Cryptographie quantique

White paper

E. Karpov, T. Durt, F. Vanden Berge, N. J. Cerf, T. d'Hondt

L'information et les communications sont des piliers de nos sociétés modernes. L'information possède une valeur intrinsèque qui suscite bien des convoitises a tel point qu'il est souvent nécessaire de la protéger. Dans le secteur financier par exemple la fuite d information confidentielle peut occasionner des pertes colossales. Les banques Belges n'ont pas été épargnées par les attaques de cyber-criminels. Pour exemple, Dexia, KBC et Argenta ont été « hackées » en début d'année 2007. « La Commission bancaire, financière et des assurances (CBFA) a de son côté chiffre ce phénomène. Après avoir fait le tour des banques, la sentinelle du secteur parle d'un total de « 51 ou 52 cas de hacking réussis en Belgique ». Le montant total dérobé atteint 800.000 euros (soit en moyenne près de 16.000 euros par cas) » [1]. Plus récemment on a appris qu'au moins une dizaine de comptes avaient été vidés chez Dexia en décembre 2008 [2]. En ce qui concerne l'espionnage économique, l'exemple du système d'écoute américain ECHELON capable de surveiller toutes les télécommunications mondiales et soupçonné d'avoir intercepte dans les années 2000 des données sensibles échangées par des compagnies européennes, montre l'importance de ce problème. Selon une nouvelle étude de McAfee, la compagnie mondial spécialisée en logiciel antivirus, le vol de donnais dues aux cyber-criminels peuvent coûter au business globalement 1 trillion de dollars de pertes de la propriété intellectuel et de dépenses pour réparer le dommage l'année passée [2]. L'escroquerie informatique ne touche pas seulement les banques ou les grosses compagnies. Des informations confidentielles relatives à l'état de sante de particuliers ou de patients du secteur hospitalier sont elles aussi susceptibles d'être compromises lors de cyber-attaques.

Les origines des failles en matière de sécurité informatiques sont diverses. L'utilisateur final est toujours un maillon faible étant donne la vulnérabilité des systèmes d'exploitation individuels face aux virus et autres programmes espions. Mais les moyens de défense se sont aussi développés. Pour peu que l'utilisateur soit prudent, que le programme « antivirus » soit à jour et que le « pare-feux » fonctionne, le système local est bien protégé. Même ainsi, les systèmes informatiques fonctionnent dans un environnement distribué (Internet) dans lequel l'échange de données joue un rôle essentiel, de sorte que l'écoute des lignes de communications constitue une menace potentielle extrêmement sérieuse pour la confidentialité des données échangées. Il est par exemple facile d'écouter des lignes de communications qui passent par des câbles en cuivre (une antenne suffit). Même les communications par fibre optique sont vulnérables : l'on peut assembler à partir de composants bon marche en vente libre un appareil d'écoute simple et efficace qui permet d'intercepter l'information transmise par fibre optique. Les utilisateurs des lignes de communications ne peuvent pas se protéger contre ce type d'attaques simplement en renforçant leurs « lignes de défense » locales ; ils doivent aussi protéger l'information envoyée. Ce problème est similaire a celui pose par la sécurité de troupes armées placées dans un environnement hostile. Elles sont relativement bien protégées à l'intérieur de leur base mais si une unité quitte sa base elle s'expose à de nouveaux types d'attaques ce qui nécessite des mesures de sécurité accrues (l'utilisation de véhicules blindés par exemple).

Le problème de la confidentialité de l'information a été résolu il y a déjà bien longtemps. La solution en est le cryptage ou chiffrage. Une fois chiffré le message est illisible, comme il le serait dans un « coffre blindé fermé à clé ». Pour poursuivre cette analogie, l'on peut alors déchiffrer le message a la seule condition de posséder la « clé » adéquate. Le niveau de sécurité de la transmission dépend tant de la qualité la qualité du chiffre (du « blindage du coffre ») que de la qualité de la clé (de la qualité de la « serrure », c'est-à-dire de l'impossibilité de deviner la configuration de son « dessin »). La guerre permanente entre les créateurs et les briseurs de codes a une longue histoire. Le déchiffrage des codes allemands (Enigma), par une équipe de cryptographes britanniques et polonais pendant la seconde guerre mondiale, en est un des exemples les plus connus, en particulier de par le rôle clé joue par les services de décryptage allies lors de la bataille de l' Atlantique.

En 1936, l'ingénieur Vernam a breveté la conception d'un chiffre « parfait ». En 1945, Claude Shannon, le créateur de la théorie de l'information, a pu prouver que la sécurité du code de Vernam était absolue ou « inconditionnelle ». Pour utiliser ce code (décrit en appendice ou l'on a regroupe des informations plus techniques et abstraites en rapport avec la cryptographie quantique), les deux

parties, doivent, afin d'envoyer des messages secrets, posséder la même « clé » secrète – une séquence de bits aléatoires (des chiffres zéro et un), dont la longueur de la séquence doit impérativement être égale à la longueur du message à communiquer. Malheureusement, l'indéchiffrabilité du code de Vernam est contrebalancée par le fait qu'il ne peut pas être utilisé plus d'une fois sans compromettre la sécurité (c'est la raison pourquoi il a été aussi appelé en Anglais « One-Time Pad »). Cela implique, que les parties en présence « consomment » une quantité de clé égale à la quantité d'information à communiquer. Vu sous cet angle on pourrait dire que le code de Vernam a transforme le problème du chiffrage en un problème d'établissement ou d'échange de clé secrète entre deux parties.

L'établissement d'une clé sécrète consiste en deux étapes:

- 1. génération de la clé par une des parties
- 2. distribution de la clé à l'autre partie

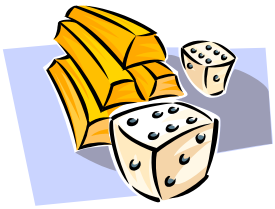
La génération de la clé requiert une série de nombres aléatoires, et donc des sources d'entropie – les générateurs de nombres aléatoires. Pour garantir que la clé soit secrète, ces nombres doivent être *purement aléatoires* (sans aucun biais) et *imprévisibles*.

La distribution de clé quant à elle requiert la présence de voies de communication sécurisées.

Si ces conditions ne sont pas satisfaites, l'espion peut (1) tenter de deviner la procédure de génération de la clé afin de la déduire de son cote ou encore (2) tenter d'intercepter la clé pendant sa distribution.

Comme nous allons le montrer maintenant, la physique quantique a permis d'apporter des parades originales à ces deux types d'attaque.

1. La génération de nombres aléatoires est un problème très ancien. Les « applications » les plus connues en sont les jeux de hasard : des dés, des cartes et une roulette peuvent utilisés comme générateurs de nombres aléatoires. Néanmoins, le caractère apparemment aléatoire de ce type de systèmes est dû aux propriétés chaotiques de leur dynamique. Ce type de chaos reste intrinsèquement déterministe, car il est régi par les lois du mouvement déterministes de la physique « classiques ». Par conséquent, les nombres générés n'ont pas de propriété d'être *imprévisibles*, ce qui peut, en principe, compromettre la sécurité du codage. Le même caractère déterministe est en outre partage par les algorithmes mathématiques qui génèrent les nombres aléatoires (ceux-ci sont appelés pour cette raison des générateurs « pseudo-aléatoires »). En opposition avec les systèmes précédemment décrits, les systèmes quantiques sont régis par les lois intrinsèquement probabilistes de la mécanique quantique, ce qui nous offre une possibilité de générer des nombres naturellement aléatoires. Pour conclure, le problème de génération de clé est résolu par la mécanique quantique. Il existe déjà différentes versions de générateurs de nombres aléatoires quantiques (QRNG) sur le marché : des cartes internes PCI ou des accessoires séparés de type USB ou OEM. Ce n'est pas un hasard si parmi les premiers clients de ces appareils on trouve les fournisseurs de jeux de hasard en ligne.



2. Maintenant que l'on dispose d'une clé, il nous faut encore la distribuer en toute confidentialité. Cela semble facile : les deux parties (les cryptographes les appellent Alice et Bob) peuvent se rencontrer, échanger la clé et garder chacun sa copie pour l'utiliser quand il sera nécessaire d'envoyer son message secret. Des gouvernements (le fameux téléphone rouge entre Moscou et Washington lors de la guerre froide), des agents secrets, des révolutionnaires (Che Guevara) ont utilisé cette méthode par le passé (l'image montre un « livre de codes » du KGB utilise dans les années 40). Mais une telle méthode n'est pas tout à fait sécurisée. Pour preuve le « livre » se trouve maintenant dans le musée de Londres. D'autre part, au cas ou il s'avérerait nécessaire d'envoyer plusieurs messages, Alice et Bob vont épuiser la clé tôt ou tard et, pour continuer la communication secrète, ils devront se rencontrer à nouveau, ce qui n'est pas toujours possible. (C'est pourquoi les agents du

KGB ont du utiliser la même clé plusieurs fois ce qui a diminue le niveau de confidentialité et permis occasionnellement à des agents de la CIA de décrypter, a l' époque, des messages cryptés par des diplomates soviétiques.)

Jusqu'aux années 80, un seul moyen de distribuer la clé secrète (à part « de la main à la main ») était d'utiliser des algorithmes dont la sécurité est basée sur la complexité computationnelle. Par exemple, si un nombre est le produit de deux grands nombres premiers a priori inconnus, il est difficile de trouver ces multiplicateurs à partir de ce nombre. En gros tout ce qu'on peut faire est de diviser ce nombre par des nombres premiers de plus en plus grands jusqu' à ce que le reste soit nul, auquel cas le code est brise. La complexité de ce problème s'accroît très vite (exponentiellement) avec la grandeur de ce nombre et donc, si on utilise un ordinateur pour résoudre ce problème directement par la méthode des « essais et erreurs », le temps de calcul croît lui aussi exponentiellement et on ne peut briser le code dans un temps raisonnable.

Les clés générées par tels algorithmes sont donc raisonnablement secrètes mais pas inconditionnellement secrètes. Cela signifie par exemple qu'il n'y a pas de garantie que quelqu'un ait trouvé un algorithme particulièrement astucieux qui permette de résoudre ce problème complexe relativement vite. En outre la performance toujours croissante des ordinateurs en vente sur le marche rend obsolètes des standards qui étaient considérés comme sécurisés par le passe. Le standard cryptographique DES a par exemple été remplacé par un standard plus complexe le 3DES. Enfin, l'ordinateur quantique pourrait, en principe, réduire la complexité de problèmes tels que la factorisation des grands nombres, ce qui à terme constitue une menace potentielle pour la confidentialité de tout échange crypte base sur ce type de standards.

Le développement récent d' une discipline nouvelle appelée Information Quantique, résultant du mariage heureux entre la théorie de l' Information et la physique quantique a permis de concevoir un protocole de distribution de clé dont la sécurité est *inconditionnelle* : la confidentialité ne se base plus sur les *complexités* computationnelles, mais sur des *impossibilités* imposées par les lois de la physique. Le physicien suisse Nicolas Gisin (université de Genève) a proposé une explication visuelle de la cryptographie quantique avec des bulles de savons et des balles de tennis [3]. Si les chiffres de la clé sont inscrits sur les balles de tennis il est possible en principe de les rattraper, de lire la clé et de la renvoyer au récepteur, ni vu ni connu. Dans ce cas les utilisateurs ignorent si oui ou non la clé a été compromise. Mais si les la clé est inscrite sur le bulles de savons, les rattraper signifie les détruire. Le problème pour l'espion est que s'il essaye de « ne pas toucher » la bulle il ne peut pas lire la clé correctement. La fragilité d'états quantiques (bulles de savon) et l'impossibilité de les copier garantit la sécurité inconditionnelle des protocoles de distribution de clé quantiques. En dernier ressort ces limites sont imposées par des lois physiques incontournables (le principe d'incertitude de Heisenberg entre autres), ce qui explique pourquoi la sécurité de la cryptographie quantique ne dépend pas de la puissance technique de l'espion (la partie tierce qui veut intercepter la communication).

La description théorique du premier protocole de distribution quantique de clé secrète a été publiée en 1984 et la première expérience montrant le fonctionnement du principe, remonte a 1992 (la distance de transmission était alors de …30 cm !). Depuis lors, plusieurs systèmes de distribution de clés sécrètes basées sur un échange des signaux quantique ont été commercialisés, et la cryptographie quantique est devenue le fer de lance de l'Information Quantique. Elle constitue une nouvelle discipline a part entière qui regroupe une large communauté de chercheurs issus des institutions académiques et des grandes compagnies du secteur ***TIC*** (Technologie de l'Information et de Communications). Pour designer la distribution quantique de clé secrète nous allons utiliser désormais l'abréviation anglaise ***QKD*** (Quantum Key Distribution) qui est devenue un terme international.

La communauté Européenne a reconnu la cryptographie quantique parmi ses priorités. Suite à un grand projet européen « intégré » un réseau « pilote » de communication QKD par fibre optique été implémenté dans des conditions réelles dans l'environnement métropolitain de la ville de Vienne. La communication vocale entre les nœuds du réseau a été sécurisé avec des clés sécrètes distribuées par cinq plateformes différentes, développées par les membres du projet européen SECOQ. Cet événement a permis de démontrer le bon fonctionnement de ces différentes plateformes et de leur intégration ainsi que l'utilisation cohérente de la « réserve » de clé sécrète distribuée par ces plateformes. Il faut dire que si des démonstrations de distributions de clé

« quantique » one été déjà réalisées a Singapour, au Japon et aux Etats-Unis, c'est l'Europe qui la première a coordonne par les techniques QKD la transmission cryptée dans un réseau de plusieurs nœuds reliés par des systèmes différents développés avec la participation, entre autres, de Hewlett Packard, Siemens, Thales et Toshiba. « Ces systèmes fonctionnent. Ils tiennent dans une boîte. Il n'y a même plus besoin d'avoir un physicien à côté. » (P. Grangier [4]).

Mis a part son succès au niveau européen, la recherche en cryptographie quantique est aussi présente au niveau local où elle trouve le support d'organismes financiers régionaux. Parmi ces exemples il faut mentionner l'utilisation de la cryptographie quantique pour sécuriser le transfert des résultats des votes du canton de Genève vers le centre de recueillement fédéral Suisse en 2007 et 2008. L'agence gouvernementale allemande en charge de la sécurité des communications, la BSI, a inclus la cryptographie quantique dans son rapport de 2006 comme une technologie émergente et prometteuse. Actuellement, la BSI finance un projet « pilote » d'implémentation d'une ligne de transmission quantique. En France, Thales finance un projet de recherche visant à une démonstration de sa plateforme de cryptographie quantique développée dans le cadre du projet européen SECOQC en collaboration avec l'Institut Optique de Palaiseau, antenne du CNRS. Une équipe de « Centre of Quantum Information and Communication » de l'ULB a aussi participé au développement de cette plateforme. Pour appliquer ses connaissances et son expérience à l'échelle régionale bruxelloise, l'équipe a lancé en 2007 un projet dans le cadre du programme « Prospective Research for Brussels ». L'objectif en était d'étudier les besoins en matière de communication sécurisée dans la région bruxelloise et de trouver des applications possibles (niches) à la technologie de la cryptographie quantique.

Le principe de fonctionnement de la technique d'échange de clé QKD

Le code de Vernam nécessite l'existence d'une clé (ou suite aléatoire de nombres) que seules les parties autorisées sont sensées connaitre. Les clés sont renouvelées par QKD qui, de manière imagée, les protège par ses « bulles de savon ».

Tous les protocoles QKD consistent en deux phases :

1. Dans un premier temps une des parties (traditionnellement dénommée Alice ou A) envoie a l'autre partie (traditionnellement dénommée Bob ou B) des signaux « quantiques » ou « bulles de savon » que celle-ci mesure.
2. Dans un second temps les deux parties se livrent a un traitement « classique » de résultats de mesure.

C'est pourquoi tous les systèmes QKD utilisent une ligne optique pour envoyer des signaux « quantiques » et une ligne de communications classique qui est publique (pas chiffrée) mais authentifiée (c'est-à-dire qu'il est impossible qu'une tierce partie malintentionnée, traditionnellement dénommée Eve ou E pour espion ou « eavesdropper », puisse se faire passer pour Alice ou Bob). La ligne optique peut être établie à l'air libre ou plus communément par le biais d'une fibre optique.

C'est pendant la première étape que les impossibilités quantiques jouent un rôle principal dans la sécurité de QKD. En vertu du principe d'incertitudes de Heisenberg, il n'est pas possible de mesurer simultanément avec une précision infinie certains paramètres physiques dits conjugués. Par exemple, la position et la vitesse d'une particule ou l'intensité et la phase de la lumière (qui est comme on le sait depuis Maxwell un champ électromagnétique oscillant). Cela implique une *impossibilité* de copier un état quantique inconnu sans le modifier. Si l'espion écoute le canal quantique il modifie nécessairement l'état transmis, ce qui se traduit par des erreurs de communication (des « bulles sont détruites »). En vérifiant ces erreurs à la prochaine étape (classique) du protocole, Alice et Bob peuvent détecter la présence de l'espion, voire ils peuvent chiffrer la quantité d'information maximale dont celui pourrait disposer.

Après la mesure des signaux quantique l'échange des messages classiques est donc nécessaire pour

- l'estimation du canal (détection éventuelle de la présence de l'espion)
- la réconciliation des données (une correction d'erreurs)
- la distillation de la clé finale par des fonctions de type « hash » (privacy amplification)

Une description de QKD plus détaillée se trouve dans l'annexe II.

Bien que l'échange de ces messages classiques soit fait sur une voie publique, au vu et au su de tous, la sécurité de la clé n'est pas compromise car à chaque étape « classique » la quantité de l'information révélée est contrôlée et à la dernière étape la clé est réduite proportionnellement.

Il est bon de noter que l'authentification des utilisateurs de la ligne requiert en elle même une courte clé (en tous points similaire a un code PIN). A la fin de la session une clé courte est donc conservée pour commencer la session suivante.

Vue sous cet angle, la distribution de clé est donc une *expansion* de clé initiale courte pré-distribuée.

L'infrastructure nécessaire pour le fonctionnement de QKD

La plupart des systèmes QKD sont adaptés à l'échange de données (quantiques et classiques) par le biais de fibres optique télécom standards de 1550 nm et donc aucune autre installation du câble n'est nécessaire s'il existe déjà une ligne de communication par fibre optique, a la seule condition-obligatoire-que la ligne optique entre Alice et Bob soit continue – sans répéteurs ni amplificateurs. Tous les deux pourraient, en effet, être détournes par l'espion.

Par multiplexage, il est possible d'utiliser la même ligne pour envoyer des signaux quantiques et des messages publics mais pour assurer la qualité des communications il est conseillé dans la pratique de prévoir une ligne optique séparée pour le lien quantique.

Les caractéristiques particulières de QKD

Les chercheurs qui travaillent dans le domaine de la cryptographie quantique considèrent le système QKD comme le seul système de distribution de clé secrète véritablement sécurisé.

- C'est le seul système qui garantie à 100% la détection de la présence d'espion.
- La sécurité de la clé quantique est absolue, dite « inconditionnelle » car elle ne dépend pas de la puissance des algorithmes ou de la technologie de l'espion.
- Par conséquent, elle est aussi « éternelle » car elle ne peut être compromise par aucun événement futur. Par contre, dans le cas du chiffrage basé sur la complexité algorithmique/ computationnelle, l'adversaire peut toujours garder le message chiffré en attendant l'apparition de nouvelles méthodes de crypto-analyse plus adaptées pour déchiffrer le message. Un exemple en est le décryptage récent de documents officiels belges cryptes qui a révélé le rôle crucial, voire déterminant du gouvernement Belge dans l'assassinat de LUMUMBA au Katanga le 17 janvier 1961. Comme Shannon l'a montre, en l'absence de la clé il n'y a pas et il n'aura aucun moyen de décrypter le message lorsqu' il est chiffre selon le « one-time pad ». L'avantage de la cryptographie quantique est qu'elle permet, grâce a l'usage de « bulles de savon » non copiables de garantir que nulle tierce partie ne connaît ni ne connaitra jamais la clé, car, pour revenir a la métaphore précédemment évoquée, si c'était le cas, les « bulles de savon » seraient irrémédiablement endommagées et Alice et Bob s'en rendraient compte a l' instant.

D'autre part, l'état actuel du développement de cette technologie présente des limitations :

- La distance maximale varie de 25 à 100 km selon le système.
- La bande passante de la clé « finale » est de l'ordre de 1-2 Mbit/sec. Cette limitation peut être contournée le cas échéant par une application de QKD comme une partie d'une solution de la distribution de la clé « classique » [5].

Enfin, il faut être conscient du fait que les systèmes QKD ne permettent de résoudre qu'un seul problème, a savoir celui de la distribution (rafraichissement) de la clé secrète, donc ils doivent être une partie d'un environnement global qui apporte une solution complète au problème de la sécurité informatique (de même qu'une carte de banque est inutile en l'absence de distributeur).

Les domaines principaux où QKD peut être utile :

- Les échanges d'information sensible entre entités gouvernementales ou militaires ;
- Les banques et les institutions financières : les transferts interbancaires, les communications Agence Bancaire – Distributeur automatique de type ATM, etc. ;
- Les communications cryptées entre membres des services de sécurité présents dans des infrastructures critiques comme les nœuds des réseaux de transport (les aéroports, les gares), les centrales de production et de distribution d'énergie, les pipelines ou gazoducs;
- Les opérateurs télécom;
- etc.

Les particuliers en tous genres peuvent, eux aussi, bénéficier de la sécurité quantique s'ils disposent d'une ligne de communication optique.

Pourquoi la cryptographie et particulièrement la cryptographie quantique sont elles nécessaires ?

Pour répondre à cette question il faut prendre en compte le niveau de sécurité offert par la technologie actuelle, la valeur de l'information à protéger et les critères de sécurité à respecter.

Sans protection des données on s'expose a de substantielles pertes financières et a des pertes d'informations « sensibles » (l'espionnage industriel en est une illustration). Il faut aussi tenir compte du fait que parfois des données qui ne sont pas considérés individuellement comme critiques pourraient devenir critiques si elles étaient corrélées minutieusement. La aussi la cryptographie, le chiffrage sont nécessaires.

Le niveau de la protection, le niveau de chiffrement, dépendent des critères de sécurité et ces critères évoluent en fonction pas seulement de la valeur des données à protéger mais aussi en fonction du niveau de risque, qui augmente avec l'évolution des possibilités d'espionnage. La puissance des ordinateurs augmente en permanence et, comme il n'y a pas de preuve théorique de la sécurité des algorithmes cryptographiques classiques, les données protégées par la cryptographie asymétrique (celle-ci englobe par exemple le chiffrage base sur la factorisation de grands nombres) peuvent être considérées (comme on l'a illustre avec l'exemple de l'affaire Lumumba) comme fragiles a long terme.

La cryptographie quantique propose une solution dont la sécurité ne dépend pas de la puissance technologique de l'espion. Elle permet donc de répondre au défi proposé par l'évolution des critères de sécurité et des techniques de décryptage. A ce jour, la cryptographie quantique est la seule qui propose une sécurité « éternelle ».

Les réponses à d'autres questions intéressantes se trouvent dans l'appendice I.

Les autres applications de la cryptographie quantique :

Parmi les applications futures il faut mentionner une distribution de clé pour les appareils mobiles avec les terminaux de type ATM développée par les chercheurs de Hewlett Packard [6].

Cette solution est conçue pour les applications ou le client peut « charger » régulièrement sa réserve de clé sécrète, réserve qu'il peut utiliser ultérieurement pour les protocoles d'authentification ou pour protéger son code PIN pendant les payements ou la consultation d'un compte *en ligne*.

Avec la physique quantique, on peut essayer de trouver des solutions pour les autres ‘’primitives’’ cryptographiques telles que l’identification des personnes en communication (les ‘’parties’’), l’authentification de messages envoyés et reçus, la protection de l’intégrité de messages etc. La résolution décès problèmes fait partie des objectifs du projet CRYPTASC financé par le département Recherche de la Région Bruxelles Capitale.

Potentiel des techniques QKD dans la Région Bruxelles Capitale.

1. Tous les domaines principaux où la technologie QKD peut-être utile sont largement présents.

   La Région Bruxelles Capitale :

   - Est un centre politique à tous les niveaux intermédiaires entre le niveau local et le niveau international :
     - International :
       - le Parlement et la Commission Européens,
       - les missions des pays auprès de la Commission Européenne,
       - le Quartier Général de l’OTAN,
       - les ambassades ;
     - National :
       - le Parlement et le gouvernement fédéral Belge,
     - Régional :
       - les parlements et les gouvernements régionaux (Bruxelles-Capitales, Flandre)
     - Local :
       - Communes ;
   - Est un important centre financier et bancaire :
     - plus de 100 banques à Bruxelles, actives dans tous les secteurs financiers ; parmi elles une bonne quarantaine de banques étrangères présentes et actives sur le marché de la capitale de l'Europe ;
     - d'importantes institutions financières, telles que Euroclear et Bank of New York, ont également installé leur quartier général à Bruxelles ;
   - Est l’un des leaders mondiaux dans le développement des applications TIC et des infrastructures informatiques
     - cartes d’identité électroniques ;
     - systèmes innovants de payement électronique Bancontact/Mistercash et PROTON ;
     - réseau régional de télécommunications IRISnet dont la gestion et le contrôle sont assurés par le Centre Informatique de la Région Bruxelloise (CIRB) qui mène plusieurs projets ‘’e-government’’ http://www.eid.irisnet.be/;
     - réseau ISABEL www.isabel.be, qui a fait de Bruxelles, lors de son lancement, un des leaders mondiaux en termes d'applications ‘’e-banking’’ et ‘’e-business’’ ;
   - Dispose de nombreux atouts dans le domaine des applications mobiles sur PDA, GSM etc.:
     - présence massive de grands opérateurs télécom et d'opérateurs alternatifs ;
     - lancement de projets WiFi via le CIRB ;
     - des initiatives privées WiFi, telles qu’Ozone, http://www.ozone.net .

2. Les distances ne posent pas problème.

   Dans la région de Bruxelles, avec une superficie de 161,4 km^2 [7] les distances maximales ne dépassent pas 30 km. Ces valeurs sont largement en deca des limites en distance dont patit la technologie QKD. Donc pour les LAN's (Local Area Network) et MAN's (Metropolitan Area Network) dans la région Bruxelloise les limites de QKD en distance ne sont aucunement contraignantes.

3. Le réseau des liens optiques est déjà très développé.

   Le Centre Informatique de la Région Bruxelloise (CIRB) possède un réseau de lignes optiques, qui sont proposées pour les utilisateurs publics comme pour les utilisateurs privé (Public Private Partnership). Ces lignes optiques sont prêtes à être utilisées pour distribuer la clé quantique.

4. Les services et applications qui ont besoin de solutions en matière de sécurité :

   - Services de type réseaux LAN (Local Area Network), VPN (Virtual Private Network), RAS (Remote Access Service) proposés par le CIRB.

     Pour lier les sites éloignés LAN ou les segments VPN, le cryptage (l'analogue des voitures blindées) est nécessaire car ces liens passent par des lignes de communications vulnérables aux attaques « physiques » et les segments VPN sont liés par le réseau internet ouvert à tous.

   - Les applications publiques (CIRB) :

     e-health: télématique médicale – l'échange électronique, entre des hôpitaux des médecins-traitants et des spécialistes, de données qui contiennent des informations privées couvertes par le sceau du *secret médicale* est en application par exemple dans le programme de télémammographie, ou encore dans le projet Rabat dont l'accès est accordé aux personnes autorisées et protégé par un mot de passe, mais l'envoi de données aux personnes autorisées est fait par l'internet dont la confidentialité doit être assurée.

     e-Government: IrisBox est une application destinée à l'envoi de formulaires électroniques, ainsi qu'au paiement éventuel en ligne et qui servira pour l'échange entre administrations communales de tous les documents/ services intégrant une signature électronique.

     Le projet fédéral FEDPKI vise à développer un système pour protéger les échanges électroniques de données (authentification, encryptage et signature électronique) dans le réseau à haut débit développé par le projet FEDMAN, qui relie les services publics fédéraux.

     L'application ISABEL permet aussi de soumettre par voie électronique sa déclaration à la TVA, au précompte professionnel et aux Douanes et Accises (NCTS).

     A court terme, il est possible d'envisager des applications de type *evoting* suite aux exemples d'utilisation de QKD pour sécuriser le transfert des résultats des votes dans le canton de Genève en Suisse en 2007 et 2008.

   - Les applications privées :

     e-banking: En 2008 la Belgique a obtenu la première place dans un classement européen mesurant la qualité de l'e-banking dans sept pays européens avec un indice global de satisfaction de 87,38 / 100 [8].

Pour ces applications la compagnie belge Banksys à été reconnue mondialement : reprises par Atos Origin, l'une des premières sociétés de services informatiques internationaux, via sa filiale Atos Worldline, Banksys fusionne en 2007 avec BCC qui gère les paiements par carte de crédit pour presque toutes les banques belges, et ensemble ils prennent le nom Atos Worldline, symbole de leurs nouvelles ambitions.

5. Générateurs de nombres aléatoires

   Selon l'avis des chercheurs de l'ULB et de la VUB ceux-ci constituent l'application de la cryptographie quantique la plus prometteuse et porteuse a court et moyen terme, de par son implémentation dans la région bruxelloise.

   D'une part, toutes les compétences scientifiques et le savoir faire pour la production existent à Bruxelles ou peuvent être trouvé en Belgique.

   D'autre part, il se fait déjà sentir un besoin de générateurs de nombres aléatoires dans le domaine de la sécurité des communications ainsi que dans le domaine des jeux de hasard en ligne et des installations de jeux dans les casinos. A Bruxelles, les taxes payées par les casinos apportent une quote-part substantielle au budget de la région. Un projet visant à créer une compagnie « spin-off » pour le développement d'un générateur quantique de nombres aléatoires est actuellement financé par le département de recherche régional.

En conclusion, la technologie émergente de la cryptographie quantique offre une opportunité unique de renforcer la sécurité de communications. Bruxelles possède un potentiel pour le développement de cette nouvelle technologie et pour proposer des solutions basées sur cette technologie sur le marché.

Appendice I

FAC's de « SECOQC Business White paper » [9] sauf la question « Pourquoi.. » qui a été répondue ci-dessus.

Appendice II

L'introduction « plus scientifique » a la cryptographie quantique de Thomas.

Références

[1] P. Gérard, F. Dlpirre, *Pas si sûre, la banque en ligne*, Le Soir, 07 octobre 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 décembre 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

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

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

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

[6] 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.

[7] *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/

[8] *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

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

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