Kwantum Cryptografie

White paper

Auteurs editors : E. Karpov, T.Durt,
Bijdragen auteurs : F. Vanden Berghe, N. J. Cerf, T. D'Hondt

Informatie en communicatie zijn 2 begrippen die de basispeilers van onze moderne maatschappij vormen. Informatie heeft vaak een zodanig belangrijke waarde, dat men zich genoodzaakt voelt om ze te beschermen. Zo kan bijvoorbeeld een informatielek in de financiële sector voor kolossale verliezen zorgen. Ook de Belgische banken zijn niet gespaard gebleven voor aanvallen door cybercriminelen. De commissie voor het bank-, financie- en assurantiewezen (CBFA) registreerde dat enkele banken zoals Dexia, KBC en Argenta begin 2007 gehackt werden. Na een analyse binnen de sector, kan men spreken over een totaal van 51 of 52 geslaagde digitale inbraken in België. Het totale gestolen geldbedrag bedraagt hierdoor omtrent 800.000 Euro (dus een gemiddelde van 16.000 Euro per inbraak) [1]. In december 2008 heeft men vastgesteld dat er minstens een tiental rekeningen bij Dexia geplunderd zijn [2]. Voor wat betreft economische spionage, heeft het Amerikaanse afluister systeem ECHELON, sinds het jaar 2000 verscheidene malen gevoelige informatie, die uitgewisseld wordt tussen Europese bedrijven kunnen onderscheppen. Ook in deze tak van informatietechnologie kunnen dus veiligheid problemen aangetoond worden. Een nieuwe studie van het softwarebedrijf McAfee, dat gespecialiseerd is in anti-virus programma's, heeft aangetoond dat in het voorbije jaar de verliezen te wijten aan cyber criminaliteit oplopen tot 1 biljoen dollar. Deze schatting omvat voornamelijk de verliezen in termen van intellectuele eigendom, diefstal van gegevens en de nodige uitgaven om de opgelopen schade door virussen en andere kwaadwillige aanvallen te herstellen [3]. Bovendien beperkt informatiecriminaliteit zich niet tot banken of grote bedrijven. Vertrouwelijk informatie van particulieren zoals medische gegevens zijn ook onderhevig aan cyberaanvallen.

De oorzaak van veiligheidsfouten op het gebied van elektronische informatie zijn bijgevolg divers en de eindgebruiker is altijd de dupe van kwetsbare informatiesystemen die het gevolg zijn van virussen of andere spy-ware. Aan de andere kant zijn de manieren om zich hiertegen te beschermen ook sterk geëvoleerd. Om het lokale computersysteem goed te beveiligen moet de gebruiker een goed up-to-date anti-virus programma gebruiken en nagaan of de firewall aanstaat een goed werkt. Desalniettemin functioneren vele informatica toepassingen over een gedistribueerd netwerk (internet) waarbij uitwisseling van gegevens een centrale rol speelt. Hierbij is afluisteren op de communicatielijnen één van de belangrijkste bedreigingen voor het uitwisselen van vertrouwelijke gegevens. Zo is het bijvoorbeeld helemaal niet zo moeilijk om een klassieke communicatielijn (koperdraad) af te luisteren, een simpele antenne volstaat hiervoor. Zelfs communicatie via optische vezelkanalen zijn kwetsbaar voor spionage: Er bestaan namelijk goedkope toestellen, die vrij verkrijgbaar zijn, waarmee men op een efficiënte manier informatie kan onderscheppen die over optische vezelkanalen werd verstuurd. De eindgebruikers van deze communicatiekanalen kunnen zich op geen enkele manier tegen dergelijke spionage aanvallen beschermen. De enige

oplossing hiervoor is het beschermen van de informatie die over dergelijke kanalen wordt gestuurd. Dit probleem is analoog aan het uitwisselen van boodschappen bij het leger wanneer men in vijandelijk gebied verkeert. De informatie wordt binnenin de legerbasis goed beschermd maar wanneer een eenheid de basis verlaat om de informatie over te brengen, is deze kwetsbaar voor aanvallen. Dit leidt tot een bescherming van de boodschap tijdens het transport door bijvoorbeeld geblindeerde voertuigen.

Het probleem van betrouwbaarheid van informatie werd reeds lang geleden opgelost. De oplossing bestaat erin de informatie te versleutelen of te coderen. Een vercijferd bericht is onleesbaar voor de buitenwereld (zoals een kluis die op slot is). Om in dezelfde analogie verder te gaan, kan men dan het bericht ontcijferen op voorwaarde dat men de juiste sleutel heeft. De betrouwbaarheid van de verzonden informatie hangt dan af van enerzijds de kwaliteit van cijfer (de kwaliteit van de kluis) en anderzijds van de kwaliteit van de sleutel (de kwaliteit van het slot op de kluis, m.a.w. de moeilijkheid naar het raden van de 'tanding' van de sleutel.). De voortdurende 'oorlog' tussen de makers en krakers van codes kent een lange geschiedenis. Zo is de ontcijfering van de Duitse booschappen (Enigma) door Britse en Poolse cryptologen tijdens de tweede wereld oorlog één van de bekendste voorbeelden hiervan.

In 1936 heeft Gilbert Vernam het concept van de perfecte versleuteling gepatenteerd. Claude Shannon, de grondlegger van de informatietheorie, heeft later, in 1945, kunnen bewijzen dat de veiligheid van de Vernam codering absoluut is. Om deze code te gebruiken, moeten de twee partijen dezelfde sleutel hebben (een reeks van random bits) alvorens een geheime boodschap te verzenden of te ontvangen. Hierbij moet de lengte van de sleutel even lang zijn als de lengte van de boodschap. (Meer technische details hierover staan beschreven in appendix II). Om deze optimale betrouwbaarheid te kunnen blijven garanderen mag men weliswaar de sleutel voor het (de)coderen van de Vernam boodschap niet meer dan één keer gebruiken. Daarom wordt deze methode in het engels ook een 'One-Time Pad' genoemd. Dit heeft tot gevolg dat de partijen die vertrouwelijk informatie uitwisselen een hoeveelheid sleutels nodig hebben die gelijk is aan de hoeveelheid informatie die gecommuniceerd wil worden. De Vernam codering heeft dus het probleem van versleutelingen verlegd naar het probleem van geheime sleutelverdeling tussen twee partijen (key distribution).

Het probleem van key distribution bestaat uit twee delen:

1. het genereren van een sleutel door één van de twee partijen
2. de verzending van de sleutel naar de andere partij

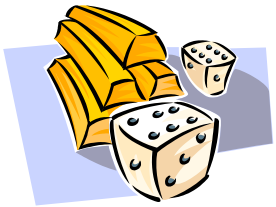
Voor de aanmaak van een sleutel heeft men een grote reeks random getallen nodig en bijgevolg dus een bron van entropie. Het is belangrijk dat deze getallen zo willekeurig mogelijk zijn en dus zonder verband.

Voor de verdeling van de sleutel heeft men daarenboven nog veilige communicatiekanalen nodig.

Indien slechts één van deze voorwaarden niet voldaan is, dan kan een spion (1) proberen de procedure te achterhalen voor het aanmaken van de sleutel of (2) proberen de sleutel te onderscheppen tijdens zijn distributieproces.

In wat nu volgt, tonen we aan dat de kwantum fysica een originele oplossing biedt voor de twee bovenstaande mogelijke spionageaanvallen.

1. het creëren van random getallen is een zeer oud probleem. De meest gekende toepassingen van dit probleem bevinden zich o.a bij de gokspelen: dobbelstenen, kaarten en de roulette kunnen hier gebruikt worden als random getal generatoren. Niettemin is het random karakter van deze toepassingen gebaseerd op de chaotische eigenschappen van hun dynamica. Dit type chaos blijft intrinsiek deterministisch omdat deze onderhevig zijn aan de deterministische bewegingen van de klassieke fysica. Bijgevolg hebben de gegenereerde getallen in principe niet de eigenschap van onvoorspelbaarheid hetgeen kan leiden tot het compromitteren van de codering. Hetzelfde deterministische karakter is o.a. ook aanwezig in de wiskundige algoritmes die random getallen genereren. Om deze reden worden ze dan ook pseudo-random getal generatoren genoemd. In tegenstelling tot de hierboven beschreven systemen wordt de kwantum mechanica geregeerd door intrinsieke probabilistische wetten. Deze geven ons de mogelijkheid om op een 'natuurlijke' manier random getallen te generen. Het probleem van de creatie van kryptografische sleutels is hiermee al opgelost. Er bestaan namelijk al een aantal commerciële kwantum random getal generatoren zoals QRNG of OEM. Het is dan ook niet toevallig dat bij de eerste klanten van deze apparatuur zich leveranciers van digitale gokspelen bevinden.



2. Nu we over een kryptografische sleutel beschikken, moet deze nog in alle veiligheid over het netwerk kunnen verdeeld worden naar de verschillende gebruikers. Dit probleem lijkt niet zo moeilijk. Beide partijen (Alice en Bob) kunnen elkaar gewoon ontmoeten de sleutel uitwisselen tot wanneer deze zal gebruikt worden om vertrouwelijke boodschappen te communiceren. Overheden (de fameuze rode telefoon tussen Washington en Moskou tijdens de koude oorlog), geheim agenten en revolutionairen (Che Guevara) hebben deze methode reeds in het verleden gebruikt. Maar een dergelijke methode is niet helemaal betrouwbaar. Denk maar aan omkoping, marteling of doding van de boodschappers van de sleutel. Daarenboven moet dit procedé vaak herhaald worden hetgeen niet altijd mogelijk is. Het is trouwens om deze reden dat KGB agenten verschillende malen dezelfde sleutel gebruikt hebben en waardoor CIA agenten occasioneel berichten hebben kunnen ontcijferen van Sovjet diplomaten.

Tot de jaren '80 was de enige manier om kryptografische sleutels te verdelen (buiten de fysieke manier) mogelijk door gebruik te maken van algoritmes waarvan de veiligheid gebaseerd was op de computationele complexiteit ervan. De ontbinding van een getal in twee priemfactoren is hier een gekend voorbeeld van. Een sleutel maken bestaand uit het product van

twee grote priemgetallen is zeer snel en eenvoudig maar de twee priemfactoren terugvinden op basis van deze sleutel alleen vraagt zeer veel rekenwerk. De enige manier is dit getal delen door steeds grotere priemgetallen tot de rest van de deling nul is en bijgevolg de code gekraakt is. De rekencomplexiteit van deze methode groeit exponentieel met de lengte van de sleutel en bijgevolg is de enige veiligheid dat deze manier garandeert, de onaanvaardbare rekentijd dat het neemt om met de huidige supercomputers deze ontbinding in twee priemfactoren te doen.

Kryptografische sleutels die op deze manier gegenereerd worden zijn dus aanvaardbaar maar niet onconditioneel betrouwbaar. Dit wil zeggen dat er geen garantie is dat iemand slim genoeg is om een algoritme te ontwikkelen of te hebben ontwikkeld om dergelijk probleem snel op te lossen. Bovendien, met de steeds maar stijgende rekencapaciteit van computers, komt de oude standaard van 'onaanvaardbare rekentijd dus veiligheid' in het gedrang. De oude kryptografische DES standaard is bijvoorbeeld al vervangen geworden door een nieuwe 3DES standaard. Daarenboven zou de kwantum computer wel eens voor de oplossing van het complexiteitsprobleem, waarop encryptie tegenwoordig gebaseerd is, kunnen zorgen.

Recente ontwikkelingen in het domein van kwantum informatie – het onderzoeksdomein dat informatie theorie en kwantum fysica combineert – hebben aangetoond dat er een kwantumsleutelverdelingsprotocol gemaakt kan worden waarbij de veiligheid onconditioneel kan gewaarborgd worden. De betrouwbaarheid van dit protocol baseert zich niet meer op computationele complexiteit maar op fysische onmogelijkheden. De Zwitserse fysicus Nicolas Gisin (Universiteit van Geneve) heeft hiervoor een visuele uitleg gecreëerd gebruik makend van zeepbellen en tennisballen [4]. Als de cijfers van de sleutel geschreven worden op tennisballen is het in principe mogelijk om ze te vangen de sleutel te lezen en ze verder te gooien naar de ontvanger. In dit geval weten de eindgebruikers niet of de veiligheid van de sleutel gecompromitteerd is of niet. Maar indien men de sleutel schrijft op zeepbellen, dan zal men ze doen uiteenspatten bij het opvangen, waardoor ze niet meer door een spion kunnen doodgegooid worden naar de ontvanger. De fragiliteit van kwantum toestanden (zeepbellen) en de onmogelijkheid om ze te kopiëren, garandeert de onvoorwaardelijke veiligheid van kwantumsleutelverdelingsprotocollen. Deze beperkingen worden opgelegd door de fysica en kunnen dus bijgevolg niet omzeild worden (bijvoorbeeld het onzekerheidsprincipe van Heisenberg). Dit bewijst dat de veiligheid van kwantumcryptografie niet afhangt van het kunnen van de spion maar enkel van de wetten van de kwantummechanica.

De theoretische beschrijving van het eerste kwantumsleutelverdelingsprotocol werd reeds gepubliceerd in 1984 en voor het eerste succesvolle experiment van dit principe moeten we teruggaan naar 1992 (de afstand van de sleuteltransmissie was toen 30 cm). Sedertdien werden verschillende kwantumsleutelverdelingssystemen gecommercialiseerd en is kwantumcryptografie uitgegroeid tot het uithangbord van de kwantum informatie. Ze bestaat uit een nieuwe discipline waarin onderzoekers, academici en grote ICT bedrijven de

handen in elkaar slaan. Wanneer we het over kwantumsleutelverdeling hebben zullen we voortaan de Engelse afkorting QKD (Quantum Key Distribution) gebruiken, omdat dit met de jaren de wereldwijde term is geworden.

De Europese gemeenschap heeft kwantumcryptografie erkent als één van haar prioriteiten. Doormiddel van een groot Europees project werd een QKD netwerk, gebruik makend van optische vezel, opgesteld in het centrum van de stad Wenen. De vocale communicatie tussen de verschillende 'knopen' van het netwerk werd beveiligd gebruik makend van geheime sleutels die verdeeld werden vanuit 5 verschillende platformen, elk ontwikkeld door de medewerkers van het project SECOQC. Dit evenement heeft aangetoond dat de verschillende platformen goed met elkaar kunnen geïntegreerd worden en dat de QKD tussen de verschillende platformen coherent kan gebruikt worden. Het moet gezegd worden dat de eerste demonstraties van dergelijke experimenten reeds gedaan werden in Singapore, Japan en de Verenigde Staten maar het is Europa dat voor het eerst QKD gecodeerde transmissies heeft kunnen doen in een netwerk met verschillende knooppunten, elk gekoppeld aan een verschillend systeem. Deze systemen werden ontwikkeld met de hulp van o.a Hewlett Packard, Siemens, Thales en Toshiba. Merk op dat deze systemen echt werken en verkocht worden, men heeft dus geen fysicus nodig om ermee te werken (P.Grangier [5]).

Het Europese succes achterwege gelaten, bewijst de kwantum cryptografie ook zijn nut op locale schaal, waar ze gesteund wordt door regionale financiële instellingen. Ook moet vermeld worden dat voor de transfer van de Zwitserse verkiezingsuitslagen van het canton Geneve er gebruik is gemaakt van kwantum cryptografie voor de beveiliging van de resultaten. Ook in Duitsland, heeft het overheidsagentschap dat instaat voor de communicatieveiligheid (BSI), kwantum cryptografie vermeld in haar rapport van 2006 als een groeiende en veelbelovende technologie. Dit agentschap financiert momenteel een piloot project voor de ontwikkeling van een kwantum transmissielijn. In Frankrijk financiert Thales een onderzoeksproject met het oog op een demonstratie van haar kwantum cryptografie platform in het kader van het Europese project SECOQ en in samenwerking met l'Institut Optique de Palaiseau. Ook het "Centre of Quantum Information and Communication" van de ULB neemt deel aan dit project. Dit onderzoekscentrum lanceerde trouwens in 2007 een project in het kader van programma "Prospective Research for Brussel". Het doel van dit project is het bestuderen van beveiligde communicatienoden in de Brusselse regio en het vinden van mogelijke toepassingsgebieden (niches) voor kwantumcryptografie.

Het principe van QKD

Vernam codering beschermt vertrouwelijke berichten tijdens de transfer over communicatiekanalen, maar heeft een sleutel nodig om gedecodeerd te worden. Deze sleutels worden verkregen via QKD waarbij de zekerheid gegarandeerd wordt door de kwantumfysica.

Elke QKD protocol bevat een deel dat de sleutel verzendt en een deel dat het kwantumsignaal meet en deze resultaten op een klassieke manier verwerkt. Daarom bevat een QKD systeem altijd een optische lijn waar het

kwantumsignaal over gestuurd wordt (bv door de lucht, door glasvezel) en een klassieke lijn voor authenticiteit van het signaal na te gaan.

Tijdens het kwantumgedeelte van het protocol, verzendt de ene partij een kwantumsignaal waarna de ontvangende partij een meting of een verandering hierop uitvoert. In het laatste geval wordt het signaal dan teruggestuurd naar de oorspronkelijke verzender die vervolgens een meting hierop uitvoert.

Het is in deze kwantum stap van het protocol waar bepaalde fysische onmogelijkheden optreden dat de cruciale veiligheid zit van QKD. Zo weten we door het onzekerheidsprincipe van Heisenberg dat het onmogelijk is om nauwkeurig bepaalde fysische eigenschappen simultaan te meten. Bijvoorbeeld de positie en de snelheid van een deeltje of de intensiteit en de phase van licht. Dit leidt tot de onmogelijkheid om ongekende kwantumtoestanden te kopiëren zonder ze onherroepelijk te veranderen. Afluisteren op een kwantumkanaal vertaalt zich dus in fouten tijdens de communicatie over dat kanaal. Bij het nakijken van deze fouten tijdens het klassieke gedeelte van het protocol kunnen beide partijen de aanwezigheid van een spion waarnemen.

Na een uitwisseling van een kwantum signaal is er nog een klassieke uitwisseling van boodschappen nodig voor de volgende redenen:

- detectie van een afluisteraar op het kanaal
- fouten corrigeren (error correction)
- de distillatie van de uiteindelijke sleutel d.m.v. hash functies (privacy amplification)

Ondanks de uitwisseling van deze boodschappen over een klassiek kanaal, komt de veiligheid van de sleutel niet in het gedrang omdat bij elke “klassieke” stap, de hoeveelheid onthulde informatie gecontroleerd en de laatste fase van het proces fameus gereduceerd wordt.

De sleutelverdeling is eigenlijk een uitbreiding op een initieel kortere voorverdeelde sleutel die nodig is voor the authenticiteit van het kanaal te bepalen. Tijdens het verloop van het protocol wordt namelijk een deel van de gegenereerde sleutel gebruikt voor de authenticiteit van het publieke kanaal na te gaan waarna op het einde van de sessie een korte sleutel wordt bijgehouden voor het begin van de volgende sessie.

Een meer gedetailleerde uitleg is te vinden in appendix II.

De benodigde infrastructuur voor de werking van QKD

De meeste QKD systemen zijn voorzien om te werken met standaard telecom optische vezel netwerken van 1550 nm. Een nieuwe kabelvoorziening is bijgevolg niet nodig. De enige vereiste is dat de optische lijn tussen twee communicatiepunten voorzien van een QKD apparaat continu is, dus zonder tussenstations of signaalversterkers. Beiden spelen hierbij een rol van spion.

Door middel van multiplexing is het dus mogelijk dezelfde lijn te gebruiken voor zowel kwantumsignalen als publieke berichten. Maar voor de kwaliteitsgarantie is het aangeraden om het optisch kanaal voor kwantumsignalen apart te houden.

QKD karakteristieken

Onderzoekers in het domein van kwantumcryptografie beschouwen QKD als het enige sleutelverdelingsprotocol waarbij de geheime coderingsleutel gegarandeerd veilig is.

- Het is het enige systeem dat met 100% garandeert dat een afluisteraar ontmaskerd zal worden.
- De veiligheid van de kwantumsleutel is absoluut en dus onconditioneel. De veiligheid hangt niet meer af van algoritmes of spionage technologie.
- Bijgevolg is deze vorm van veiligheid ook oneindig omdat ze door geen enkel systeem in de toekomst zal kunnen in het gedrang komen. (Fysische wetten zullen altijd blijven gelden.) Dit is daarentegen niet het geval voor de huidige klassieke cryptografie waarbij de rekencapaciteit van de computers met de jaren toeneemt en bijgevolg de kans op het kraken van de sleutel meer en meer doet vergroten. Een mooi voorbeeld hiervan is de ontcijfering van geheime Belgische overheidsdocumenten over de moord op Lumumba in januari 1961.

Langs de andere kant hebben de recente ontwikkelingen in deze technologie nog enkele beperkingen:

- De maximale afstand tussen 2 gebruikers is gelimiteerd tussen de 25 en 100 km afhankelijk van het systeem.
- De bandbreedte voor de finale sleutel is slechts 1-2 Mbit/sec. Deze beperking kan verlegd worden door klassieke key distribution oplossingen toegepast op QKD [6].

QKD biedt maar een oplossing voor één probleem van sleutelverdeling. Ze zijn dus maar deel van de gehele oplossing voor de informaticaveiligheid.

De voornaamste toepassingsdomeinen van QKD

- Overheids- of militaire instellingen
- Banken en financiële instellingen: interbancaire transfers, interbancaire communicatie, ...
- Cruciale infrastructuren zoals transport (luchthavens, treinstations), energiedistributiebedrijven.
- Telecom operatoren
- Etc.

Ook particuliere eindgebruikers kunnen hierbij baat hebben indien ze over een optische vezellijn beschikken.

Waarom is cryptografie en specifiek kwantumcryptografie noodzakelijk

Om op deze vraag te kunnen antwoorden moeten we de huidige stand van zaken op gebied van elektronische veiligheid, de waarde van de informatie en veiligheidcriteria beschouwen.

Financiële of informationele verliezen door industriële spionage tonen aan dat gegevens moeten beschermd worden. Men mag niet vergeten dan individuele informatie van kritiek belang kan worden indien als ze minutieus gecorreleerd zou worden. Cryptografie is bijgevolg onontbeerlijk.

De veiligheidsniveaus van codering hangen niet alleen sterk af van de waarde van de informatie maar ook van de mogelijkheden om de codering te kraken. De rekensnelheid van computers stijgt meer en meer, en er is geen bewijs dat cryptografische algoritmes veilig zijn. De oplossingen die de klassieke cryptografie biedt, mogen beschouwd worden als potentieel onveilig naar de toekomst toe.

Kwantumcryptografie biedt een oplossing die in principe niet afhangt van de technologische middelen van de spion. Ze biedt dus een definitieve oplossing voor de toekomstige veiligheidscriteria.

Kwantumcryptografie is de enige die een oneindige veiligheidsoplossing biedt.

Antwoorden op andere vragen kan men terugvinden in appendix I.

Overige toepassingen van kwantumcryptografie

Onder de toekomstige toepassingen moet men mobiele sleutelverdelers beschouwen. Een voorbeeld hiervan is de terminals van het type ATM die ontwikkeld werden door onderzoekers van HP [7].

Deze biedt oplossingen om als gewone gebruiker op geregelde tijdstippen een reserve aan te leggen van geheime sleutels die hij of zij dan voor andere toepassingen kan gebruiken zoals authenticiteitprotocollen om de PIN code te beschermen tijdens betalingen over het internet.

Met behulp van kwantumfysica kan men proberen oplossingen te vinden voor andere cryptografische primitieven zoals persoonsidentificatie tijdens een communicatieverbinding of de authenticiteit van berichten dat men krijgt. Oplossingen voor deze problemen liggen binnen de doelstellingen van het CRYPTASC project dat gefinancierd wordt door het Brussels Hoofdstedelijk Gewest.

QKD potentieel binnen het Brussels Hoofdstedelijk Gewest

1. Alle voornaamste domeinen waar QKD van nut kan zijn, zijn aanwezig.

   Het Brussels Hoofdstedelijk Gewest:
   - Is een politiek centrum, van lokaal tot internationaal vlak:
     - Internationaal:
       - Het parlement van de Europese Commissie
       - De missies van de landen t.o.v de Europese Commissie
       - Het hoofdkwartier van de NAVO
       - De ambassades
     - Nationaal:
       - Het parlement van de Belgische federale overheid
     - Regionaal:
       - De parlementen en regionale overheden
     - Lokaal:
       - De gemeenten
   - Is een belangrijk bank- en financieel centrum:
     - Meer dan 100 actieve banken die actief zijn in alle financiële sectoren. Onder hen een veertig tal buitenlandse banken die actief zijn op Europees vlak.
     - Belangrijke financiële instellingen zoals Euroclear en Bank of New York zijn bovendien ook gelegen in Brussel
   - Is een wereldwijde leider op het gebied van ICT en informatica infrastructuren
     - Elektronische identiteitskaarten
     - Innoverende elektronische betalingsmethoden zoals Bankcontact/Mistercash en PROTON
     - Regionaal telecommunicatienetwerk IRISnet waarvan het beleid in handen is van het CIRB (Centre Informatique de la Région Bruxelloise) die onder andere meerdere e-government projecten leiden (http://www.eid.irisnet.be/)
     - Het ISABEL (www.isabel.be) netwerk die van Brussel, bij de lancering van ebanking en e-business, een wereldwijde leider maakt.
   - Verdeler van verschillende elektronische gadgets die betrekking hebben op gsm, PDA, etc.
     - Massieve aanwezigheid van een groot aantal telecom- en alternatieve operatoren
     - Lancering van WiFi projecten via de CIRB
     - Privé WiFi initiatieven zoals Ozone (http://www.ozone.net)

2. Afstanden vormen geen probleem

   In de Brusselse regio, met haar 161,4 km^2 [8], zijn de maximale afstanden niet meer dan 30 km. Deze afstanden vallen zonder enig probleem binnen de maximaal toegelaten afstanden voor QKD op dit moment. Er is dus geen probleem voor LAN (Local Area Network) en MAN (Metropolitan Area Network) netwerken te gebruiken binnen deze regio.

3. Er is reeds de aanwezigheid van een optische vezelnetwerk

   Het CIRB heeft in het verleden reeds een volledig netwerk van optische vezels aangelegd die kunnen gebruikt worden door publieke of privé

gebruikers (Public Private Partnership). Deze lijnen zijn klaar om gebruikt te worden voor QKD.

4. Diensten en toepassingen die nood hebben aan veiligheidsoplossingen

- Diensten van het type LAN (Local Area Network), VPN (Virtual Private Network), RAS (Remote Access Service) voorgesteld door het CIRB.

  Voor website in uit elkaar gelegen LANs en segmenten van VPNs is encryptie noodzakelijk omdat deze linken over communicatielijnen gebeuren die onderhevig kunnen zijn aan fysieke aanvallen. VPN linken gaan trouwens over het internet dat beschikbaar is voor iedereen.

- Publieke Toepassingen (CIRB):

  e-Health: - Elektronische medisch dossier: elektronische uitwisseling van medische gegevens tussen verschillende artsen en specialisten die privé informatie bevatten over de patient is in aanmaak zoals in het programma van telemammografie.

  - Bijvoorbeeld het Rabat project waarbij toegang verleend wordt aan bevoegde personen is beveiligd met een paswoord maar het verlenen van die bevoegdheid wordt gedaan over het internet waarbij deze informatie moet beveiligd worden.

  e-Government: - Irisbox dat voor doel heeft het verzenden van elektronische formulieren is een toepassing die zal dienen voor uitwisseling van alle documenten en diensten (en die een digitale handtekening toelaat) tussen de verschillend gemeentelijke administratiediensten.

  - Het federale project FEDPKI ontwikkeld momenteel een systeem voor uitwisseling van elektronische gegevens tussen verschillende publieke federale overheidsdiensten die ontwikkeld werden door het project FEDMAN.

  - ISABEL is tevens ook een oplossing voor het elektronisch indienen van de BTW aangifte en de aangiftes bij Douane en Accijnzen.

  - In de nabije toekomst is het mogelijk om toepassingen van het type e-voting te implementeren gebruik makend van QKD. Zwitserland gebruikte reeds dit systeem om de vertrouwelijkheid te garanderen bij de transfer van de stemresultaten van het Canton Geneve.

- Prive Toepassingen:

  e-Banking: In 2008 heeft België de eerste plaats gekregen in een Europees klassement die de kwaliteit van e-banking is nagegaan in zeven Europese landen. België kreegt hierin een quotering van 87,38/100 [9].

Het Belgische systeem Banksys heeft voor haar toepassingen een wereldwijde erkenning gekregen. Banksys werd overgenomen door Atos Origin, één van de eerste bedrijven in internationale informatica diensten. Via haar filiaal Atos Worldline, fusioneerd Banksys met BCC, het bedrijf voor heel België de betalingen per creditcard beheert. Samen gaan ze onder de naam Atos Worldline, hetgeen symbool staat voor hun nieuwe ambities.

5. Random getal generatoren

Volgens onderzoekers van de VUB en de ULB is dit één van de meest veelbelovende korte termijn toepassingen binnen de kwantumcryptografie binnen de Brusselse regio. Langs de ene kant is reeds alle wetenschappelijk know-how in Brussel aanwezig voor de productie van dergelijk toestel. Langs de andere kant bestaat de nood aan random getallen reeds geruime tijd op het gebied van communicatieveiligheid en gokspelen (zowel elektronisch als in casino's). In Brussel alleen bezorgen de taxen van casino's een niet te verwaarlozen budget van de regio. Een project met als doel een spin-off te creëren voor de commercialization van kwantum random getalgeneratoren wordt reeds gefinancierd door het onderzoeksdepartement van Brussel.

Tot slot kunnen we nog zeggen dat de steeds meer opduikende kwantumtechnologie een kans vormt om onze huidige communicatie beveiligingsmethoden te versterken. Brussel bevat een groot potentieel voor de ontwikkeling en marketing van deze technologie.

Referenties

[1] P. Gérard, F. Dlpirre, Pas si sûre, la banque en ligne, Le Soir, 07/10/2007, 20:04, http://www.lesoir.be/actualite/economie/pas-si-sure-la-banque-en-2007-10-07-553788.shtml

[2] Rédaction en ligne, Des pirates informatiques contre Dexia, Le Soir, 13/12/2008, 23:15, http://www.lesoir.be/la_vie_du_net/actunet/des-pirates-informatiques-2008-12-13-673609.shtml

[3] Elinor Mills , Cybercrime cost firms $1 trillion globally, McAfee study says, cent news, 28/01/2009 http://news.cnet.com/8301-1009_3-10152246-83.html

[4] D. Lapousserie, Première mondial en physique, Science et Avenir, Octobre 2008.

[5] D. Lapousserie, Les nouvelles prouesses de la physique, Science et Avenir, Décembre 2008, 5051.

[6] Cerberis, id Quantique http://www.idquantique.com/products/cerberis.htm

[7] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, J. G. Rarity, Low Cost and Compact Quantum Cryptography. New J. Phys. 8 No 10 (October 2006) 249.

[8] Chiffres clés pour la région de Bruxelles-Capitale, spf économie, pme, classes moyennes et énergie, Direction générale statistique et information économique, http://www.statbel.fgov.be/

[9] E-banking: la Belgique en tête d'un classement européen, Le Soir, Rédaction en ligne, 15 décembre 2008, 13:35 http://www.lesoir.be/la_vie_du_net/actunet/e-banking-la-belgique-en-tete-2008-12-15-674030.shtml

[10] SECOQC Business White Paper, http://www.secoqc.net/downloads/SECOQC_Business_Whitepaper_01b.pdf

[11] SECOQC White Paper http://www.secoqc.net/downloads/secoqc_crypto_wp.pdf