Communications sécurisées avec des variables quantiques continues

Pr. Philippe Grangier
Laboratoire Charles Fabry, Institut d'Optique,
CNRS et Université Paris Saclay
Exposé à l'Académie Européenne Interdisciplinaire des Sciences,
Institut Henri Pincaré, Paris, France
4 décembre 2023
(Compte-rendu rédigé par Abdel O. Kenoufi et Michel Gondran)

Après une présentation du Professeur Philippe Grangier (PG) par le Président de l'AEIS, M. Victor Mastrangelo, le conférencier commence par citer quelques uns des projets et partenaires universitaires (CNRS, Institut d'Optique de l'Université Paris-Saclay, LIP6 de Sorbonne Université, INRIA,...), industriels (Nokia Bell Labs, Thales, OrdiOKD, ...) et institutionnels (Région Ile de France, Commission Européenne), dans lesquels lui et ses équipes sont impliqués. Il présente ensuite le plan de son exposé divisé en trois parties et propose aux auditeurs de ne pas hésiter à l'interrompre pour poser des questions.

1. Dans la première partie de l'exposé, PG présente les outils mathématiques pour les descriptions discrètes et continues de la lumière quantique et des objets physiques dont il va parler, en l'occurence les photons.
   La description discrète, tout à fait adaptée à l'aspect corpusculaire du photon, se base sur la décomposition de Fourier du champ électromagnétique et considère chacun des modes comme un oscillateur quantifiable. Le formalisme mathématique adapté est dit de seconde quantification, car utilisant les opérateurs de nombre d'occupations d'un mode $\hat{N} = \hat{a}^+\hat{a}$ où $\hat{a}^+$ et $\hat{a}$ sont respectivement les opérateurs de création et d'annihilation d'un mode donné. Cela permet de construire la matrice de l'opérateur de densité, quantité mathématique centrale pour la physique statistique.
   La description continue, quand à elle, est plutôt adaptée à la description ondulatoire des photons. Elle utilise habituellement une description polaire par les amplitudes et les phases des ondes, mais le caractère potentiellement multivalué de l'opérateur de phase est susceptible d'être problématique. C'est pour cela qu'on passe aux opérateurs cartésiens dits de quadrature $\hat{X} = \frac{\hat{a}+\hat{a}^+}{\sqrt{2}}$ et $\hat{P} = \frac{\hat{a}-\hat{a}^+}{\mathrm{i}\sqrt{2}}$. Ces deux opérateurs ne commutant pas, il apparait nécessairement une relation d'incertitude d'Heisenberg, ce qui implique des précisions inverses sur les mesures de l'une ou l'autre de ces deux observables et donc introduit nécessairement la notion de probabilités de mesures. C'est pour se représenter ce nuage de probabilité que PG utilise la fonction de Wigner $W(\hat{X}, \hat{P})$, bien connue en traitement du

signal, et qui est une fonction génératrice de toutes les fonctions d'autocorrélation spatiale de la fonction d'onde. Elle n'est rien de moins que la transformée de Wigner-Weyl de la matrice de densité et est la représentation de cet opérateur dans l'espace des phases. Elle n'est toutefois pas une distribution de probabilités car elle peut être négative mais permet de réaliser une véritable tomographie quantique.

A la question d'Eric Chenin sur les coefficients devant $\hbar$ dans les relations d'incertitudes, PG répond que la normalisation des unités enlevait le facteur $\frac{1}{2}$.

PG décrit les dispositifs expérimentaux correspondants à chacune des descriptions :

— Variante discrète basée sur le comptage de photons : APD, VLPC, TES, ...,

— Variante continue par démodulation basée sur la détection homodyne, c'est-à-dire basée sur des interférences et des soustractions de courants.

PG continue en exhibant des représentations graphiques de la fonction de Wigner dans quatre différents cas :

— Gaussienne :
  — Etat cohérent $|\alpha>$ (égalité dans l'inégalité large d'Heisenberg),
  — Etat comprimé,

— Non-Gaussienne :
  — Etat de Fock |N=1 $>$,
  — Etat du "chat" $|\alpha> + |-\alpha>$.

PG explique ensuite pourquoi ces tomographies quantiques permettent de visualiser grâce aux représentations de leurs fonctions de Wigner, des "chats" de Schrödinger de deux types , dont les fonctions d'ondes ne diffèrent que par un facteur de phase et qui sont des combinaisons linéaires d'états cohérents :

$|\Psi>_{\text{even}} = c_e\big(|\alpha> + |-\alpha>\big)$ et $|\Psi>_{\text{odd}} = c_o\big(|\alpha> - |-\alpha>\big)$ avec $c_e,\ c_o \in \mathbb{C}$.

Leur utilité provient du fait qu'ils sont à la base des processus d'informations quantiques, et des études de la décohérence qui détruit les effets quantiques caractérisés par des oscillations de la fonction de Wigner. Pour terminer cette première partie, PG explique comment déterminer la fonction de Wigner d'un "chat" au travers d'une expérience datant de 2007 qui utise des photons dits optiques. Il est à noter que ces "chats" sont donc "observables" grâce à cette fonction d'autocorrélation et que les expériences les caractérisant ont été effectuées avant les travaux de Serge Haroche (co-lauréat du Prix Nobel de Physique 2012 pour la manipulation et la mesure de systèmes quantiques individuels), qui utilise par contre des photons micro-ondes à 40 GHz piégés dans une cavité supra-conductrice à une température de $100\ \mu$K.

A la question de Jean-Pierre Treuil demandant quel est l'équivalent de l'ouverture de la boîte dans l'expérience du "chat" de Schrödinger, acte qui projette l'état du "chat" en l'état "vivant" ou en l'état "mort", autrement dit l'action de la décohérence. PG répond que même lorsqu'on ne décide pas d'observer le "chat", ce dernier se "dégrade" tout seul car bon

nombre de photons se perdent. De plus, pour réaliser la réduction du paquet d'ondes, une campagne de mesures de la distribution des positions est nécessaire, et cela doit être réalisé pour chaque quadrature. Ce qui implique d'effectuer des milliers de mesures et de détections. Le conférencier termine cette première partie en présentant une application des "chats" micro-ondes dans des cavités pour le calcul quantique réalisée par la start-up Alice & Bob issue de l'ENS et l'INRIA. Elle se base sur la création de qubits de "chats", les bien nommés cat-qubits. PG répond par la négative à deux questions, la première demandant si la NASA avait commencé et abandonné la construction d'un ordinateur quantique, la deuxième interrogant sur la possible analogie entre le fonctionnement neuronal du cerveau humain et l'ordinateur quantique. Il souligne toutefois que seuls IBM, Google et récemment Amazon s'étaient lancés et continuent leurs recherches dans le domaine de l'informatique quantique et qu'il n'y a aucuns liens entre le fonctionnement neuronal du cerveau humain et un ordinateur quantique.

2. La seconde partie de la présentation décrit les deux types de cryptographies quantiques : variantes discrètes ou continues pour les distributions de clefs quantiques. PG rappelle les problématiques de base de la cryptographie et l'utilité des échanges sécurisés de clefs chiffrées et basées sur des algorithmes utilisants la physique quantique pour la transmission des clefs *via* la transmission de photons.

   Le principe étant d'utiliser les inégalités d'incertitude d'Heisenberg dans le but d'établir une borne sur l'information manquante/restante au sens d'interceptée, voire volée, ou tout simplement erronée, afin de reconstituer l'information originelle.

   A nouveau, une distinction s'établit sur la méthode utilisée :

   — discrète : envois de photons l'un après l'autre et l'information est codée grâce à leurs polarisations, c'est à dire des bits superposables ou qubits, comme par exemple dans les protocoles BB84, Decoy State, . . .,

   — continue : détection d'états cohérents par quadratures de champs électromagnétiques avec corrections d'erreurs *a posteriori*, comme par exemple dans CV-QKD. L'information étant codée dans une modulation aléatoire d'amplitude et de phase, la lecture est effectuée par un choix aléatoire de quadrature pour chaque état cohérent détecté.

   Jean-Pierre Treuil et Victor Mastrangelo interrogent sur les éventuelles redondances dans les clefs trop grandes et l'apparition d'erreurs consécutives. PG répond que des procédures dites de "hachage" permettent de les minimiser.

   PG cite une méthode à variables continues qu'il avait déjà développé quelques années auparavant avec son équipe et qui a l'avantage de ne pas utiliser de compteurs de photons, de systèmes de refroidissement et de détection d'étas cohérents. Il montre ensuite l'explosion des publications académiques et industrielles dans ce domaine de recherche. Le conférencier présente l'intérêt de CV-QKD au niveau de la Théorie de l'Information pour borner l'information manquante/restante. Cette partie se poursuit par une description de

quelques réalisations expérimentales en collaboration avec l'industriel français Thales sur une distance de 12 kms.

Pour terminer cette partie, PG présente quelques challenges d'ingénieries électroniques réalisés pour les télécommunications cohérentes particulièrement au niveau de la réduction des bruits quantiques, des technologies lasers et du traitement rapide de données (traitement du signal embarqué sur FPGA). Une discussion est engagée sur l'état de la concurrence commerciale internationale dans ce type de technologies.

3. La dernière partie propose une projection dans le futur où des extensions de ces applications peuvent être envisagées, notamment sur des interactions entre photons et des protocoles de communications à longue distance. Une première approche est de créer des réseaux satellitaires point-à-point sécurisés. PG présente une liste de quelques projets internationaux allant dans ce sens, en mentionnant les performances de la plupart d'entre eux.

   Une deuxième approche, évitant d'utiliser des satellites et absolument sûre, est basée sur l'utilisation de répéteurs (mémoires) quantiques basés sur des états intriqués et la téléportation quantique permettant de les transférer, et les rendant ainsi non-interceptables. Idéal pour la transmission d'une clef! Cependant, leur réalisation est ardue et pose de nombreux problèmes malgré les nombreuses recherches initiées dans le domaine. Afin d'éviter la perte d'informations, PG explique comment lui et son équipe ont imaginé produire un état de "Hamlet", ou "chat" intriqué. Cependant, cette approche n'a pas été très fructueuse expérimentalement. Il termine son exposé par une approche déterministe d'une équipe française du CNRS et Paris-Saclay utilisant la propagation de qubits photoniques.

   Wolfgang Elsäßer demande s'il est possible de remplacer directement les états cohérents par des états de "chat" afin d'assurer une communication sécurisée. PG répond par l'affirmative en suggérant d'utiliser des états intriqués plutôt que des états de "chat". Ceci étant, l'avantage des états cohérents est qu'ils sont plus faciles à produire. De plus, pour des raisons de débit notamment, les états cohérents sont très adaptés aux communications point-à-point, les états intriqués le sont plus pour les répéteurs quantiques.

   Une question de Victor Mastrangelo souhaiterait savoir ce qu'utilisent les banques. PG répond que certains systèmes à variables discrètes sont vendus par des conccurents à des banques suisses mais que peu d'informations sont disponibles sur le sujet. Cependant, ces dispositifs servent plus à sécuriser des données confidentielles transmises depuis un site de sauvegarde (back-up) et une banque.

   Eric Chenin interroge la sensibilité de ces systèmes par rapport aux potentiels orages magnétiques, ou autres. Il cite l'exemple d'un énorme orage magnétique ayant eu lieu dans les années 1950. PG répond que de grandes compagnies comme Google prennent déjà en compte le risque dû aux rayons cosmiques.

   Abdel Kenoufi demande si des efforts ont été effectués dans le domaine de la miniaturi-

sation ou du moins dans l'intégration et la réduction des dimensions des dispositifs expérimentaux. PG répond que d'importants travaux ont été réalisés pour la cryptographie quantique au travers de la réalisation de PIC (Photonic Integrated Chipset) dont les gravures peuvent aller jusqu'à l'échelle du millimètre, mais restent difficiles à contrôler. Pour le calcul quantique, malgré une rude conccurence entre de nombreuses sociétés, dont des start-up telles Pasqal (dont PG est à l'origine), les dimensions sont celles de systèmes de quelques centaines d'atomes pouvant effectuer des calculs. D'autres approches comme à Grenoble, essaient de graver des systèmes sur du Silicium et du Germanium, mais cela reste cependant difficile pour l'instant. PG cite Thierry Breton qui a lancé un programme de nano-électronique qui possède un volet Calcul Quantique.

Victor Mastrangelo demande si des systèmes moléculaires biologiques pourraient être des candidats pour une informatique quantique. PG répond que certaines molécules entrants dans les processus de photo-synthèse pourraient l'être, mais que cela constitue une voie de recherche peu explorée à l'heure actuelle.

Dans sa seconde question à PG, Abdel Kenoufi aimerait savoir ce qu'il en est des simulateurs quantiques et si la société française ATOS, qui a été dirigée auparavant par Thierry Breton, actuellement Commissaire Européen en charge entre autres du Numérique, et à l'origine de nombreux programmes de recherche en technologies quantiques, est impliquée dans ces recherches. PG répond que ce ne sont pas des simulateurs quantiques mais plutôt des émulateurs informatiques simulants le fonctionnement d'un ordinateur quantique. Enfin il termine en expliquant que Thierry Breton a permis à ATOS d'initier et de continuer à participer aux projets de recherche avec lesquels PG collabore toujours.