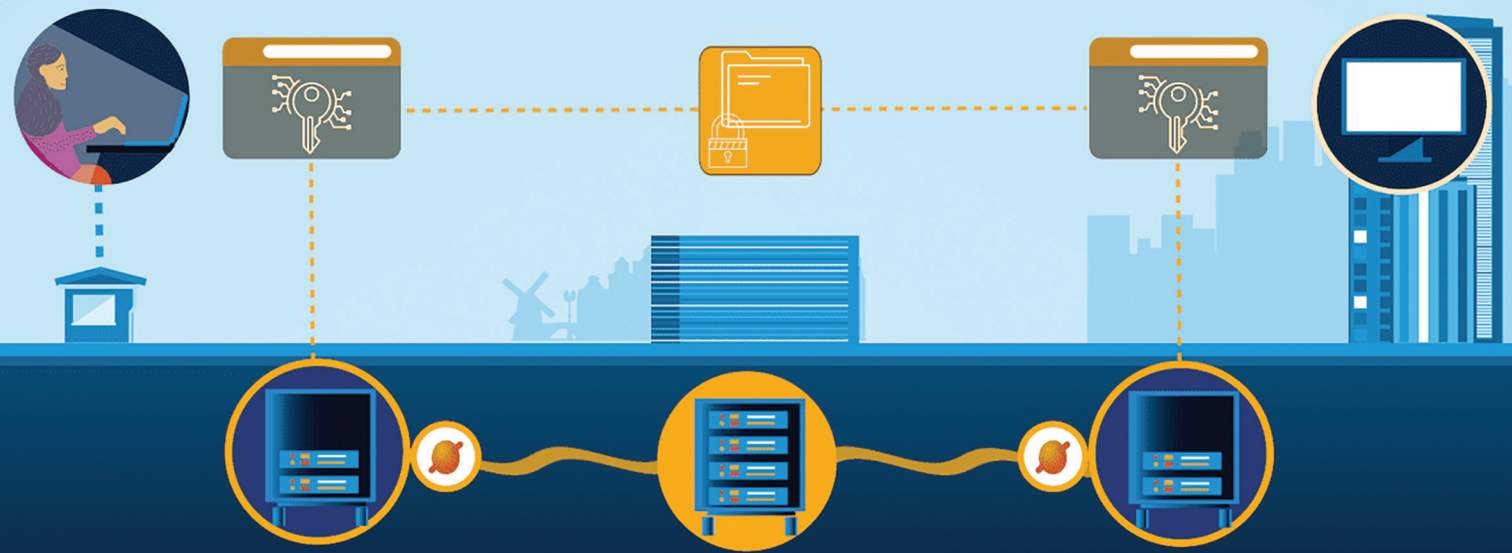
Doe het veilig, doe het quantum!



Delft runt... Rijswijk runt... Den Haag runt... We zijn live! Op 6 juli 2021 was het zover: via knooppunt Charlie in Rijswijk is het een onderzoeksteam van QuTech gelukt om via standaardglasvezelkabels quantumverstrengeling te genereren tussen signalen vanuit Delft en Den Haag, die hiermee inherent veilige cryptografische sleutels konden delen. Dit was de eerste geslaagde poging van een succesvolle demonstratie van *quantum key distribution* tussen steden in Nederland. Gedurende de demonstratie heeft het systeem meer dan zestig uur ononderbroken sleutels gegenereerd: een cruciale stap om quantum key distribution in de samenleving te realiseren [1].

De toekomst van encryptie

Encryptie wordt overal om ons heen al toegepast, van het sturen van een appje tot een digitale banktransactie. Het idee van digitale versleuteling is dat een bericht onherkenbaar wordt gemaakt door het te coderen met een *digitale sleutel*, een lijst van enen en nullen. Alleen met de juiste sleutel kan het versleutelde bericht gedecodeerd en gelezen worden. Een digitale sleutel moet eerst worden onderschept om een dergelijke versleutelde code te kunnen kraken. Een cruciale stap tijdens de encryptie is daarom het verdelen van de geheime sleutels tussen de partijen die veilig willen communiceren.

Op dit moment worden digitale sleutels gedefinieerd met behulp van wiskundige algoritmes. Hierdoor moeten hackers eerst een moeilijke berekening oplossen om de sleutel te achterhalen [2]. Het kraken van een sleutel vergt veel rekenkracht, waardoor het met de huidige computers miljoenen jaren kan duren om deze berekening uit te voeren. Echter, een quantumcomputer is in staat om deze algoritmes veel sneller te kraken [3]. Hoewel quantumcomputers op dit moment nog niet ver genoeg ontwikkeld zijn om dergelijke taken uit te voeren, bestaat er de mogelijkheid om berichten die vandaag verzonden worden af te tappen en op te slaan om later gekraakt te worden op het moment dat quantumcomputers hier wel klaar voor zijn. We hebben dus een nieuwe manier van sleutelgeneratie en -verdeling nodig om onze data te beschermen, onafhankelijk van een algoritme.

Measurement-device-independent quantum key distribution

Om de dreiging van het kraken van de encrypties door de quantumcomputer tegen te gaan moeten we vuur met vuur bestrijden of beter gezegd: quantum met quantum. Een technologie genaamd *quantum key distribution* (QKD) maakt gebruik van quantummechanische verschijnselen om in de toekomst veilig te communiceren over een digitaal netwerk. In deze technologie wordt gebruikgemaakt van quantuminformatiebits, ook wel qubits genoemd. Deze qubits zijn fundamenteel anders dan klassieke bits: waar klassieke bits de waarden 0 óf 1 kunnen hebben, kunnen qubits ook elke combinatie van 0 én 1 tegelijk zijn. Dit fenomeen wordt in de quantummechanica een superpositie genoemd. Na het meten van een qubit in superpositie stort deze in naar de waarde 0 óf 1.

Een voorbeeld van encryptie met behulp van quantummechanica is de zogenoemde *measurement-device-independent* QKD (MDI-QKD), zie figuur 1. In dit protocol willen twee zendpunten, Alice (Delft) en Bob (Den Haag), een sleutel delen. Om dit te kunnen doen sturen ze informatie in de vorm van qubits naar een centraal ontvangpunt, Charlie (Rijswijk). Bij Charlie ondergaan de qubits van Alice en Bob een interactie waardoor ze verstrengelen. Verstrengeling is een quantummechanisch fenomeen waarin twee qubits niet meer los van elkaar beschreven kunnen worden, wat resulteert in volmaakt gecorreleerde meetuitkomsten. Doordat de meetresultaten gecorreleerd zijn, kunnen Alice en Bob aan de hand van de hun verstuurde qubits en de meetuitkomsten weten wat de ander voor qubits heeft gestuurd, zonder expliciet met elkaar te communiceren. De informatie van deze qubits wordt dan gebruikt om een geheime sleutelbit te maken. Vervolgens kan de gegenereerde sleutel gebruikt worden om met bestaande encryptietechnieken data te versleutelen en te verzenden over het netwerk.

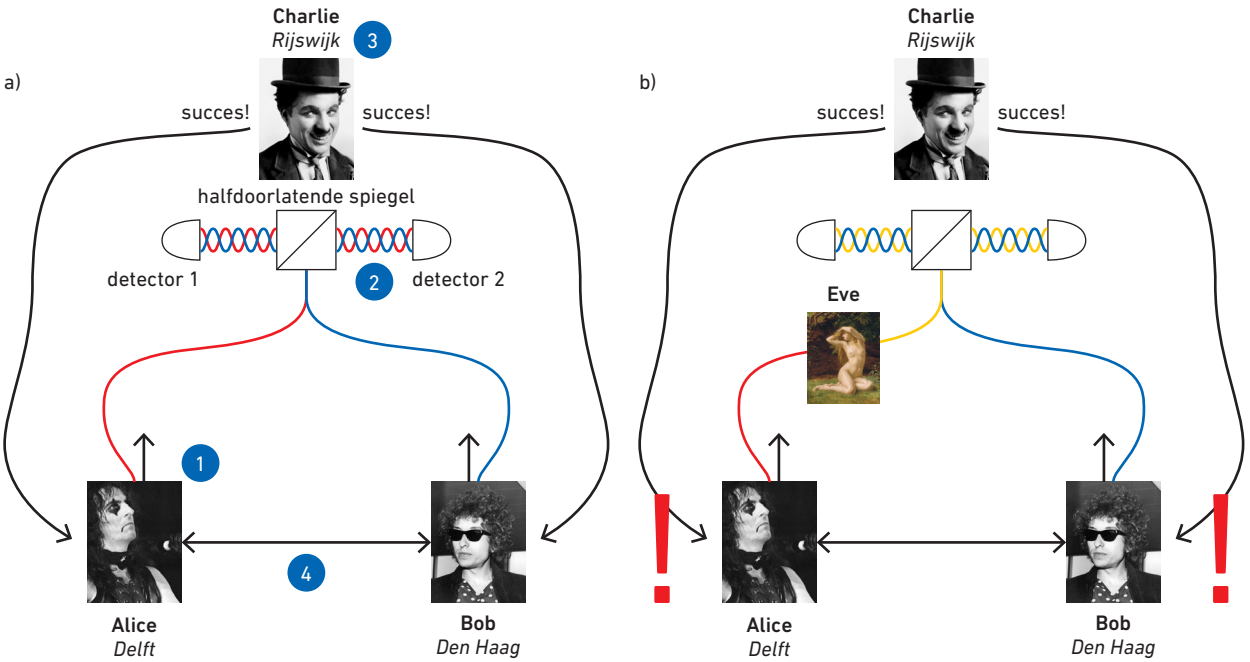
De qubits die Alice en Bob maken zijn willekeurig en gezien de uiteindelijke sleutel bestaat uit informatie over de qubits, zal deze ook willekeurig zijn. Ze verdelen deze sleutel dus onafhankelijk van een algoritme, waardoor ze beschermd zijn tegen de rekenkracht van de quantumcomputer.

Demonstratie in de praktijk

Het QuTech-team heeft dit MDI-QKD-protocol onlangs gedemonstreerd. Gedurende de demonstratie stonden de zendpunten Alice en Bob in respectievelijk Delft en Den Haag. Zij genereerden hier de qubits en verzonden deze vervolgens naar het centrale knooppunt Charlie in Rijswijk over standaardglasvezels.

Het zou onpraktisch zijn om voor quan-

Remon Berrevoets (1995) studeerde technische natuurkunde aan de TUD, waarna hij ook zijn bevoegdheid tot natuurkundedocent behaalde. Momenteel is hij werkzaam als optisch engineer bij QuTech, waar hij apparaten voor fundamenteel veilige datacommunicatie ontwerpt, bouwt en test. remonb@live.nl



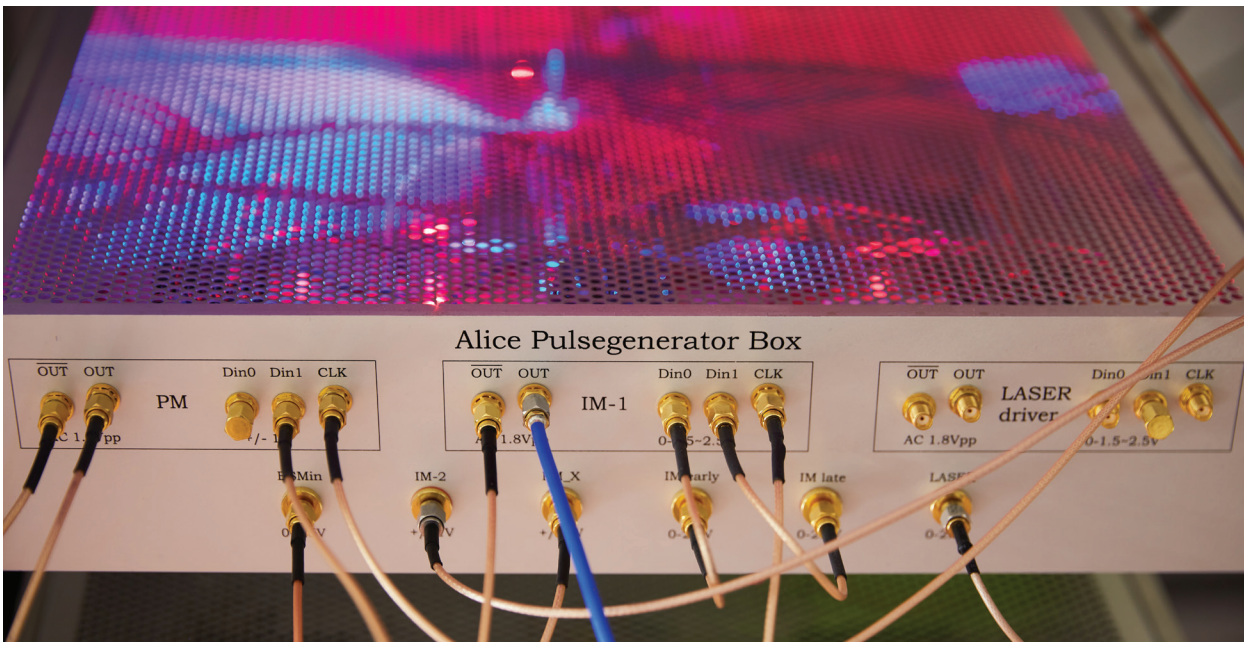
Figuur 1. Grafische weergave van het MDI-QKD-protocol zonder (a) en met (b) afluisteraar. a) Stap 1: twee locaties (Alice en Bob) sturen een qubit met een bepaalde waarde op naar een centraal punt (Charlie). Stap 2: de qubits van Alice en Bob worden bij Charlie samengevoegd op een halfdoorlatende spiegel. Hier vindt mogelijk verstrengeling plaats. Er vindt een Bell-toestandmeting plaats. Stap 3: als de Bell-toestandmeting succesvol is, stuurt Charlie deze informatie terug naar Alice en Bob, die deze informatie opslaan. Stap 4: Alice en Bob herhalen stappen 1 t/m 3 meerdere malen, totdat ze een veelvoud aan Bell-toestandmetingen hebben ontvangen. Vervolgens kijken ze samen of er te veel foutieve Bell-toestandmetingen waren en of hun sleutel zo veilig is om te gebruiken. b) Hetzelfde protocol als in (a). Een afluisteraar, Eve onderschept de qubits van Alice en verandert hierdoor hun waarde. De qubits van Bob verstrengelen nu met de qubits vanuit Eve en niet de originele qubit van Alice. Dit levert foutieve Bell-toestandmetingen op, wat Alice en Bob in stap 4 van het protocol kunnen detecteren. Deze sleutel gaan ze vervolgens niet gebruiken. Afbeelding Eve: Valentine Cameron Prinsep, Foto: Charlie Chaplin: P.D Jankens, Foto Alice Cooper: Hunter Desportes, Foto Bob Dylan: Svenska Dagbladet via IMS Vintage Photos.

EEN VEILIGE QUANTUMSLEUTEL

Wat zorgt er voor dat een quantumsleutel zo veilig is? De veiligheid is gebaseerd op twee kerneigenschappen van de quantummechanica: het *no-cloning*-theorema en het instorten van de qubits golffunctie. Het no-cloning-theorema luidt dat het onmogelijk is om een onbekende qubit te kopiëren. Wanneer een afluisteraar iets wil leren over een qubitwaarde, zal er dus een meting op de originele qubit plaats moeten vinden. Deze meting zorgt ervoor dat de golffunctie van de qubit instort. In de context van QKD betekent dit dat de afluisteraar door af te luisteren de qubitwaarde verandert. Zoals beschreven in het *kader Van qubits naar sleutel*, is de qubitwaarde cruciaal voor het ontstaan van verstrengeling. De verandering die de afluisteraar creëert heeft grote gevolgen voor de mogelijke verstrengeling bij het centrale punt. Het kan leiden tot 'succesvolle' Bell-toestandmetingen die eigenlijk onsuccesvol hadden moeten zijn en omgekeerd. Wanneer de locaties vanaf waar de originele qubits verzonden waren zien dat er te vaak foutieve Bell-toestandmetingen zijn, breken ze het protocol af en gebruiken ze hun sleutel niet. Door alleen veilige sleutels te gebruiken blijft al het dataverkeer tussen de locaties dus beschermd.

VAN QUBITS NAAR SLEUTEL

Normale computerbits maken gebruik van de waardes 0 of 1 om informatie op te slaan. Net zoals computerbits hebben qubits ook een waarde. In het MDI-QKD-protocol wordt vanaf twee locaties een qubit met een bepaalde waarde naar een centraal punt gestuurd. Wanneer de qubits samenkomen kunnen ze *verstrengelen zodra ze exact tegenovergestelde waardes* hebben. Er vindt geen verstrengeling plaats wanneer de qubits *exact dezelfde waarde* hebben.
In het centrale punt wordt een Bell-toestandmeting gedaan: dit is een specifieke meting die verstrengeling kan meten. Een succesvolle Bell-toestandmeting betekent dat er verstrengeling tussen de twee qubits plaatsvond. Vanuit het centrale punt wordt de succesvolle Bell-toestandmeting terug gerapporteerd naar de oorspronkelijke twee locaties.
Het ontvangen van een succesvolle Bell-toestandmeting geeft belangrijke informatie: omdat de locaties weten welke qubitwaarde ze zelf verstuurd hebben en de qubitwaarde van de andere locatie exact tegenovergesteld moet zijn weten ze ook wat deze andere qubitwaarde was! Deze waarde wordt nu als een bit gebruikt in een geheime sleutel. Kortom: de locaties hebben door middel van quantumverstrengeling informatie uitgewisseld, zonder deze informatie met elkaar te communiceren!



Figuur 2. De Alice Pulsegenerator Box bevat alle elektronica om superkorte elektrische pulsen te creëren, soms wel minder dan een halve nanoseconde lang. Deze elektrische pulsen worden vervolgens gebruikt om de qubits te maken waarmee we het MDI-QKD-protocol gedemonstreerd hebben. Foto: Paul Brussee.

tumnetwerken een apart glasvezelnetwerk aan te moeten leggen, dus het samenleven van quantumsignalen en conventioneel internetverkeer is cruciaal. Om te demonstreren dat dit samenleven mogelijk is hebben we onze qubits over hetzelfde glasvezelnetwerk verstuurd als het klassieke internetnetwerk. Doordat onze qubits bestaan uit individuele fotonen, worden ze al snel overstemd door ruis van andere signalen. De signalen in klassieke netwerken zijn meer dan een miljoen keer sterker dan de signalen van qubits, wat de samenleving van de twee niet-triviaal maakt.

Door verschillende golflengtes voor de klassieke kanalen en het quantummechanische kanaal te gebruiken, zijn we erin geslaagd drie signalen tegelijk over dezelfde glasvezel te sturen: onze qubits, een 100 Mb/s netwerk en een 10 Gb/s netwerk. De klassieke internetsignalen werden gegenereerd door routers en alle data over het 10 Gb/s kanaal werden automatisch versleuteld met de quantumsleutel. Om een toepassing te demonstreren, hebben we daarnaast de gegenereerde quantumsleutel gebruikt om een videostream tussen Delft en Den Haag te versleutelen. Dit quantumnetwerk tussen steden, waar de qubits samenleven met klassiek internet en dat geïntegreerd is met conventionele routers, laat zien dat onze technologie gereed is voor praktische toepassingen. Een belangrijke stap naar het veilige quantumnetwerk van de toekomst.

Hoe verder?

Nu we gedemonstreerd hebben dat onze technologie klaar is voor gebruik, willen we zo veel mogelijk toepassingen ervan laten zien. Op deze manier kunnen we de wereld duidelijk maken waarvoor en hoe deze technologie gebruikt kan worden. Om de technologie zo compatibel mogelijk te maken met de dagelijkse realiteit is het van belang dat we ons systeem zo veel mogelijk integreren met apparatuur van derde partijen. In een project dat we recent hebben afgerond werden de signalen verstuurd over telescopen en werd de quantumsleutel gebruikt om een financiële transactie te versleutelen. Het gebruik van het centrale knooppunt Charlie maakt het ook geschikt om meer gebruikers toe te voegen. Zo willen we de schaalbaarheid van het netwerk demonstreren en Nederland voorzien van een veilig quantumnetwerk [4].

Samenvatting

De bedreiging die de quantumcomputer vormt voor de veiligheid van ons dataverkeer kan worden tegengegaan met QKD-technologie. We hebben laten zien dat ons systeem kan worden gestationeerd in de echte wereld, waar de quantumsignalen samen kunnen leven met het klassieke internet. Hiermee hebben wij een belangrijke stap gezet naar het veilige communicatienetwerk van de toekomst.

REFERENTIES
1 R. C. Berrevoets et al., *Deployed MDI-QKD and Bell-State Measurements Coexisting with Standard Internet Data and Networking Equipment* (2021) online beschikbaar: https://arxiv.org/abs/2112.14254.
2 R. Rivest et al., *On Digital Signatures and Public-Key Cryptosystems* (1977).
3 P. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, IEEE, p. 124 - 134 (1994).
4 S. Wehner et al., *Quantum Internet: A vision for the road ahead*, *Science* **362** (2018).
5 W. K. Wootters en W. H. Zurek, *The no-cloning theorem*, *Physics Today*, p. 76 - 77 (2009).