COMPRENDRE
LA DISTRIBUTION QUANTIQUE DE CLÉ POUR DES COMMUNICATIONS SÛRES

Corentin LANORE* et Jean-Daniel BANCAL
Université Paris Saclay, CEA, CNRS, Institut de physique théorique, 91191 Gif-sur-Yvette, France
***corentin.lanore@ipht.fr**

La distribution quantique de clé tire profit des lois de la physique quantique pour étendre une clé secrète entre deux utilisateurs distants. Cela leur permet de communiquer avec la garantie qu'aucun acteur extérieur n'est en mesure de déchiffrer leurs échanges. Après quarante ans de développements théoriques et expérimentaux, la sécurité pratique de cette technologie quantique est maintenant à portée de main.

https://doi.org/10.1051/photon/2025313055

Article publié en accès libre sous les conditions définies par la licence Creative Commons Attribution License CC-BY (https://creativecommons.org/licenses/by/4.0), qui autorise sans restrictions l'utilisation, la diffusion, et la reproduction sur quelque support que ce soit, sous réserve de citation correcte de la publication originale.

La vie privée est un aspect important de notre société. Lorsque l'on discute entre amis ou en famille, par exemple, on sait à qui on s'adresse. Cet *a priori* est remis en question avec l'essor de la communication en ligne où nos échanges peuvent traverser la planète avant d'atteindre leurs destinataires.

La communication sur un réseau public présente des risques lorsque les informations transmises sont sensibles. Or, il est commun de transmettre des données médicales à destination d'un médecin sur internet, ou bien les requêtes bancaires d'un site marchand permettant de valider un achat. On imagine aisément les conséquences que pourraient avoir ces communications si elles n'étaient pas systématiquement chiffrées. En offrant des garanties d'intégrité et de sécurité pour nos informations transmises électroniquement, la cryptographie – science du chiffrement – tient un rôle important dans notre société connectée.

En effet, les protocoles cryptographiques permettent d'accomplir certaines tâches avec des garanties de sécurité établies au moyen de preuves mathématiques. Comme toute démonstration, ces preuves reposent sur des hypothèses. Le contexte de la communication à distance impose un ensemble d'hypothèses minimales dites "classiques" (*c.f.* Encart 1). Cependant, les protocoles de chiffrement actuels ne permettent pas d'obtenir une sécurité dans ce cadre simple et font appel à des hypothèses supplémentaires, comme l'hypothèse dite de "complexité", qui réduisent le niveau de sécurité.

L'idée sous-jacente à l'hypothèse de complexité est que si le déchiffrement d'un message est en ● ● ●

principe possible mais requiert un effort de calcul qu'un supercalculateur actuel ne peut atteindre en un temps raisonnable, alors la garantie de sécurité est effective. Un problème complexe souvent utilisé à cet effet est le problème de la factorisation, pour lequel aucun algorithme classique efficace n'a été trouvé depuis l'antiquité. L'essentiel des protocoles cryptographiques actuels, y compris RSA, Diffie-Hellman ou même les courbes elliptiques reposent sur ce principe.

Cependant, cette sécurité est aujourd'hui mise à mal. On sait en effet que l'ordinateur quantique couplé à l'algorithme de Shor promet à terme le décryptage des messages basés sur cette hypothèse de complexité en un temps raisonnable. Les défis technologiques à surmonter pour réaliser un tel déchiffrement sont encore importants, ce qui laisse le temps de préparer une réponse. Concrètement, deux pistes sont envisagées :

1. Élaborer de nouveaux protocoles classiques qui prennent en compte les capacités d'un ordinateur quantique. Il s'agit de la cryptographie post-quantique.
2. Élaborer des protocoles fondamentalement nouveaux qui tirent profit des lois de la physique quantique, c'est ce que propose la distribution quantique de clé.

Ces deux approches ont chacune des avantages et des inconvénients qui leur sont propres. D'un côté, la cryptographie post-quantique est à priori facile à mettre en œuvre car elle se résume à la mise à jour des algorithmes de chiffrement existants vers de nouvelles normes en cours de définition. Cependant, sa sécurité est intrinsèquement limitée, car sa démonstration reviendrait à résoudre des problèmes considérés comme extrêmement difficiles, du type P=NP. En l'absence de preuve de sécurité complète, on ne peut qu'espérer que les protocoles choisis tiennent le coup.

De l'autre côté, la solution quantique est plus difficile à mettre en œuvre : elle requiert des équipements dédiés et un certain nombre de défis technologiques doivent encore être relevés avant qu'elle ne puisse être plus largement adoptée. Cependant, la théorie quantique offre ce que les protocoles classiques ne parviennent pas à atteindre: une sécurité forte, prouvée sans condition supplémentaire que les hypothèses cryptographiques classiques. En voici le principe.

DISTRIBUTION QUANTIQUE DE CLÉ DÉPENDANTE DES DISPOSITIFS

Le chiffrement quantique s'appuie sur un protocole classique simple, appelé le "masque jetable". Cette

LE SCÉNARIO CRYPTOGRAPHIQUE

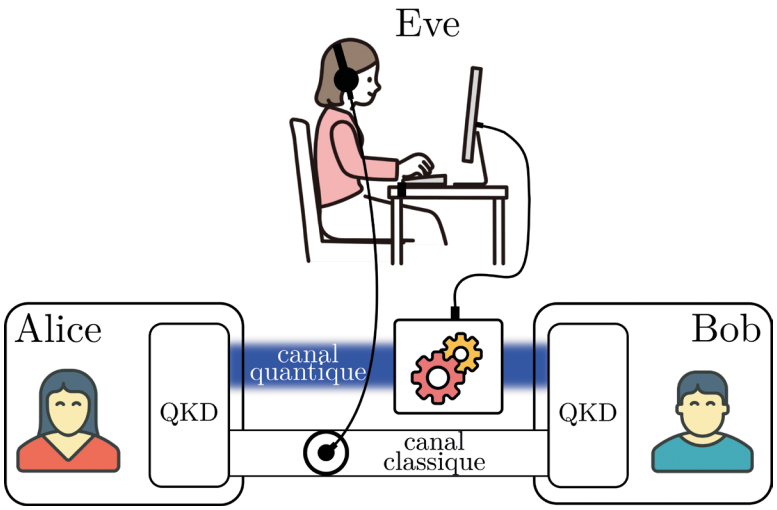


Figure 1. Distribution quantique de clé en présence d'un adversaire. Remerciements : pixelbazaar (Alice et Bob), soco-st (Eve), SVG Repo (Engrenage)

Deux utilisateurs distants, communément appelés Alice et Bob, souhaitent communiquer de façon secrète. Ils se font confiance, mais leur canal de communication est accessible à un adversaire, Eve, qui désire écouter leur conversation.
Eve est cependant limitée dans ses actions. Par exemple, elle n'a pas accès aux laboratoires d'Alice et de Bob, sinon elle pourrait directement lire le message secret sur leur écran. De plus, on peut supposer que leurs opérations classiques se déroulent comme prévu, car elles peuvent être vérifiées par la suite si nécessaire. Finalement, comme le message est inconnu de l'adversaire, cela veut dire qu'Alice et Bob sont en mesure de générer des nombres dont Eve n'a pas connaissance. Ces conditions définissent les hypothèses cryptographiques classiques sous lesquelles on souhaite garantir la sécurité.
Notons qu'il est inutile pour Eve d'interrompre la communication entre Alice et Bob ou de modifier le contenu de leurs messages classiques, sinon ils se rendraient compte de sa présence et arrêteraient de communiquer. En revanche, Eve peut perturber les systèmes quantiques échangés sans se faire remarquer.

méthode permet à deux personnes de communiquer de façon confidentielle du moment qu'elles partagent une clé secrète suffisamment longue. Le problème se réduit ainsi à l'extension d'une clé secrète à distance (Encart 2). Or cette étape n'est pas réalisable avec des moyens classiques et nécessite donc une description quantique.

Le premier protocole de distribution quantique de clé, dont la sécurité ne dépend pas d'une hypothèse de complexité, a été proposé en 1984 par Charles Bennett et Gilles Brassard (BB84). Il peut être compris dans un scénario basé sur l'intrication, et porte alors le nom de BBM92 [1]. Dans ce protocole, des états intriqués sont distribués à Alice et Bob, sous la forme de photons intriqués en polarisation par exemple, et sont mesurés localement dans des directions choisies (voir Figure 3).

Notons que d'autres formes d'intrication, comme en énergie-temps, peuvent également être utilisées. Différents degrés de liberté quantiques ont par ailleurs inspiré une variété de protocoles de distribution quantique de clé. On peut mentionner les protocoles à variables continues inspirés des champs optiques continus, ainsi que les protocoles à référence de phase distribuée inspirés par les impulsions laser faibles.

Un état maximalement intriqué a la propriété que lorsque ses deux particules sont mesurées dans la même direction, les résultats obtenus sont à la fois identiques pour les deux particules et aléatoires, c'est à dire imprédictibles pour toute tierce personne. C'est exactement ce qu'on attend d'une clé secrète partagée : qu'elle soit partagée entre Alice et Bob, et aléatoire. Ainsi, si les utilisateurs sont en mesure de se convaincre qu'ils partagent bien un état maximalement intriqué, ils peuvent être certains que leurs résultats forment une clé secrète.

Après avoir mesuré tous leurs photons, Alice et Bob annoncent leurs choix de mesures respectifs et révèlent une partie de leurs résultats. En fonction de ces informations, et en connaissant les mesures effectuées, ils en déduisent si les états distribués ont été suffisamment intriqués pour former une clé. Ils appliquent alors un ensemble de traitements classiques à leurs données afin d'extraire la clé finale.

Si tout se passe bien, la sécurité de la clé obtenue ainsi peut être formellement prouvée. Cependant, l'histoire a montré que ce n'est pas parce qu'un protocole est théoriquement sûr que son implémentation expérimentale l'est également. Pour que la sécurité tienne en pratique, il faut que le modèle utilisé dans l'analyse de sécurité corresponde exactement à l'implémentation physique.

ATTAQUES ET AMÉLIORATIONS

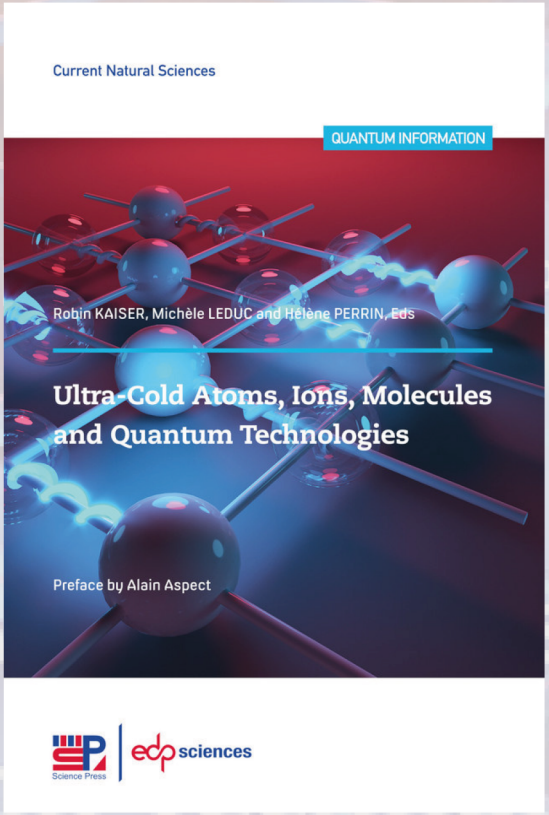
En effet, plusieurs attaques ont mis en évidence l'impact que peut avoir un décalage entre la modélisation physique des systèmes quantiques et leur comportement réel [2]. "L'attaque par aveuglement" en est un exemple, qui ouvre une faille de sécurité en faisant fonctionner les détecteurs d'Alice et Bob dans un régime différent de celui pour lequel ils ont été prévus [3].

Une réponse efficace à cette attaque a été apportée par les protocoles dits "indépendants des dispositifs de mesure". ● ● ●

Ultra-cold Atoms, Ions, Molecules and Quantum Technologies

By
Robin Kaiser,
Michèle Leduc,
Hélène Perrin

Preface By
Alain Aspect



The field of cold atoms was born fourty years ago and today remains a theme regularly awarded Nobel Prizes and at the forefront of physics research. This book presents the most recent developments and traces the exceptional growth of this field over the last years.

Also available in e-book format
For sale on
laboutique.edpsciences.fr

ISBN : 978-2-7598-2745-9
168 illustrated pages
Price : 95 €

Prix Roberval

LE MASQUE JETABLE

Nombre de méthodes de chiffrement ont été inventées à travers les siècles sans être nécessairement sûres. Il en existe cependant dont la sécurité est prouvée mathématiquement, c'est le cas du "masque jetable". Cette méthode repose sur une clé secrète initialement partagée entre Alice et Bob. Pour communiquer secrètement le message binaire "011001" au moyen du masque jetable, Alice encode son message en effectuant l'addition binaire (modulo 2) entre chaque chiffre du message et de la clé partagée "111011". Elle envoie ensuite le résultat "100010" dans un canal public (internet par exemple) à Bob. Il lui suffit alors de faire l'addition binaire avec sa clé (identique à celle d'Alice) pour retrouver le message initial.
Cette méthode est sûre, car le message envoyé sur le canal public est totalement aléatoire pour quelqu'un qui n'a pas accès à la clé de chiffrement. Cependant, la clé doit être aussi longue que le message envoyé et elle ne peut être réutilisée pour envoyer un second message. Dans une communication continue, il faut donc être capable d'allonger une clé secrète de sorte à compenser la longueur de clé qui est consommée lors de chaque étape de communication. La distribution quantique de clé résout ce problème en permettant d'étendre une clé secrète à volonté.

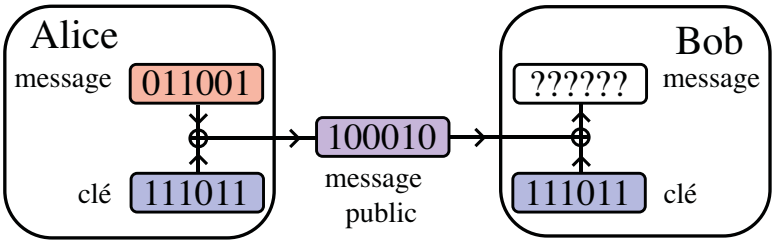


Figure 2. Illustration de l'utilisation du masque jetable

L'idée est de ne pas faire confiance à la caractérisation des détecteurs lors de la preuve de sécurité. Ainsi, la sécurité obtenue ne dépend pas de l'adéquation entre le fonctionnement réel des détecteurs et leur comportement attendu, et reste valide si les détecteurs sont aveuglés.

Mais l'idée de se protéger des attaques en réduisant la confiance sur les appareils quantiques peut être poussée plus loin. En effet, comme les mesures, les sources quantiques peuvent également se comporter différemment de ce qui est attendu d'elles, ouvrant la porte à un nouveau décalage entre théorie et expérience.

La distribution de clé indépendante des dispositifs quantiques remplit cette mission en ne reposant sa sécurité sur la caractérisation d'aucun appareil quantique (Encart 4). Suite à une première proposition dans cette direction en 1991 par Artur Ekert [4], une preuve théorique complète a été obtenue en 2014 [5] et une première réalisation expérimentale en 2022 [6].

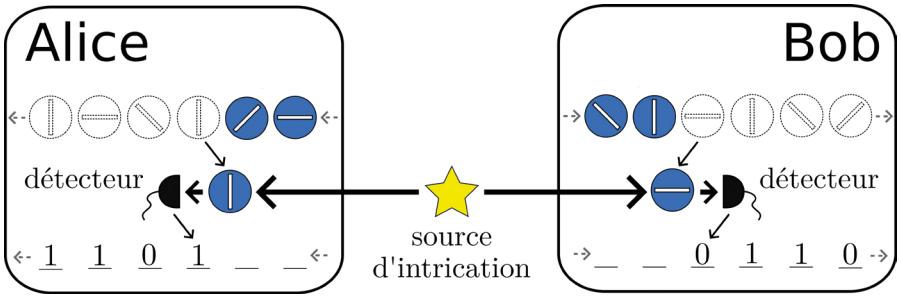
La réalisation de ce protocole reposant sur une modélisation quantique simplifiée ouvre la voie à un niveau de sécurité sans précédent dans l'histoire des communications à distance. En effet, il permet finalement de garantir la sécurité des communications uniquement au moyen des hypothèses cryptographiques classiques. La sécurité obtenue est ainsi pratique et non plus seulement théorique.

CONCLUSION

La distribution quantique de clé fournit un moyen de communiquer sûr, dont la sécurité ne repose pas sur une hypothèse de "complexité" qui pourrait être mise à mal à tout moment. Longtemps limitée par le décalage entre description théorique et réalité expérimentale, la distribution quantique de clé a maintenant atteint une sécurité pratique, qui fait entièrement abstraction des détails quantiques. Son implémentation est exigeante mais reste sensiblement plus accessible que d'autres technologies quantiques en développement comme le calcul quantique universel par exemple.

Les défis à relever pour rendre cette sécurité accessible à tous sont encore multiples. En particulier, une amélioration des capacités à produire des états intriqués à la fois

Figure 3. Exemple d'installation de distribution quantique de clé basée sur l'intrication. Des états maximalement intriqués $|\phi^+\rangle = (|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)/\sqrt{2}$ (ici en polarisation) sont partagés. Pour chaque état reçu, Alice et Bob font des choix de mesure, représentés par les filtres de polarisation, et notent si leur détecteur clique ou pas. Ces résultats de mesure permettent de vérifier la qualité de la source et forment la clé brute.



LA DISTRIBUTION DE CLÉ INDÉPENDANTE DES DISPOSITIFS QUANTIQUES EMPLOYÉS

Afin de protéger la cryptographie quantique des attaques sur l'implémentation physique (interférences extérieures sur les sources ou sur les détecteurs), il est nécessaire de faire abstraction des dispositifs employés. Cela revient à considérer les appareils comme des "boîtes noires", dont on ne connaît pas initialement les détails. Leur description doit alors être déduite des interactions classiques effectuées avec ces appareils : les choix et les résultats des mesures.
Dans ce contexte, la sécurité se montre en effectuant un test de Bell. En effet, la violation d'une inégalité de Bell implique que l'état distribué est intriqué, et garantit l'imprédictibilité des résultats de mesure. Effectuer un test de Bell est exigeant expérimentalement, mais les avancées expérimentales ont récemment permis la première extension de clé indépendante des dispositifs quantiques [6].

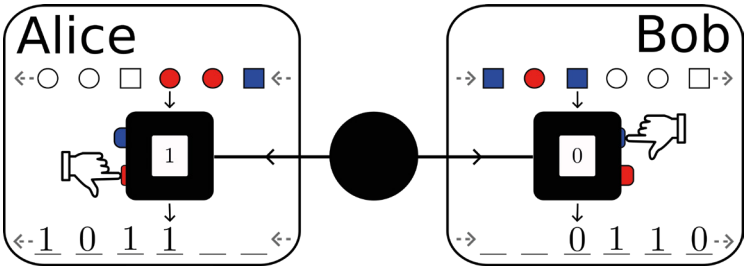


Figure 4. Illustration de la distribution de clé indépendante des dispositifs quantiques.

de bonne qualité et à longue distance est capitale. Cet effort passe par des avancées sur les briques élémentaires comme les sources de photons, ainsi que par le développement des répéteurs et des réseaux quantiques. Le taux de clé actuellement disponible sur les systèmes de cryptographie quantique commerciaux reste encore bien en deçà des débits de la plupart des communications et demande donc aussi à être augmenté. De plus, une réduction de la taille des implémentations expérimentales, par exemple au moyen de circuits intégrés optiques, permettrait de favoriser une adoption de la cryptographie quantique à grande échelle. À terme, ces efforts permettront à la fois d'atteindre une sécurité optimale et de démocratiser l'accès à cette technologie.

RÉFÉRENCES

[1] C. H. Bennett, G. Brassard, N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992)
[2] D. Rusca, N. Gisin, arXiv:2411.04044
[3] L. Lydersen *et al.*, Nature Photonics **4**, 686 (2010)
[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
[5] U. Vazirani, T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014)
[6] D. Nadlinger *et al.*, Nature **607**, 682 (2022)


CIAO
IMPROVE YOUR TELESCOPE RESOLUTION
Adaptive Optics solution
VIS-NIR / SWIR
Astronomy, SSA
FSO, SatCom & Quantum com.
www.imagine-optic.com
sales@imagine-optic.com
+33 1 64 86 15 60
imagine optic