POSITION-BASED QUANTUM CRYPTOGRAPHY AND CATALYTIC COMPUTATION

OMSCHRIJVING PROJECT

Hoe kun je zeker weten dat iemand eerlijk is over zijn/haar locatie? Voor veel toepassingen is het belangrijk om zeker te zijn over iemands plaats: denk bijvoorbeeld aan het leger ('Komt het lanceercommando echt vanuit de legerbasis?') of meer alledaagse situaties ('Waar woont de besteller van deze pizza?' en 'Staat de server waar ik mee verbonden ben echt op de verwachte plek?'). Helaas is het niet mogelijk om locatie helemaal betrouwbaar te verifiëren wanneer alle berichten verstuurd worden als gewone bits en bytes: het is voor een groep samenwerkende aanvallers, die allemaal niet op de beweerde locatie zijn, altijd mogelijk om een andere locatie na te bootsen.

Dit promotieonderzoek gaat dieper in op het gebruik van *quantum-informatie* voor positie-verificatie, waarbij in plaats van bits er *qubits* verstuurd worden, hun quantum-equivalent. De protocollen die ontwikkeld zijn, gebruik makende van quantum-mechanica, kunnen veel lastiger worden omzeild, alleen door aanvallers die onrealistisch veel 'verstrengelde deeltjes' hebben – deeltjes in een lastig te maken quantumtoestand. In het proefschrift worden verschillende protocollen geanalyseerd, eerdere voorstellen gebroken, en nieuwe protocollen voorgesteld die lastig te breken zijn, maar relatief eenvoudig te implementeren.

WAT IS DE IMPACT?

Het gebruik van quantuminformatie voor cryptografische toepassingen heeft potentie om bijna-onbreekbare beveiligingen te maken – omdat de veiligheid gebaseerd is op natuurwetten (zoals de onzekerheid van Heisenberg) – in plaats van aannames over de moeilijkheid van wiskundige problemen.

Het is nodig om quantumdeeltjes nog iets beter te beheersen dan nu mogelijk is, om position-based quantum cryptography daadwerkelijk toe te passen. Er is een grote wetenschappelijke gemeenschap met deze technische kant bezig, dus de vereiste precisie is waarschijnlijk over enkele jaren mogelijk. Dan kunnen de eerder genoemde praktische toepassingen uitgevoerd worden. Denk ook bijvoorbeeld aan een zelfrijdende auto, die (zelfs als zijn software gehackt is) onmogelijk kan liegen over zijn plek op de weg tegenover de andere zelfrijdende auto's – een extra manier om veiligheid te waarborgen.

Naast de praktische impact, zijn er ook theoretische resultaten in andere gebieden voortgekomen uit dit proefschrift. Technieken die ontwikkeld werden om protocollen voor positie-verificatie te analyseren, zijn recent gebruikt om een nieuw cryptografisch protocol te maken voor het rekenen op versleutelde gegevens.[1]

WIE ZIJN DE MENSEN ERACHTER?

Het promotieonderzoek is uitgevoerd door Florian Speelman (BSc in Natuurkunde, MSc Computational Science), begeleid door prof. dr. Harry Buhrman, professor aan de Universiteit van Amsterdam en directeur van QuSoft, het instituut voor quantum software. Veel resultaten in het proefschrift zijn behaald in samenwerking met andere onderzoekers, waaronder meerdere publicaties met dr. Christian Schaffner op die gebied, onderzoeker aan de Universiteit van Amsterdam en QuSoft.

WAT ZIJN DE TOEKOMSTPLANNEN?

Op korte termijn is er contact met experimenteel natuurkundigen om 'proof-of-concept' experimenten uit te voeren, om te laten zien dat de voorgestelde protocollen in principe uit te voeren zijn met de huidige technologie. Grootschalige implementatie wordt vooral zeer interessant samen met een 'quantum internet', wanneer het sturen van quantum-informatie tussen mensen steeds makkelijker wordt.

---

[1] Yfke Dulek, Christian Schaffner, and Florian Speelman. *Quantum homomorphic encryption for polynomial-sized circuits.* In Advances in Cryptology – CRYPTO 2016, part III p. 3–32, 2016.