Sterkere quantumversleuteling dankzij telescooptruc

Nieuws Gieljan de Vries 28-01-2021 11:00:00 Deel dit artikel:

Seinen we ooit cryptosleutels over zonder kans op afluisteren? Een techniek voor scherpere telescoopfoto's brengt zulke quantumversleuteling een stap dichterbij.

Ze mogen alles van ons weten, maar echt belangrijke zaken als bankgegevens, verkiezingsdata en medische dossiers houden we toch liever geheim. Dankzij *quantum key distribution* kan dat misschien nog veiliger, door beveiligingssleutels gegarandeerd afluistervrij te versturen. Chinese wetenschappers leggen de lat in dit onderzoek weer wat hoger met een ruisarme quantumverbinding via satellieten. Wat komt er op ons af?

Fragiel

Wat nou, gepantserde glasvezelkabels? Als het aan de Chinese fysicus Yuan Cao en zijn collega's ligt, versturen we de diepgeheime cryptografische sleutels voor onze databeveiliging voortaan open en bloot door de buitenlucht. Via lasers en telescopen moeten quantumsleutels zelfs via satellieten kunnen reizen.

Dat klinkt als een feest voor afluisteraars, maar is perfect veilig, want informatie in quantumdeeltjes zoals licht is ontstellend fragiel. Elke afluisterpoging zorgt dat het lichtdeeltje onherroepelijk verandert. Zo ontdekken de zender en ontvanger het meteen als er iemand meeluistert, stelt dr. Yfke Dulek, zelf niet betrokken bij dit onderzoek en als quantumcryptograaf verbonden aan het Amsterdamse onderzoekscentrum QuSoft.

Artistieke impressie van quantum key distribution in de binnenstad: sets lasers en telescopen op hoge gebouwen sturen een cryptografische sleutel over in de vorm van fragiele en daardoor niet af te luisteren lichtdeeltjes.
© Yao Zheng/Micius Salon

Dobbelen op afstand

In theorie is quantum key distribution een gegarandeerd veilige manier om de lange cijferreeksen van een beveiligingssleutel door te sturen. Zulke sleutels moeten willekeurig zijn, én alleen bekend bij zender en ontvanger. "Ook zonder quantumtoeren kan dat door elkaar fysiek op te zoeken en een paar dobbelstenen te gooien", schetst de Amsterdamse quantumcryptografe. "Onhandig." Ook bijna-niet-te-ontwarren-rekenrecepten om lange codes te produceren hebben zo hun beperkingen: ooit bedenkt iemand een manier om ze sneller te kraken.

Quantum key distribution pakt zulke problemen in één keer aan. Alice en Bob (de traditionele namen voor de zender en ontvanger van een geheime boodschap) wisselen hun sleutel uit in de vorm van een serie lichtdeeltjes (fotonen), met in elk foton één getal van hun cryptosleutel. Probeert iemand de code af te luisteren (de traditionele *eavesdropper* Eve), dan zien Alice en Bob de quantumtoestand meteen instorten. Dulek: "Dan gooi je simpelweg de sleutel weg en begin je opnieuw." Als er eenmaal een veilige sleutel is, kan daarmee de boodschap worden verhusseld en verstuurd.

Corrigeren voor een kaarsvlam

Tot zover de standaard quantum key distribution. Wat is er zo nieuw aan het Chinese onderzoek? Dulek: “Deze onderzoekers denken na over wat er gebeurt als de quantumapparaten van Alice en Bob niet helemaal goed functioneren. Dan moet je weer allemaal extra maatregelen nemen om te zorgen dat de sleutel geheim blijft.” Ook weet het team de kwaliteit van hun quantumverbinding te verbeteren door atmosferische ruis te onderdrukken.

Quantumsleutels door de dampkring sturen, geeft namelijk nogal wat verstoring, net zoals de kolkende lucht boven een kaarsvlam het beeld erachter vervormt. Dat heeft hetzelfde effect als een luistervink op de lijn: zender en ontvanger weten niet meer zeker of een cijfer wel veilig is verzonden. Als het quantumsignaal maar ver genoeg door de atmosfeer moet ploegen, blijft er zo geen sleutel meer over.

Cao en collega’s corrigeren voor de atmosferische ruis dankzij *adaptive optics*, een techniek uit de sterrenkunde. Naast de quantumsleutel zenden ze een laserbundel mee en kijken hoe die verstoord wordt; diezelfde ruis kunnen ze vervolgens uit de quantumboodschap filteren. Astronomen gebruiken deze truc om met hun telescopen door de verstoring van de dampkring heen te turen.

Adaptive optics bij de Europese Very Large Telescope op de Chileense berg Paranal. Om hun beeld haarscherp te krijgen, sturen de astronomen laserbundels de hemel in. Hoe die verbogen worden door de woelige atmosfeer, vertelt de sterrenkundigen hoe ze hun waarnemingen moeten corrigeren.

Quantum-bankgeheim

Cao en collega's zijn niet de eersten die cryptosleutels verzenden via een quantumverbinding. Bedrijven als Id Quantique en MagiQ Technologies bieden al kastjes aan die quantumsleutels versturen via een glasvezelverbinding. In 2007 werd de techniek gebruikt om stemmen in de Zwitserse verkiezingen naar de telkamer te sturen. Een Chinees team haalde in maart 2020 een afstand van 509 km per glasvezel, maar met zoveel ruis dat een praktische toepassing er niet in zat.

Hoe snel moeten we over op quantumcrypto? "Ik heb er best vertrouwen in dat berichten die met klassieke cryptografie zijn versleuteld op dit moment nog niet gebroken kunnen worden", zegt quantumcryptografe Dulek. "Maar hoe zit dat over twintig of vijftig jaar? Als je nu een bericht verstuurt met staatsgeheimen die nog vijftig jaar veilig moeten blijven, moet je er ook zeker van zijn dat niemand meeluistert, de versleutelde communicatie opslaat, en het over een paar decennia alsnog weet te ontsleutelen."

Door de nu nog grote opstartkosten is quantum key distribution vooral relevant voor partijen die echt belangrijke geheime informatie uit moeten wisselen, zoals banken of overheden. Voor de meeste toepassingen is de cryptografie die we nu gebruiken voldoende. Toegang tot je rekening krijg je voorlopig gewoon via een pincode of met je vingerafdruk.