacht door onderzoekers, die minder extra qubits nodig hebben, maar wel andere eisen stellen aan de versleutelaar. Deze schema's vallen in twee groepen protocollen. De ene groep protocollen, onder de naam 'blind quantum computation', voegt als extra eis toe dat de computer van de cliënt meehelpt met de berekening.[1] Dit doet de cliënt door interactief tijdens de berekening enkele qubits te sturen – het is dus voor deze protocollen

AUTEUR

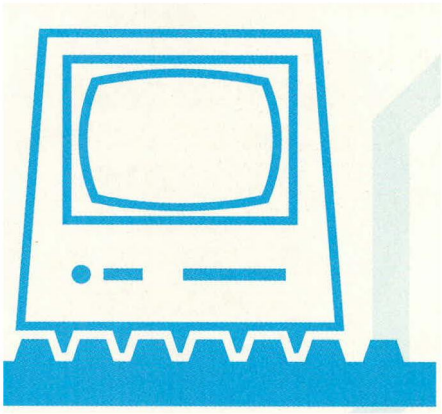


FLORIS SPEELMAN

Florian Speelman is in 2016 gepromoveerd op onderzoek uitgevoerd op het Centrum Wiskunde & Informatica in Amsterdam, en heeft de afgelopen twee jaar gewerkt als onderzoeker in de QMATH-groep (Universiteit van Kopenhagen).

Publicatie : AG Connect
Datum : 31 okt 2018
cm2 : 1.129
Pagina : 70
Advertentiewaarde : € 14.900,00
Regio : Nederland
Frequentie : 10x per jaar
Oplage : 4.346

Het is tijd om kwantumsoftware te schrijven



wel nodig om enige kwantumcapaciteit te hebben, maar wel veel minder dan de kwantumserver. Het is dan ook belangrijk dat er een snelle en betrouwbare kwantumverbinding is tussen de cliënt en de server. Onderzoeksgroepen werken op dit moment in de Quantum Internet Alliance[4] aan het bouwen van een kwantuminternet, waarbij het QuTech-instituut in Delft een van de internationale voorlopers is. Naast de interactieve communicatie (die de toepasbaarheid wel vermindert) kan de overhead van deze schema's heel klein zijn. Veilig op afstand kunnen rekenen, ook zonder zelf een kwantumcomputer te moeten hebben, is dus een van de mogelijke toepassingen van het kwantuminternet.

Een bijkomend voordeel van deze groep protocollen is ook de mogelijkheid tot verificatie: niet alleen worden de data van de berekening beschermd, maar het is voor de gebruiker ook mogelijk om te controleren of de server de berekening correct heeft uitgevoerd.

De andere groep bestaat uit protocollen die gebruikmaken van twee kwantumservers. Deze twee servers werken samen, en gebruiken daarvoor kwantumcorrelaties tussen verstrengelde deeltjes. Voor deze schema's hoeft de cliënt geen enkele kwantumcapaciteit te hebben – een gewone computer is genoeg. Een complicatie is echter wel dat deze schema's verstrengelde deeltjes nodig hebben om te werken, en twee servers in plaats van één, waardoor ze minder praktisch kunnen zijn dan die uit de eerdergenoemde groep. Op het moment is het efficiëntste schema uit deze groep bedacht door een internationale samenwerking, waaronder onderzoekers werkend bij QuSoft in Amsterdam.[7]

TOEKOMSTPERSPECTIEF

Nu de ontwikkelingen op het gebied van kwantumhardware sneller gaan, is het ook tijd om kwantumsoftware te schrijven voor de toekomstige computers. Er zijn al meerdere programmeertalen ontworpen voor de kwantumcomputer, waaronder bijvoorbeeld Microsofts Q# en Google's Cirq. Deze protocollen voor veilig rekenen zijn een uitstekende kandidaat om daarin te implementeren. We zullen dan in de nabije toekomst een compiler hebben die kwantumberekeningen kan beveiligen op zo'n manier dat zelfs de server niet vertrouwd hoeft te worden – voor een veilige 'kwantumcloud'.

REFERENTIES

1 Anne Broadbent, Stacey Jeffery 'Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity' https://link.springer.com/chapter/10.1007/978-3-662-48000-7_30
2 Yfke Dulek, Christian Schaffner, and Florian Speelman 'Quantum Homomorphic Encryption for Polynomial-Size Circuits' https://theoryofcomputing.org/articles/v014a007
3 Urmila Mahadev 'Classical Homomorphic Encryption for Quantum Circuits' https://arxiv.org/abs/1708.02130
4 Zvika Brakerski 'Quantum FHE (Almost) As Secure As Classical' https://link.springer.com/chapter/10.1007/978-3-319-96878-0_3
5 Joseph F. Fitzsimons 'Private quantum computation: an introduction to blind quantum computing and related protocols' https://www.nature.com/articles/s41534-017-0025-3
6 Quantum Internet Alliance: http://quantum-internet.team
7 Andrea Coladangelo, Alex Grilo, Stacey Jeffery, Thomas Vidick 'Verifier-on-a-Leash: new schemes for verifiable delegated quantum computation, with quasilinear resources' https://arxiv.org/abs/1708.07359