Quantumsleutels: de praktische onveiligheid

Met behulp van de quantummechanica kunnen we volledig veilig berichten versleutelen. Althans, dat zegt de theorie – maar zijn er in de praktijk toch manieren om die volledig veilige berichten te kraken? Lieuwe Bakker bespreekt hoe veilig '100% veilig' uiteindelijk in de praktijk is.

Een tijdje geleden schreef ik een artikel over zogeheten quantum-sleutelverdelingprotocollen. Hierin beschreef ik hoe we communicatie tussen twee personen écht veilig kunnen maken. Niet door slimme wiskunde te gebruiken, maar door de natuurwetten toe te passen!

Vanuit dat idee lijkt het een vrij simpele stap naar echt veilige communicatie. Deze sleutels zouden, zoals in het vorige artikel beschreven, gebruikt kunnen worden voor encryptie-algoritmes, zoals het one-time pad – een van de weinige, wiskundig bewezen compleet veilige encrypties die we hebben. Ondanks de overtuigende argumenten die we in het vorige artikel zagen, zijn er echter nog wel vraagtekens te plaatsen bij deze quantum-sleutelverdelingmethodes. Eén heel eenvoudig uit te buiten probleem zal ik in dit korte artikel nader toelichten. Daarvoor is wat kennis nodig van het BB84-protocol dat ook in het vorige artikel ter sprake kwam, dus laat ik dat hieronder eerst kort samenvatten.

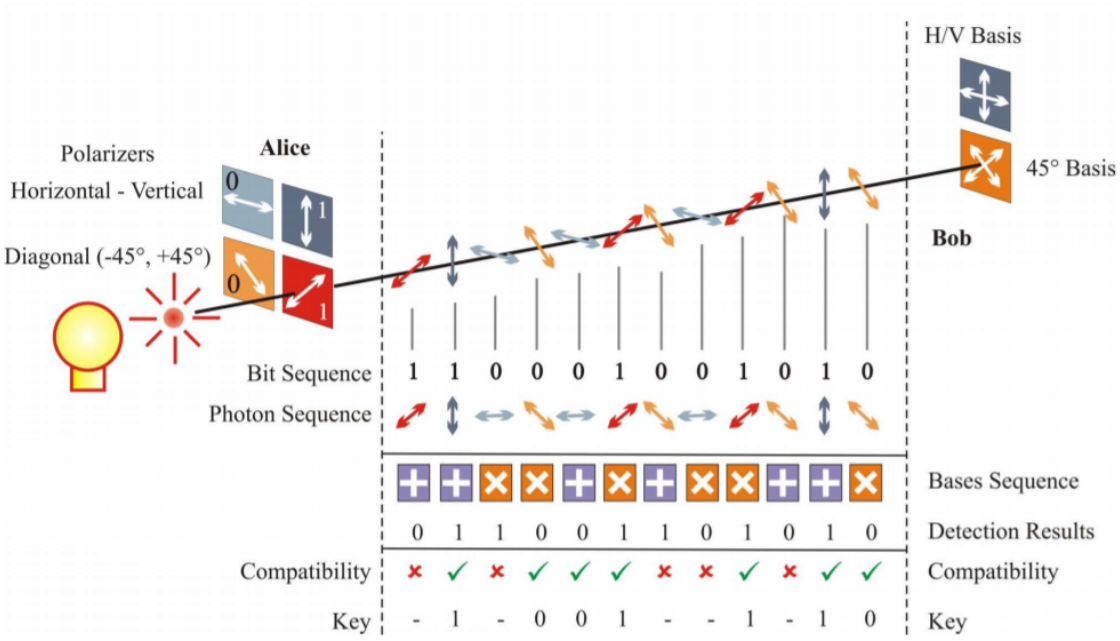
Het BB84-protocol voor quantum-sleutelverdeling

Stap 1: Persoon A (Alice) stuurt fotonen met bepaalde polarisaties (verticaal, horizontaal of diagonaal) naar persoon B (Bob). De keuze voor een polarisatie codeert een 'bit', een 1 of een 0.

Stap 2: Bob meet de polarisaties door te 'gokken' welke meting hij moet doen: hij meet de verticale/horizontale polarisatie of juist de diagonale polarisatie. De helft van de keren zal Bob goed gokken wat hij moet meten (dat wil zeggen: zal hij meten in een richting die Alice gekozen heeft), en de andere helft van de keren niet.

Stap 3: Bob vertelt na afloop aan Alice welke metingen hij voor elk foton heeft gedaan (verticaal/horizontaal of juist diagonaal), en Alice vertelt aan Bob welke keuzes goed waren. Bob bewaart vervolgens alleen de ‘juiste’ metingen.

Stap 4: Er gebeurt er een serie aan ‘checks’ om te verifiëren dat de sleutel écht veilig is. Hierbij wordt waargenomen of een afluisteraar ‘Eve’ de communicatie tussen Alice en Bob heeft afgetapt. Zie het eerdere artikel over quantumsleutels voor meer details over hoe deze checks werken.



Afbeelding 1. Het BB84-protocol.Het BB84-protocol zoals geïntroduceerd in het eerste artikel van deze serie. Alice stuurt licht naar Bob. Dit licht polariseert ze ofwel verticaal/horizontaal, ofwel diagonaal. Deze polarisaties komen overeen met een bit (een 1 of een 0) zoals te zien in de figuur. Bob meet de polarisaties door te gokken welke polarisatie hij moet meten. Vervolgens communiceert Bob naar Alice zijn keuzes voor metingen (verticaal/horizontaal of diagonaal), en Alice vertelt aan Bob bij welke metingen hij de juiste keuze heeft gemaakt. Daarmee houden Alice en Bob alleen die bits over, waarbij ze allebei dezelfde polarisatie hebben gebruikt. Door nu een deel van de sleutel via een publiek kanaal met elkaar te vergelijken kunnen Alice en Bob vaststellen dat ze

alles goed hebben gedaan, en dat er geen afluisteraar aanwezig was.

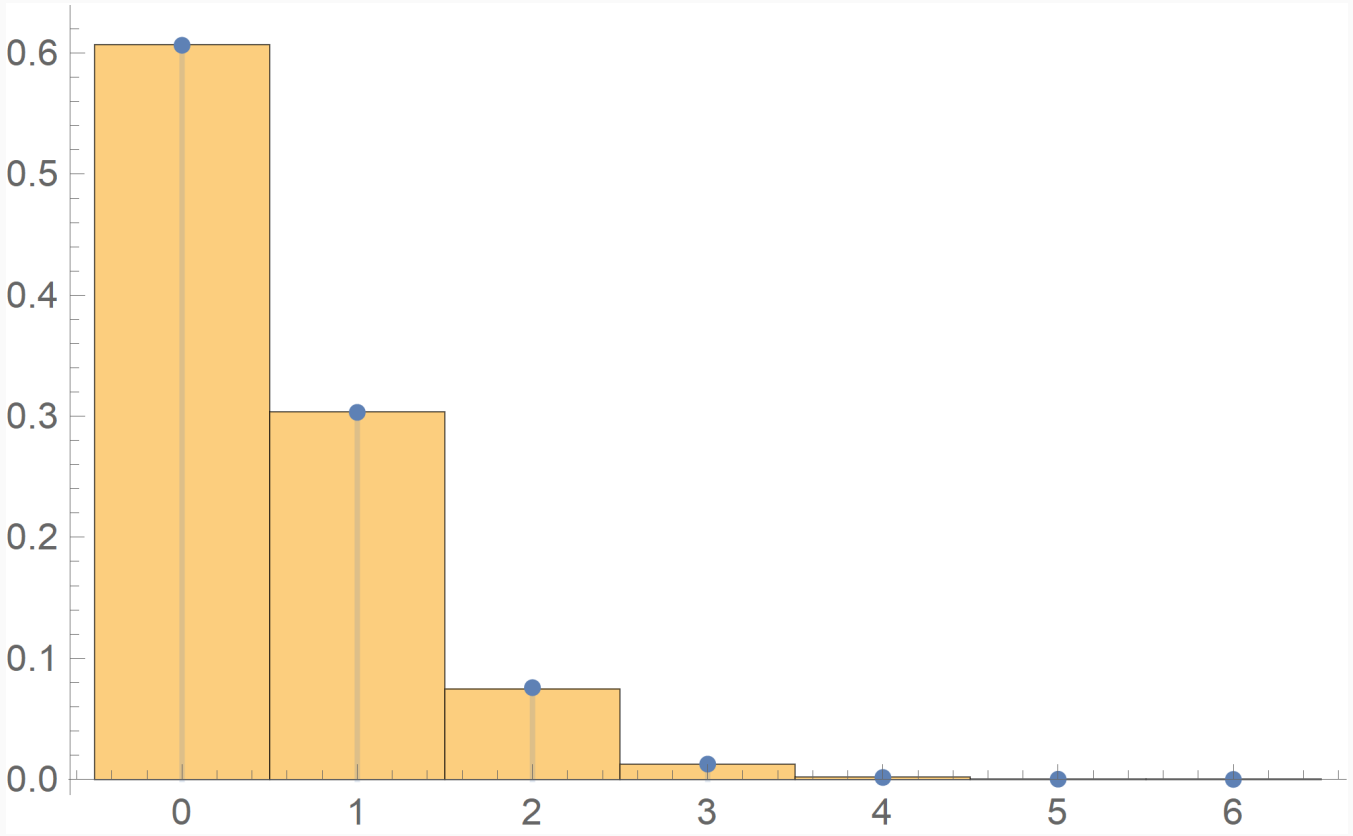
De hierboven beschreven communicatiemethode is volledig veilig, omdat persoon E (Eve) niet in staat is om de communicatie met behulp van fotonen af te luisteren zónder ruis aan het signaal toe te voegen. Als ze die ruis zien weten Alice en Bob dat er iemand aan het meeluisteren is, en zo weten ze dus altijd wanneer een sleutel echt geheim is en wanneer niet.

Geld is natuurlijk het probleem

Nu kun je je wellicht alsnog afvragen hoe een quantum-sleutelverdelingsprotocol zoals BB84 tóch 'gekraakt' kan worden. Het antwoord zit natuurlijk niet in het veranderen van de natuurwetten, dat is voor zover wij weten onmogelijk. Nee; de truc zit hem erin om bijvoorbeeld de apparaten die gebruikt worden aan te vallen. Om dit nader te verklaren wil ik nog één keer een belangrijk detail van BB84 benadrukken: het protocol maakt gebruik van *individuele* fotonen per bit. Het is, voor het bewijs van veiligheid, van belang dat er slechts één foton per keer wordt uitgezonden. De reden daarvoor is dat het niet mogelijk is om dit enkele foton te bewerken, zonder de hiervoorgenoemde ruis te introduceren. Maar wat nu als Alice per ongeluk *twee* fotonen tegelijkertijd uitzendt om een bit te coderen? Stel dat ze bijvoorbeeld twee fotonen uitzendt, die dan door hetzelfde polarisatiefilter gaan en die dus allebei verticaal gepolariseerd zullen zijn. Als dat gebeurt leidt het tot een methode die gebruikt kan worden om BB84 te kraken.

Wellicht is het goed om eerst te vertellen waar de bovenstaande gedachte vandaan komt. Immers, Bennet en Brassard, de ontwerpers van BB84, ontwierpen hun experiment toch voor het gebruik van enkele fotonen? Waarom zou men dat in het gebruik dan niet ook doen? Het antwoord is simpel: kosten. Een machine die precies één foton per keer uitzendt is een duur en groot apparaat. In de praktijk is het veel gemakkelijker om een laser te maken, met behulp van een goedkope – maar wel stabiele en betrouwbare – laserbronnen. Deze lasers genereren lichtsignalen van wel miljoenen fotonen tegelijk. Het lichtsignaal wordt vervolgens op een bepaalde manier bewerkt waardoor het 'lijkt' op een enkel foton… gemiddeld gezien

dan. De verdeling van het aantal fotonen dat zo'n signaal bevat wordt beschreven door een zogeheten Poissonverdeling. Stel bijvoorbeeld dat het gemiddelde aantal fotonen in elke laser puls 0,5 is. Dan kunnen we met behulp van de Poissonverdeling berekenen dat 60 procent van de laserpulsen géén foton bevat, 30 procent van de signalen heeft één foton, en ongeveer 9 procent heeft 2 of meer fotonen. Dit betekent dus dat ongeveer 23 procent van alle niet-lege signalen (9 van de 39) bestaat uit meer dan één foton, en dus, zoals we hieronder in meer detail zullen zien, onveilig is.

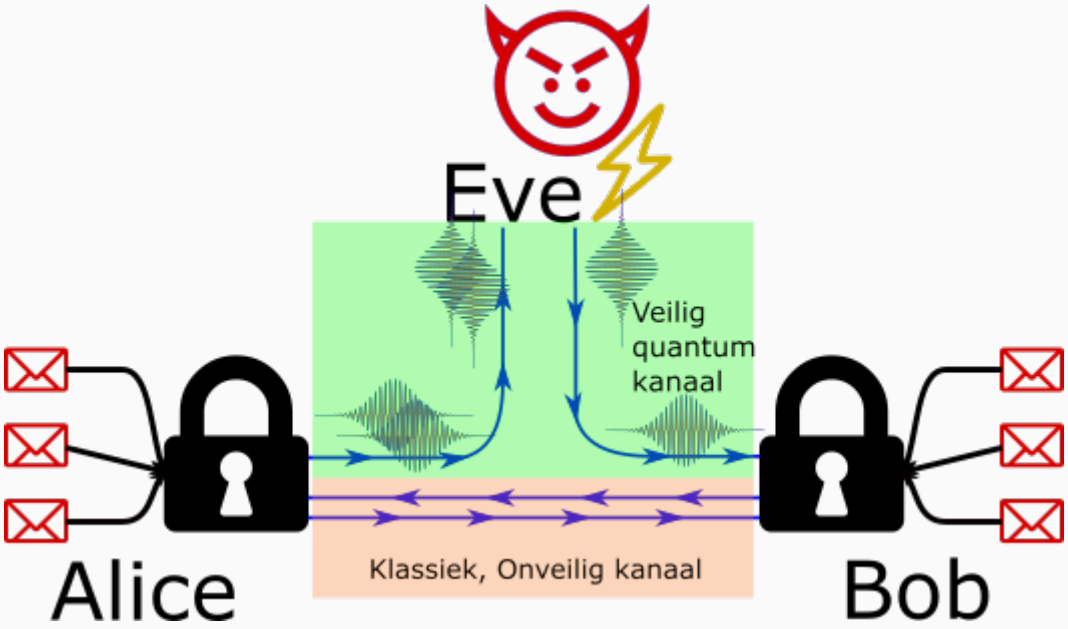


Afbeelding 2. De Poissonverdeling. Een voorbeeld van een Poissonverdeling zoals genoemd in de tekst. Het 'gemiddelde' (de gemiddeld verwachtte uitkomst) is in dit voorbeeld 0.5. Dit vertaalt zich naar ongeveer 60% van de keren geen foton, 30% van de keren één foton, en in de rest van de gevallen 2 of meer fotonen.

Foton-aantal splitsende aanvallen

Het tussenkopje hierboven (in het Engels: *photon number splitting attacks*) is de algemene naam die gebruikt wordt om het hierboven beschreven proces, waarmee Eve quantum-sleutelverdelers kan aanvallen, te benoemen. Daar moet ik bij zeggen dat het in de praktijk natuurlijk extreem lastig voor Eve zal zijn om een quantum-sleutelverdelingsprotocol te kraken. Daarvoor is speciale apparatuur nodig, en volledige toegang tot alle communicatiekanalen die Alice en Bob gebruiken. Vanuit theoretisch oogpunt – en om 100% zeker te zijn van de veiligheid – doen we echter alsof afluisteraar Eve dit allemaal kan doen. Sterker nog; Eve kan in onze hypothetische situatie álles doen, zolang het maar niet tornt aan de natuurwetten en de wetten van de wiskunde.

Laten we dus aannemen dat Eve een volledige, vrije toegang heeft tot het communicatiekanaal tussen Alice en Bob, zoals in afbeelding 3. Alice en Bob doen hun ding, en sturen elkaar fotonen. Nu gaat Eve aan de slag. Zij positioneert zich midden in het communicatiekanaal van Alice en Bob – ze knipt bijvoorbeeld de glazvezelkabel die gebruikt wordt om de fotonen te geleiden door de helft, zodat ze er tussen kan staan. Als Alice en Bob alleen signalen gebruikten van *enkele* fotonen zou er niets zijn dat Eve kan doen om het signaal onmerkbaar af te luisteren. Wat Eve echter wél kan doen, zonder ruis te genereren op het signaal van Alice en Bob, is meten hoeveel fotonen er zich in het signaal bevinden. In technische termen: foton-aantallen en polarisatie zijn niet gerelateerd door Heisenbergs onzekerheidsprincipe, wat wil zeggen dat je het één kunt meten zonder het ander te beïnvloeden. Nu is Eve’s werk vrij eenvoudig. Elk signaal dat slechts 1 foton heeft blokkeert Eve volledig. Als een signaal meer dan 1 foton heeft, dan splitst ze het signaal, bewaart één foton in haar eigen administratie, en stuurt alle andere fotonen door naar Bob. Het enige wat Eve nu hoeft te doen, is wachten tot Alice en Bob hun gebruikelijke verificaties doen, en Eve heeft met haar kopie van het signaal een sleutel die precies hetzelfde is als de sleutels van Alice en Bob. Daarmee heeft Eve het doel bereikt: Alle communicatie tussen Alice en Bob kan nu schaamteloos worden afgeluisterd!



Afbeelding 3. Een foton-aantal splitsende aanval. Een schematische weergave van een ‘aantal-splitsende aanval’ door Eve. Eve onderschept het ‘veilige’ quantumsignaal (de fotonen) tussen Alice en Bob. Vervolgens meet Eve het aantal fotonen in elke lichtpuls. Als het aantal 1 is blokkeert Eve het signaal. Als er 2 (zoals in het figuur) of meer fotonen zijn, dan houdt Eve er één voor zichzelf, en stuurt de overige fotonen door naar Bob. Zo kan Eve het protocol ‘kraken’ en zelf een exacte kopie van dezelfde sleutel als Alice en Bob bemachtigen.

Oplossingen voor de aanvallen

Het feit dat ik op deze website kan schrijven over dit type aanval betekent natuurlijk ook dat er door veel mensen over nagedacht is. Huidige, in de praktijk gebruikte quantum-sleutelverdelingsmachines hebben extra protocollen in zich, waarmee ook in het geval van foton-aantal splitsende aanvallen de sleutelveiligheid gegarandeerd kan worden. De standaard methode hiervoor heet de ‘lokaas-toestandmethode’ (in het Engels: *decoy state method*). Bij deze methode verstuurt Alice niet slechts één signaal naar Bob, maar meerdere signalen – 3 bijvoorbeeld. Alice en Bob spreken vooraf de verwachte aantallen van de fotonen

af, via een publiek kanaal, wat Eve zonder problemen kan en mag afluistere).

Nu is de grap dat Bob aan zijn ontvangende kant een ‘verwacht aantal fotonen’ heeft, wat bepaald wordt door de voorafgesproken laserintensiteiten. Doordat Eve een foton ‘wegpakt’ uit het signaal; interfereert dit met het totale aantal fotonen dat verstuurd wordt. Dit verstoort de verwachte metingen van Bob, waar ze achter komen bij de controleprocedures aan het eind van de quantum-sleutelverdeling. Een simpele methode, en bovendien één die werkt! Eve kan niets doen aan dit probleem, want zelfs al zou ze proberen om de foton-aantallen te herstellen naar hun gewenste aantallen door zelf een extra foton uit te zenden voor elk foton dat ze ‘steelt’, dan nog introduceert Eve interferentie op het signaal, net zoals in het ‘normale geval’. Het blijft immers onmogelijk voor Eve om een foton gegarandeerd op de juiste manier te meten en vervolgens een exacte kopie naar Bob te sturen, juist vanwege Heisenbergs onzekerheids relatie!

De korte en krachtige conclusie: met de juiste extra trucs is BB84 nog steeds hack-proof, ook als we goedkope machines willen bouwen!

In de zomerperiode publiceert de QU-site elke vrijdag een artikel. In september gaan we weer terug naar het schema van twee artikelen per week: elke dinsdag en elke vrijdag.