La cryptographie quantique : l'incertitude quantique au service de la confidentialité

Frédéric GROSSHANS[*] et Philippe GRANGIER[+]
[*] Laboratoire Aimé Cotton, CNRS, Université Paris-Sud et ENS Cachan, 91405 Orsay
[+] Laboratoire Charles Fabry, Institut d'Optique Graduate School et CNRS, 2 avenue Fresnel, 91127 Palaiseau
frederic.grosshans@u-psud.fr

Depuis sa découverte en 1927, le principe d'incertitude de Heisenberg a souvent été perçu comme une limitation fondamentale imposée par la mécanique quantique aux mesures physiques. La cryptographie quantique exploite cette « faiblesse » et en fait une force, permettant de garantir un secret absolu sur des communications cryptées. Fondée sur une idée originale de S. Wiesner, refusée en 1969 par une revue scientifique, la cryptographie quantique s'est développée à partir de la publication par C.H. Bennett et G. Brassard, en 1984, d'un protocole d'échange quantique de clés. C'est aujourd'hui un domaine pluridisciplinaire en pleine expansion, à la veille d'applications commerciales et militaires.

Cryptographie classique et cryptographie quantique

Les systèmes usuels de cryptographie sont fondés sur la complexité algorithmique de leur déchiffrement : un système est considéré comme sûr si un espion a besoin d'une puissance de calcul déraisonnable pour déchiffrer le message en un temps raisonnable. Tout le travail des cryptologues consiste à trouver des algorithmes qui compliquent au maximum la tâche de l'espion et à évaluer leur complexité, en donnant des définitions rigoureuses des termes « raisonnable » et « déraisonnable » mentionnés plus haut.

Malheureusement, la sécurité des algorithmes à clé publique connus à ce jour et massivement utilisés sur Internet repose sur une conjecture mathématique, c'est-à-dire sur une affirmation mathématique que beaucoup de mathématiciens pensent vraie sans avoir réussi à la démontrer. En étant très pessimiste, on peut imaginer que cette conjecture est fausse, et que quelqu'un trouvera un jour – ou a déjà trouvé – un moyen de briser les codes considérés aujourd'hui comme sûrs. Sans aller aussi loin, le secret garanti par ce type de cryptographie est limité dans le temps à quelques dizaines d'années, ce qui est gênant pour certaines applications (signature électronique, communications diplomatiques, protection de la vie privée). Par exemple, un ordinateur de bureau peut aujourd'hui décrypter en quelques heures certains messages chiffrés par de gros ordinateurs dans les années 1970. Si la vitesse des ordinateurs continue à croître aussi vite que par le passé, ce problème persistera, sans oublier que la situation peut être aggravée par d'autres progrès techniques, tant logiciels (algorithmes de déchiffrement, calculs distribués) que matériels (ordinateurs moléculaires, ordinateurs quantiques, autres ordinateurs « exotiques »…).

Il existe un moyen d'éviter ces défauts, c'est de fonder un système de cryptographie sur la théorie de l'information et non sur la complexité algorithmique. C.E. Shannon a démontré en 1945 que les seuls systèmes de cryptographie sûrs, indépendamment de toute hypothèse sur la capacité de calcul de l'adversaire, exigent une clé secrète aléatoire aussi longue que le message, cette clé ne devant être utilisée qu'une seule fois. En résumé, pour pouvoir transmettre un message secret, il faut déjà pouvoir communiquer secrètement ! Ce type de cryptographie est cependant utilisé, par exemple dans le téléphone rouge entre Moscou et Washington, la distribution de clés se faisant au moyen de coursiers supposés dignes de confiance. Le but de la cryptographie quantique, appelée aussi « distribution quantique de clés », est de permettre à deux partenaires de partager une clé dont le secret est garanti par les lois de la physique quantique, plus fiables que l'intégrité d'un coursier.

Principes de la cryptographie quantique

L'idée fondamentale de la cryptographie quantique est d'exploiter le principe d'incertitude de Heisenberg (*encadré 1*) pour interdire à un espion d'apprendre quoi que ce soit d'utile sur une transmission d'information. Suivant les habitudes du domaine, appelons Alice et Bob les personnes qui veulent échanger un message secret et Ève l'espion. Si Ève veut intercepter les signaux envoyés par Alice, elle doit effectuer une mesure sur ceux-ci et les perturber. Cette perturbation peut être évaluée par Bob et Alice, ce qui leur permet de détecter la présence d'Ève et d'estimer la quantité d'informations qu'elle a interceptées : moins la transmission entre

Encadré 1

Principe d'incertitude de Heisenberg

Au cours des années 1920, les physiciens ont découvert qu'il était fondamentalement impossible de tout savoir sur les propriétés physiques d'un objet microscopique. Chaque grandeur physique mesurable (appelée « observable »), par exemple la position d'un objet, est intrinsèquement reliée à une autre, par exemple la vitesse, de sorte qu'on ne puisse jamais mesurer simultanément deux observables complémentaires avec une précision arbitraire. Ce « principe d'incertitude » nous dit que le prix à payer pour mesurer très précisément une observable est alors de détruire complètement l'information sur l'autre. La mesure simultanée des deux observables est toutefois possible, mais limitée à une précision « moyenne ». Bien sûr, cet effet est infinitésimal pour des objets de taille macroscopique, mais est essentiel aux petites échelles (photons uniques, atomes, électrons, etc.). En d'autres termes, ce « principe d'incertitude de Heisenberg » limite la quantité d'information disponible sur les propriétés physiques de ces objets. De plus, il nous dit qu'en général une mesure perturbe le système, ce qui limite la précision des mesures ultérieures. Ce principe, bien ancré dans les principes fondamentaux de la mécanique quantique, est une loi de la physique et non une limitation technologique : c'est ce qui lui donne sa pertinence dans les systèmes de cryptographie quantique.

Alice et Bob est bonne, plus le signal est perturbé, et plus Ève peut avoir d'informations sur ce qui a été transmis.

La cryptographie quantique est fondée sur l'utilisation de deux canaux : un canal quantique par lequel transitent des objets régis par les lois de la mécanique quantique (il s'agit en général d'une fibre optique par laquelle Alice envoie à Bob des impulsions lumineuses) et un canal classique qu'Ève peut écouter sans restriction, mais ne peut pas modifier. Des protocoles de cryptographie classiques permettent de réaliser un tel canal, authentifié de manière inconditionnellement sûre : Alice et Bob sont ainsi certains qu'ils se parlent bien l'un à l'autre. On ne peut pas empêcher Ève d'espionner le canal quantique, mais on peut savoir après la transmission si elle l'a fait. Il ne faut donc pas envoyer de message dans ce canal mais une suite d'éléments aléatoires, qui serviront ensuite à produire une clé s'ils n'ont pas été interceptés. Cette clé, parfaitement secrète, peut ensuite servir à chiffrer classiquement le message.

Protocoles de cryptographie quantique

Le protocole de cryptographie quantique le plus connu est désigné par l'acronyme BB84, et a été proposé par C.H. Bennett et G. Brassard en 1984. Ce protocole (*encadré 2*) a inspiré de nombreuses variantes, qui sont largement utilisées dans les systèmes opérationnels à l'heure actuelle, en employant des compteurs de photons pour détecter les signaux lumineux transmis d'Alice à Bob. Une autre famille de protocoles, que l'on appelle « protocoles à variables continues », utilise des méthodes interférométriques, que l'on appelle détections homodynes ou hétérodynes (*encadré 3*). Ils ont l'avantage d'éviter les compteurs de photons, qui posent certains problèmes technologiques aux longueurs d'ondes utilisables pour des transmissions par fibres optiques (1 550 nm).

Dans tous les cas, l'idée de base de tous les protocoles est la même : Alice envoie un signal aléatoire à Bob, en le « codant » sur deux quantités physiques « conjuguées », c'est-à-dire qui ne peuvent pas être connues simultanément d'après les inégalités de Heisenberg. Ève, ne sachant pas quelle grandeur est utilisée, doit tenter de mesurer (plus ou moins bien) les deux grandeurs simultanément : mais ce faisant, toute information significative qu'elle va acquérir sur l'une des quantités va perturber l'autre et introduire du « bruit », autrement dit des erreurs, dans la transmission entre Alice et Bob. Ces derniers pourront évaluer statistiquement ces erreurs, en comparant publiquement une partie de leurs données, qui ne seront plus utilisées par la suite. Connaissant alors un taux d'erreur (statistique), la mécanique quantique leur fournit, statistiquement aussi, la fraction de l'information dont a pu s'emparer Ève.

Encadré 2

Le protocole BB84

La grandeur physique mesurée est la polarisation d'un photon unique, qui correspond à la direction de vibrations de l'onde lumineuse. Le protocole BB84 n'utilise que des polarisations linéaires, qui peuvent se représenter comme des directions de vibrations perpendiculaires à la direction de propagation du photon. Par exemple, Alice peut choisir d'envoyer des photons polarisés horizontalement (qu'on notera « - »), verticalement (« | »), à 45° à gauche (« \ ») ou à 45° à droite (« / »). Le principe d'incertitude de Heisenberg appliqué à la polarisation de photons uniques nous dit qu'on ne peut distinguer à coup sûr que des polarisations orthogonales, qui dépendent de l'orientation de l'« analyseur » choisie pour faire la mesure. Le mieux que l'on puisse faire est de choisir une direction privilégiée, ou base, et d'obtenir une réponse binaire : si l'on choisit la base verticale, notée « + », on ne pourra avoir comme résultat que « le photon était polarisé verticalement » ou « le photon était polarisé horizontalement ». Si la polarisation du photon était inclinée de 45°, alors le résultat de la mesure sera totalement aléatoire, et aucune information ne pourra être extraite sur sa polarisation antérieure. Pour mesurer les photons inclinés de 45°, il faut utiliser une base diagonale, notée « X », qui nous dit si le photon est penché à gauche ou à droite, mais nous donne des réponses aléatoires s'il est vertical ou horizontal. Les bases « + » et « X » sont dites complémentaires ou incompatibles : il est physiquement impossible de mesurer la polarisation d'un photon simultanément dans ces deux bases.

S'il n'y a pas d'espion...

Si Alice envoie à Bob des photons polarisés aléatoirement parmi les quatre possibilités suivantes : horizontal (« - »), vertical (« | »), penché à gauche (« \ »), penché à droite (« / ») et que Bob mesure leur polarisation avec une base aléatoire (« + » ou « X »), la moitié du temps, Bob se « trompera » de base. Par conséquent, la moitié de ses mesures seront inutilisables, mais l'autre moitié lui donnera une information utile sur la polarisation envoyée par Alice (*figure 1*). Bob et Alice peuvent alors par une discussion publique rejeter les mauvais choix de base. Seuls les photons pour lesquels Alice et Bob ont choisi la même base serviront à l'élaboration de la clé, puisque ce sont les seuls pour lesquels Bob connaît la polarisation du photon émis par Alice. Un photon penché à gauche ou horizontal correspondant à un bit à 0 et un photon penché à droite ou vertical à un bit 1. Alice et Bob construisent alors leur clé secrète bit à bit. Cette clé n'était pas déterminée au début du processus, mais se construit au fur et à mesure : ce n'est pas un système de transmission d'information mais de distribution de clés. S'il n'y a pas d'espion, il n'y a pas eu de perturbation du canal et les clés d'Alice et de Bob sont identiques. Ils peuvent le vérifier en choisissant de comparer certains bits de la clé grâce au canal classique et en extrapolant le taux d'erreurs obtenu à l'ensemble de la clé. Comme on suppose que l'espion peut toujours écouter le canal classique, Alice et Bob devront « sacrifier » les bits qu'ils ont comparés et ne conserveront que les autres dans leur clé secrète.

Si l'espion essaie de tout savoir...

Si Ève essaie d'espionner la ligne, elle peut essayer de mesurer les photons envoyés par Alice, et renvoyer à Bob d'autres photons de polarisations conformes à ce qu'elle a mesuré. Mais elle se trompera aussi de base la moitié du temps, et les photons qu'elle renverra à Bob seront alors émis dans la mauvaise base, ce qui induit un taux d'erreurs de 25 % (*figure 2*). Alice et Bob peuvent alors détecter l'espion en évaluant ce taux d'erreurs par un sondage sur certains de leurs bits, qu'ils n'utiliseront pas pour la clé. En fait, l'attaque optimale d'Ève est plus subtile, mais

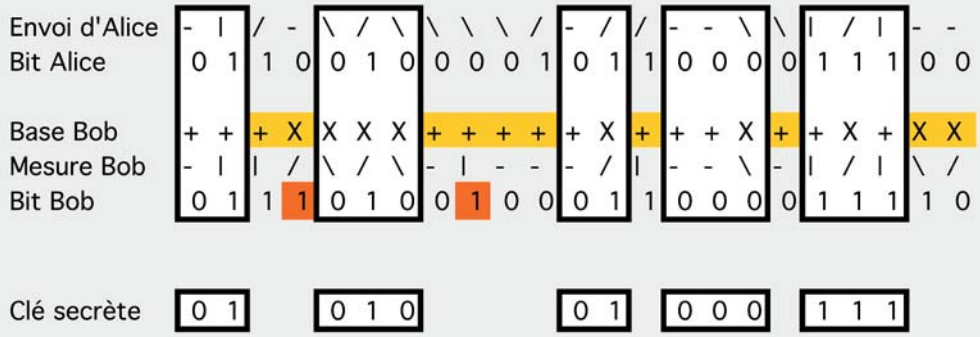

Figure 1. Échange de clé en l'absence d'espion, suivant le protocole BB84. Alice envoie des photons à Bob suivant les 4 polarisations -, \, | ou /. Bob mesure cette polarisation aléatoirement suivant les bases + et X. Il se trompe une fois sur deux (en jaune), ce qui induit des erreurs (en rouge). La clé secrète, constituée des bits correspondant aux bons choix de base, ne présente aucune erreur, ce qui garantit l'absence d'espion.

On peut remarquer qu'Alice et Bob ignorent aussi initialement si la mesure effectuée par Bob correspond bien à la grandeur aléatoirement utilisée par Alice pour envoyer son signal (voir exemples dans les encadrés). Cependant, ils peuvent s'accorder sur cette grandeur, après que Bob a effectué ses détections : cette « révélation » arrive ainsi trop tard pour Ève et elle ne peut plus lui être d'aucune utilité.

Finalement, après avoir éliminé les mesures effectuées avec des grandeurs différentes et évalué le taux d'erreurs de leur canal quantique, Alice et Bob possèdent deux chaînes de bits corrélées (mais en général différentes) et partiellement connues d'Ève. Le but de la réconciliation entre Alice et Bob est d'obtenir des chaînes identiques en discutant via un canal classique authentifié, tout en révélant le moins d'informations possible, au moyen de techniques apparentées aux codes correcteurs d'erreurs. À l'issue de

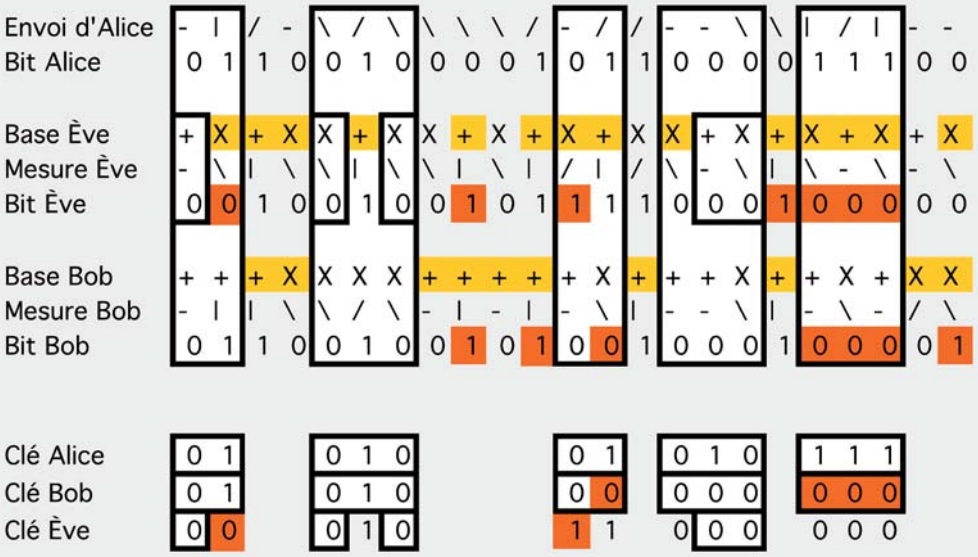

Figure 2. Échange de clé en présence d'Ève. Si Ève, l'espion, essaie de mesurer le photon envoyé par Alice et de le renvoyer à Alice, elle se trompera de base une fois sur deux (en jaune), ce qui induira un taux d'erreur de 25 % chez Bob (en rouge), même lorsqu'il aura choisi la bonne base.

induit quand même un taux d'erreurs de 11 %, aisément détectable. Si Alice et Bob mesurent un taux d'erreurs supérieur à 11 %, ils doivent donc interrompre le processus et ne pas utiliser leur clé. Si Ève peut les empêcher de communiquer secrètement, elle n'aura toutefois rien appris d'autre qu'une série de nombres aléatoires qui ne seront jamais utilisés.

Comment maintenir l'espion dans l'ignorance ?

Les choses sont donc claires si le taux d'erreurs est nul (il n'y a pas d'espion) ou s'il est supérieur à 11 % (l'espion en sait trop, et la distribution de clé est impossible). En pratique, le taux d'erreurs ne sera jamais nul pour des raisons expérimentales et, par prudence, on doit supposer que ces erreurs sont induites par un espion qui a choisi de faire des mesures partielles, plus discrètes mais moins efficaces. Il est alors possible de produire une clé secrète par un traitement informatique des données, tant que ce taux d'erreurs est inférieur à 11 %. Ce traitement supplémentaire peut en général se décomposer en deux étapes : la réconciliation et l'amplification de secret (*figure 3*).

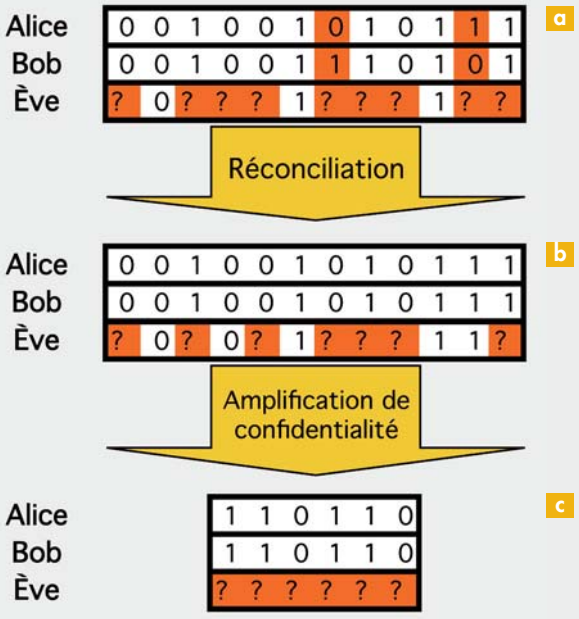

Figure 3. Génération d'une clé secrète en présence d'Ève. En général, Alice et Bob partagent initialement une chaîne de bits corrélés, partiellement connus d'Ève *(a)*. Des algorithmes de réconciliation corrigent leurs erreurs *(b)*, tout en révélant peu d'information supplémentaire à Ève. Des techniques d'amplification de confidentialité leur permettent ensuite de générer une clé plus courte, inconnue d'Ève *(c)*.

cette étape, Alice et Bob partagent une clé commune et partiellement secrète.

Ce qu'Ève sait de cette clé provient de deux sources, toutes les deux connues d'Alice et de Bob : son attaque initiale sur le canal quantique, qui peut être évaluée par le taux d'erreurs, et l'information révélée au cours de la réconciliation. La clé partiellement secrète issue de l'étape de réconciliation peut être transformée, par amplification de confidentialité en une clé plus courte, mais parfaitement secrète. Ces techniques reposent sur des fonctions de hachage qui mélangent complètement les bits de la clé initiale, la clé finale étant extraite de ce mélange, comme on mélange les cartes avant de les distribuer, pour que personne ne puisse connaître les cartes présentes dans un jeu. Ce mélange est tel que seuls Alice et Bob ont suffisamment d'informations sur la clé issue de l'étape de réconciliation pour connaître le résultat final. Les informations partielles

Encadré 3

Le protocole GG02

Les grandeurs mesurées dans les protocoles à variables continues ne sont pas les propriétés de photons individuels, mais sont les « quadratures du champ électrique » d'impulsions lumineuses. Si l'on représente le champ électrique dans un « diagramme de Fresnel » bien connu des opticiens, les quadratures sont en fait les composantes cartésiennes de ce champ, qui sont ici plus commodes à utiliser que l'amplitude et la phase (*figure 4*). Ces grandeurs sont analogues à la position et la vitesse (ou plus précisément la quantité de mouvement) d'une particule, quantités pour lesquelles le principe d'incertitude de Heisenberg a été découvert initialement. Comme la position et la vitesse, il ne s'agit pas de quantités binaires, ou même discrètes, mais des variables continues pouvant prendre une infinité de valeurs.

Pour une telle variable, le résultat d'une mesure ne donnera jamais la valeur exacte de la grandeur physique correspondante, mais une fourchette dans laquelle cette valeur se trouvera. Cette fourchette sera d'autant plus étroite que l'appareil de mesure sera bon, et sa largeur (techniquement, la « variance » de la mesure) caractérise la qualité d'un appareil de mesure. Cette variance peut en principe être arbitrairement petite pour une quadrature isolée, et il est en effet possible de la mesurer avec grande précision au moyen de dispositifs interférométriques appelés « détections homodynes ». En revanche, toute mesure ajoute un bruit inversement proportionnel à sa variance sur la quadrature complémentaire, ce qui limite la qualité des dispositifs mesurant simultanément les deux quadratures, les « détections hétérodynes ».

Cette relation d'incertitude s'applique, que les deux quadratures soient mesurées ensemble ou séparément. Ainsi, dans un protocole de cryptographie quantique, la qualité d'une mesure de l'espion, Ève, influe sur la variance observée par Alice et Bob sur la quadrature complémentaire. Ces derniers connaissent alors la précision de la mesure d'Ève. Pour convertir cette précision sur des variables continues en quantité d'information (mesurée en bits), il faut utiliser la théorie de l'information développée par C.E. Shannon pendant la guerre. Cette approche nous a permis, en 2002, de proposer un protocole de cryptographie quantique utilisant des lasers ordinaires et des détections homodynes, GG02.

En pratique, cet usage de la théorie de l'information impose l'usage de codes correcteurs d'erreurs élaborés, ce qui rend le rapport entre les grandeurs physiques continues et les bits de la clé plus indirect que pour BB84, mais le principe reste le même : il s'agit d'extraire une chaîne aléatoire secrète à partir de variables (ici continues) corrélées et partiellement connues de l'adversaire.

Les premières démonstrations expérimentales de ce protocole ont été réalisées en 2003. Depuis, la société SeQureNet a mis au point le premier appareil de distribution quantique de clés ne faisant appel qu'à des composants télécoms standards, commercialisé sous le nom de Cygnus. Il fonctionne sur un lien fibré monomode jusqu'à des distances de l'ordre de 80 km (16 dB de pertes optiques). L'équipement fournit en continu à un débit allant de quelques centaines à plusieurs dizaines de milliers de bits par seconde des clés utilisables pour réaliser différentes tâches cryptographiques, telles que l'authentification d'utilisateurs ou le chiffrement de liens réseaux haut débit. La quantité de clé produite dépend des paramètres physiques du lien fibré et, en particulier, des pertes introduites par la fibre optique et du bruit ajouté par l'introduction d'éventuels équipements de mesure. Le dispositif permet une surveillance de l'évolution de ces paramètres en cours de fonctionnement, et donc la détection éventuelle de la présence d'un espion sur le lien optique.

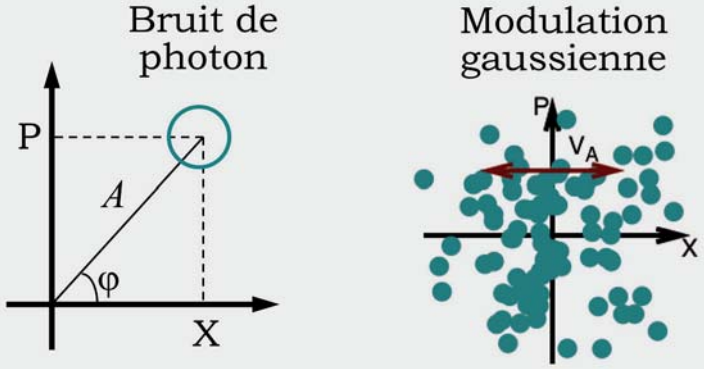

Figure 4. Les quadratures sont les composantes cartésiennes X et P du champ électrique quantifié, et ne peuvent être connues simultanément à cause des inégalités de Heisenberg. Alice module aléatoirement l'amplitude et la phase du signal qu'elle envoie à Bob, avec une dispersion V_A. Ève ne peut pas intercepter ce signal sans introduire des erreurs de transmission.

dont disposait Ève sont en revanche suffisamment brouillées à cette étape pour ne rien lui apprendre d'utile.

À l'issue de ce processus, Alice et Bob disposent tous les deux de la même clé (*figure 3*). Celle-ci est parfaitement secrète, quelles que soient les capacités technologiques de l'espion éventuel. Ils peuvent alors l'utiliser dans un protocole de cryptographie classique, dont la sécurité est aussi grande que celle de la clé qui a été échangée.

Avantages et inconvénients de la cryptographie quantique

La cryptographie quantique présente un avantage fondamental par rapport à sa contrepartie classique : lorsqu'elle est correctement mise en œuvre, elle est inviolable par principe, quelles que soient les capacités technologiques de l'adversaire. Un message chiffré aujourd'hui avec une clé transmise par cryptographie quantique ne pourra jamais être décrypté sans que la clé soit rendue publique. Les systèmes de cryptographie classiques sont au contraire perpétuellement menacés d'obsolescence, et la protection qu'ils fournissent ne peut guère être évaluée au-delà de quelques dizaines d'années.

Le revers de cette inviolabilité se retrouve sur les contraintes imposées sur le support physique constituant le canal quantique : les pertes et les fluctuations de polarisation sont les problèmes majeurs des transmissions par fibres optiques, dont la portée maximale pour la cryptographie quantique est aujourd'hui de l'ordre de 100 km ; des distances supérieures ont été atteintes, mais avec des débits très faibles. Les systèmes de transmission à l'air libre sont eux limités par des difficultés de visée et de lumière parasite. Depuis un peu moins de dix ans, des réseaux chiffrés ont été réalisés entre des bâtiments situés dans une même agglomération : à Vienne en 2008 (http://www.secoqc.net/html/conference/), à Tokyo en 2010 (http://www.uqcc.org/QKDnetwork/), et un réseau est actuellement en installation dans la région de Washington (http://www.battelle.org/media/press-releases/-first-commercial-

quantum-key-distribution-protected-network-in-u.s).

Quelle cryptographie quantique demain ?

Une technologie sur le point de sortir des labos

Bien qu'encore très éloignés de dispositifs « grand public », des systèmes de distribution quantique de clé commencent à être commercialisés. Les détecteurs de photons uniques disponibles aux longueurs d'onde télécom (1 550 nm) limitent la portée dans les fibres à quelques dizaines de kilomètres et les débits réalisés restent très modestes. Les dispositifs à variables continues, bien que moins répandus à l'heure actuelle, ont l'avantage d'éviter complètement les problèmes liés aux compteurs de photons ; ils demandent en revanche des logiciels de traitement des données (codes correcteurs d'erreurs) très sophistiqués. Dans ce contexte, l'installation de réseaux de distribution quantique de clés commence à être envisagée par des institutions financières.

Des systèmes d'échange de clés terre-satellite sont également en cours de conception en Europe, aux États-Unis, et surtout en Chine, essentiellement pour des usages diplomatiques et militaires. Un tel système permet en effet de contourner les limitations de portée – si l'on admet que l'espion n'est pas dans le satellite – et ne nécessite pas de déploiement de réseau de fibres, avantage crucial sur un champ de bataille.

Les systèmes de cryptographie quantique sont donc bien sortis des laboratoires, mais sont encore confinés à des applications spécifiques, pour lesquelles l'exigence de sécurité l'emporte largement sur les considérations de coût ou de simplicité.

Des progrès technologiques…

Les recherches actuelles dans le domaine de la cryptographie cherchent à contourner plusieurs limitations d'ordre technologique. Des progrès ont été faits sur les photodiodes à avalanches utilisées pour détecter les photons uniques, mais les systèmes les plus performants requièrent un refroidissement dans l'hélium liquide, peu commode pour des dispositifs commerciaux. Du côté des variables continues, ce problème n'existe pas mais il est remplacé dans une certaine mesure par une plus grande exigence sur les logiciels de correction d'erreurs, qui ont aussi fait des progrès considérables. Cela a permis d'augmenter à 80 km la distance « pratique » de distribution de clé par cette technique.

Il est important de remarquer que, dans tous les cas, les protocoles doivent être mis en œuvre correctement : comme en cryptographie classique, des maladresses de réalisation peuvent ouvrir des « canaux cachés », qui peuvent être utilisés par un espion. Il ne faut pas oublier en effet qu'une « preuve de sécurité » est essentiellement un théorème mathématique qui repose sur des hypothèses, qui peuvent physiquement être satisfaites, mais qui ne le sont pas en cas d'erreur de conception de l'appareillage : plusieurs erreurs de ce type ont eu quelques échos dans la presse.

… et théoriques

À plus long terme, des systèmes utilisant des variables continues, fondées sur des systèmes de communication cohérents, devraient permettre de remplacer les détecteurs de photons uniques par des photodiodes usuelles, beaucoup plus rapides, efficaces et nettement moins chères. Une intégration plus poussée des dispositifs, permettant de réduire leur encombrement et leur coût, est également envisageable. Des travaux théoriques se poursuivent aussi pour rendre les preuves de sécurité à la fois très générales et très proches de la réalité des dispositifs concrets.

D'autres voies de recherche à long terme sont poursuivies, tant sur les plans théoriques qu'expérimentaux, comme la possibilité de réaliser des répéteurs quantiques, l'étude d'autres fonctions cryptographiques que la distribution de clés, comme par exemple le tirage à pile ou face « à distance ». La cryptographie quantique est donc actuellement à la fois un domaine scientifique très actif, et un domaine industriel émergent : ce double aspect est au cœur du développement actuel des technologies quantiques.