

Een beveiligde transmissie: de quantumcryptografie

P. Navez¹ en G. Van Assche^{1,2}

April 2002

¹ Université Libre de Bruxelles, dienst Théorie de l'Information et des Communications (Prof. N. Cerf).

² Proton World, member of ERG Group, Smart Card Security Center of Excellence (Y. Moulart).

De quantumcryptografie, de meest recente hightech-nieuwigheid, garandeert absolute vertrouwelijkheid van de informatie die verzonden wordt via een optische vezel. Het geheim van deze krachttoer schuilt in de mogelijkheid om informatie over te brengen via het elementaire bestanddeel van licht: het foton.

Kwetsbaarheid van de conventionele gecodeerde transmissies

Hoe kunnen we ons ervan verzekeren dat onze gecodeerde boodschappen niet begrepen worden door een ongewenste derde? De discipline die op deze vraag een antwoord tracht te geven, is de cryptografie.

In de traditionele cryptografie kan enkel de code van Vernam een onvoorwaardelijk veilig kanaal creëren tussen een zender (Alice) en een ontvanger (Bob). Deze code vraagt Alice en Bob een vooraf bepaalde codeersleutel goed te keuren. Alice vercijfert het bericht aan de hand van deze codeersleutel, waarna het gecodeerde bericht enkel nog kan worden ontcijferd aan de hand van diezelfde sleutel, dus door Bob. De codeerregel is eenvoudig. Laten we veronderstellen dat Alice een bit aan informatie wil verzenden. Daartoe gebruikt ze een bit van de sleutel, waarmee ze een "of-exclusief" handeling uitvoert met de te verzenden bit. Om de verzonden bit te ontcijferen, moet Bob nu, van zijn kant, dezelfde handeling uitvoeren, teneinde de eerste "of-exclusief" handeling te annuleren.

Jammer genoeg vertoont de code van Vernam een groot nadeel. Om ervoor te zorgen dat de methode niet doorbroken kan worden, moet de sleutel uit evenveel codeerbits bestaan als er bits aan informatie te verzenden zijn, want de codeersleutel kan slechts eenmaal gebruikt worden. Indien een sleutel meer dan eens gebruikt wordt, kan de code van Vernam doorbroken worden; op die manier zijn de Duitsers er tijdens de Tweede Wereldoorlog dan ook in geslaagd de gecodeerde informatie bij opeenvolgende transmissies te ontcijferen.

Strikt genomen moet de codeersleutel van tevoren manueel door Alice aan Bob overhandigd worden. Dit betekent dat, indien men een gigabit aan gecodeerde informatie wil verzenden, Alice en Bob elkaar eerst moeten ontmoeten om

bijvoorbeeld een cd-rom met een miljard willekeurige bits te overhandigen. Ondanks het feit dat deze procedure veilig is, is ze niet echt praktisch in gebruik, aangezien Alice en Bob verplicht zijn elkaar eerst te ontmoeten vooraleer ze met elkaar kunnen communiceren over een afstand van 10.000 km.

Daarom hebben de wiskundigen enkele andere cryptografiemethoden ontwikkeld teneinde deze moeilijkheden te verhelpen.

Het eerste verschil tussen de code van Vernam en de huidige cryptografiemethodes bestaat erin dat de eenvoudige "of-exclusief" handeling vervangen wordt door een heel wat complexere handeling tussen de sleutel en het leesbare bericht. Op die manier wordt het bijna onmogelijk om het leesbare bericht terug te vinden op basis van het gecodeerde bericht, of zelfs de sleutel te vinden op basis van het leesbare én het overeenkomstige gecodeerde bericht, en dit zelfs indien de sleutel heel wat kleiner is dan het te verzenden bericht. Dit is bijvoorbeeld zo bij het cryptografie-algoritme per blok DES [4] of het meer recente Belgische Rijndael algoritme dat werd geselecteerd als de nieuwe AES [5] standaard.

Dankzij deze algoritmes kunnen Alice en Bob nu een kleine sleutel uitwisselen waarmee ook grote berichten gecijferd en ontcijferd kunnen worden. De prijs die we daarvoor moeten betalen, is het verlies van absolute veiligheid door toevoeging van een hypothese. In theorie is het nu mogelijk het leesbare bericht terug te vinden op basis van het gecodeerde bericht, maar dit is voldoende moeilijk om te veronderstellen dat de vijand niet over voldoende berekeningsmiddelen beschikt om daarin te slagen.

In de praktijk is deze hypothese heel realistisch. Een hacker zal over het algemeen over heel wat meer faciliteiten beschikken om de tekortkomingen van een computersysteem te doorprikken dan om berekeningen te maken die noodzakelijk zijn om het algoritme te doorbreken, ook al beschikt hij over de krachtigste computer. Toch kan niets garanderen dat de verdere ontwikkelingen in de wiskunde of de informatica er op lange termijn niet in zullen slagen om het leesbare bericht te ontcijferen op basis van het gecodeerde bericht.

De tweede verbetering dankzij de moderne cryptografie is de invoering van de cryptografie met openbare sleutel, waardoor Alice en Bob elkaar niet langer eerst moeten ontmoeten om de sleutel te overhandigen wanneer ze elkaar gecodeerde boodschappen willen zenden.

In de systemen met openbare sleutel die tegenwoordig algemeen gebruikt worden, beschikt elke correspondent over twee sleutels. Eén van deze sleutels is openbaar en dus door iedereen gekend (vb.: gepubliceerd in een lijst); met deze sleutel kan het bericht enkel gecijferd worden, niet ontcijferd. De tweede sleutel, daarentegen, is geheim en dient om het bericht te ontcijferen. Om een bericht te versturen van Alice naar Bob, wordt de volgende procedure gevolgd. Tenzij ze die al heeft, verschaft Alice zich de openbare sleutel van Bob (via een openbare database of ze vraagt de sleutel gewoon aan Bob). Vervolgens gebruikt Alice de openbare sleutel van Bob om het vertrouwelijke bericht te coderen en ze verzendt de gecodeerde informatie naar Bob. Hij is de enige persoon die beschikt over de overeenkomstige geheime sleutel en dus de enige persoon die in staat is om het bericht dat Alice hem net heeft gestuurd, te

ontcijferen. De essentie van dit systeem is dat de cryptografie openbaar gebeurt, zodat eender wie een gecodeerd bericht naar Bob kan sturen, maar om dit bericht te ontcijferen is uiteindelijk de geheime sleutel nodig.

Opnieuw moeten de praktische voordelen van de cryptografie met openbare sleutel vergeleken worden met het relatieve verlies aan veiligheid dat hiermee gepaard gaat. Er bestaat een link tussen de openbare sleutel en de overeenkomstige geheime sleutel, waardoor het in theorie dus mogelijk is om de één terug te vinden op basis van de andere. Toch is het gelukkig erg moeilijk om deze handeling uit te voeren binnen de huidige kennis en de capaciteit van de huidige computers.

Om dit idee duidelijk te maken, nemen we even het voorbeeld van het Rivest-Shamir-Adleman (RSA) algoritme dat gebruikt kan worden op basis van een codeersysteem met openbare sleutel [4]. In dit systeem kan de link tussen de openbare en de geheime sleutel enkel gevonden worden indien men in staat is getallen bestaande uit meerdere honderden cijfers te factoriseren, wat op dit ogenblik erg moeilijk is. Want ook al is het makkelijk om twee grote priemgetallen te vermenigvuldigen, ze recupereren op basis van het product is al heel wat moeilijker. Jammer genoeg leggen de successen die geboekt worden op het vlak van de factorisatie de lat steeds hoger voor de cryptografen die zich moeten baseren op steeds grotere sleutelgroottes, en bijgevolg ook op steeds grotere te factoriseren getallen. Bovendien zal een wiskundige, indien hij op een dag een algoritme ontdekt waarmee hij snel grote cijfers kan factoriseren, alle berichten die gecodeerd werden met RSA kunnen ontcijferen zonder dat ook maar iemand dit merkt, aangezien hij toegang heeft tot alle openbare sleutels.

Deze dreiging werd dan ook zo groot, dat de natuurkundigen een nieuwe manier hebben uitgedacht om berekeningen te maken via een quantumcomputer. Deze nieuwe generatie computers, die zich hoofdzakelijk nog in de theoretische fase bevindt, is in staat om enkele bekende moeilijke problemen snel op te lossen met de traditionele computertechnieken. Zo heeft Peter Shor [6] een quantumalgoritme ontdekt (dat met andere woorden op een quantumcomputer draait) waarmee grote getallen gefactoriseerd kunnen worden in redelijke termijnen.

De veiligheid op lange termijn van de huidige codeertechnieken lijkt dus vanuit verschillende hoeken bedreigd te worden. Zo biedt de cryptografie met openbare sleutel, bijvoorbeeld, geen enkele langetermijngarantie inzake de vertrouwelijkheid van de gegevens die ze moet beveiligen, ondanks het feit dat deze codeertechniek erg populair is en toch nog steeds een voldoende breed veiligheidsniveau biedt. Daarom willen wij hier een alternatieve manier voorstellen voor het beheren van de vertrouwelijkheid van een bericht, zonder enige veronderstelling te maken inzake de technologie of de complexiteit, m.a.w. inzake de praktische snelheid van deze of gene wiskundige berekening met de huidige computers.

Oplossing: de quantumcryptografie

Betekent dit dan dat we gedoemd zijn tot het manueel uitwisselen van vooraf bepaalde codeersleutels van enkele megabits om een absolute vertrouwelijkheid te garanderen? Wanneer we de meest fundamentele fysicawetten die we tot op vandaag kennen erop nakijken, is dit niet zeker. De quantumfysica, die de innerlijke dynamica

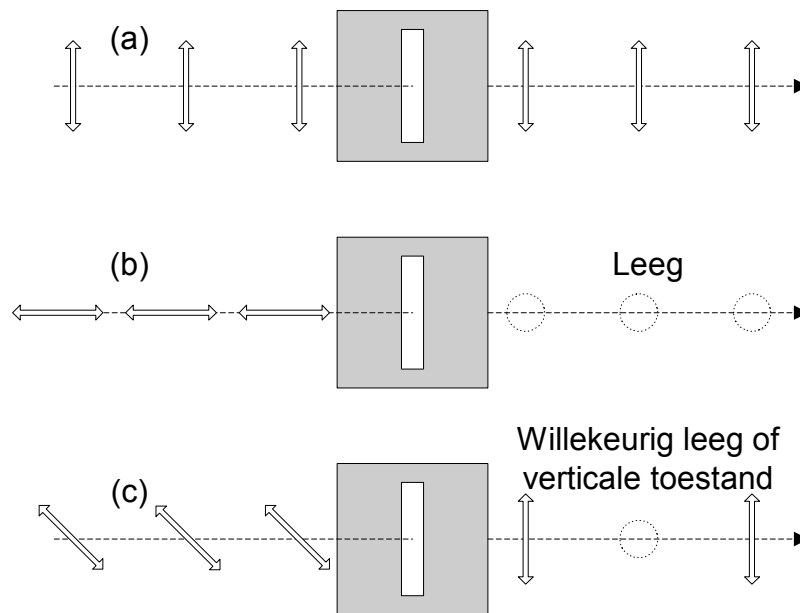
van elk elementair deeltje (fotonen, atomen, ...) van ons universum beschrijft, zou een oplossing kunnen bieden voor dit probleem en toelaten communicatieprotocollen op te stellen die geen zwakke plekken bevatten op het vlak van veiligheid. Dit is het doel van de quantumcryptografie.

De quantumcryptografie ontstond zo'n vijftien jaar geleden toen twee wetenschappers, Charles Bennett en Gilles Brassard [1], het idee kregen om de principes uit de quantumfysica te gebruiken voor het vertrouwelijk overbrengen van berichten. De transmissie gebeurt via impulsen van een individueel foton (licht "quanta") die door een zender (Alice) verzonden worden naar een ontvanger (Bob) via een optische vezel.

De zogenaamde "non-cloning" stelling verhindert in de quantumfysica dat een derde partij (Eve) de verzonden informatie kan decoderen. Hierbij wordt dus aangetoond dat het niet mogelijk is de quantumtoestand van het licht en vooral de toestand van het foton te reproduceren of te klonen, op behalve indien men beschikt over een precieze en vooraf gekende karakterisering van die quantumtoestand. Met andere woorden: precies het feit dat men een foton moet observeren om het te karakteriseren, denatureert het volledig zonder dat men het later opnieuw kan omzetten in zijn oorspronkelijke toestand of zelfs klonen. Deze "non-cloning" stelling blijkt slecht nieuws te zijn voor elke poging om de quantumtoestand van een foton volledig te karakteriseren. Ze is echter positief op het vlak van de cryptografie. Eve, die de gecodeerde informatie wil verzamelen zonder opgemerkt te worden, zal de quantumtoestand van het foton immers van tevoren moeten kopiëren. En aangezien dit onmogelijk is, zal ze de toestand waarin het foton zich bevindt, zo goed mogelijk moeten raden. Hierdoor brengt ze wijzigingen aan die het foton denatureren, waardoor ze zich uiteindelijk blootstelt aan latere detectie door Alice of Bob.

Het belangrijkste doel bestaat er dus in Alice en Bob in staat te stellen een codeersleutel uit te wisselen, terwijl ze er toch zeker van zijn dat elke derde die eventueel meeluistert, gedetecteerd kan worden. Indien deze codeersleutel correct werd verzonden, kunnen Alice en Bob hem gebruiken in combinatie met de hierboven beschreven code van Vernam teneinde een onvoorwaardelijk veilig codeersysteem te verkrijgen, en dit zelfs op afstand.

Uitgaand van het "non-cloning" idee, hebben de onderzoekers een communicatieprotocol uitgewerkt waarbij ze gebruik maakten van de polarisatie van het foton om bits te coderen die een codeersleutel kunnen bevatten. Het foton beschikt immers over twee zogenaamde polarisatietoestanden die zich vooral van elkaar onderscheiden via een polarisatiefilter (zoals, bijvoorbeeld, een calcietkristal). Dit betekent dat een verticaal gepolariseerde lichtstraal zal passeren door de filter die in dezelfde richting opgesteld staat. De horizontaal gepolariseerde lichtstraal, daarentegen, zal niet door de filter passeren, maar zal er door geabsorbeerd worden. Indien de lichtstraal nu diagonaal in een hoek van 45° gepolariseerd wordt, zal slechts de helft van de lichtintensiteit door de filter passeren. En wat zou er gebeuren als we slechts één diagonaal gepolariseerd foton door de filter zouden sturen? Het foton kan duidelijk niet in twee gedeeld worden, aangezien het een ondeelbare lichtkern is. Net zoals de hierboven reeds genoemde quantumtheorie toont de ervaring aan dat het foton in 50% van de gevallen door de polarisatiefilter zal passeren en in de andere 50% geabsorbeerd zal worden.



Figuur 1: Eén foton dat door een filter passeert die enkel verticaal gepolariseerd licht doorlaat. (a) De verticaal gepolariseerde lichtstralen passeren door de filter, zonder geabsorbeerd te worden. (b) De horizontaal gepolariseerde lichtstralen worden allemaal geabsorbeerd. (c) De diagonaal gepolariseerde lichtstralen worden willekeurig geabsorbeerd of doorgestuurd. Een waarnemer die zich achter de filter bevindt, kan de toestand van het foton vóór de filter dus niet precies vastleggen in verhouding tot een hetzij verticale, hetzij horizontale polarisatietoestand.

Een perfect protocol

Indien Alice zich beperkt tot het invoeren van codeerbits in zowel de verticale als de horizontale polarisatietoestand, is Bob in staat deze bits te lezen, waarbij hij de polarisatie van elk foton kan onderscheiden dankzij de filter. Maar in dit geval is Eve in staat de boodschap te onderscheppen zonder zelf ontdekt te worden. Het volstaat dat ze deze bits op dezelfde manier als Bob detecteert en ze vervolgens opnieuw encodeert in de polarisatie van de fotonen op dezelfde manier als Alice, waarna ze de bits opnieuw verstuurt naar Bob. Alice kan daartegenover een strategie ontwerpen waarbij de polarisatie-encoding van de fotonen telkens in 50% van de gevallen horizontaal en verticaal gericht is, of in 50% van de gevallen diagonaal in een hoek van 45° en 135° . In dat geval moet Eve reeds een onderscheid maken tussen vier mogelijke polarisatietoestanden, terwijl een polarisatiefilter er slechts twee kan onderscheiden volgens orthogonale assen, en het volgens de principes van de quantummechanica niet mogelijk is een as te realiseren die één toestand uit vier mogelijke polarisatietoestanden isoleert.

Deze onmogelijkheid illustreert de fameuze “non-cloning” stelling. Indien een dergelijke polarisatiefilter zou bestaan, zouden we de polarisatietoestand van het foton ondubbelzinnig kunnen karakteriseren en evenveel klonen in dezelfde toestand creëren als nodig. Zo zou Eve een kopie voor zichzelf kunnen houden en er een ander versturen naar Bob, dit alles zonder opgemerkt te worden. Gezien de “non-cloning” stelling richt ze haar polarisatiefilter best willekeurig in een verticale of diagonale richting, wat onvermijdelijk fouten met zich brengt en de communicatie stoort.

Wat hier bij Eve gebeurt, doet zich onvermijdelijk ook voor bij Bob die, anderzijds, ook moet beschikken over de as waarin hij de polarisatie meet. Om in deze situatie codeerbits te kunnen uitwisselen, moet Bob dus openlijk de polarisatieassen waarin hij zijn meting heeft uitgevoerd, meedelen aan Alice. Vervolgens vergelijkt Alice de assen waarin ze elke bit heeft verzonden met de assen die Bob geselecteerd heeft. Indien deze assen overeenkomen, laat Alice dit openlijk weten aan Bob, waarbij een codeerbit uitgewisseld wordt; komen de assen niet overeen, dan zal de bit gewoon verworpen worden, aangezien er geen enkele overeenkomst bestaat.

De interventie van Eve kan Alice en Bob enkel op een dwaalspoor brengen m.b.t. de uitgewisselde codeerbit. Veronderstellen we bijvoorbeeld dat Eve het foton meet in een diagonale polarisatie, terwijl Alice het verzonden heeft met een verticale polarisatie. Eve stuurt een foton terug naar Bob in de polarisatie die ze gemeten heeft. Indien Bob per vergissing een horizontale polarisatie meet, zal de uitgewisselde codeerbit verschillend zijn, ofschoon de polarisatieassen die gekozen werden door Alice en Bob overeenkomen. Om de aanwezigheid van Eve te detecteren, volstaat het dan een klein aantal bits op te offeren van het grote aantal dat werd uitgewisseld. Dit deel van het aantal bits wordt openlijk verzonden tussen Alice en Bob om het foutenpercentage tijdens de communicatie te controleren. Indien dit foutenpercentage, dat ook rekening houdt met onvermijdelijke fouten die te wijten zijn aan technische onvolkomenheden, abnormaal hoog is, betekent dit dat de communicatie werd onderschept.

Veilig, wie doet beter?

In dit protocol steunt de veiligheid onder andere op het niet-bestaan van een polarisatiefilter waarmee een onderscheid kan gemaakt worden tussen vier verschillende toestanden. Hoe kunnen we hierin dan geloven, behalve om de natuurkundigen enig vertrouwen te schenken? De quantumtheorie maakt het mogelijk alle gekende natuurkundige fenomenen te interpreteren op de meest precieze manier die ons tot op vandaag bekend is. Deze theorie beschrijft evenzeer de microscopische fenomenen die zich voordoen op het vlak van de elementaire deeltjes en atomen, als de macroscopische fenomenen die voortvloeien uit de collectieve dynamica van diezelfde deeltjes en atomen. En indien het feit dat deze theorie tijdens een hele eeuw nog nooit in gebreke werd gesteld, niet volstaat om de lezer te overtuigen, zouden we ons dan niet kunnen voorstellen dat een onzichtbaar persoon de vertrouwelijke informatie op de computer van iemand anders kan doorzoeken? Voorlopig voorspelt de quantumtheorie nog niet dat dergelijke mogelijkheden of zelfs andere kwaadaardige demonen zouden kunnen bestaan. Met andere woorden: geloven in de realiteit die ons vandaag omringt is ook geloven in de voorspellingen van de quantumfysica.

De huidige technologische ontwikkelingen

Op basis van ditzelfde fundamentele principe hebben talrijke laboratoria op experimentele wijze protocollen voor quantumcryptografie kunnen realiseren. Via een optische kabel van het gewone telefoonnet kon vertrouwelijke quantuminformatie worden verzonden over een afstand van 20 kilometer, onder het Lemmanmeer. Zonder in detail te treden, kunnen we stellen dat het toestel voor het verzenden van de

informatie eerder gebruik maakte van optische interferometrie dan van lichtpolarisatie. Maar ook al werkte de apparatuur perfect, toch vertoonde ze nog enkele zwakke punten. Het eerste probleem is dat de transmissie wegens het signaalverlies in de optische vezel enkel mogelijk is over een relatief korte afstand. Daardoor is de mogelijke toepassing ervan voor quantumcommunicatie beperkt tot de grenzen van een grote stad. Dit probleem wordt in detail bestudeerd door de wetenschappers, maar is tot op vandaag nog niet helemaal opgelost. Het tweede nadeel bestaat erin dat de experimentele beheersing van de productie van impulsen op een foton, alsook de detectie ervan nog steeds niet perfect blijken. Een perfecte beheersing van de fotodynamica vanaf creatie tot detectie zou een aanzienlijk debiet van codeerbits mogelijk maken. Het onderzoek en de ontwikkelingen op dit vlak kennen duidelijk een permanente evolutie en zullen binnen een relatief korte termijn de commercialiseringsfase bereiken.

Op dit ogenblik worden diverse andere verbeteringen in de quantumcryptografie bestudeerd, onder andere aan de Universit  Libre de Bruxelles op de dienst Th orie de l'Information et des Communications (Informatie- en Communicatietheorie n). Er lopen momenteel verschillende onderzoeksprojecten in samenwerking met de dienst Optique et Acoustique (Optica en Akoestiek) en de dienst Physique Th orique (Theoretische Fysica) die tot doel hebben het debiet aan uitgewisselde codeerbits te verhogen of het bereik van het codeertoestel door het gebruik van hogere dan binaire alfabetten uit te breiden. Andere theoretische werken in samenwerking met andere Europese laboratoria concentreren zich op de mogelijkheid om intense lichtbundels (meerdere fotonen) te gebruiken waarbij de quantumkenmerken die de quantumcryptografie mogelijk maken, behouden blijven, en dit met als doel de technologische uitdagingen die gepaard gaan met het gebruik van  en enkel foton te omzeilen. Op die manier zouden bepaalde soorten toestanden van de lichtstraal, de zogenaamde "coherente" en "gecomprimeerde" toestanden, gebruikt kunnen worden.

De quantumcryptografie: een onderwerp dat diverse disciplines omvat

Zoals we kunnen vaststellen, omvat de quantumcryptografie een groot aantal disciplines. Men stelt er zich zowel abstracte vragen inzake wiskunde en fundamentele fysica, met betrekking tot de quantummechanica, alsook vragen waarbij men op zoek gaat naar de verhoogde prestaties van de gebruikte optische werkmiddelen (laser, detector, optische vezel), vragen die te maken hebben met de aanpassing van de resultaten aan industri le doeleinden, zonder dan nog te spreken van de ethische vragen die tegenwoordig overal ter wereld gesteld worden inzake vertrouwelijkheid. Kortom, de quantumcryptografie is een actueel onderwerp dat een erg brede waaier aan kennis dekt, gaande van fundamentele fysica tot industri le toepassingen. Het resultaat van dit onderzoek zou moeten leiden tot een verhoogde beveiliging van onze vertrouwelijke transmissies die steeds talrijker worden door de opkomst van e-commerce en de toenemende financi le transacties.

Wenst u meer te weten omtrent dit onderwerp?

Wenst u meer te weten omtrent dit onderwerp? Dan raden wij u de populair-wetenschappelijke artikels [1] en [2] aan, of het meer technische tijdschriftartikel [3].

Referenties

- [1] C.H. Bennett, G. Brassard, A.K. Ekert, Sc. Am. **267**, 50 (1992).
- [2] N. Cerf, N. Gisin, La Recherche **327**, 46 (2000).
- [3] N.Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
- [4] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press (1996).
- [5] J. Daemen, V. Rijmen, The block cipher Rijndael.
- [6] P.W. Shor, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, 124 (1994).