Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 93 (2002)

Heft: 17

Artikel: Un saut quantique en cryptographie

Autor: Ribordy, Grégoire / Guinnard, Olivier / Gisin, Nicolas

DOI: https://doi.org/10.5169/seals-855442

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 08.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Un saut quantique en cryptographie

La cryptographie quantique constitue la première application de la théorie quantique de l'information. Elle permet l'échange, sur des réseaux optiques, de clés de chiffrement dont la sécurité est garantie de façon absolue par les lois de la physique quantique. Pour la première fois dans l'histoire de la cryptographie, la sécurité d'une méthode de chiffrement ne dépend plus de la puissance de calcul à disposition de l'adversaire: Elle repose sur les principes de la physique quantique. Le premier prototype a été testé récemment en Suisse.

Les champs d'application de la physique classique et de la physique quantique sont très différents. La physique classique décrit les objets dits macroscopiques. C'est elle qui, par exemple, permet d'analyser la chute d'une pomme. Elle fut développée progressivement au cours des deux derniers millénaires. A la fin du 19e siècle, un certain nombre de situations, pour lesquelles la description proposée par cette théorie n'était pas adaptée, furent mises en lumière. Des physiciens comme Max Planck et Albert Einstein entreprirent donc de développer un nouvel ensemble de théories, connu sous le nom de physique quantique. Celle-ci s'applique au monde microscopique, comme par exemple les molécules, les atomes ou les particules élémentaires. Chacune ayant son champ d'application, physique quantique et classique sont complémentaires. Néanmoins, leurs prédictions diffèrent de façon radicale. Ainsi par exemple, alors que la physique classique est intrinsèquement déterministe, la physique quantique prévoit que certains phénomènes sont fondamentalement aléatoires. Cette dernière impose aussi des limitations sur la précision avec laquelle la mesure d'une propriété d'un système peut être effectuée (conséquence du principe d'incertitude d'Heisenberg).

Grégoire Ribordy, Olivier Guinnard, Nicolas Gisin, Hugo Zbinden

Bien que la physique quantique eut une forte influence sur le développement technologique au 20e siècle – elle a par exemple permis l'invention du laser ou du transistor – son impact sur le traitement de l'information commence seulement à apparaître. La théorie quantique de l'information constitue un champ de recherche nouveau et dynamique au carrefour de l'informatique et de la physique. Il s'intéresse aux conséquences de l'utilisation d'un système quantique comme support d'information logique (bit[1]). Au delà de considérations pratiques, le fait qu'un bit soit écrit sur un morceau de papier, mémorisé dans un transistor ou inscrit sur l'état d'un atome – un système quantique – a des conséquences importantes sur les opérations de traitement pouvant lui être appliquées. Avec un système quantique, les propriétés et les possibilités de traitement de l'information sont révolutionnaires et sans équivalent en théorie classique de l'information. Pour bien insister sur cette différence, on parle, dans le cadre de la théorie quantique de l'information, de bit quantique ou qubit. Le but ultime de ce nouveau domaine est le développement d'un ordinateur quantique traitant un ensemble de qubits. Les travaux de recherche ont ainsi déjà démontré qu'un tel système, quand il verra le jour, possédera une puissance de calcul sans commune mesure avec celle des ordinateurs conventionnels, grâce à un parallélisme massif. Ces travaux sont particulièrement intéressants si l'on considère que la puissance des ordinateurs actuels croît grâce à la miniaturisation des transistors permettant d'en multiplier le nombre dans un microprocesseur. Dans un futur proche, cette miniaturisation se heurtera à des barrières physiques, puisque l'on estime que d'ici dix à quinze ans, leur taille sera tellement petite que leur comportement sera influencé par les lois de la physique quantique.

Bien que le développement de l'ordinateur quantique constitue un objectif relativement éloigné, deux applications de la théorie quantique de l'information permettent déjà aujourd'hui d'améliorer de façon significative la sécurité des échanges d'information. Il s'agit de la génération de nombres aléatoires (voir

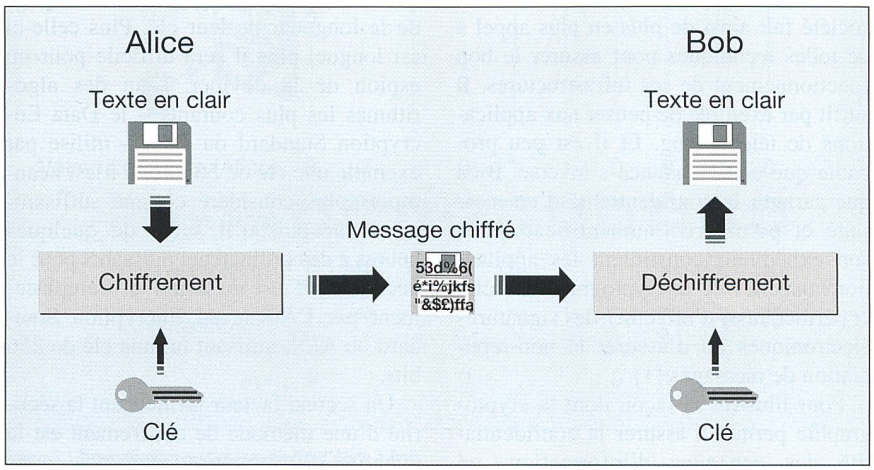


Figure 1 Principe général de la cryptographie

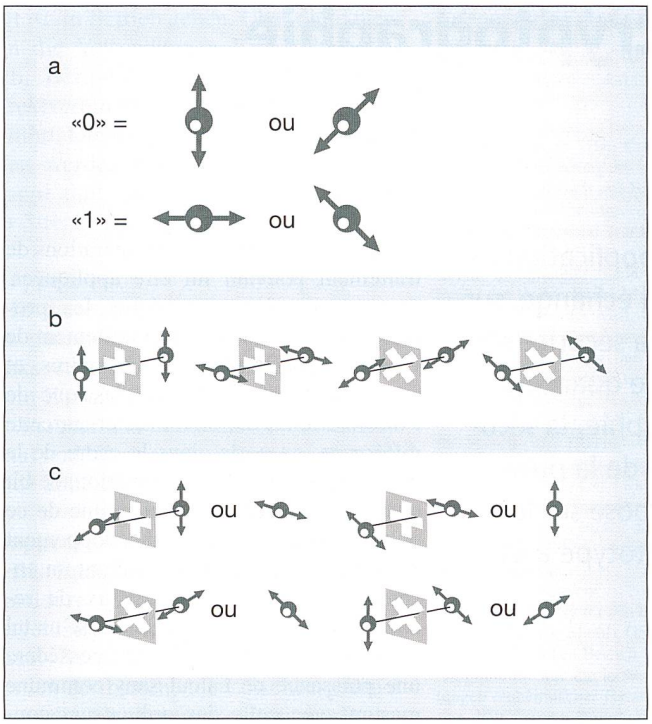


Figure 2 La polarisation des photons

encadré 1) et de la distribution quantique de clé cryptographique, qui constitue le sujet principal de cet article.

La cryptographie

La cryptographie constitue un ensemble de techniques permettant de garantir la confidentialité et l'intégrité des échanges d'information. Il s'agit d'une science ancienne, puisqu'il y a près de deux mille ans Jules César l'utilisait déjà. Jusqu'à récemment, elle est restée confinée aux domaines militaires et diplomatiques. Toutefois le développement des télécommunications et des échanges d'information sous forme électronique au cours des vingt-cinq dernières années a permis d'émanciper la cryptographie de son statut de science «top secrète». Notre société fait ainsi de plus en plus appel à de telles techniques pour assurer le bon fonctionnement de ses infrastructures. Il suffit par exemple de penser aux applications de télébanking. Et il est peu probable que cette tendance s'inverse. Bien que garantir la confidentialité d'un message et permettre l'authentification de son expéditeur constituent les applications usuelles de la cryptographie, celle-ci permet aussi d'effectuer des signatures électroniques ou d'assurer la non-répudiation de messages [1].

Pour illustrer la façon dont la cryptographie permet d'assurer la confidentialité des échanges d'information, on considérera la figure 1. L'expéditeur du message – traditionnellement appelé Alice – combine le message en clair avec une clé secrète au moyen d'un algorithme cryptographique, de façon à obtenir le message chiffré. Celui-ci est transmis au destinataire – Bob – qui le déchiffre au moyen de la clé et d'un algorithme de déchiffrement. Un espion – dénommé Eve – ne possédant pas la clé ne pourra pas déduire le message original à partir de la transmission chiffrée. En guise d'illustration, ce processus de chiffrement revient à placer le message en clair dans un coffre-fort. Ce dernier est verrouillé par Alice au moyen de sa clé. Quant à Bob, il ne peut l'ouvrir qu'après l'avoir déverrouillé.

Il existe de nombreux algorithmes de chiffrement différents. D'une manière générale, la sécurité qu'ils offrent dépend de la longueur de leur clé. Plus celle-ci est longue, plus il sera difficile pour un espion de la deviner. L'un des algorithmes les plus courants – le Data Encryption Standard ou DES – utilise par exemple une clé de 56 bits. Il n'est néanmoins plus considéré comme suffisamment sûr puisqu'il suffit de quelques heures à des ordinateurs puissants pour le décrypter. Il est en cours de remplacement par l'Advanced Encryption Standard ou AES, utilisant lui une clé de 256 bits.

Un second facteur influençant la sécurité d'une méthode de chiffrement est la quantité d'information encryptée avec une clé donnée: plus l'on change souvent la clé, moins un espion aura de matériel pour l'aider dans sa tentative de déchiffrement. Dans le cas extrême où la clé est aussi longue que le message et qu'elle n'est utilisée qu'une seule fois, la sécurité est absolue. Cette méthode, connue sous le nom anglais de «One-Time-Pad» (masque jetable), est d'ailleurs la seule à offrir un tel niveau de sécurité. Dans les autres cas, un espion a en effet toujours la possibilité d'essayer une à une toutes les clés. Toutefois, si la clé est suffisamment longue, cette recherche peut s'avérer si fastidieuse qu'elle ne pourra pas être réalisée en pratique.

En cryptographie, on suppose en général que le type d'algorithme de chiffrement utilisé n'est pas secret, ce qui a pour conséquence de faire reposer toute la sécurité de la méthode sur le fait que la clé reste inconnue pour l'espion. Cela implique qu'un processus adéquat soit utilisé pour la génération de cette clé (voir encadré 1) et qu'elle soit échangée entre Alice et Bob d'une façon garantissant qu'elle ne peut pas être interceptée par Eve. Ce problème, connu sous le nom de problème de distribution de la clé, est fondamental en cryptographie.

Distribuer les clés

Pendant longtemps, on a cru que la seule possibilité de résoudre le problème de la distribution de la clé était de procéder à l'échange d'un support physique. Alice peut par exemple envoyer par la poste à Bob une disquette contenant la clé. Néanmoins, à l'ère de l'autoroute de l'information, cette solution n'est clairement pas pratique. En outre, comment s'assurer du fait que la disquette n'a pas été interceptée et copiée par Eve?

A la fin des années soixante et au début des années septante, des chercheurs du GCHQ[2)] britannique inventèrent une nouvelle approche. Pour reprendre l'image introduite ci-dessus, ils proposèrent de remplacer le coffre-fort par un cadenas. Bob distribue à tous ses interlocuteurs des cadenas ouverts, tout en en gardant les clés. Alice, avant de lui envoyer un message, utilise un des ces cadenas pour le protéger. Elle peut le fermer sans en avoir la clé. Bob peut ensuite ouvrir le cadenas au moyen de la clé qu'il a conservé. En pratique, cette méthode de chiffrement implique l'utilisation de deux clés. Une clé, dite publique, sert à chiffrer le message. Elle est envoyée à Alice par Bob. Une seconde clé, dite privée, permet uniquement le déchiffrement. Bob la garde secrète. La cryptographie à clé publique était née. Ces travaux furent néanmoins classés top secrets par les

autorités britanniques et ces techniques cryptographiques furent redécouvertes de façon indépendante au milieu des années septante par des chercheurs américains.

En pratique, ces cadenas prennent la forme de fonctions mathématiques dites à sens unique, qui se calculent facilement, mais sont difficiles à inverser (encadré 2). Comme les algorithmes de cryptographie à clé publique font appel à des calculs complexes, ils sont relativement lents. En pratique, on peut considérer qu'ils sont typiquement mille fois plus lents que les algorithmes conventionnels. Ils ne sont donc, en général, pas employés pour l'encryption de volumes importants d'information, mais plutôt pour échanger une clé, dite de session, utilisée ensuite pour le chiffrement à l'aide d'un algorithme comme DES ou AES.

Bien que la cryptographie à clé publique soit extrêmement pratique, elle est entachée de deux défauts primordiaux.

Vulnérabilité au progrès technologique

Premièrement, cette technique cryptographique est vulnérable au progrès technologique. Inverser une fonction à sens unique est possible, pourvu que l'on dispose de suffisamment de temps. Les ressources nécessaires pour casser ces algorithmes, en terme de puissance ou de temps de calcul, dépendent de la longueur de la clé. Cette dernière doit donc être sélectionnée de façon très prudente. Il faut en effet être capable de prédire la puissance informatique dont disposera un espion potentiel au cours du temps pendant lequel les informations chiffrées auront de la valeur. Rien n'empêche en effet Eve d'enregistrer les échanges d'information et de les stocker jusqu'au moment où elle pourra s'offrir un ordinateur suffisamment puissant pour les déchiffrer. Une telle estimation est possible lorsque la durée de vie des informations est de l'ordre de quelques mois, comme dans le cas de numéros de cartes de crédit, mais elle est beaucoup plus difficile quand elle couvre une décennie.

Ainsi en 1977, les trois inventeurs du RSA – l'algorithme de cryptographie à clé publique le plus courant – lancèrent un défi. Il s'agissait de déchiffrer un message protégé par une clé de 129 chiffres décimaux ou 428 bits. A l'époque, ils prédirent que ce défi prendrait au moins 40 millions de milliards ($40 \cdot 10^{15}$) d'années. En 1994, un groupe de scientifiques ayant utilisé Internet pour distribuer la charge de calcul annonça qu'il était parvenu à déchiffrer ce message. En outre, il est prouvé qu'un ordinateur quantique, lorsqu'il pourra être construit, pourra, grâce à son parallélisme massif et ses capacités de factorisation, déchiffrer les messages protégés par la cryptographie à clé publique.

Inverser les fonctions à sens unique

La seconde vulnérabilité de la cryptographie à clé publique tient au fait qu'il n'existe aucune preuve formelle de l'impossibilité d'inverser les fonctions à sens unique. Malgré les efforts d'innombrables spécialistes de la théorie des nombres, on ne sait toujours pas à l'heure actuelle si un algorithme permettant de factoriser rapidement un grand nombre au moyen d'un ordinateur conventionnel – on a vu plus haut qu'un tel algorithme existe pour les ordinateurs quantiques – peut exister ou non. S'il existait, la sécurité de la cryptographie à clé publique serait instantanément réduite à néant. Les progrès théoriques sont encore plus difficiles à prédire que les progrès technologiques. L'invention de la cryptographie à clé publique le démontre bien, puisque selon son inventeur, il ne lui a pas fallu plus d'une demi-heure pour concevoir cette technique et résoudre ainsi un problème qui avait occupé les plus éminents cryptographes pendant des siècles. Il se pourrait même qu'un tel algorithme ait déjà été découvert mais qu'il ait été conservé secret par son inventeur.

Ces deux vulnérabilités constituent donc une menace sérieuse et rendent le développement d'autres techniques de distribution de clés cryptographiques indispensable.

La cryptographie quantique

Principe

La cryptographie quantique permet de résoudre le problème de la distribution des clés de chiffrement. Elle permet d'échanger entre deux stations une clé dont la sécurité est garantie par les lois de la physique quantique. Cette clé peut ensuite être utilisée avec des algorithmes de chiffrement conventionnels. Ainsi, le terme de «distribution quantique de clé» constitue une appellation plus exacte pour cette technique. Contrairement à ce qu'on pourrait penser, le principe qui la sous-tend est relativement simple. Elle exploite le fait, que, selon la physique quantique, il n'est pas possible d'observer un système sans le perturber de façon irrémédiable. Cette interaction entre l'observateur et l'objet observé est fondamentale en physique quantique.

Ainsi lorsque, par exemple, vous lisez cet article, la feuille de papier sur laquelle il est imprimé doit être éclairée. L'impact des particules de lumière – les photons – aura pour effet d'augmenter, très légèrement certes, sa température. Il modifie donc la feuille de papier. Cet effet est très faible et ne sera pratiquement pas perceptible avec un objet macroscopique

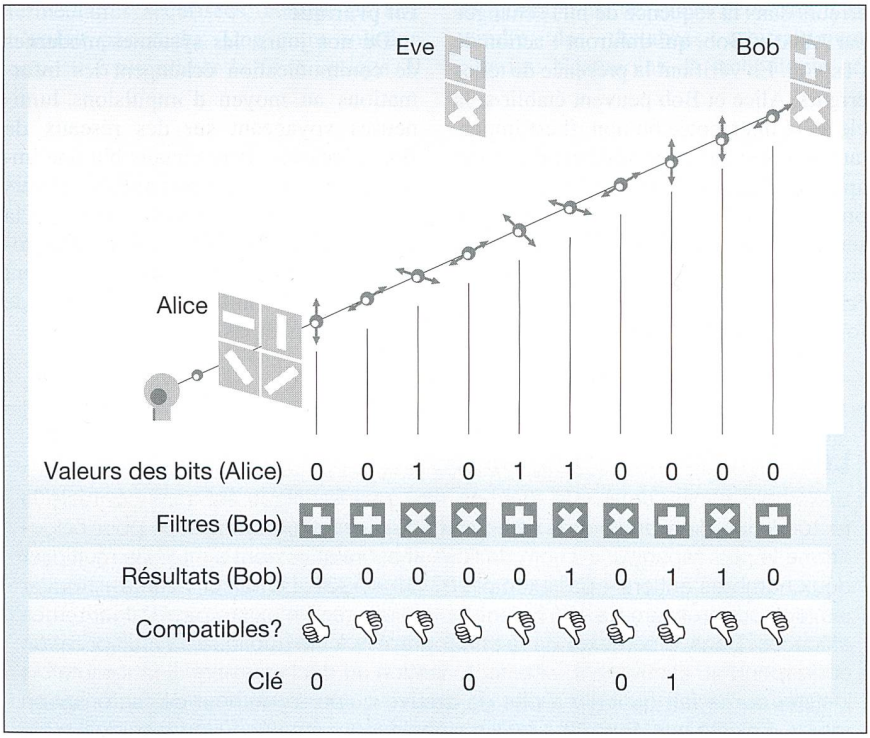
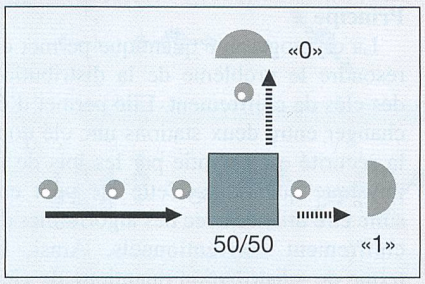


Figure 3 Transmission quantique de clé d'Alice à Bob
Si un espion intercepte l'information il change la polarisation du photon aléatoirement.

Génération de nombres aléatoires

La génération de nombres aléatoires est une primitive essentielle dans le domaine de la cryptographie. On peut par exemple songer à la génération d'une clé de cryptage, qui consiste en une séquence aléatoire de bits. La production d'une telle séquence n'est pas triviale. Un ordinateur conventionnel ne peut produire que des nombres pseudo-aléatoires, puisqu'il est régi par la physique classique et qu'il est, à ce titre, déterministe. Ces derniers n'étant pas adéquats pour les besoins de la cryptographie, une source physique de hasard doit être utilisée. Comme la physique quantique est la seule théorie qui prévoit des phénomènes aléatoires, il est naturel de l'exploiter dans ce but. *id Quantique* a ainsi développé un générateur basé sur le choix que fait un photon sur un miroir semi-réfléchissant. Rappelons qu'un photon est une particule élémentaire insécable et que, selon les lois de la physique quantique, le fait qu'il soit réfléchi ou transmis est fondamentalement aléatoire. Une valeur de bit est associée à chaque cas. Une séquence est générée en répétant ce processus.



Génération de nombres aléatoires au moyen d'un processus quantique: la réflexion ou la transmission d'un photon sur un miroir semi-réflechissant

comme la feuille de papier. La situation est drastiquement différente dans le cas d'un objet microscopique. Ainsi si un système quantique est utilisé comme support d'un bit d'information, son interception se traduira forcément par sa perturbation, puisque l'espion est forcé de l'observer. Cette perturbation causera des erreurs dans la séquence de bits échangée par Alice et Bob, qui trahiront l'action de l'espion. En vérifiant la présence de telles erreurs, Alice et Bob peuvent établir si la clé a été interceptée ou non. Il est important de noter que cette vérification se fait après l'échange d'information et que la présence de l'espion peut être décelée seulement a posteriori. C'est pourquoi cette technique doit être utilisée pour échanger une clé et non un message. Une fois que la confidentialité de la clé a été vérifiée, elle peut être utilisée en toute confiance pour le chiffrement de messages. Finalement, il faut insister sur le fait que les lois de la physique empêchent formellement une interception de la clé sans que des perturbations soient introduites.

En pratique

De nos jours, les systèmes modernes de communication échangent les informations au moyen d'impulsions lumineuses voyageant sur des réseaux de fibres optiques. Pour chaque bit, une impulsion est émise et transmise, au travers d'une fibre optique, au récepteur qui la détecte et la transforme en signal électronique. Ces impulsions sont typiquement constituées de millions de particules de lumière ou photons.

Les fonctions à sens unique

L'exemple le plus connu de fonction dite à sens unique est sans conteste la factorisation de grands nombres entiers. Elle est d'ailleurs utilisée pour l'algorithme le plus répandu, du nom de RSA. Il est relativement simple de multiplier deux nombres entiers – par exemple $37 \cdot 53 = 1961$. Le calcul inverse – trouver les facteurs premiers de 1961 – est fastidieux, car il n'existe pas d'algorithmes efficaces. Dans le contexte de la cryptographie à clé publique, la multiplication correspond au chiffrement, et la factorisation au déchiffrement. Il faut toutefois insister sur le fait qu'il n'y a pas de preuve qu'un algorithme de factorisation rapide n'existe pas. Peut-être qu'il n'a pas encore été découvert – ou qu'il a été gardé secret.

En cryptographie quantique, on suit le même principe mais avec des impulsions constituées d'un unique photon. Un photon représente une quantité d'énergie minuscule – en lisant cet article, vos yeux en détectent des milliards à chaque seconde – qui constitue un système quantique élémentaire. En particulier, il n'est pas possible de le casser en deux. Ainsi, un espion ne peut pas prendre un demi-photon, tout en laissant l'autre moitié poursuivre sa route. S'il veut intercepter le bit échangé, il lui faut détecter le photon et donc interrompre la communication. Il est clair que dans ce cas, rien ne l'empêche de préparer un nouveau photon selon le résultat qu'il a obtenu pour l'envoyer au destinataire. Toutefois en cryptographie quantique, Alice et Bob coopèrent pour empêcher Eve de suivre cette stratégie, en s'assurant qu'elle ne pourra le faire sans introduire des erreurs.

Le transfert de la clé

La valeur des bits est inscrite sur une propriété du photon, sa polarisation par exemple. La polarisation d'un photon est la direction d'oscillation du champ électromagnétique qui lui est associé. Elle peut être, par exemple, verticale, horizontale ou diagonale (+45° et –45°).

La figure 2a représente la convention décidée par Alice et Bob. Un filtre permet de distinguer entre des photons polarisés verticalement et horizontalement; un autre entre des photons polarisés en diagonale.

Quand un photon traverse le filtre correct, sa polarisation n'est pas affectée (figure 2b). En revanche, quand un photon traverse le faux filtre sa polarisation se transforme de façon aléatoire (figure 2c).

La figure 3 illustre l'échange d'une clé: Pour chaque bit de clé, Alice envoie un photon dont la polarisation est choisie au hasard entre les quatre états. Elle note ses choix.

A la réception d'un photon, Bob choisit aléatoirement un filtre. Il note son choix lui aussi, ainsi que la valeur qu'il obtient. Si Eve tente d'espionner le séquence de photons, elle modifiera certaines des polarisations.

Une fois que tous les photons ont été échangés, Bob annonce à Alice la séquence de filtres qu'il a choisie. Celle-ci répond en lui indiquant dans quels cas le filtre choisi était correct. Dans ces cas-là, Alice et Bob s'attendent à avoir les mêmes valeurs de bits. Ecouter cette communication ne permet pas à Eve de déduire la clé.

Alice et Bob suppriment les bits pour lesquels le faux filtre a été utilisé, de manière à produire la clé finale. Finalement

Alice et Bob valident la clé en vérifiant qu'elle ne contient aucune perturbation. Dans le cas contraire, ils concluent que la clé a été corrompue par Eve.

Les caractéristiques importantes d'un système de cryptographie quantique

Est-ce que la cryptographie quantique fonctionne réellement déjà en dehors de laboratoires de physique? Pour le prouver, *id Quantique* a développé un prototype (figure 4) qui a été testé sur le réseau de fibres optiques de Swisscom. Il permet d'échanger une clé de cryptage entre deux stations connectées chacune à un PC par le port USB[3)].

La première caractéristique importante d'un système de cryptographie quantique est le débit de clé. Il est typiquement de quelques centaines à quelques milliers de bits par seconde, suivant la distance. Cette valeur est basse par rapport au débit des systèmes de télécommunication actuels. Il s'agit toutefois du prix à payer en échange d'une sécurité absolue garantie par les lois de la physique quantique. Cette limitation n'est d'ailleurs pas aussi critique qu'il n'y paraît. Il faut se rappeler que le système n'est utilisé que pour échanger une clé. Les données chiffrées peuvent ensuite transiter par un canal à haut débit. Ainsi par exemple, une clé de 256 bits peut être changée plusieurs fois par seconde. Il faut insister sur le fait que grâce à cette technique une clé peut être générée juste avant d'être utilisée, simplifiant ainsi sa gestion et rendant son stockage superflu.

La seconde caractéristique importante d'un système de cryptographie quantique est la distance de transmission. Les fibres optiques sont constituées de verre de très haute qualité. Elles ne sont toutefois pas parfaitement transparentes. Il arrive ainsi qu'un photon soit absorbé lors de sa propagation et n'atteigne pas l'extrémité de la fibre optique. Dans les systèmes de télécommunication conventionnels, des répéteurs sont utilisés pour régénérer le signal. Ils sont espacés environ de 80 km et amplifient le signal optique. En cryptographie quantique, il n'est pas possible d'utiliser de tels répéteurs. Tout comme un espion, ils corrompent la transmission et introduisent des erreurs[4)]. Ainsi, le débit décroît avec la distance, puisque de moins en moins de photons atteignent l'extrémité de la fibre. Les photons perdus ne sont simplement pas pris en compte pour la constitution de la clé. Finalement quand la distance devient trop grande, le nombre de photons transmis devient trop faible pour permettre l'établissement d'une clé. La technologie actuelle permet ainsi d'atteindre une distance de l'ordre de 70 km. Le prototype d'*id Quantique* a été testé entre Genève et Lausanne, sur une distance de 67 km (figure 5). Comme la transparence des fibres optiques est proche de sa limite physique, il y a peu d'améliorations à attendre de ce côté-là.

Pour augmenter la distance de transmission, il serait bien entendu possible de chaîner les liens grâce à des stations intermédiaires sécurisées, auxquelles Eve n'aurait pas accès. Une autre solution consiste à supprimer la fibre optique. Il est ainsi possible d'échanger une clé entre une station terrestre et un satellite en orbite basse[5)]. Le satellite se déplace et se trouve quelques heures plus tard au-dessus d'une seconde station, située à des milliers de kilomètres de la première et à laquelle il retransmet la clé. Dans ce cas, le satellite est implicitement considéré comme une station sécurisée. Cette technologie est moins mûre que la cryptographie quantique au travers de fibres optiques. Des groupes de recherche ont toutefois déjà effectué des expériences préliminaires, mais aucun échange avec un satellite n'a encore été réalisé.

Finalement, des chercheurs ont aussi proposé de réaliser des répéteurs quantiques relayant des qubits, sans les mesurer et donc sans les perturber. Ces travaux n'en sont encore qu'à un stade théorique. En principe, ils devraient permettre d'atteindre des distances arbitrairement grandes. Néanmoins, la technologie né-

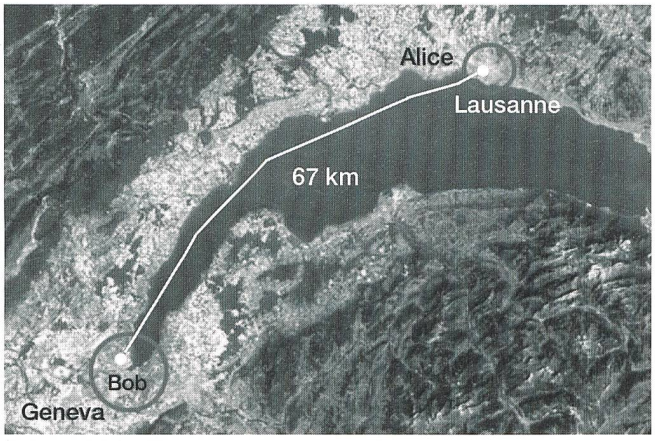


Figure 5 Le prototype a été testé sur une distance de 67 km de Genève à Lausanne

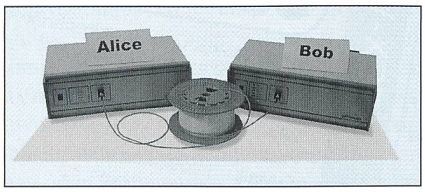


Figure 4 Système de transmission quantique de clé

Ein Quantensprung in der Kryptografie

Die quantenmechanische Kryptografie ist die erste Anwendung der Quantenmechanik in der Informationstechnologie. Sie erlaubt die absolut sichere Übertragung von Schlüsseln über optische Netze. Damit hängt die Sicherheit einer Verschlüsselungsmethode – zum ersten Mal in der Geschichte der Kryptografie – nicht mehr von der dem Spion zur Verfügung stehenden Rechenleistung ab. Ein erster Prototyp wurde kürzlich zwischen Genf und Lausanne über eine Distanz von 67 km getestet. Mit dieser Länge stösst die Übertragung über Glasfaser an die Grenze des physikalisch Möglichen. Auf Grund der quantenmechanischen Eigenschaften ist die Verwendung von Verstärkern nicht möglich. Für den urbanen Bereich allerdings bietet diese Distanz bereits Anwendungsmöglichkeiten – etwa für die sichere Datenübertragung zwischen Regierungsstellen.

Bei der Übertragung des Schlüssels verwendet der Absender die zufällig polarisierten Photonen und der Empfänger beliebige Polarisationsfilter. Sobald die Übertragung abgeschlossen ist, werden Filtersequenz und Polarisationsreihenfolge verglichen und daraus der Schlüssel definiert. Eine Störung der Übermittlung verändert die Polarisation der Photonen, und der Spion wird entlarvt.

cessaire à la réalisation de ces répéteurs n'est pas encore maîtrisée.

Déploiement de cette technologie

La technologie de la cryptographie quantique est suffisamment mûre pour permettre le déploiement des premiers systèmes d'échange de clé sur fibre optique et ce sur des distances de plusieurs dizaines de kilomètres. Elle permet de sécuriser toutes les transactions (voix, données, etc.) entre deux sites d'un réseau métropolitain. On peut par exemple penser aux échanges d'informations entre un bâtiment bancaire et un centre d'archivage. De façon similaire, la sécurité des échanges entre des bâtiments gouvernementaux dans une capitale pourrait aussi bénéficier de cette technologie. Forte de cette conviction, *id Quantique* est actuellement à la recherche de ses premiers clients.

Référence

[1] *Simon Singh*: Histoire des codes secrets. De l'Egypte des pharaons à l'ordinateur quantique. Paru chez J.-C. Lattès, Paris, 1999. (Deutsche Ausgabe: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. dtv, München, 2001).

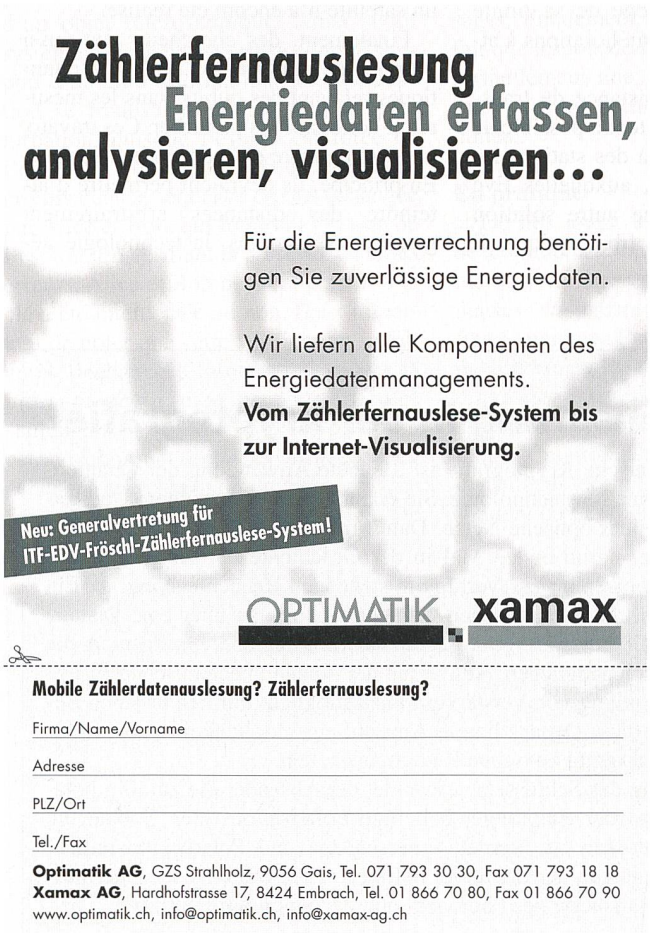
Adresses des auteurs

Prof. *Nicolas Gisin*, GAP-Optique, Université de Genève, 1211 Genève
nicolas.gisin@physics.unige.ch
Olivier Guinnard, id Quantique SA, rue Cingria 10 1205 Genève, olivier.guinnard@idquantique.com
Dr *Grégoire Ribordy*, id Quantique SA, rue Cingria 10, 1205 Genève
grégoire.ribordy@idquantique.com
Dr *Hugo Zbinden*, GAP-Optique, Université de Genève, 1211 Genève
hugo.zbinden@physics.unige.ch

[1] Le bit constitue l'unité élémentaire d'information et peut prendre deux valeurs: 0 ou 1.

[2] GCHQ: Government Communication Headquarters. La cryptographie à clé publique a été inventée par Clifford Cocks du GCHQ. www.gchq.gov.uk

[3] USB: Universal Serial Port

[4] Le fait que ces répéteurs ne puissent pas être utilisés n'est pas lié à une quelconque imperfection technique, mais plutôt à l'impossibilité physique d'amplifier un signal quantique sans le perturber.

[5] L'absorption atmosphérique a lieu uniquement dans les premiers kilomètres. Elle peut être très faible, pourvu qu'une longueur d'onde adéquate soit sélectionnée – et qu'il fasse beau.