Compte Rendu : Avancements quantiques en sécurité

Yohann Bertrand

BERY77060100

3e année au baccalauréat

Université du Québec à Trois-Rivières

Département de physique

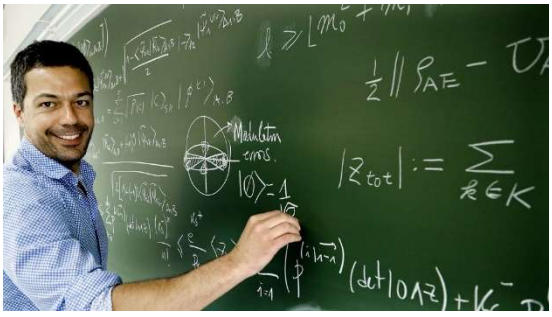
Introduction

De nos jours, nous envoyons à chaque instant des millions d'informations sensibles à chaque instant. Depuis les informations bancaires de monsieur/madame, tout le monde à des informations confidentielles du gouvernement. Toutes ces données doivent absolument être cryptées pour assurer le fonctionnement de notre société. En ce moment, il existe de nombreux algorithmes de cryptage répandu à travers le monde, mais la méthode la plus populaire consiste en un système de cryptage qui base sa sécurité sur la difficulté de nos ordinateurs ou de l'homme à factoriser de très larges nombres. Le système RSA en particulier est basé sur la supposition que si l'on prend deux nombres premiers extrêmement grands et qu'on les multiplie, il est virtuellement impossible de trouver avec le nombre résultant les deux nombres de départ. Par contre, pour un ordinateur quantique, qui peut faire une multitude de calculs simultanément, briser ce genre d'algorithme deviendra non seulement possible, mais facilement réalisable. Et donc, lorsqu'un ordinateur quantique complètement fonctionnel sera réalisé, ce qui semble de plus en plus probable, presque toute la cryptographie conventionnelle sera obsolète. C'est dans cette optique que l'article : « A quantum leap in security »[1] de Marcos Curty, Koji Azuma et Hoi-Kong Lo explique des nouveaux protocoles de sécurité basée sur la cryptographie quantique qui pourrait devenir la nouvelle norme en matière de sécurité de demain.

[1] Voir référence 1

L'article se divise en plusieurs parties, en premier, on a une introduction qui porte sur la nécessité de trouver des algorithmes de cryptographie résistant à des ordinateurs quantiques. Ensuite, on explore une des solutions de cryptage quantique qui semble très prometteur : le système QKD (**Q**uantum **K**ey **D**istribution : distribution de clé quantique) et l'on explique la base de son fonctionnement. Après quoi, on expose les différents progrès actuels réalisés et les défis restants encore à surmonter. Puis, on étudie comment le principe d'échange d'intrication pourrait renforcer la sécurité des installations QKD. Par la suite, l'Article nous décris le système MDI QKD (**M**esurement **D**evice **I**ndependent: indépendant du système de mesure) et nous expose ses avantages et inconvénients. Il nous montre aussi le système TF QKD (**T**win **F**ield: champs jumeaux), une autre alternative avec ces avantages et ses inconvénients. Finalement, il nous laisse entrevoir les possibilités d'application de ces systèmes ainsi que des modifications qui les rendrait encore plus versatiles qui sont encore en développement.

Le but de l'article est de nous présenter des systèmes fonctionnels de cryptage quantique utilisant l'interférence quantique et de montrer l'état de leur développement. Il décrit avec beaucoup d'attention les principes fondamentaux de ces systèmes (surtout le fonctionnement de l'interférence quantique pour générer des états de Bell) et leur fonctionnement général.



Marcos Curty Alonso est professeur en théorie du signal et de communication à l'université de Vigo en Espagne. Ayant fait ses études en ingénierie des télécommunications il a complété son doctorat en 2004 sous la supervision de David J. Santos, au sein du groupe de recherche en photonique et communications de l'université de l'université de Vigo. Il a aussi fait des études à l'université Friedrich-Alexander d'Erlangen-Nuremberg en Allemagne où il a rejoint le groupe de théorie de l'information quantique et obtenu un doctorat en physique théorique en 2006 sous la supervision du professeur Norbert Lütkenhaus. Il a ensuite été chercheur postdoctoral à l'université de Toronto dans le groupe de recherche du professeur Hoi-Kong Lo et à l'institut de calcul quantique de l'université de Waterloo dans le groupe de recherche du professeur Norbert Lütkenhaus. Il a aussi été professeur adjoint au département de génie électronique et de communication de l'université de Saragosse en Espagne.[2]

[2] Voir référence 2

Koji Azuma est un chercheur très estimé des laboratoires de recherche de base NTT (NTT BRL) au Japon et un membre du groupe de recherche en physique quantique théorique du laboratoire de science et technologie quantique et du centre de recherche de physique quantique théorique au NTT BRL. Ayant obtenu sa maitrise en 2007 avec sa thèse intitulée « Roles of entanglement in quantums operations » supervisée par le professeur Naoto Nagaosa et son doctorat en Science en 2010 pour sa thèse intitulée « Long-distance quantum communication with remote nondestructive parity measurement » supervisé par le professeur Nobuyuki Imoto. Il a passé ses dernières années comme chercheur dans plusieurs groupes de recherche au NTT BRL. Passant de simple chercheur à chercheur réputé à chercheur senior. Boursier de 2007 à 2010 de la société du Japon pour la promotion des sciences (DC1), ces intérêts de recherche portent sur la théorie de l'information et le traitement de l'information quantique.[3]

Hoi-Kong Lo est un professeur du département d'ingénierie électrique et informatique et du département de physique de l'université de Toronto. Il a réalisé un baccalauréat en mathématique à l'université de Cambridge en 1989, puis une maitrise et un doctorat de physique à l'institut de technologie de Californie (Caltech) en 1991 et 1994. Il fut ensuite un membre de l'institut de recherche avancée de Princeton de 1994 à 1996. Il rejoint le laboratoire Hewlett-Packard à Bristol (Royaume-Uni) comme chercheur postdoctoral en 1996 et en 1997 il devint un membre senior de l'équipe technique, là-bas. Il est ensuite devenu chef scientifique et vice-président senior de « MagiQ technologies inc. » en 1999, un leader du marché de la commercialisation de l'information quantique. En 2003, il rejoint finalement l'université de Toronto comme professeur associé ou il deviendra un professeur à temps plein en 2009. Il a été notamment boursier de l'institut canadien de recherche avancé (CIFAR) en 2010 et titulaire de chaire de recherche canadienne

[3] Voir référence 3

depuis 2003 en plus de plusieurs autres prix et distinctions gagnés tout au long de sa carrière en recherche. Son intérêt de recherche principal est le traitement de l'information quantique, en particulier la cryptographie quantique. Il est d'ailleurs l'un des premiers à démontrer l'impossibilité d'une classe entière de protocole de cryptographie quantique incluant la mise en gage quantique (quantum bit commitment) rectifiant une croyance erronée du milieu. Il a aussi apporté une preuve de la sécurité du protocole QKD.[4]

Synthèse :

La compréhension du protocole de QKD et par conséquent des protocoles MDI QKD et TF QKD requirent une connaissance générale de plusieurs concepts de mécanique quantique et de la cryptographie en générale. C'est pourquoi nous ferons un **résumé** avant d'entrer dans les concepts étudier par l'article. Ensuite, nous expliquerons le fonctionnement en détail du **protocole QKD**. S'en suivra l'explication des protocoles améliorés du QKD : le **MDI QKD** et le **TF QKD**. Finalement, on verra des pistes d'améliorations de ces protocoles et en général **l'avenir de la cryptographie quantique.**

Résumé

Pour comprendre le fonctionnement du système QKD, il faut savoir ce qu'est l'intrication (ou l'enchevêtrement) quantique. Deux particules sont dites intriquées lorsqu'on ne peut expliquer leur état séparément, ensemble elles forment un système lié qui ne peut être décrit qu'avec 1 seule fonction d'onde. L'état de l'un est complètement dépendant de celui de l'autre, peu importe la distance qui sépare les deux particules. Par exemple si nous avons 2 particules intriquées et qui ont chacune 50 % de chance d'être dans l'état 1 et 50 % d'être dans l'état 2. Si l'on observe chacune des particules séparément on pourrait vérifier que les probabilités sont correctes pour chacune, mais si l'on comparait les résultats des deux particules on remarquerait que lorsque la première particule était dans l'état 1 la deuxième l'était aussi et la même chose pour l'état 2.

Cette particularité avait beaucoup irrité des physiciens du début du 20^{e} siècle comme Einstein, Podolsky et Rosen qui ont créé le paradoxe EPR qui montrait que si deux particules intriquées

[4] Voir référence 4

(localisé à un point précis de l'espace-temps) étaient séparées par une distance très grande et qu'on mesurait leur état simultanément (dans l'optique de la simultanéité de la relativité restreinte) la particule 1 n'aurait pu « avertir » la particule 2 de l'état qu'elle a choisi sans voyager plus vite que la lumière ce qui briserait le principe de causalité. De ce paradoxe, ils concluaient que la mécanique quantique n'était pas complète et ne décrivait pas entièrement la réalité. Einstein en a donc conclu que la mécanique quantique renfermait peut-être des variables cachées qui nous seraient inconnues, ce qui reviendrait à dire que les particules auraient déjà convenu entre eux de leur état au préalable, mais que nous n'avons pas la capacité actuelle de connaitre cet état.

Niels Bohr a répondu que la fonction d'onde n'était pas localisée dans un point fixe de l'espace, mais qu'elle existait bien dans tous les points de l'espace simultanément. Plus tard, John Stewart Bell proposera une façon de mettre en pratique le paradoxe pour déterminer une fois pour toutes la nature de la mécanique quantique. Sans entrer dans les détails de son expérience, il a réussi à déterminer qu'une théorie à variable cachée locale ne pouvait pas représenter la réalité. Pour ce faire, il a conçu des inégalités qu'un système à variable cachée locale (comme un système classique) devrait respecter et lorsqu'on testait un cas comme les cas EPR, ces inégalités (qu'on appelle les inégalités de Bell) sont systématiquement brisées.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B)$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B)$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$$

Figure 1 : les 4 états de Bell

Plus encore, il a découvert que certains états intriqués violent plus ou moins cette inégalité et que 4 états particuliers maximisent la violation de l'inégalité et donc ont une intrication maximale : les états de Bell. Ces états sont particulièrement utiles pour représenter des qubits, car lorsqu'on mesure un qubit dans un état particulier et que l'on connait l'état de Bell décrivant le duo de qubits on connait exactement la valeur de l'autre qubit (0 : 0 et 1 : 1 pour les états Φ et 0 : 1 et 1 : 0 pour les états Ψ).

Protocole QKD

Le protocole QKD repose sur le fait qu'on ne peut prendre de l'information sur un système quantique sans le perturber. Le principe général est de transférer un string (chaine de caractère) de bits secrets qui sera appelé dans ce compte rendu la clé cryptographique entre deux parties que l'on appellera Alice et Bob. Aussi nous voulons empêcher un troisième parti que l'on appellera Eve d'intercepter la clé. Dans les faits, Eve en plus de représenter une personne

malveillante qui tente consciemment d'intercepter le message représente tous les défauts de communication qui pourrait perturber l'envoi ou la réception de la clé comme le bruit.

Dans les faits, le protocole QKD est un dérivé du protocole du masque jetable, un procédé datant du début du 20e siècle. Dans celui-ci, on crée une clé aussi longue que le message, avec des caractères complètement aléatoires et l'on utilise la clé pour crypter et décrypter le message et ensuite on jette la clé. Si ces étapes sont respectées, la sécurité du message crypté est théoriquement absolue. Dans notre monde ou les messages à transmettre sont des 0 et des 1 le principe utilisé pour crypter ses messages est la fonction OU exclusif qui a la particularité que lorsqu'on applique la fonction avec la clé de cryptage pour décrypter le message on n'a qu'a réappliqué la fonction avec la même clé. Bien sûr dans notre monde la difficulté de ce système c'est de transmettre la clé secrète sans qu'elle soit interceptée, ce qui nous amène à l'utilisation de l'intrication quantique.

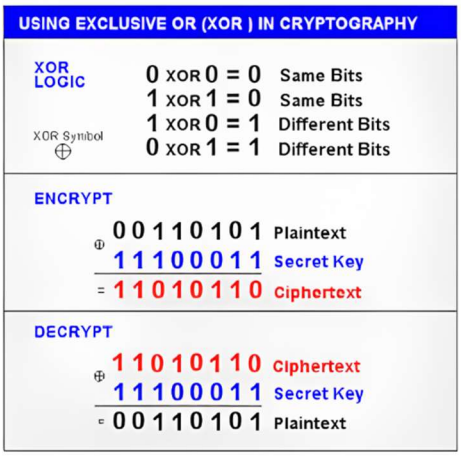


Figure 2 : OU exclusif en cryptographie

Pour distribuer la clé de manière sécurisée, on utilise un état intriqué entre Alice et bob. Par exemple, ils peuvent créer ensemble l'état $|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}} (|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)$ et donc ils s'entendent pour dire que l'état $|0\rangle$ est égale au bit 0 et $|1\rangle$ au bit 1 ils ont alors une clé secrète. Bob doit bien sûr inverser la valeur de ses bits pour avoir les mêmes qu'Alice. En créant et mesurant successivement des milliers d'états comme celui-ci ils peuvent former une clé de cryptographie quantique permettant de crypter un message.

Avec cette technique, des chercheurs ont développé des systèmes QKD avec des fréquences de 10 GHz, des distances de transmission atteignant 421 km et ils ont même réussi à multiplexer des signaux quantiques avec des signaux classiques, ce qui est essentiel pour implanter ce type de technologie dans nos infrastructures actuelles et qui cela permet en plus d'augmenter le taux de clé. Le multiplexage est le processus par lequel on envoie plusieurs signaux par le même médium par exemple en envoyant plusieurs signaux avec chacun leur fréquence propre comme la radio.

Pour atteindre de plus grande distance, on utilise en ce moment des réseaux avec nœuds de confiance qui est ni plus ni moins qu'une chaine ou chaque nœud représente un système QKD qui fait le lien avec ses plus proches voisins. La beauté de ce système est que chaque nœud peut encore crypter le message qu'il reçoit et faire passer sa clé au destinataire, qui lui pourra décrypter le message entièrement en appliquant toutes les clés les unes à la suite des autres. Une autre façon d'augmenter la distance de communication serait par l'utilisation de répéteur quantique qui pourrait augmenter la distance de propagation de l'état intriqué virtuellement infiniment. Car même si des états intriqués peuvent être séparés par une distance théoriquement infinie, en pratique, les particules qu'on utilise peuvent être perturbées et se dissiper. Plus une particule parcourt une grande distance, plus les chances qu'elle n'atteigne pas sa cible augmentent, ce qui limite actuellement la plupart des technologies quantiques à grande échelle.

Malgré tout, le système QKD comporte encore plusieurs failles de sécurité potentielles. En effet, il est possible pour Eve de voir quel détecteur s'active et donc de décrypter la clé. Par exemple, il a été démontrer qu'avec un détecteur à photons simple, si Eve envoie de la lumière suffisamment intense, elle peut déterminer lequel des détecteurs s'active grâce à une rétroaction lumineuse lors de l'activation du détecteur. Aussi comme précédemment mentionnée, la transmission des photons diminue exponentiellement avec la distance ce qui limite les transmissions longue distance.

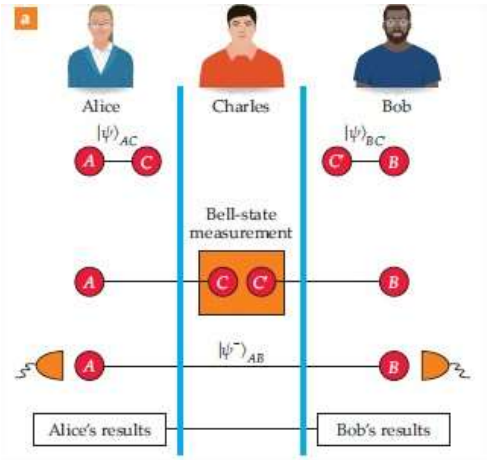


Figure 3 : échange d'intrication

Une solution pour corriger ces failles est l'échange d'intrication (parfois appelé la téléportation quantique). Ce principe implique qu'Alice et bob créent une paire de photons intriqués chacun de leur côté. Ensuite, chacun envoie un photon à Charles qui détecte les photons et les pousse dans un état de Bell. Ce faisant, le photon resté chez Alice et celui chez Bob deviennent alors intriqués ensemble. Ils mesurent alors une partie de leurs résultats pour vérifier qu'ils partagent un état de Bell. Pour savoir s'ils partagent un état de Bell, ils mesurent leur état selon la base Z : $|0\rangle$ et $|1\rangle$ ou la base X : $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ en choisissant la base à utiliser complètement aléatoirement. Ils prennent toutes les fois qu'ils ont choisis la même base et ensuite, ils comparent un sous-ensemble de donnée pour voir si leurs données corrèlent en vérifiant chaque fois s'ils avaient la même valeur. S'ils partagent un état de Bell suffisamment

parfait (selon un critère préétabli entre eux), ils peuvent former la clé avec les bits non divulgués.

Une façon un peu différente et surprenante pour les non-initiés de la mécanique quantique d'exploiter l'échange d'intrication est ce qu'on appelle un protocole de préparation et de mesure. En effet, les mesures de Charles et d'Alice et Bob commutent, ils peuvent donc mesurer leur état avant d'envoyer la deuxième particule à Charles. En pratique, ils peuvent créer la particule dans l'état souhaité, faire leur mesure dans l'état aléatoire et seulement ensuite l'envoyer à Charles. Et tant que Charles fait sa mesure correctement et annonce que les particules sont intriquées, les mesures d'Alice et Bob concorderont. L'Article appelle ce phénomène une intrication virtuelle et permet à Alice et Bob de ne pas attendre les mesures de Charles pour faire les mesures de leur côté.

En ce moment pour transmettre des photons on utilise des lasers émettant des WCP (**W**eaks **C**oherents **Pulses** : pulsations cohérentes faibles) qui produisent en moyenne 0,1 photon par pulsations ce qui équivaut à beaucoup de pulsations contenant 0 photon, quelques-unes contenant 1 photon et une très petite partie qui en contiennent 2 et plus. Le problème c'est que si par hasard la source envoie plusieurs photons, Eve pourrait en prendre 1 et envoyer l'autre et donc voler une partie de la clé. Pour éviter le problème, on peut utiliser une méthode appelée la méthode de leurres où Alice envoie 1 vrai signal avec une intensité et plusieurs faux signaux avec d'autre intensité plus forte. Elle compare ensuite le taux de perte des signaux à photons unique vs ceux à multiphotons et si elle détecte une anomalie (une perte plus grande pour les signaux à multiphotons), cela veut dire que Eve a tenté une attaque et Alice peut avorter la transmission de la clé.

MDI QKD

Le protocole MDI QKD est une manière de réaliser le protocole QKD en utilisant l'échange d'intrication. Pour ce faire, Alice et Bob préparent un état de Bell avec des photons polarisés $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle - |V\rangle\,|H\rangle)$ et mesure dans la base Z ou X au hasard. Charles mesure les photons avec le principe d'interférence à 2 photons pour identifier 2 des 4 états de Bell possible et la clé sera formée avec les mesures dans l'état Z. La méthode des états leurres sert à estimer le nombre de bits de la clé qui a pu être transmis par des photons uniques. Aussi, les états mesurés en X et les états leurres servent à estimer la quantité d'information que Eve a pu apprendre sur la clé. La clé est ensuite formée en appliquant des corrections d'erreur et des protocoles d'amplification de la confidentialité à la clé brute.

La méthode d'inférence à 2 photons consiste à utiliser l'effet Hong-Ou-Mandel qui stipule que 2 photons indistinguables qui entrent en même temps dans 2 ports d'un séparateur de rayon ressortiront toujours dans le même port de sortie. Et puisque les photons sont indistinguables et dans le même état, ils forment ensemble un état de Bell. Il est à noter que l'effet Hong-Ou-Mandel ne marche qu'avec un décalage temporel nul et que plus le décalage est important plus la probabilité que les deux sortent dans le même port diminue jusqu'à atteindre 50 %.

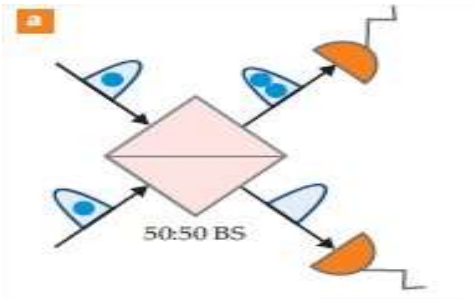


Figure 4 : interférence à 2 photons

Le protocole MDI QKD a permis de produire un taux de transmission de clé secrète de 1 Mb/s, d'atteindre une distance de transmission de 404 km dans de la fibre optique, ce qui permettrait en ce moment de crypter un appel vidéo HD entre Toronto et Ottawa.

TF QKD

Le protocole TF QKD lui utilise le principe d'interférence à un seul photon. Dans ce protocole, Alice et Bob, créez chacun un état $|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle \pm |1\rangle|0\rangle)$. L'état $|0\rangle$ représentant un état de vacuum et l'état $|1\rangle$ un état de photon unique. Donc en pratique, seul le photon d'Alice ou de Bob a besoin de rejoindre Charles permettant de doubler la distance de transmission possible par le protocole MDI. Et en plus, Charles n'a même pas à être fiable, car il ne reçoit aucune information sur la clé secrète (ce qui est aussi valable pour le protocole MDI QKD). Pour encoder les valeurs de bits, Alice et Bob donnent à leurs photons (au hasard et de manière indépendante) une phase de 0, π ou une phase aléatoire. Les phases de 0 ou π correspondent à des 0 ou des 1 et les phases aléatoires forment des états leurres. Lorsqu'ils choisissent d'envoyer une phase aléatoire, ils varient aléatoirement l'intensité du signal pour créer des états leurres. Cependant, le protocole TF QKD demande que les signaux de Bob et Alice gardent leur stabilité de phase. Heureusement, des techniques d'autocompensation existent pour pallier ce problème. Des chercheurs ont d'ailleurs déjà atteint des distances de transmission de plus de 500 km.

L'avenir de la cryptographie quantique

Dans l'avenir, les protocoles QKD pourront fournir des niveaux sans précédent de sécurité et de performance. Aussi cela pourrait fournir des moyens de communication crypter accessible où chacun possèderait un transmetteur QKD à base de puce et tous partageraient une unité de mesure avec des détecteurs à photons uniques assurant l'échange d'intrication. Aussi plusieurs

chercheurs sont déjà en train de développer des protocoles pour gérer des systèmes asymétriques où la perte de signal ne serait pas égale du côté de Alice ou Bob. Des protocoles permettant des configurations asymétriques qui autoriseraient Alice et Bob à utiliser des intensités de signal différent. Aussi plusieurs travaillent à créer des systèmes de sécurisation du transmetteur QKD qui saurait gérer les imperfections des machines et en même temps empêcher la manipulation des dispositifs.

Analyse :

L'article porte principalement sur le fonctionnement du protocole QKD et de ses variations le MDI QKD et le TF QKD, aussi il décrit assez bien le principe de fonctionnement des méthodes de détections à un et deux photons. En somme, l'article fait un bon résumé de ce qui a été accompli à ce jour d'aujourd'hui pour le protocole QKD et ce qui reste encore à faire. Malgré tout, en parlant de l'échange d'intrication, ils mentionnent le scénario « prepare-and-measure » et parlent de « partager une intrication virtuelle » et n'élaborent pas beaucoup plus sur le sujet. C'est dommage, car cela semble être un concept très intéressant et pas connu du grand public et on le nomme avec une très faible explication. Comme nous l'avons déjà montré plus haut, les auteurs ont tous les trois un curriculum assez impressionnant dans le domaine de la cryptographie quantique, et plus généralement, dans le domaine de la communication et de la physique. Hoi-Kong Lo, plus particulièrement, est un des premiers à avoir prouvé la sécurité du système QKD il y a de ça plusieurs années et l'on voit qu'il ne cesse depuis d'améliorer l'idée en trouvant de nouvelles façons d'appliquer le protocole de base en regardant ces articles publiés. À eux trois, ils ont montré que le protocole QKD et ses variantes n'étaient pas qu'un principe fonctionnant en théorie, mais qu'il est possible de le réaliser en pratique. La structure de l'article s'enchaine naturellement, on nous parle d'abord de la nécessité de trouver une solution de cryptage alternative à ce que l'on utilise aujourd'hui, ensuite on introduit le protocole QKD, son fonctionnement, ses progrès et les défis qu'il reste à franchir. Pour pallier le problème d'attaque externe, il nous explique alors le principe d'échange d'intrication et les méthodes de mesures possibles pour le réaliser. S'en suit les variantes du QKD de base MDI QKD et TF QKD qui sont des méthodes pratiques d'application du protocole. Puis finalement, ils nous expliquent ce qui reste à accomplir pour utiliser ces protocoles dans la vie de tous les jours.

Partie critique :

Le protocole QKD (et ses variantes) est assurément une technologie très prometteuse et ambitieuse. Elle répond à un problème de plus en plus concret et de l'avis de plusieurs experts

inévitable, la venue d'un ordinateur quantique capable de briser tous nos algorithmes de cryptographie. L'article mentionne que face à cette éventualité plusieurs ont déjà commencé à imaginer des algorithmes résistant à l'ordinateur quantique, et donc, le protocole QKD est en concurrence avec ces algorithmes. En effet, le protocole QKD à plusieurs limites actuellement : la portée, le taux de transmission relativement faible et la nécessité de créer de nouveaux appareils pour utiliser cette technologie. Le développement et l'aboutissement de cette technologie pourraient se faire grandement accélérer si dans quelque temps un répéteur quantique fonctionnel était développé, mais cette technologie fait toujours défaut. Savoir si demain le cryptage se fera avec le protocole QKD, une version améliorée de celui-ci ou d'un algorithme standard résistant à l'ordinateur quantique est pratiquement impossible. Cela dépendra sûrement des technologies qui seront développées dans les années qui suivent et de la technologie qui sera la plus aboutie lorsque les premiers ordinateurs quantiques apparaitront en masse. Personnellement, nous avons trouvé que les idées de l'article s'enchainaient très bien, que les figures et schémas étaient très clairs et facilitaient la compréhension de l'article. Nous avons aimé qu'ils nous donnent des exemples de pistes existantes avec leur source pour améliorer le système tout au long de l'article. Comme nous l'avons précédemment mentionné, une explication un peu plus grande sur le scénario « prepare-and-measure » aurait facilité la compréhension de l'article et à plusieurs endroits on mentionnait des protocoles de renforcement de sécurité de la clé et des compensations que l'on pouvait appliqués sans toutefois mentionner en quoi ils consistaient et nous aurions aimé avoir une explication brève de leur fonctionnement ou au mois source pour diriger notre recherche. Sinon, l'article semblait au mieux de nos compétences très honnêtes dans ces résultats et montrait clairement les failles actuelles du QKD.

Conclusion :

En conclusion, le protocole QKD est un procédé très intéressant qui répond à un problème très actuel. Il a l'audace de proposer une approche complètement différente de ce qu'on utilise actuellement et bien que dépendant d'un très vieux principe, c'est une technologie à la fine pointe de nos capacités actuelles. Que le protocole QKD ou ses variantes deviennent les bases de la cryptographie de demain est encore impossible à prédire, mais cette technologie pourrait très bien s'implémenter en parallèle de bien d'autres utilisant son excellente sécurité, mais sa portée (actuellement) réduite pour gérer des communications cryptées à faible portée.

Bibliographie :

1 : A quantum leap in security: Physics Today: Vol. 74, No. 3 (scitation.org)

https://physicstoday.scitation.org/doi/10.1063/PT.3.4699

2 : Curty Alonso, Marcos | atlanTTic (uvigo.es)

https://atlanttic.uvigo.es/en/team/staff/marcos-curty-alonso/

3: Home Page of Koji Azuma (ntt.co.jp)

http://www.brl.ntt.co.jp/people/azuma/

4 : Prof. Hoi-Kwong Lo (utoronto.ca)

https://www.comm.utoronto.ca/~hklo/