Zeitschrift: bulletin.ch / Electrosuisse
Herausgeber: Electrosuisse
Band: 102 (2011)
Heft: 7

Artikel: Physique quantique et cryptographie
Autor: Ribordy, Grégoire / Trinkler, Patrick
DOI: https://doi.org/10.5169/seals-856830

Physique quantique et cryptographie

Production et distribution sécurisée de clés cryptographiques

Les réseaux de données jouent un rôle de plus en plus important dans notre société et il est important de protéger les communications qui y transitent au moyen de techniques de chiffrement. L'efficacité de ces dernières dépend bien entendu de la complexité de la clé utilisée, mais aussi de la sécurité de sa transmission. Or, la physique quantique peut être mise à profit non seulement pour produire des clés aléatoires, mais aussi pour les distribuer de façon sécurisée.

Grégoire Ribordy, Patrick Trinkler

L'essor des technologies de l'information a révolutionné l'organisation et le fonctionnement des entreprises en permettant la délocalisation de l'information. Cette dernière peut être traitée ou stockée dans différents sites de façon transparente. Cette évolution a été rendue possible par la mise en place de réseaux informatiques rapides et performants qui irriguent l'entreprise. Mal maîtrisée, cette évolution peut toutefois créer de nouveaux risques liés à la perte d'informations sensibles.

Rôle de la cryptographie

Heureusement, il existe des moyens permettant de garantir la confidentialité des informations véhiculées par ces réseaux informatiques. Les technologies de chiffrement consistent à combiner les informations sensibles avec une clé de chiffrement avant leur transmission pour les protéger. Un adversaire qui souhaiterait accéder à ces données chiffrées, mais ne connaîtrait pas la clé de chiffrement, n'aurait pas d'autre choix que d'essayer toutes les clés, une par une. Si la clé est suffisamment longue, le temps nécessaire pour réaliser une telle tâche devient si grand que l'on peut la considérer comme impossible. Le destinataire légitime de l'information, qui dispose d'une copie de la clé, peut déchiffrer les informations et les rendre à nouveau intelligibles. Comme la clé permet à la fois de chiffrer et déchiffrer les données, la sécurité de ces procédés repose entièrement sur la clé et sa protection durant tout son cycle de vie.

Générer des clés aléatoires

La première étape dans la gestion d'une clé de chiffrement est sa génération. Si l'on veut éviter de donner la possibilité à un adversaire de deviner cette clé, il est essentiel qu'elle soit constituée d'une séquence de bits aléatoires. Produire des nombres aléatoires n'est toutefois pas une tâche triviale. Les ordinateurs par exemple se comportent de façon déterministe et ne peuvent donc pas produire du hasard sans l'ajout d'une source physique d'entropie.

Contrairement à la physique classique, la physique quantique – la théorie physique qui décrit le monde microscopique et qui a été développée au cours des premières décennies du 20e siècle – est fondamentalement aléatoire. Elle prédit le résultat des mesures de façon probabiliste et il est donc logique de faire appel à un processus quantique comme source de hasard. On peut ainsi par exemple générer des nombres aléatoires en envoyant des grains de lumière – des photons – sur un miroir semi-réfléchissant. Ces photons seront réfléchis ou transmis avec une probabilité de 50 %. En associant une valeur de 0 ou de 1 à chacun de ces événements, une séquence de bits aléatoires d'origine quantique peut être engendrée (figure 1).

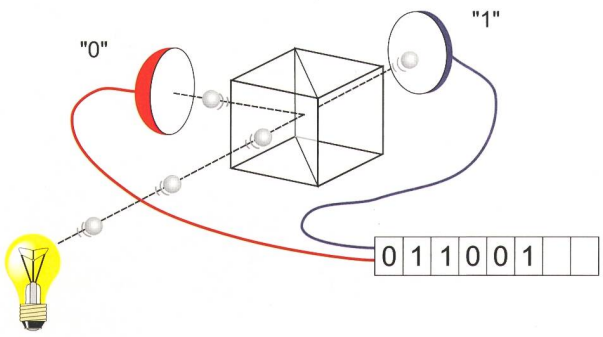
De tels générateurs existent maintenant depuis plusieurs années et sont commercialisés par la société genevoise ID Quantique. Ils sont utilisés pour générer des clés de chiffrement et ont aussi trouvé d'autres applications, comme par exemple dans le domaine de la recherche statistique, des loteries ou de la cryptographie.

Distribution conventionnelle de clés

La seconde étape dans la gestion d'une clé de chiffrement est sa transmission. Il est essentiel qu'elle se fasse de façon sécurisée pour éviter que la clé ne tombe entre les mains d'un adversaire.

Cryptographie à clé publique

Les approches conventionnelles d'échange de clé exploitent des algorithmes dits de cryptographie à clé publique. Avec ces procédés, on utilise deux clés. La clé publique permet de chiffrer les données, mais pas de les déchiffrer. La clé privée quant à elle permet de déchiffrer les communications. Le problème de la transmission de la clé ne se pose ainsi plus, car il est possible de transmettre une clé publique sans mesures de sécurité particulières. Si cette clé était interceptée par un adversaire lors de sa transmission, ce dernier pourrait certes chiffrer des communications, mais pas les déchiffrer. Pour ce faire, il faudrait qu'il mette



ID Quantique

Figure 1
Génération de nombres aléatoires au moyen d'un processus quantique par réflexion ou transmission d'un photon sur un miroir semi-réflechissant.

la main sur la clé privée, mais celle-ci n'ayant pas besoin d'être transmise, elle est plus facile à protéger.

Ces procédés sont relativement gourmands en ressources de calcul. Ils ne sont donc en général pas utilisés pour chiffrer des communications, mais pour protéger l'échange d'une clé secrète, en passant par les étapes suivantes :

- Une des deux parties souhaitant échanger des informations de façon sécurisée prépare une paire de clé publique et clé privée.
- Elle transmet la clé publique à son partenaire au moyen du canal de communication.
- Le partenaire génère une clé secrète et la chiffre au moyen de la clé publique préalablement reçue.
- Le message chiffré produit est retourné vers la première partie qui n'aura plus qu'à utiliser la clé privée pour le déchiffrer et récupérer la clé secrète, qui pourra être employée pour sécuriser des communications.

Il faut noter que la clé secrète contient typiquement 256 bits. Son chiffrement au moyen d'un algorithme de cryptographie à clé publique ne pose donc pas de problèmes de ressources.

Vulnérabilités

Malheureusement, les algorithmes de chiffrement à clé publique souffrent de vulnérabilités. Ils sont en effet basés sur des problèmes mathématiques complexes – par exemple la factorisation de nombres entiers – mais il n'existe pas de preuve de leur sécurité. Des progrès théoriques, comme l'invention d'un algorithme permettant de factoriser les nombres entiers de façon efficace, la remettrait ainsi complètement en cause.

Ces algorithmes de chiffrement sont en outre aussi vulnérables à un ordinateur quantique. Ces calculateurs d'un type nouveau utilisent les lois de la physique quantique pour traiter l'information. Ils en sont encore au stade de la recherche, mais leur développement rendrait lui aussi caduque la cryptographie à clé publique. Un algorithme permettant de factoriser les nombres entiers de façon efficace sur un ordinateur quantique a en effet été inventé il y a déjà une quinzaine d'année. Dès qu'un tel ordinateur aura été développé, cet algorithme pourra être utilisé pour mettre en défaut les algorithmes de cryptographie à clé publique. Finalement, cette cryptographie est aussi vulnérable à l'augmentation de la puissance de calcul des ordinateurs conventionnels.

ID Quantique

Figure 2 Système commercial de chiffrement avec distribution quantique de clé. Equipement inférieur : serveur quantique de clé. Equipement supérieur : boîtier de chiffrement Gigabit Ethernet.

En résumé, les techniques de cryptographie à clé publique sont largement utilisées, mais leur résistance est inappropriée pour sécuriser des communications devant rester confidentielles pour des durées excédant quelques années. Il est en effet possible pour un adversaire de stocker des données chiffrées dans l'attente que la technologie nécessaire à leur déchiffrement devienne disponible.

Distribution quantique de clés

Les fibres optiques forment la colonne vertébrale des réseaux de données. Elles transportent l'information sous forme d'impulsions lumineuses constituées de millions de photons. Contrairement à une opinion encore largement répandue, ces réseaux ne sont pas sûrs. Il est tout-à-fait possible pour un adversaire d'intercepter quelques pourcents de la lumière sans perturber les impulsions et d'obtenir ainsi une copie des données.

La physique quantique apporte aussi une solution à ce problème. Un de ses principes, connu sous le nom de principe d'incertitude d'Heisenberg, stipule qu'il n'est pas possible d'effectuer une mesure sans perturber « l'objet » mesuré. Ceci peut être utilisé pour mettre en évidence la présence d'un espion sur un réseau.

Cryptographie quantique

L'idée de la cryptographie quantique est d'utiliser pour chaque bit d'information une impulsion constituée d'un seul photon. Un photon étant un système quantique élémentaire, il est décrit par les lois de la physique quantique. Pour chaque bit, sa valeur est codée en modulant une propriété d'un photon, sa polarisation par exemple. Lors de la transmission de ce dernier, une mesure de son état de polarisation par un espion induira automatiquement une modification détectable par l'émetteur et le récepteur.

En pratique, cette approche ne permet évidemment pas d'empêcher l'espionnage, mais elle permet de le détecter (le lecteur intéressé trouvera une description complète du protocole de cryptographie quantique le plus répandu à la référence [1]). Comme cette mise en évidence intervient a posteriori, il ne serait pas approprié d'utiliser cette technologie pour sécuriser des données. Elle est plutôt utilisée pour transmettre une séquence de bits aléatoires et pour vérifier que celle-ci n'a pas été interceptée. La séquence peut ensuite être utilisée comme clé de chiffrement.

Bien que l'appellation cryptographie quantique soit souvent utilisée, il est plus précis de parler de distribution quantique de clés. Cette technologie permet en effet d'échanger sur un réseau optique des clés dont la sécurité ne repose que sur la physique quantique.

Dans la pratique

Les premières démonstrations de distribution quantique de clés furent réalisées au milieu des années 90. La technologie a ensuite été graduellement améliorée, de façon à augmenter son débit (nombre de bits de clés échangés par seconde) et sa portée.

Une portée limitée

Les fibres optiques sont constituées de verre d'une très grande pureté, mais cela n'empêche pas la lumière y voyageant d'être progressivement absorbée. Avec les communications conventionnelles, cet affaiblissement est compensé

par des amplificateurs optiques. Dans le cas des communications quantiques, il n'est pas possible d'amplifier le signal, car cela le perturberait. La portée de la distribution quantique de clés est donc limitée.

Les systèmes de première génération

Les performances des systèmes de première génération, basés sur des protocoles développés dans les années 90 et commercialisés depuis une petite dizaine d'années, sont limitées par le type de source de photons utilisé. En principe, l'émetteur doit pouvoir transmettre des impulsions lumineuses contenant exactement un photon. Si une impulsion contient deux photons ou plus, il est possible pour un espion de s'emparer d'une des particules sans modifier l'autre. Il pourra ainsi mesurer son état sans perturber celui qui parviendra au récepteur et il n'est plus possible de garantir la sécurité de cette technologie. Au contraire, si une impulsion ne contient aucun photon, il ne sera pas possible de transmettre un bit.

En pratique, bien que des sources de photons uniques existent, il s'agit d'une technologie encore peu efficace et difficile à mettre en œuvre. Elle requiert par exemple un refroidissement cryogénique, ce qui n'est pas compatible avec les contraintes liées à un équipement destiné à être déployé dans un réseau.

Pour contourner cette difficulté, les systèmes de première génération utilisent comme source un laser produisant des impulsions intenses – c'est-à-dire qu'elles contiennent des millions de photons – et qui sont atténuées par exemple en les faisant traverser un milieu absorbant pour ne garder qu'un seul photon. Il est toutefois important de noter que le nombre de photons dans une impulsion n'est pas précisément déterminé, mais statistiquement distribué selon la loi de Poisson autour d'une valeur moyenne.

Si le facteur d'atténuation est choisi de façon telle que le nombre moyen de photons dans les impulsions atténuées vaut 1, une partie non négligeable de ces impulsions contiendra plus qu'un photon, ce qui pourra être la source d'une faille de sécurité. Pour garantir une sécurité optimale, il est nécessaire d'atténuer les impulsions pour que le nombre moyen de photons soit inférieur à 1 (typiquement 0,1 ou 0,2). Cela signifie que la plupart des impulsions sont vides, mais que celles qui ne le sont pas ont une probabilité extrêmement faible de contenir plus d'un photon. Pour ces systèmes de première génération, le coût de la sécurité se résume à une efficacité limitée. Seule une faible fraction des impulsions transportent effectivement un bit d'information. Cela a pour effet de réduire leur débit de clé et leur portée.

Les systèmes commerciaux actuels

Les systèmes commerciaux actuels, qui utilisent une source basée sur un laser atténué, permettent d'échanger des clés sur une distance pouvant atteindre une centaine de kilomètres au travers d'une fibre optique standard.

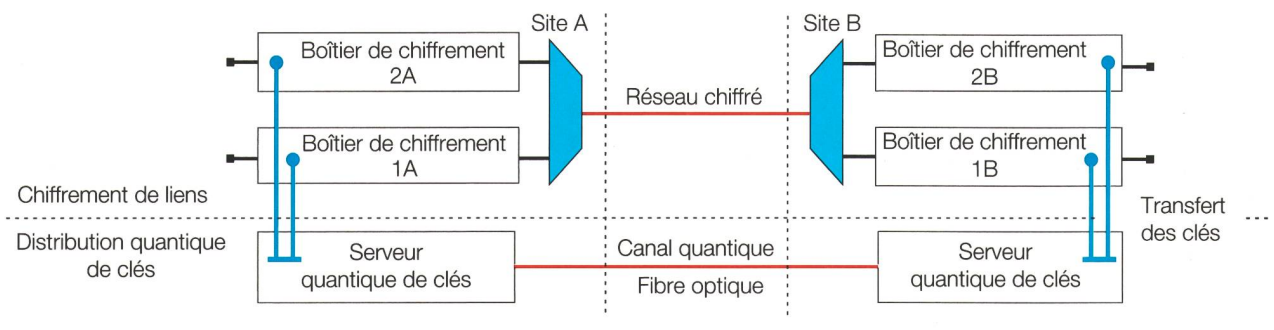
Un système de distribution quantique de clé d'ID Quantique est constitué de deux boîtiers 19". Chacun est doté d'une connexion optique, d'une connexion de « management », ainsi que d'une série de ports pour l'interfaçage avec un équipement de chiffrement pour le transfert des clés (figure 2). Il se configure et s'administre comme un équipement réseau conventionnel et ne requiert aucune connaissance en physique quantique.

Dans une configuration standard, une paire de boîtiers quantique sera installée dans deux sites distants et connectée par une liaison optique. On y ajoutera ensuite une paire de boîtiers de chiffrement – un par site – pour chaque liaison à sécuriser (figure 3). Ces boîtiers de chiffrement utilisent des clés de 256 bits distribuées quantiquement pour chiffrer les données au moyen de l'algorithme AES (Advanced Encryption Standard ou standard de chiffrement avancé). Le chiffrement est réalisé de façon matérielle, au moyen d'un FPGA (Field-programmable Gate Array ou réseau de portes programmables in situ), pour garantir un impact nul sur la capacité du lien.

En pratique, avant de procéder au chiffrement on combine encore la clé quantique avec une clé distribuée au moyen d'un procédé conventionnel. Cette combinaison est faite de façon à produire une clé résultante aussi résistante que la plus résistante des deux clés initiales. Cette approche a l'avantage de permettre la certification du système. Il est en effet plus aisé d'évaluer la sécurité du processus conventionnel d'échange de clé, pour lequel des standards existent déjà, que de la distribution quantique de clé.

Sécurisation de réseaux métropolitains

Ces systèmes offrent une solution permettant de garantir une sécurité à long terme pour les communications dans les réseaux métropolitains. La première application au monde de cette technologie a eu lieu à l'automne 2007, date à laquelle le Centre des Technologies de l'Information de l'Etat de Genève l'a déployée pour sécuriser un lien Gigabit Ethernet critique reliant lors des élections fédérales le site de dépouillement



ID Quantique

Figure 3 Configuration permettant de sécuriser les communications entre deux sites. Un serveur quantique de clé est installé dans chacun des sites et relié à l'autre par une fibre optique. Dans cet exemple, deux liens doivent être sécurisés au moyen de deux paires de boîtiers de chiffrement qui reçoivent leurs clés des serveurs quantiques.

Université de Genève

Figure 4 Tracé de la liaison optique mise à disposition par Swisscom pour les tests du système de distribution quantique de clé de seconde génération.

centralisé et le centre de calcul de l'Etat. Ce déploiement s'est passé sans encombre et a donné satisfaction, de sorte que le système a été utilisé pour toutes les élections qui ont eu lieu depuis cette date.

Cette technologie suscite aussi un grand intérêt dans les secteurs financiers, gouvernementaux ou dans le domaine de la santé, pour lesquels une confidentialité durable est importante. Elle a par exemple été déployée l'an dernier par la société Siemens IT Services and Solutions aux Pays-Bas pour sécuriser les communications entre ses deux centres de calcul.

Derniers développements

Fort de ces succès, le développement de la distribution quantique de clé continue. La recherche actuelle se concentre le long de deux axes.

Augmentation de la portée et du débit

Le premier consiste à améliorer les performances de cette technologie en termes de portée et de débit de clé. Les centres de recherche principaux – situés en Europe, au Canada et au Japon – se concentrent ainsi depuis quelques années sur le développement de systèmes de seconde génération. Pour mémoire, les systèmes de première génération exploitent un protocole quantique supposant l'utilisation d'une source de photons uniques parfaite. Leurs performances – en termes de portée et de débit, mais bien entendu pas de sécurité – sont donc dégradées du fait de l'imperfection des impulsions produites par une source à laser atténué.

Mesure de l'énergie

Il a été expliqué plus haut qu'en physique quantique une mesure perturbe le système mesuré. Cette affirmation est correcte, mais il est intéressant d'aller un pas plus loin. Un photon est un système quantique décrit par plusieurs grandeurs comme sa polarisation, sa direction ou son énergie. Ce qu'indique la physique quantique, c'est que la mesure d'une grandeur induit une perturbation de cette grandeur, mais pas des autres quantités. Il est ainsi par exemple possible de mesurer l'énergie d'un photon sans modifier sa polarisation.

Ceci peut être utilisé par un espion pour mesurer le nombre de photons dans une impulsion, qui est proportionnelle à son énergie, sans perturber sa polarisation. Dans le cas de la transmission d'impulsions laser atténuées, l'espion peut utiliser cette propriété pour trier les impulsions contenant plusieurs photons (elles contiennent plus d'énergie) des impulsions n'en contenant qu'un. Cela lui permet de déterminer quelles impulsions il peut attaquer sans induire de perturbation.

Les systèmes de seconde génération

Les systèmes de seconde génération utilisent quant à eux de nouveaux protocoles développés au début des années 2000 prenant en compte d'emblée l'imperfection de la source. Schématiquement, pour rendre impossible l'attaque mentionnée ci-dessus, il suffit pour l'émetteur et le récepteur de vérifier que non seulement la polarisation des photons n'a pas été perturbée, mais aussi leur énergie. Cela rend possible de travailler avec des impulsions moins fortement atténuées et permet donc une amélioration sensible des performances.

Une des institutions travaillant sur ce type de système est l'Université de Genève, qui détient actuellement le record mondial de portée sur fibre installée (140 km entre Genève et Neuchâtel, voir **figure 4**) et en laboratoire (250 km). On peut s'attendre à

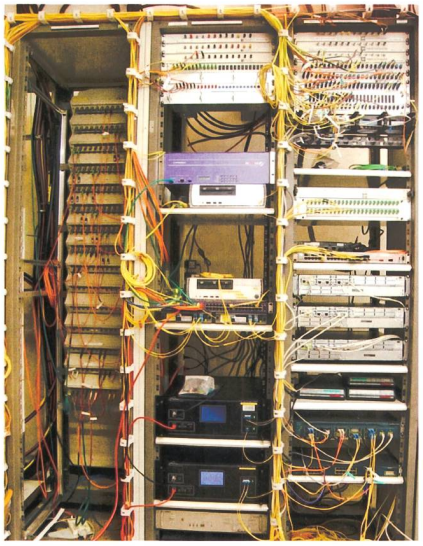

ID Quantique

Figure 5 Equipements déployés dans le cadre du réseau pilote Swiss Quantum dans le centre de calcul du CERN qui en hébergeait un des nœuds.

voir apparaître des produits commerciaux basés sur ces approches de seconde génération d'ici deux ou trois ans.

Déploiement de réseaux pilotes

Le second axe de recherche est le déploiement de réseaux pilotes permettant d'explorer l'utilisation de la cryptographie quantique dans des topologies plus complexes qu'un lien point à point. Il est évidemment possible de déployer plusieurs liens quantiques dans un réseau maillé ou en chaîne, mais les protocoles permettant aux différents systèmes quantiques d'interagir doivent être développés et testés.

Un second objectif de ces réseaux pilotes est de réaliser des tests en conditions réelles sans risquer de perturber un réseau de production. Un exemple notable de ces déploiements pilotes est le réseau SwissQuantum (figure 5) [2], mis en place par ID Quantique et l'Université de Genève, assistées par la HES-SO, au printemps 2009 dans la région genevoise. Ce réseau triangulaire est constitué de trois liaisons. Le projet s'est parfaitement déroulé et les équipements ont totalisé plus de 45 000 heures de fonctionnement entre mars 2009 et janvier 2011, démontrant la maturité de cette technologie. On peut ainsi affirmer sans se tromper que nous sommes bien entrés dans l'ère des technologies quantiques de l'information.

Références

[1] G. Ribordy, O. Guinnard, N. Gisin et H. Zbinden: Un saut quantique en cryptographie. Bulletin SEV/VSE 17/02, pp. 11-16, 2002. www.electrosuisse.ch/display.cfm?id=115821.
[2] www.swissquantum.com

Informations sur les auteurs

Grégoire Ribordy a étudié la physique à l'EPFL et obtenu son diplôme en 1995. Après avoir travaillé pendant un an dans la division R&D de la société Nikon à Tokyo, il a rejoint le Groupe de Physique Appliquée de l'Université de Genève où ses activités de recherche ont porté sur la cryptographie quantique et les techniques de détections de photons uniques. Il a obtenu son doctorat en 2000 et fondé en 2001 avec trois associés la société ID Quantique, qu'il dirige encore. Grégoire Ribordy a reçu en 1998 le prix de la Société Suisse d'Optique et de Microscopie, ainsi que le prix de Vigier de soutien à l'entrepreneuriat en 2002.

ID Quantique SA, 1227 Carouge, gregoire.ribordy@idquantique.com

Patrick Trinkler a mené des études en électronique à l'Ecole d'Ingénieur de St-Imier (HES-SO Arc) et obtenu le titre d'ingénieur ETS en 1998. Il a ensuite rejoint l'entreprise TT-Novatech en tant que collaborateur scientifique et a participé à des projets de transfert de technologie avec des entreprises comme ETA (Swatch Group). En 2001, il a intégré la société Thermo Fischer à Ecublens en tant qu'ingénieur R&D et a participé au développement d'un spectromètre destiné à l'industrie métallurgique. En 2003, il a rejoint ID Quantique SA à Carouge en tant qu'ingénieur R&D, entreprise dans laquelle il occupe le poste de directeur R&D depuis 2007.

ID Quantique SA, 1227 Carouge, patrick.trinkler@idquantique.com

Zusammenfassung **Quantenphysik und Kryptographie**

Erzeugung und sichere Verteilung kryptographischer Schlüssel

Datennetze gewinnen in unserer Gesellschaft zunehmend an Bedeutung und es gilt, die dort übermittelten Daten mithilfe von Verschlüsselungstechnologien zu schützen. Dabei hängt die Wirksamkeit dieser Technologien natürlich von der Komplexität des verwendeten Schlüssels ab, aber auch von der Sicherheit der Übertragung.

In diesem Artikel wird erläutert, wie mithilfe der Quantenphysik kryptographische Schlüssel erzeugt werden können, die vollkommen zufällig generiert wurden. Anschliessend werden die neuesten Entwicklungen hervorgehoben, die ebenfalls dank der Quantenphysik die Sicherheit der Übertragung über immer größere Entfernungen sicherstellen. CHe