optique quantique TA

Lautaro Labarca
labl2714@usherbrooke.ca

November 12, 2024

Contents

1 Course-1. Qubit code.

L'objectif est de familiariser les étudiants avec la dynamique simple des qubits. Pour ça, on va faire un exercice computationnel. Nous allons esquisser quelques étapes analytiques pour obtenir les formes simples que nous étudierons numériquement, mais aucun détail de ces dérivations n'est fourni. En général, elles sont simples, mais légèrement fastidieuses à reproduire. Si ce n'est pas déjà fait, il est bon de compléter les étapes manquantes. Le chapitre 4 de Nielsen et Chuang [1], le chapitre 2 de Sakurai [2], et la page Wikipédia sur les transformations unitaires couvrent tout le nécessaire pour combler ces lacunes. En guise de spoiler, la semaine prochaine, lors de la révision des devoirs, nous passerons en revue tous les détails analytiques fastidieux, mais nécessaire.

1.1 Configuration de qutip avec Visual Studio Code

Tout d'abord, nous devons installer Python. Allez sur le lien [3]. Utilisez simplement la version recommandée. Pendant que Python s'installe, nous pouvons installer Visual Studio Code [4]. Ensuite, créez simplement un dossier pour le cours, ouvrez-le, et téléchargez-y le notebook utilisé en classe [5]. Créez un environnement virtuel en tapant dans la palette de commandes `Python: Create Environment`. Maintenant, utilisez simplement la palette de commandes pour ouvrir le terminal.

Dans le terminal, tapez `pip install qutip`. De la même manière, installez `numpy` (manipulations basiques de tableaux), `matplotlib` (signification évidente), `scipy` (manipulations de tableaux plus efficaces, précises et variées, avec de nombreuses fonctions spécifiques comme l'intégration, les séries, les polynômes, et le fitting), `tqdm` (pour voir des barres de progression). Vous pouvez voir toutes les versions installées avec `pip list`. Vérifiez les compatibilités dans la documentation d'installation de `qutip`, à savoir essentiellement `numpy` < 2.0, `scipy` > 1.8, `python` > 3.9, `matplotlib` $> 1.2.1$. Avec cela, vous êtes prêts à exécuter tous les codes utilisés dans ce cours. Enfin, configurez GitHub Copilot. L'utilité de cet outil c'es top. Avec Visual Studio Code, c'est très facile : il suffit d'installer l'extension et de lier votre compte GitHub étudiant.

Alternativement, créez un compte sur Cocalc, allez dans vos projets, démarrez-en un nouveau et téléchargez le notebook qubit-drive-pulse.ipynb trouvé sur le GitHub [5].

1.2 Pourquoi nous intéressons-nous aux qubits?

Tout d'abord, le qubit est l'objet mathématique le plus simple qui capture les caractéristiques essentielles de la mécanique quantique non relativiste. Avec les qubits, nous pouvons avoir la superposition, c'est-à-dire l'interférence. En particulier, le fait qu'il y ait deux signes est suffisant, voir par exemple [6]. De plus, avec deux qubits ou plus, nous pouvons étudier l'entrelacement, probablement la caractéristique la plus frappante de la mécanique quantique comme l'a posée Einstein et ses collaborateurs [7] (sérieusement, l'article est très facile à lire, allez le lire), ce qui peut conduire à des corrélations non locales entre les particules entrelacées comme le montrent d'abord [8, 9] basées sur les inégalités de Bell [10] (très simples à lire également, c'est fantastique). Plus récemment, les inégalités ont été violées en utilisant des circuits supraconducteurs dans [11]. Il est à noter que certains chercheurs affirment encore que les inégalités de Bell telles que proposées par Bell n'ont pas encore été testées, voir par exemple [12].

Deuxièmement, pour la physique fondamentale, les qubits, en raison de leur simplicité, sont très utiles pour concevoir des expériences mesurant une force ou une interaction désirée. Par exemple, des tests ont été réalisés pour rechercher la matière noire [13]. Cet expérience, comme beaucoup d'autres, est basée sur le schéma montré dans fig. 1. De plus, les qubits (sous forme d'atomes, on mesure les probabilités de transition ; si une seule transition est pertinente, alors les deux niveaux correspondants forment un qubit) sont utilisés dans des expériences mesurant la constante gravitationnelle (je manque d'une référence particulière pour cela) et font partie de propositions testant la nature quantique de la gravité, voir par exemple le dossier [14].

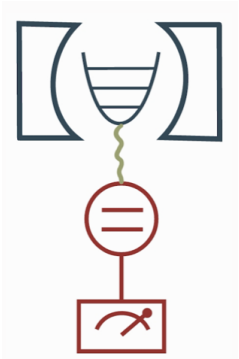


Figure 1: Oscillateur couplé à un qubit. Dans ce cas, le qubit est utilisé pour extraire des informations de l'oscillateur, mais l'inverse est également utilisé.

Troisièmement, les qubits forment la base de l'informatique et de l'information quantiques. Au-delà de la promesse de démontrer que le modèle computationnel le plus fondamental n'est pas la machine de Turing classique, mais l'ordinateur quantique, ils promettent d'améliorer les protocoles cryptographiques. Nous verrons cela dans le chapitre 4.[1]

[1] Il y a eu tant de choses écrites à ce sujet que je préfère ne pas commenter davantage pour le moment. De plus, je manque de temps, donc je ne vais pas inclure d'autres références pour l'instant, mais je pourrais mettre à jour cela à l'avenir.

1.3 Dynamique simple des qubits

En général, la dynamique d'un qubit conservatif est générée par l'Hamiltonien

$$\hat{H}(t) = f(t)\sigma_z + g(t)\sigma_x + h(t)\sigma_y. \tag{1.1}$$

Ainsi, formellement, l'évolution est donnée par

$$\hat{U} = \mathcal{T}[i\exp\left\{\int_0^t \mathrm{d}t' f(t')\sigma_z + g(t')\sigma_x + h(t')\sigma_y\right\}] \equiv \exp\{i\alpha(t)\sigma_z\}\exp\{i\beta(t)\sigma_x\}\exp\{i\gamma(t)\sigma_z\}, \tag{1.2}$$

où la dernière équivalence est due à la décomposition des rotations, voir [1] chapitre 4. En résumé, toute évolution non dissipative d'un qubit unique est simplement une rotation et nous pouvons la visualiser dans la sphère de Bloch. Dans le code partagé [5], vous trouverez une animation montrant l'impulsion de $\pi/2$ permettant de préparer $|+\rangle$ à partir de $|0\rangle$.

En raison de la décomposition des rotations ci-dessus, nous pouvons nous concentrer simplement sur les Hamiltoniens de la forme,

$$\hat{H}(t) = f(t)\sigma_z + g(t)\sigma_x. \tag{1.3}$$

L'Hamiltonien ci-dessus est couramment généré dans les circuits supraconducteurs en utilisant un qubit avec une fréquence dépendante du temps (par exemple, en faisant passer un flux magnétique à travers un SQUID), et en excitant le qubit à travers une ligne de charge (la partie $g(t)\sigma_x$). Pour simplifier, concentrons-nous sur $f(t) = \omega_0/2$ constant, ou ω_0 étant la fréquence du qubit. En passant à un cadre tournant à la fréquence ω, nous obtenons dans le cadre d'interaction un Hamiltonien de la forme suivante

$$\hat{H}(t) = \Delta\sigma_z + g(t)\sigma_x. \tag{1.4}$$

Notez que $g(t)$ est modifié, mais pour notre étude qualitative, la forme exacte n'est pas importante. En fait, nous simplifierons encore davantage, et nous poserons $\Delta = 0$, pour obtenir

$$\hat{H}(t) = g(t)\sigma_x. \tag{1.5}$$

Ensuite, l'évolution unitaire est donnée par

$$\hat{U}(t) = \exp\left[-i\int_0^t \mathrm{d}t' g(t)\sigma_x\right]. \tag{1.6}$$

Ainsi, en redimensionnant simplement $g(t) \to 2\pi g(t)$, et en utilisant le fait qu'une rotation autour de l'axe x dans la sphère de Bloch par un angle θ est donnée par

$$\hat{R}_x(\theta) \equiv \exp\{-i\theta\sigma_x/2\}, \tag{1.7}$$

nous obtenons

$$\hat{U}(t) = \hat{R}_x(2I), \quad \text{avec} \quad I = \int_0^t \mathrm{d}t' g(t). \tag{1.8}$$

Cela signifie que si nous ne considérons que le sous-espace des qubits, seule l'intégrale de l'impulsion, c'est-à-dire son amplitude totale, est importante, et sa forme est sans importance pour la fidélité de l'état final. Cependant, en ajoutant un troisième état, nous verrons que ce n'est plus le cas et que la forme de l'impulsion, et en particulier son profil de fréquence, jouent un rôle crucial.

1.4 Profil de fréquence de l'impulsion et ses effets sur les fuites (leakage)

Ici, je vais développer un exemple avec un qutrit, avec des détails. Le code associé est téléchargé dans [5] et s'appelle qutrit. Cela devrait (légèrement) vous être utile pour l'exercice 1 de votre devoir. Nous pouvons commencer à étudier le problème dans sa forme abstraite la plus générale pour mieux le comprendre. Du fait que l'évolution quantique est linéaire, nous pouvons imaginer le scénario général où l'évolution du qutrit est générée par un Hamiltonien hermitien arbitraire $\hat{H}(t)$, c'est-à-dire

$$\frac{\partial\,|\psi(t)\rangle}{\partial t} = \hat{H}(t)\,|\psi(t)\rangle\,, \tag{1.9}$$

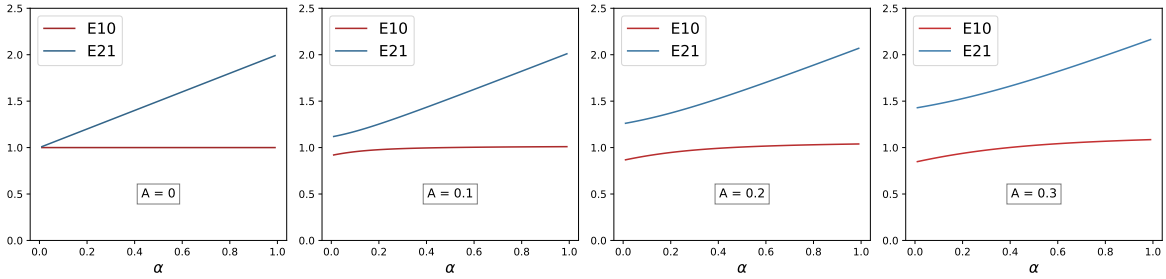


Figure 2: Énergies propres du qutrit en fonction de l'anharmonicité pour différentes amplitudes de contrôle. E10 correspond à $E_1 - E_0$.

sous forme matricielle

$$\begin{pmatrix} \dot{c}_0(t) \\ \dot{c}_1(t) \\ \dot{c}_2(t) \end{pmatrix} = \begin{pmatrix} H_{11}(t) & H_{12}(t) & H_{13}(t) \\ \bar{H}_{12}(t) & H_{22}(t) & H_{23}(t) \\ \bar{H}_{13}(t) & \bar{H}_{23}(t) & H_{33}(t) \end{pmatrix} \begin{pmatrix} c_0(t) \\ c_1(t) \\ c_2(t) \end{pmatrix}, \tag{1.10}$$

où les barres représentent la conjugaison. Pour simplifier encore davantage, disons que l'Hamiltonien ne couple que les états voisins, c'est-à-dire $H_{13}(t) = 0$. De plus, simplifions encore notre analyse en supposant que les termes diagonaux sont constants dans le temps et que les termes hors diagonale évoluent de manière harmonique à la fréquence ω_0, c'est-à-dire que la transformée de Fourier de $H_{ij}(t)$ est $\delta(\omega - \omega_0)$. Nous écrivons donc,

$$\begin{pmatrix} \dot{c}_0(t) \\ \dot{c}_1(t) \\ \dot{c}_2(t) \end{pmatrix} = \begin{pmatrix} H_{11} & A_{12}e^{i\omega_0 t} & 0 \\ \bar{A}_{12}e^{-i\omega_0 t} & H_{22} & A_{23}e^{i\omega_0 t} \\ & \bar{A}_{23}e^{-i\omega_0 t} & H_{33} \end{pmatrix} \begin{pmatrix} c_0(t) \\ c_1(t) \\ c_2(t) \end{pmatrix}. \tag{1.11}$$

De plus, avec un simple décalage des énergies, nous pouvons fixer H_{11} à zéro, donc nous avons

$$\begin{pmatrix} \dot{c}_0(t) \\ \dot{c}_1(t) \\ \dot{c}_2(t) \end{pmatrix} = \begin{pmatrix} 0 & A_{12}e^{i\omega_0 t} & 0 \\ \bar{A}_{12}e^{-i\omega_0 t} & H_2 & A_{23}e^{i\omega_0 t} \\ & \bar{A}_{23}e^{-i\omega_0 t} & H_3 \end{pmatrix} \begin{pmatrix} c_0(t) \\ c_1(t) \\ c_2(t) \end{pmatrix}. \tag{1.12}$$

Enfin, faisons une simplification supplémentaire en supposant $A_{12} = A_{13} \equiv A \in \mathbb{R}$, afin d'isoler la composante en fréquence du champ de contrôle dans notre analyse. En faisant cela, nous trouvons maintenant les valeurs propres. Pour ce faire, nous résolvons simplement l'équation déterminantielle $\det(H - \lambda I) = 0$, qui dans ce cas se lit :

$$\lambda(H_2 - \lambda)(H_3 - \lambda) + A^2(H_3 - 2\lambda) = 0. \tag{1.13}$$

Les valeurs propres ne dépendent alors pas de la fréquence du contrôle, mais seulement de son amplitude et de l'anharmonicité relative entre H_2 et H_3. Il est également à noter que l'équation ci-dessus est un polynôme de degré trois, et bien que nous puissions essayer de trouver des solutions analytiques, cela serait plutôt fastidieux, nous allons donc les résoudre numériquement. Pour ce faire, nous fixons $H_2 = 1$, $H_3 = 1 + \alpha$. Notez que ce choix signifie que $\omega = 1$ est la fréquence d'oscillation entre $|0\rangle$ et $|1\rangle$. De plus, nous fixons $A = 0.2$, ce qui correspond à un faible champ de contrôle, afin d'étudier la structure des vecteurs propres et des énergies propres en fonction de la fréquence du contrôle ω_0 et de l'anharmonicité α.

Dans la fig. 2, nous représentons les valeurs propres en fonction de α pour différentes valeurs de A, et dans la fig. 3, nous les représentons en fonction de A pour différentes valeurs de α. Il est clair qu'en augmentant α, comme attendu, l'écart entre E_{10} et E_{21} augmente. De même, l'augmentation de l'amplitude du contrôle élargit l'écart entre E_{21} et E_{10}. C'est l'écart typique qui apparaît lorsqu'un Hamiltonien est perturbé dans ses éléments non diagonaux de plus proche voisin. Maintenant, disons que nous voulons réaliser une porte, soit de $|0\rangle \to |1\rangle$ ou de $|0\rangle \to |2\rangle$. Quelle fréquence de pilotage devons-nous choisir pour maximiser la fidélité de la porte ? Pour répondre à cette question, nous

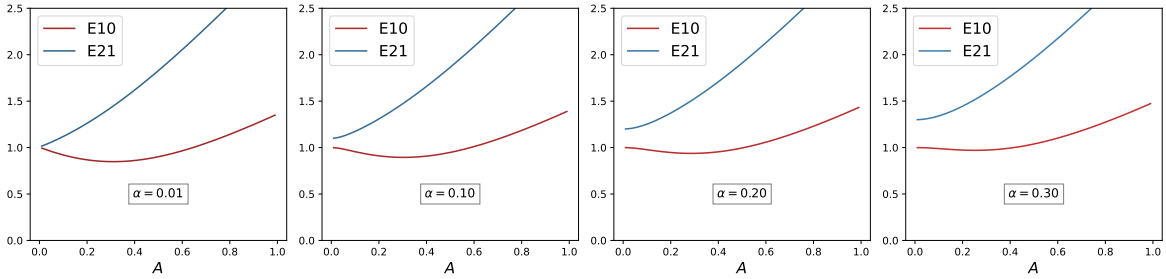


Figure 3: Énergies propres du qutrit en fonction de l'amplitude du contrôle pour différentes anharmonicités. E10 correspond à $E_1 - E_0$.

pouvons simplement résoudre l'évolution sur une durée suffisamment longue, disons $T = 10(2\pi/\omega_0)$, et trouver les valeurs maximales de

$$c_i = |\langle i|\psi(t)\rangle|. \tag{1.14}$$

Nous le faisons numériquement en fixant $A = 0.2$ et $\alpha = 0.5A$ dans la fig. 4. De toute évidence, la fréquence des termes de pilotage a une forte influence sur les fidélités atteignables. Il est certain que trouver les fréquences qui maximisent la fidélité est simple numériquement, mais qu'en est-il de prédire cette fréquence uniquement à partir des paramètres du système non piloté et de l'amplitude du pilote A par exemple. Là, dans la fig. 4, nous avons tracé les énergies $E21$ et $E10$, et bien que ces valeurs donnent un ordre de grandeur des pics, elles échouent considérablement en tant qu'outil prédictif. Si vous savez comment prédire les pics, faites-le moi savoir[2]. Nous notons que, naturellement, les profils dépendent de A et α, par exemple en fixant $A = 0.2$, $\alpha = 5A = H_2$, nous obtenons le profil intéressant de la fig. 5.

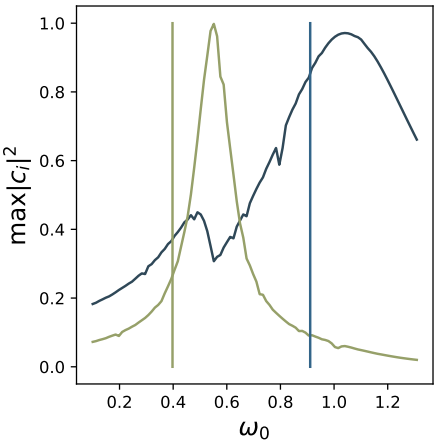


Figure 4: Maximum atteignable c_i en partant de $|0\rangle$ avec $A = 0.2$ et $\alpha = 0.5A$. c_1 en bleu, c_2 en vert. Les lignes verticales correspondent à $E10$ et $E21$.

Enfin, nous remarquons qu'il est clair que si le profil de fréquence du ton de pilotage est proche d'une résonance ou de l'autre, cela affectera les fuites. Imaginez une situation où le profil du ton de pilotage correspond à deux deltas de Dirac, l'un à la fréquence qui maximise c_1 (l'autre c_2), alors nous nous attendrions à ce que le maximum atteignable de chacun d'eux soit réduit par rapport au cas idéal. Pour cette raison, l'ingénierie des tons de pilotage est un sujet de recherche qui suscite un grand intérêt. Une approche numérique courante pour trouver des tons de pilotage idéaux est une boucle d'optimisation basée sur la descente de gradient.

[2]Attention, je ne dis pas que cette prédiction est inconnue, je dis simplement que je ne la connais pas pour le moment. Aller simplement dans l'espace de Fourier au niveau des équations pourrait probablement donner suffisamment d'informations pour comprendre.

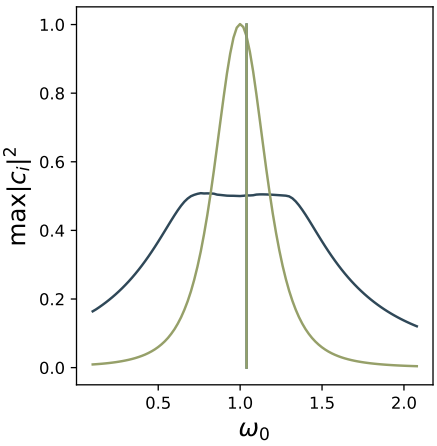


Figure 5: Maximum atteignable c_i en partant de $|0\rangle$ avec $A = 0.2$ et $\alpha = 5A = H_2$. c_1 en bleu, c_2 en vert. Les lignes verticales correspondent à $E10$.

2 Course-3. Cryptography.

2.1 Objectif

L'objectif de ce cours est de donner un aperçu de la cryptographie et d'expliquer de manière générale pourquoi la cryptographie quantique pourrait être intéressante. Idéalement, les étudiants seront capables de lire davantage dans la littérature après le cours, ou de revenir à ces notes chaque fois qu'ils auront besoin d'apprendre la cryptographie quantique pour tout problème sur lequel ils pourraient travailler.

Outline of the class (logically makes no sense, but for the impact value in the class seems adequate)

- Objectives of criptography.
- Setup, Alica, Bob, Eve, channels.
- Vernam key (one time pad), intuition on how information is decoded by spies.
- Quantum key distribution.
- No cloning theorem and information gain implies perturbation.
- BB84.
- Classical key distribution.
  - Information reconciliation and privacy amplification.
  - Shannon entropy and mutual information.
  - Error correction, repetition code.

2.2 Introduction à la cryptographie

Ainsi, en cryptographie, nous avons deux objectifs :

- Anonymat : protéger l'émetteur du message.
- Chiffrement : protéger le message.

Un exemple de cryptographie moderne ancienne est la machine Enigma. En réalité, elle a été inventée pour la Première Guerre mondiale, pas même la seconde. L'entrée sur Wikipedia contient beaucoup de détails sur son histoire, c'est une lecture intéressante. Ici, nous nous concentrerons sur la structure mathématique de la cryptographie, et en particulier sur la cryptographie quantique.

The basic criptography setup is depicted in fig. 6. Alice, has some message X, that she shares with Bob through some channel. This channel might be public (everyone has free access), prive (only Alice and Bob have access), or semi-private (Alice and Bob have free access, and some spy Eve has partial access). In theory, we can focus only in the semi-private one, but in practice, as semi-private channels are resource expensive, we also use public channels so the flow is mixed as shown in fig. 8.

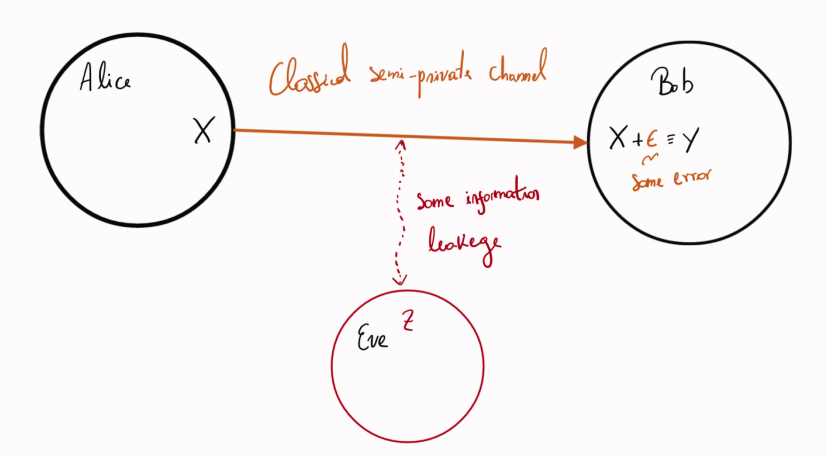


Figure 6: Classical criptography basic setup.

La méthode de chiffrement la plus courante de nos jours repose sur des *clés*. Ces clés peuvent être soit privées, soit publiques. Le chiffrement par clé publique est une invention moderne des années 1970. Avant cela, tous les systèmes cryptographiques utilisaient des clés privées. Imaginez qu'Alice veuille envoyer un message à Bob. Pour le chiffrer, Alice utilise une *clé de chiffrement*, et Bob dispose d'une *clé de déchiffrement*. Pour comprendre comment ces systèmes fonctionnent en principe, le mieux est d'observer un exemple. Un exemple commun est le *chiffre de Vernam*, car il est simple et très efficace, parfois appelé *one time pad*. Comme le montre la fig. 7, Alice utilise simplement une clé pour coder un message, et Bob utilise la même clé pour le décoder. De toute évidence, la sécurité d'un tel chiffrement dépend avant tout de la capacité à partager la clé de manière sécurisée entre Alice et Bob. La qualité la plus importante de ce codage est qu'il est prouvablement sécurisé sous les hypothèses suivantes :

- Les bits de la clé sont générés de manière véritablement aléatoire. Pourquoi ? Un générateur pseudo-aléatoire, comme son nom l'indique, utilise une *graine*. Par exemple, prenons l'heure actuelle sur une horloge. Si un espion découvre la graine et l'algorithme, alors toutes les clés peuvent être reconstruites.
- La longueur de la clé est au moins aussi longue que celle du message. Si la clé se répète, des études statistiques du message peuvent être réalisées, révélant ainsi des informations à un espion (il est d'usage d'appeler l'espion Ève).
- La clé ne doit jamais être réutilisée, ni en partie ni en totalité. Même argument que précédemment.
- Évidemment, la clé doit être conservée complètement secrète.

Cependant, qu'est-ce que cela signifie, « prouvablement sécurisé » ? Nous pouvons utiliser la théorie de l'information pour décrire cette condition mathématiquement de manière rigoureuse. Dans ce qui suit, nous ne nous soucierons pas de la rigueur, mais nous décrirons les éléments et l'intuition de base. Plaçons-nous maintenant dans la position de l'espion, et imaginons que nous essayons de déchiffrer un message simple de 7 lettres comme celui de la fig. 7, que nous écrirons sous la forme $x_1x_2x_3x_4x_5x_6x_7$. Pour rendre les choses plus concrètes, disons que nous savons que le message est dans une langue naturelle, concrètement l'anglais. Notre espace d'échantillonnage est donc celui de tous les messages de 7 lettres pouvant être formés en anglais. De plus, on peut imaginer dire que la probabilité que la première lettre soit un a, sur la base d'un simple argument de dénombrement de tous les mots disponibles dans l'espace d'échantillonnage, est donnée par

$$p(x_1 = a) = \frac{\text{tous les messages d'un (deux, trois) mots commençant par a}}{\text{tous les messages de 7 symboles}}, \tag{2.1}$$

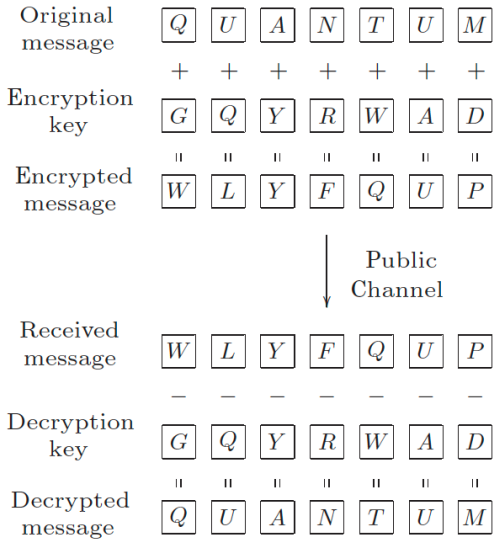


Figure 7: Vernam cipher

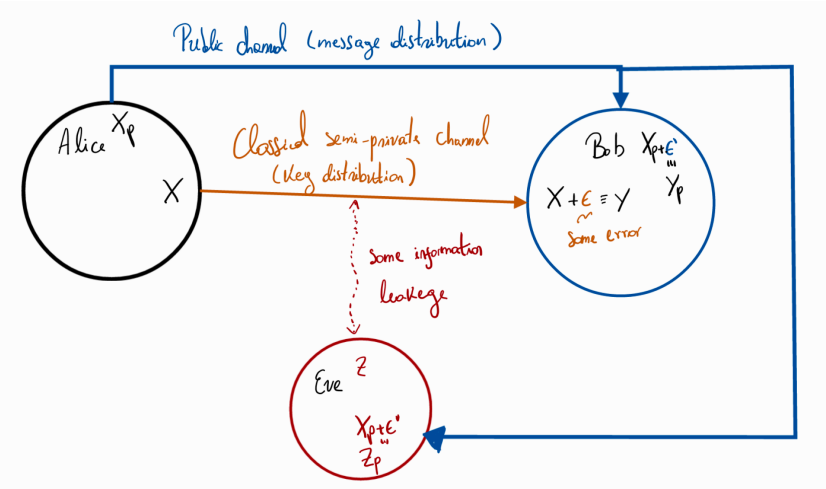


Figure 8: Private key setup.

où l'espace est également inclus comme un symbole possible. En outre, nous disposons d'informations préalables non seulement sur les occurrences, mais aussi sur les corrélations entre ces occurrences, c'est-à-dire que si la première lettre est un a, alors nous avons les probabilités conditionnelles

$$p(x_2 = b|x_1 = a) = \frac{\text{tous les messages d'un (deux, trois) mots qui commencent par a et dont la deuxième lettre est } b}{\text{tous les messages de 7 symboles qui commencent par } a}, \tag{2.2}$$

nous pouvons faire de même avec $p(x_3 = c|x_2 = b, x_1 = a)$ et ainsi de suite.

Maintenant, imaginez que dans le même canal public de 7 symboles, Alice et Bob échangent des messages, et que nous, en tant qu'espions, ne savons pas s'ils mettent à jour leur clé à chaque fois ou s'ils utilisent la même clé de 7 symboles tout le temps. Pour déterminer cela, nous pouvons examiner les occurrences de chaque symbole, leurs positions, et les corrélations entre les symboles, puis les comparer avec nos connaissances a priori. Pour organiser nos informations, nous pouvons classer les occurrences par ordre décroissant, comme par exemple, dans la table 1. Ensuite, la première chose que nous pouvons faire est de vérifier si la distribution résultante est uniforme ou si elle présente un biais. Nous pouvons le faire en utilisant la distance entre les fréquences relatives et la distribution aléatoire. Concrètement, supposons que le nombre total d'échantillons soit N, alors nous définissons

symbole	occurrences dans x_1
W	2743
Q	2525
B	2321
⋮	⋮

Table 1: Occurrences comptées par l'espionne Eve des symboles dans les messages entre Alice et Bob. Ils utilisent une clé finie, et ainsi, il y a un biais dans le comptage des symboles.

la distribution observée comme

$$p(x_1 = W) = \frac{2743}{N}, \tag{2.3}$$

et ainsi de suite pour les autres. Évidemment, la distribution aléatoire est

$$p(x_1 = W) = \frac{1}{\text{nombre de symboles}}. \tag{2.4}$$

Une mesure valide de la distance entre deux distributions est

$$\Delta(X, Y) = \sum_{\alpha \in D} |p(X = \alpha) - p(Y = \alpha)|, \tag{2.5}$$

c'est-à-dire la somme sur tout l'espace des échantillons de la différence en valeur absolue entre la probabilité d'obtenir α dans chacune des distributions. Dans notre cas particulier, nous choisissons D pour être tous les symboles, X pour représenter la distribution des fréquences observées, et Y pour représenter la distribution uniforme. Essentiellement, à mesure que nous collectons de plus en plus de messages entre Alice et Bob, si la distance entre les deux distributions diminue, nous pouvons conclure que la clé n'est pas répétée et qu'ils utilisent soit un générateur véritablement aléatoire soit pseudo-aléatoire. En revanche, si la distance augmente en moyenne, nous pouvons conclure qu'il existe un biais systématique et qu'ils répètent leur clé. Dans le premier cas, notre seule voie de progrès est de déterminer s'ils utilisent ou non un générateur pseudo-aléatoire. Il existe assurément beaucoup de littérature sur la manière de procéder, mais nous n'en parlerons pas, car c'est un domaine de recherche à part entière. Dans le second cas, nous pouvons maintenant essayer de reconstruire cette clé finie $\mathbf{k}$. Comment la trouver ? La réponse à cette question est également un domaine de recherche en soi, mais nous pouvons esquisser un algorithme pour avoir une idée de la manière dont cela pourrait être fait.

Imaginons que nous choisissions simplement une clé au hasard $\mathbf{k_0}$, puis qu'avec cette clé nous transformions les messages observés $\mathbf{x}$ en un message décodé,

$$\mathbf{x} \to \mathbf{k}_0(\mathbf{x}). \tag{2.6}$$

Nous pouvons imaginer une fonction $L : \mathbf{k}(\mathbf{x}) \to [0, 1]$, qui mesure simplement la probabilité que les mots obtenus soient effectivement des mots anglais et que le message soit cohérent ou non. Encore une fois, la manière exacte de procéder est un domaine de recherche à part entière qui, en fin de compte, a donné naissance à des IA génératrices de texte comme ChatGPT. Disons simplement ici qu'une telle fonction existe et que nous lui faisons confiance. Ensuite, nous pouvons exécuter une optimisation par descente de gradient sur l'espace des clés et trouver celle qui maximise la fonction de probabilité L. Naturellement, une telle approche présente les inconvénients généraux de l'optimisation sur des espaces de paramètres vastes, mais elle est en général résoluble, de sorte que la sécurité de l'encryption n'est plus garantie. Au-delà de ces considérations mathématiques, il est clair que les protocoles à clé privée reposent sur la capacité à créer des canaux de communication sécurisés entre Alice et Bob pour partager la clé, mais comment pouvons-nous faire cela physiquement ? C'est en répondant à cette question que la cryptographie quantique a vu le jour, et nous allons examiner un exemple concret.

2.3 Key distribution

Comme nous l'avons mentionné, l'élément clé des protocoles à clé privée est la distribution des clés. En pratique, cela est réalisé de manière classique, et il existe plusieurs techniques pour surmonter les imperfections. En principe, nous pouvons également le faire de manière quantique, ce qui est provably sécurisé.

2.3.1 Classical key distribution

Ici, nous mentionnerons très brièvement ce que sont *l'amplification de la confidentialité* et *la réconciliation de l'information*. Donner des descriptions détaillées de cette procédure est hors du cadre de ce cours, mais connaître au moins leur existence semble approprié. Ce qui est le plus important, c'est d'avoir simplement une idée de la façon dont la distribution des clés est effectuée et étudiée dans le cadre classique, et ce qui changera lorsque nous passerons à la cryptographie quantique. Nous dessinons un schéma de l'architecture de la cryptographie classique dans fig. 6. Alice a un message, X, et elle le partage avec Bob à travers un canal semi-privé, c'est-à-dire qu'Eve, l'espionne, peut obtenir seulement une partie des informations envoyées à travers le canal. Comme dans tout processus de transmission d'informations, des erreurs peuvent survenir ; en fait, Bob reçoit le message avec une certaine erreur, et son message devient donc la variable aléatoire $Y = X + \epsilon$.

Maintenant, le canal semi-privé peut être difficile à construire (il peut même s'agir d'une personne), de sorte que l'on cherche à utiliser ces canaux aussi peu que possible, en leur préférant des canaux publics simples où seuls les messages sont envoyés. Seules les clés sont partagées par les canaux semi-privés, comme illustré dans la fig. 8.

Comme chaque canal est soumis à du bruit, imaginons qu'Alice et Bob partagent des chaînes de bits aléatoires corrélées X et Y, et que la corrélation avec une autre chaîne de bits aléatoires Z, qui appartient à Eve, est limitée. Des protocoles existent qui permettent la transmission fidèle d'informations entre Alice et Bob, tout en limitant l'information à laquelle Eve a accès. Mais que signifie limiter l'information d'Eve ? Pour comprendre cela, nous devons au moins savoir ce qu'est l'entropie et l'information mutuelle entre variables aléatoires.

Shannon entropy and mutual information

L'entropie de Shannon [15][3] d'une variable aléatoire X, qui pourrait être un message composé de 7 symboles, est définie comme

$$H(X) = H(p_1, \ldots, p_n) = -\sum_x p_x \log p_x, \tag{2.7}$$

où les p_x sont les probabilités d'obtenir un mot particulier. Par convention, on comprend que $0 \log 0 = 0$. Une façon utile de penser à l'entropie est de l'interpréter comme l'information acquise en moyenne lorsque la variable aléatoire X devient connue (c'est-à-dire est mesurée). On gagne le plus d'information lorsque la distribution est uniforme, et le moins lorsqu'elle est une delta. L'entropie de deux (ou n) variables aléatoires est définie de manière analogue,

$$H(X, Y) = -\sum_{x,y} p(x, y) \log p(x, y). \tag{2.8}$$

L'entropie possède plusieurs propriétés intéressantes, et nous en listons ici deux :

- C'est une fonction lisse des probabilités uniquement.
- Elle est sous-additive, c'est-à-dire $H(X, Y) \leq H(X) + H(Y)$ avec égalité seulement si X et Y sont indépendants. Cela quantifie le fait que les corrélations limitent les résultats possibles et que nous gagnons des informations sur Y en mesurant X et vice versa.

L'information mutuelle entre deux variables aléatoires est définie comme

$$H(X : Y) = H(X) + H(Y) - H(X, Y). \tag{2.9}$$

À partir de la propriété sous-additive mentionnée ci-dessus, nous voyons que cela quantifie simplement à quel point les variables aléatoires X et Y sont corrélées, ou combien d'informations elles partagent en commun. Dans le cas extrême où $Y = X$, $H(X, Y) = H(X)$ et $H(X : Y)$ est simplement égal à $H(X)$.

[3] L'article est vraiment bon, si vous avez le temps, allez le lire. For the pedagogical introduction see chapter 11 of [1].

Maintenant, regardons le schéma de la fig. 9. Minimiser l'information d'Eve signifie minimiser l'information mutuelle $H(X:Z)$ et $H(Y:Z)$, et maximiser la fidélité de transmission de l'information signifie maximiser l'information mutuelle $H(X:Y)$. Pour maximiser l'information mutuelle entre Alice et Bob, $H(X:Y)$, qui n'est pas $H(X)$ à cause du bruit dans le canal, nous pouvons utiliser les techniques et méthodes de *correction d'erreurs*. En résumé, la *correction d'erreurs* consiste à utiliser des ressources physiques redondantes (informations redondantes) pour transmettre (communication, algorithmes) ou préserver (mémoires) un sous-ensemble des informations disponibles dans le système physique. L'exemple le plus élémentaire est le code de répétition.

The repetition code

Imaginez qu'Alice souhaite envoyer un bit à travers un canal bruyant, où l'effet du bruit est d'inverser le bit de 0 à 1 avec une certaine probabilité p. Le code de répétition consiste simplement à envoyer un groupe de bits physiques, tous initialisés à 0 ou 1, de telle sorte que Bob doit effectuer un comptage majoritaire pour décider quel bit Alice a tenté d'envoyer. Si une seule erreur se produit, trois bits suffisent pour une transmission d'information *tolérante aux fautes*.

$$000 \to \{100, 010, 001\}$$

Ainsi, avec l'utilisation de la correction d'erreurs, Alice et Bob transforment tous deux leurs messages correspondants X et Y en un message corrigé W. Dans l'exemple ci-dessus, pour Alice $000 \to 0$ et pour Bob $100 \to 0$ par exemple. Ce processus de correction des erreurs du canal bruyant est connu sous le nom de *réconciliation d'informations*.

L'étape suivante consiste à réduire l'information mutuelle $H(W:Z)$. Ce processus est appelé *amplification de la confidentialité*. Cela peut être réalisé par l'application de *hash functions*. Une fonction de hash g prend n bits et les transforme en m bits, et possède la propriété suivante. Soient x_1 et x_2 deux chaînes de bits de n bits. Alors, $g(x_1) \neq g(x_2)$ avec une probabilité d'au moins $1/2^m$. C'est une fonction très utile car, en un certain sens, elle sépare l'espace des chaînes de bits en blocs presque séparables, et trouve des applications non seulement en cryptographie mais aussi en tomographie quantique [16]. Donner plus de détails dépasse le cadre de ce cours, mais vous devriez maintenant avoir suffisamment de connaissances pour aller lire davantage sur le sujet.

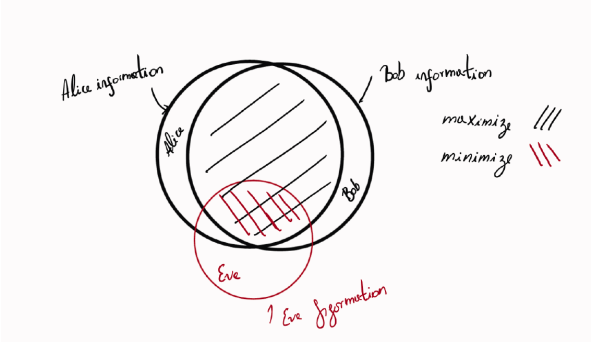


Figure 9: Objectif de la cryptographie

2.3.2 Quantum key distribution

QKD est un protocole *prouvablement* sécurisé, qui permet de créer des clés privées via un canal public. Ensuite, les clés privées peuvent être utilisées comme ci-dessus pour créer un canal de communication classique sécurisé. La condition physique minimale pour que cela soit possible est la capacité de communiquer des qubits via le canal public avec un taux d'erreur en dessous d'un certain seuil. La sécurité d'un tel schéma repose sur deux faits :

- Le théorème de non-clonage, qui est formellement pas unique au quantique, car les ensembles ne peuvent pas non plus être clonés, see [17], you will find further references there.
- Le gain d'information implique une perturbation.

Regardons donc d'abord le théorème de non-clonage.

Théorème de non-clonage

Le théorème de non-clonage stipule qu'il est impossible de réaliser la transformation suivante,

$$|\psi_A\rangle |\psi_B\rangle |\psi_C\rangle \rightarrow_{\hat{U}} |\varphi_A\rangle |\psi_B\rangle |\psi_B\rangle . \tag{2.10}$$

En d'autres termes, il n'est pas possible de cloner un état quantique arbitraire $|\psi_B\rangle$ via une évolution unitaire. La preuve est simple. Comme le système A représente une ancilla, nous ne pouvons l'ignorer pour capturer la preuve et devons supposer qu'il fait partie de la transformation unitaire. C'est-à-dire que nous souhaitons prouver qu'il n'existe pas de transformation unitaire $\hat{U}$ telle que

$$|\psi_B\rangle |\psi_C\rangle \rightarrow_{\hat{U}} |\psi_B\rangle |\psi_C\rangle , \tag{2.11}$$

pour un état quantique initial inconnu $|\psi_B\rangle$ et tout état $|\psi_C\rangle$ que nous pouvons préparer. Nous pouvons également écrire $U(|\psi\rangle |a\rangle) = |\psi\rangle |\psi\rangle$. Nous allons faire la preuve par contradiction. Supposons qu'un tel unitaire existe. Alors, il fonctionnerait pour deux états particuliers, disons $|\varphi\rangle$ et $|\psi\rangle$, c'est-à-dire

$$\begin{aligned} U(|\varphi\rangle |a\rangle) &= |\varphi\rangle |\varphi\rangle \\ U(|\psi\rangle |a\rangle) &= |\psi\rangle |\psi\rangle . \end{aligned} \tag{2.12}$$

En prenant le produit scalaire des deux équations, nous obtenons simplement,

$$\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2, \tag{2.13}$$

ce qui signifie que $|\psi\rangle$ et $|\varphi\rangle$ sont soit orthogonaux, soit égaux, une contradiction. Par conséquent, nous concluons qu'un tel $\hat{U}$ n'existe pas pour des états arbitraires, mais il peut certainement exister si nous ne nous soucions que d'un ensemble orthonormal d'états (c'est-à-dire une base particulière de l'espace). Il est curieux de voir comment nous pouvons cloner un ensemble de base, c'est-à-dire cloner chaque ket de la base, mais pas leurs combinaisons linéaires (superpositions).

Le gain d'information implique une perturbation

Plus concrètement, toute tentative de distinguer entre deux états quantiques non orthogonaux entraîne un gain d'information uniquement au prix d'une perturbation du signal. Prouver cette affirmation est également élémentaire. Supposons qu'Alice communique via un canal public avec Bob, où elle enverra des états quantiques. Prenons deux de ces états possibles qu'elle peut communiquer et qui sont non orthogonaux, disons $|\psi\rangle$ et $|\varphi\rangle$. Maintenant, Eve souhaite obtenir des informations sur ces états. Naturellement, elle possède également son propre état de registre, disons $|z\rangle$. Obtenir des informations sans perturber les états signifie effectuer la transformation suivante,

$$|\psi\rangle |z\rangle \rightarrow |\psi\rangle |v\rangle \tag{2.14}$$

$$|\varphi\rangle |z\rangle \rightarrow |\varphi\rangle |v'\rangle , \tag{2.15}$$

où évidemment pour qu'Eve puisse obtenir des informations, il doit être vrai que $|v\rangle \neq |v'\rangle$. Maintenant, toutes ces transformations doivent nécessairement être unitaires (rappelez-vous, pour obtenir une dynamique non unitaire, nous devons retracer certaines parties du système, mais si nous ne les retraçons pas, toutes les transformations sont unitaires), ce qui signifie que le produit scalaire est préservé. En prenant le produit scalaire de chaque ligne ci-dessus, nous obtenons,

$$\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle \langle v|v'\rangle \implies \langle v|v'\rangle = 1. \tag{2.16}$$

Ainsi, il est impossible d'obtenir des informations sans perturber l'état.

Ainsi, Alice exploite ce fait et transmet à Bob des états non orthogonaux. En vérifiant les perturbations dans les états transmis, Alice et Bob peuvent établir des limites supérieures sur le bruit ou

l'espionnage se produisant dans leur canal de communication. Naturellement, tout comme dans le cas classique, Alice et Bob effectueront une réconciliation de l'information (possiblement en utilisant la correction d'erreurs), et une amplification de la confidentialité (peut-être en utilisant des fonctions de hachage). Examinons maintenant un exemple particulier.

BB84

Alice commence par générer deux chaînes de bits aléatoires, a et b, chacune composée de $(4+\delta)n$ bits. Elle encode ensuite ces chaînes en $(4+\delta)n$ qubits,

$$|\psi\rangle = \otimes_{k=1}^{(4+\delta)n} |\psi_{a_k b_k}\rangle \,, \tag{2.17}$$

où

$$|\psi_{00}\rangle = |0\rangle \,, \tag{2.18}$$
$$|\psi_{10}\rangle = |1\rangle \,, \tag{2.19}$$
$$|\psi_{01}\rangle = |+\rangle \,, \tag{2.20}$$
$$|\psi_{11}\rangle = |-\rangle \,. \tag{2.21}$$

En d'autres termes, les bits b déterminent la base dans laquelle le bit a est encodé, soit Z soit X. Si des photons sont utilisés pour transmettre l'information, cela correspond à l'utilisation de la polarisation horizontale et verticale comme bases, ou de la base de polarisation inclinée à 45 degrés, voir fig. 10.

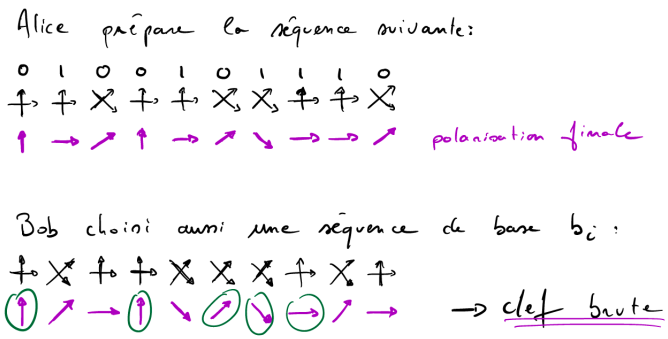


Figure 10: Alice envoie un ensemble de qubits encodés dans deux ensembles de polarisation différents. Mathieu's notes.

Concentrons-nous d'abord sur le protocole sans l'interférence d'Eve, nous discuterons de ce qui se passe lorsqu'elle intervient plus tard. Voir fig. 11 pour un diagramme. Lorsque Bob décide de mesurer, il ne connaît pas la base, mais il génère simplement une chaîne de bits aléatoires b' pour servir de base. Comme $b \neq b'$, tous les bits ne seront pas utiles à la fin, c'est pourquoi des bits redondants δn sont utilisés. Ensuite, Bob annonce qu'il a reçu l'état, et ce n'est qu'alors qu'Alice rend public la base b avec laquelle elle a envoyé les qubits (photons dans ce cas). Avec cette information, Bob peut indiquer à Alice quels bits il a mesurés dans la bonne base. En rendant δ suffisamment grand, il est presque garanti qu'au moins $2n$ mesures ont été correctes. Pour vérifier la présence d'espions, Alice sélectionne n bits aléatoires parmi les $2n$ restants et indique à Bob quels n bits de contrôle elle a choisis. Ensuite, tous deux peuvent rendre publics ces n bits. Si le nombre de bits différents E est supérieur à un certain seuil t, ils abandonnent le protocole. Sinon, ils passent à la distillation de l'information et à l'amplification de la confidentialité avec les n bits secrets restants. Dans fig. 10, la chaîne de bits partagée par Bob et Alice est celle entourée de vert, c'est-à-dire 00011.

Que se passe-t-il lorsque Eve espionne ? Si elle mesure les qubits (photons), elle doit choisir une base pour le faire, et ce choix sera incorrect en moyenne 1/2 du temps, voir fig. 12. La mesure fait s'effondrer le qubit (photon) sur un des états propres de la base choisie (polarisation). Ainsi, lorsque Bob effectue sa mesure, la probabilité qu'il obtienne un bit incorrect, aux positions où Eve a fait un choix de base incorrect, est de 1/2. Par conséquent, la probabilité totale par bit que Bob ait une erreur

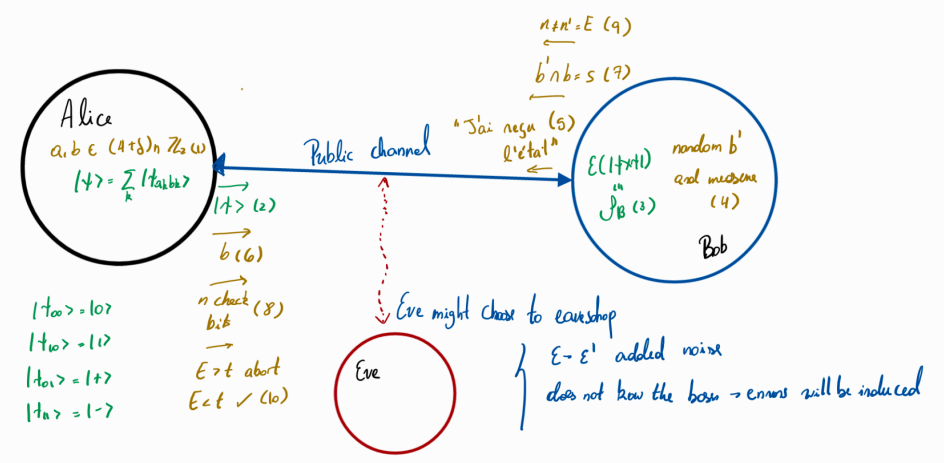


Figure 11: Diagramme pour BB84. Les chiffres entre parenthèses représentent les étapes temporelles du protocole.

est $(1/2)^2 = 1/4$. La probabilité que Bob n'ait aucune erreur si Eve a mesuré n bits est $(1/4)^n$. Donc, si un nombre suffisamment grand de bits est utilisé, si Eve essaie de mesurer beaucoup d'entre eux, l'espionnage sera presque certainement détecté. Pour 72 bits, la probabilité de ne pas détecter une erreur est d'environ 10^{-9}, en d'autres termes, en moyenne, dans un cas sur un milliard, Eve ne serait pas détectée. Si Eve choisit de n'en mesurer que quelques-uns, elle n'aura encore qu'une information marginale sur la clé résultante.

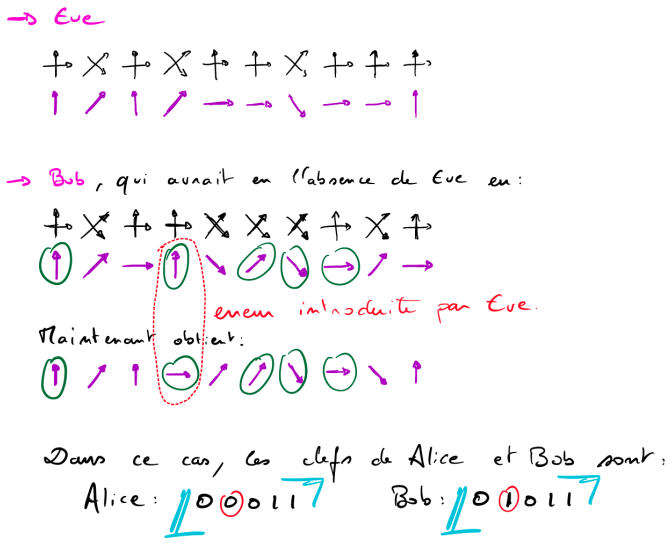


Figure 12: Que se passe-t-il lorsque Eve espionne avec une mesure ?

Generic drawbacks

Comment les protocoles QKD sont-ils vulnérables aux attaques ? Certains types d'attaques sont les mêmes que pour les protocoles de clé privée classiques, notamment :

- Attaque de l'homme du milieu : une personne usurpe l'identité de Bob.
- Coupure des communications (littéralement couper le câble de fibre optique, par exemple, ce qui n'est pas très subtil).

- Cheval de Troie. Cela consiste à envoyer un signal qui exploite une fonction non idéale de l'équipement utilisé par Alice et Bob. Par exemple, les détecteurs de photons uniques peuvent générer des « post-impulsions », c'est-à-dire des impulsions après la détection, surtout si le signal entrant était fort. Eve peut donc essayer d'exploiter cela en envoyant à Bob une impulsion forte, puis en mesurant la post-impulsion qui revient, afin d'obtenir des informations sur la base que Bob utilise pour mesurer. Cependant, si Bob change constamment de base au hasard, je ne suis pas sûr de l'efficacité de cette méthode pour Eve. Quoi qu'il en soit, c'est un sujet à aborder lorsque l'on travaille vraiment dessus.

Un autre type d'attaque pourrait exploiter le fait que, si des impulsions laser atténuées sont utilisées pour générer les photons, lorsque l'objectif est d'envoyer un seul photon, il existe une probabilité d'en envoyer deux au lieu d'un, ouvrant ainsi une fenêtre pour qu'Eve en stocke un.

People keeps studying this, see for example [18].

3 Noise in interferometer

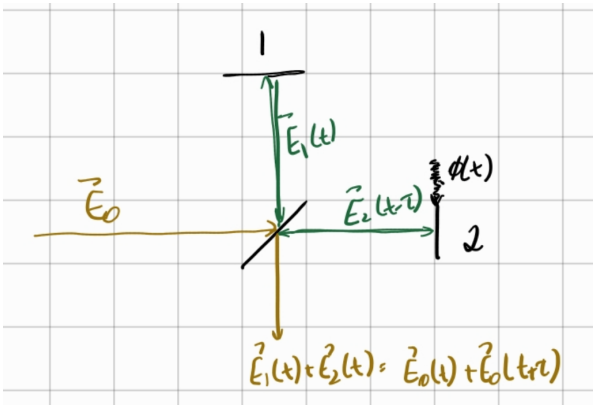


Figure 13: Interferometer.

Take the situation in fig. 13. Call E_i the field that goes to each mirror. We want to know the visibility of the field coming out of the intereferometer, that is

$$\nu = \frac{I_{max} - I_{min}}{I_{max} + I_{min}}, \tag{3.1}$$

with $I(t) = \left\langle |E(t)|^2 \right\rangle$. From linearity and its definition,

$$I(t) = \left\langle |E(t)|^2 \right\rangle = \langle |(E_1(t) + E_2(t))(E_1(t) + E_2(t))^*| \rangle = \left\langle |E_1(t)|^2 \right\rangle + \left\langle |E_2(t)|^2 \right\rangle + \langle 2Re(E_1(t)E_2(t)^*) \rangle . \tag{3.2}$$

In the noiseless case $E_1(t) = E_0 e^{-iwt}$ and $E_2(t) = E_0 e^{-iw(t+\tau)}$, where τ is the delay dependent on the mirrors positioning. Moreover, the brackets stand there to mean ensemble average. For a setup where noise is stationary, the ensemble average is equivalent to the average over long times, so we write

$$\langle f(t) \rangle \equiv \lim_{T \to \infty} \frac{1}{T} \int_0^T \mathrm{d}t f(t), \tag{3.3}$$

where $t = 0$ signals the start of the measurement record. Experimentally, we would just take some finite T and check the average is converging. If $f(t)$ is convergent over infinite time, then we might also use

$$\langle f(t) \rangle = \int_0^\infty \mathrm{d}t f(t), \quad \text{or} \quad \langle f(t) \rangle = \int_{-\infty}^\infty \mathrm{d}t f(t), \tag{3.4}$$

however in this case note that $\left\langle |E(t)|^2 \right\rangle$ would diverge, so for the connection between correlations with visibility we will derive below to be true we need to take the average, not just the integral. The

normalized first order correlation function between the two fields E_1 and E_2 is defined as

$$g^{(1)}(E_1, E_2)(t) = \frac{\langle E_1(t)E_2(t)^*\rangle}{\sqrt{\langle |E_1(0)|^2\rangle \langle |E_2(0)|^2\rangle}}. \tag{3.5}$$

In this case, as both $E_1(t)$ and $E_2(t)$ are sourced by the same field $E_0(t)$ just delayed from one another, we rewrite the first order correlation function as

$$g^{(1)}(\tau) = \frac{\langle E_1(t)E_2(t+\tau)^*\rangle}{\langle E_1(t)E_2(t)^*\rangle} = \frac{1}{|E_0|^2}\langle E_0(t)E_0(t+\tau)^*\rangle = e^{i\omega\tau}, \tag{3.6}$$

then is clear that the intensity of the field is given by

$$I(\tau) = I_1 + I_2 + 2\sqrt{I_1 I_2}Re[g^1(E_1, E_2)(\tau)] = 2I_0[1 + Re[g^{(1)}(\tau)]]. \tag{3.7}$$

From it, we get $I_{max} = 2I_0(1 + |g^{(1)(\tau)}|)$ and $I_{min} = 2I_0(1 - |g^1(\tau)|)$, which leads to $\nu = |g^1(\tau)|$. Importantly, this tells us that we can learn the amplitude of the first order correlation function between the fields in the interferometer by measuring the visibility of the outgoing field.

Now, if we add the noise, this is simply a random delay, hence,

$$g^{(1)}(\tau) = \frac{1}{|E_0|^2}\langle E_0(t)E_0(t+\tau+\phi(t))^*\rangle = e^{i\omega\tau}\left\langle e^{i\omega\phi(t)}\right\rangle. \tag{3.8}$$

Now, the ensemble average of an stationary noise source $f(\phi(t))$ is given by

$$\langle f(\phi(t))\rangle = \lim_{T\to\infty}\frac{1}{T}\int_0^T \mathrm{d}t f(\phi(t)) = \lim_{N\to\infty}\frac{1}{N(T/N)}\sum_{n=0}^{N}\frac{T}{N}f(\phi(t_n)) = \lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N} f(\phi_n) \equiv \langle f(\phi)\rangle, \tag{3.9}$$

being stationary the actual values of t_n do not matter, and we are left with the usual statistical mean of the noise. Hence, if the noise ϕ is sampled from a distribution $\varphi(\phi)$, the mean is by definition

$$\langle f(\phi)\rangle = \int \mathrm{d}\phi f(\phi)\varphi(\phi). \tag{3.10}$$

So, if for example say we have gaussian noise, that is ϕ is sampled from $\varphi \propto e^{-\phi^2/2\sigma^2}$[4], then we get $\langle e^{i\omega\phi(t)}\rangle = e^{-(\sigma\omega)^2/2}$. This means that if the standard deviation of the noise is much larger than the period of the wave all coherence is lost and indeed $|g^{(1)}(\tau)| \to 0$. In other words, if the noise displaces our mirror a distance larger than a wavelength of the incoming light source, coherence is greatly diminished. However, if the noise is weak, that is, wiggles the mirror with an amplitude smaller than the wavelength of the source, then coherence is only partially diminished. For a microwave source $\omega \sim 1$ GHz, then $\lambda \sim 1$ cm, so we expect the coherence to be preserved in general, and even for optical frequencies $\omega \sim 1$ THz, then $\lambda \sim 0.1$ mm [5].

4 Course-4. Exercises. QND

From [19]: Une mesure quantique non destructive de A est une séquence de mesures telle qu'après la première mesure, toutes les mesures ultérieures sont entièrement prévisibles (en l'absence de forces externes) à partir du résultat de la mesure précédente.

Notez qu'il s'agit d'une propriété du système à mesurer, c'est-à-dire, lorsqu'il est préparé dans un état propre de A, comment évolue le système ? L'incertitude sur A augmente-t-elle ou reste-t-elle constante? Analysons le cas le plus simple des mesures projectives. Supposons que $A(t_0) = \sum A_0 P_{A_0}$, $A(t_1) = \sum A_1 P_{A_1}$, des opérateurs hermitiens reliés par l'évolution hamiltonienne dans l'image de Heisenberg

$$\frac{\mathrm{d}A}{\mathrm{d}t} = -i[H, A] + \frac{\partial A}{\partial t}. \tag{4.1}$$

[4] credits to Nicolas for doing it in his HW and forcing me to think carefully about this.

[5] if some experimentalist can tell me how much they expect their mirrors to wiggle at room temperature please do it, will make me happy to know. Also one could probably calculate it with Einstein's model of a solid, the mass of the molecules forming it and the temperature it has. Even simpler, just consider the center of mass of the mirror to be hooked, and treat the whole thing as an harmonic oscillator.

Toute mesure projective correspond à l'échantillonnage de l'état d'un ensemble défini par l'état au moment de la mesure, et l'opérateur de mesure dans ce cas A, donc au temps t_0

$$|\psi(t_0)\rangle \in \left\{ \frac{P_{A_0}|\psi_0\rangle}{\sqrt{p(A_0)}} \right\},\ p(A_0) = \langle\psi_0|P_{A_0}|\psi_0\rangle\,. \tag{4.2}$$

Pour une mesure projective parfaite (impossible en pratique pour des raisons thermodynamiques), nous lisons la valeur propre A_0 et mettons donc à jour l'état (Copenhague) en $|\psi(t_0)\rangle = \sum_\alpha c_\alpha |A_0, \alpha\rangle$, c'est-à-dire une superposition des états propres de $A(t_0)$ de valeur propre A_0. Maintenant, $A(t)$ évolue jusqu'à $A(t_1)$, et nous répétons la mesure, donc,

$$|\psi(t_1)\rangle \in \left\{ \frac{P_{A_1}|\psi(t_0)\rangle}{\sqrt{p(A_1|A_0)}} \right\} = \left\{ \frac{P_{A_1}P_{A_0}|\psi(0)\rangle}{\sqrt{p(A_1|A_0)p(A_0)}} \right\},\ p(A_1|A_0) = \frac{\langle\psi(0)|P_{A_0}P_{A_1}P_{A_0}|\psi(0)\rangle}{\langle\psi(0)|P_{A_0}|\psi(0)\rangle}. \tag{4.3}$$

Le résultat de la mesure sera une certaine valeur propre A_1, et pour que celle-ci soit une fonction déterministe, il est nécessaire qu'un seul des projecteurs P_{A_1} soit non orthogonal à P_{A_0} ; sinon, nous aurions un ensemble avec deux éléments ou plus à échantillonner, rendant le résultat non déterministe. En d'autres termes, il faut que $p(A_1|A_0) = 1$ pour une certaine valeur A_1 et que $p(A_1'|A_0) = 0$ pour toutes les autres. Le fait que $P_{A_1}P_{A_0} = P_{A_0} \implies P_{A_1} = P_{A_0}$ nous permet d'imaginer la solution comme une sorte de QEC (Correction d'Erreur Quantique), où les blocs orthogonaux sont mappés à des blocs orthogonaux. Ainsi, nous avons

$$A(t_1) = \sum f_1(A_0)P_{A_0}, \tag{4.4}$$

et en général si nous avons un QND *continu*

$$A(t) = \sum f_t(A_0)P_{A_0}. \tag{4.5}$$

Il en résulte que $[A(t), A(t_0)] = 0$ pour tout t.

Maintenant que nous savons ce qu'est un observable QND, quels sont les observables QND d'un oscillateur harmonique $H_0 = \omega a^\dagger a$? Eh bien, il est clair que le nombre de photons $a^\dagger a$ est un observable trivial. Un couple d'observables moins triviales sont les quadratures évolutives,

$$\begin{aligned} X_1(t) &= e^{i\omega nt}qe^{-i\omega nt} = q\cos(\omega t) + p\sin(\omega t), \\ X_2(t) &= e^{i\omega nt}pe^{-i\omega nt} = p\cos(\omega t) - q\sin(\omega t), \end{aligned} \tag{4.6}$$

d'où il suit immédiatement que dans l'image de Heisenberg $[X_i(t), X_i(t')] = 0$.

Maintenant que nous savons ce qu'est un observable QND, comment peut-on les mesurer concrètement ? En utilisant un système de mesure, on a le hamiltonien total,

$$H = H_0 + H_I + H_M, \tag{4.7}$$

et naturellement on impose la même condition, $[A(t_0), A(t)] = 0$. Pour un observable A qui ne dépend pas du temps, cela se réduit à $[A, H_0 + H_M] = 0$. Étant donné qu'il s'agit d'un observable QND, nous savons déjà que $[A, H_0] = 0$, d'où la condition nécessaire $[A, H_M] = 0$.

Pour deux oscillateurs harmoniques, la mesure QND la plus simple est donnée par l'interaction

$$H_I = \chi a^\dagger a b^\dagger b, \tag{4.8}$$

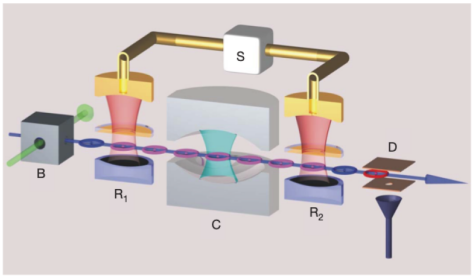
où a est l'opérateur d'annihilation du système. À ce stade, suivez simplement les notes que Mathieu m'a données avec les exercices, charge-exercices-4.

Des remarques importantes concernent la question suivante : étant donné un opérateur B de la sonde de mesure, quelle quantité d'information B porte-t-il sur l'observable QND A ? Supposons que B soit lui-même un observable QND du système de mesure, alors le seul ingrédient dynamique est H_I. Quelle est donc l'information maximale atteignable entre A et B pour tout H_I ? Un choix particulier est la corrélation entre les observables, à savoir

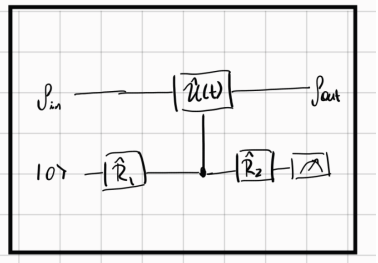
$$C^2(A, B) = \frac{|\langle AB\rangle - \langle A\rangle\langle B\rangle|^2}{V(A)V(B)} = \frac{|\mathrm{Cov}(A, B)|^2}{V(A)V(B)}. \tag{4.9}$$

Maintenant, nous allons effectuer un simple effet Zeno en mesurant un qubit.

Il est important de noter que si nous pouvions effectuer des mesures projectives d'une rapidité infinie, alors nous pourrions en effet figer l'état. Cependant, des considérations thermodynamiques nous empêchent d'avoir des mesures d'une rapidité infinie.



(a) Expérience de Haroche.



(b) Représentation par un circuit.

5 Course-5. Exercises. QND-2

Les exercices sont dans le document charge-exercise 4 et pqi2021-22.

Le premier ensemble de questions porte sur la mesure QND des photons dans une cavité réalisée par Haroche et ses collaborateurs [20, 21]. Dans cette expérience, le montage est représenté par la fig. 14a, que l'on peut schématiser comme dans la fig. 14b. Les atomes sont utilisés pour effectuer une mesure QND du champ de la cavité afin d'observer des trajectoires quantiques et de modifier l'état du champ. La cavité cible C est placée entre deux cavités ancillaires $R_{1,2}$ qui sont utilisées pour préparer les atomes avant leur entrée dans C et pour les manipuler avant de les mesurer.

5.1 État atome-champ et mesure QND

Q1. Les cavités micro-ondes $R_{1,2}$ sont utilisées pour préparer les atomes dans des états de superposition. Elles contiennent un champ *classique* $E_0\cos(\omega t+\Phi)$ (c'est-à-dire un champ d'état cohérent avec un nombre élevé de photons tel que $\mathrm{Var}[q]/|\alpha|\ll 1$), résonant avec la transition $g-e$ à ω_0, qui excite le dipôle atomique avec une fréquence de Rabi Ω. Expliquez pourquoi et comment elles réalisent la rotation

$$R(\phi)=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & e^{i\phi}\\ e^{-i\phi} & 1\end{pmatrix}. \tag{5.1}$$

Ici, ϕ est une phase que les expérimentateurs peuvent contrôler.

A1. Si les champs sont de type classique, résonants avec la transition atomique et excitant son dipôle, alors la situation est bien décrite par le Hamiltonien,

$$H=\omega_0\sigma_-^\dagger\sigma_-+\frac{\Omega}{2}(e^{i\omega t}e^{i\Phi}\,|g\rangle\langle e|+h.c.) \tag{5.2}$$

En passant à un cadre tournant avec $U=|g\rangle\langle g|+e^{i\omega t}\,|e\rangle\langle e|=R_z(\omega t)$, c'est-à-dire le cadre effectuant une rotation autour de l'axe z dans la sphère de Bloch, on obtient le Hamiltonien simplifié

$$H_U=\begin{pmatrix}0 & e^{i\Phi}\Omega/2\\ e^{-i\Phi}\Omega/2 & -\Delta\end{pmatrix}, \tag{5.3}$$

avec $\Delta=\omega-\omega_0$ le désaccord.

En résonance, $\Delta=0$, et nous pouvons écrire le Hamiltonien ci-dessus comme

$$H=R_z(-\Phi)\sigma_x R_z^\dagger(-\Phi), \tag{5.4}$$

où $R_z(\phi)$ est une rotation autour de l'axe z dans la sphère de Bloch. En général, il est pratique d'écrire la rotation générale dans la sphère de Bloch comme

$$R(\mathbf{n},\phi)\equiv\exp(-i\phi\mathbf{n}\cdot\sigma/2)=\cos(\phi/2)I-i\sin(\phi/2)\mathbf{n}\cdot\sigma, \tag{5.5}$$

où $\mathbf{n}$ est un vecteur de norme 1 et $\sigma=(\sigma_x,\sigma_y,\sigma_z)^T$ est le vecteur de Pauli. En utilisant les coordonnées sphériques $\mathbf{n}(\theta,\varphi)=(\sin\theta\cos\varphi,\sin\theta\sin\varphi,\cos\theta)$. Ainsi, nous écrivons toute rotation comme $R(\phi,\theta,\varphi)$. Par exemple, $R_z(\phi)=R(\phi,0,\varphi)$ (notez que pour $\theta=0 \mod \pi$, toute valeur de φ donne le même vecteur). Avec cette notation,

$$H=\mathbf{n}(\pi/2,-\Phi)\cdot\sigma, \tag{5.6}$$

et l'évolution est simplement la rotation autour de cet axe $R(\Omega t, \pi/2, \Phi)$ (j'ai ignoré le signe moins non pertinent sur Φ), qui se lit explicitement

$$R(\Omega t, \pi/2, \Phi) = \frac{1}{\sqrt{2}} \begin{pmatrix} \cos(\Omega t/2) & -ie^{-i\Phi}\sin(\Omega t/2) \\ -ie^{i\Phi}\sin(\Omega t/2) & \cos(\Omega t/2) \end{pmatrix}, \tag{5.7}$$

en fixant donc $\Omega t = \pi/2$ et $\Phi = -\phi - \pi/2$, on obtient la rotation souhaitée. Bien sûr, en réalité, il existe des incertitudes sur la valeur de Ω, Δ, ainsi que des problèmes de fuite et de relaxation à prendre en compte, mais le scénario idéal que nous traiterons ici est relativement simple et capture les caractéristiques pertinentes.

Q2. Les atomes et la cavité C sont désaccordés de $\delta = \omega - \omega_0$. Dans ce régime dispersif $g \ll \delta$, la cavité contenant n photons imprime sur les états des atomes une phase qui dépend de n. Expliquez qualitativement, avec des équations, quelle est cette phase.

A2. Imprimer une phase sur les états des atomes signifie que la phase attachée aux états g, e diffère. C'est la définition d'une porte de phase contrôlée entre le qubit et la cavité, représentée par l'unitaire du milieu dans fig. 14b. En général, nous pouvons écrire une telle opération comme suit :

$$|\psi\rangle \otimes (c_g |g\rangle + c_e |e\rangle) \to c_g U |\psi, g\rangle + c_e U |\psi, e\rangle . \tag{5.8}$$

L'opérateur U agit à la fois sur le qubit et la cavité. Naturellement, U dépend de l'Hamiltonien du système à partir duquel nous dérivons ces opérateurs unitaires, mais nous ignorons cela pour l'instant afin de nous concentrer sur les opérations permises par la théorie. Dans ce cas, nous utilisons le qubit comme mesure ; nous le mesurerons après l'interaction. Effectuer une mesure projective du qubit aboutit à deux états de la cavité conditionnés sur le résultat de la mesure,

$$\rho(g) = \frac{K_g \rho K_g^\dagger}{\mathrm{tr}\Big(K_g \rho K_g^\dagger\Big)};\ \rho(e) = \frac{K_e \rho K_e^\dagger}{\mathrm{tr}\Big(K_e \rho K_e^\dagger\Big)}, \tag{5.9}$$

où $K_{e/g} = \langle e/g| U(c_e |e\rangle + c_g |g\rangle)$ sont appelés opérateurs de Kraus, qui satisfont la condition $K_g^\dagger K_g + K_e^\dagger K_e = I$. Selon les postulats de la MQ, la théorie nous dit que la probabilité de mesurer le qubit dans l'état g/e est donnée par $\mathrm{tr}\Big(K_{g/e} \rho K_{g/e}^\dagger\Big)$ où ρ est la matrice de densité pour l'état de la cavité. Un cas particulier de ce scénario est celui dans lequel l'action de U consiste simplement à ajouter une phase dépendante de l'état du qubit, soit

$$|\psi\rangle \otimes (c_g |g\rangle + c_e |e\rangle) \to c_g U |\psi, g\rangle + c_e U |\psi, e\rangle = c_g |\psi, g\rangle + e^{i\alpha} c_e |\psi, e\rangle = |\psi\rangle \otimes (c_g |g\rangle + e^{i\alpha} c_e |e\rangle). \tag{5.10}$$

Dans ce cas, nous voyons que la cavité n'est pas affectée par l'interaction, et la phase α porte des informations sur son état ; ainsi, mesurer le qubit par la suite sera une mesure QND. Cela n'est possible que si $|\psi, g/e\rangle$ sont des états propres de U, et donc de l'Hamiltonien du système qubit-cavité. Concrètement, pour l'Hamiltonien de JC, nous savons que les états propres sont

$$\begin{aligned} |+, n\rangle &= \sin\theta_n |g, n\rangle + \cos\theta_n |e, n-1\rangle , \\ |-, n\rangle &= \cos\theta_n |g, n\rangle - \sin\theta_n |e, n-1\rangle , \end{aligned} \tag{5.11}$$

avec

$$\tan(2\theta_n) = -2g\sqrt{n+1}/\delta, \tag{5.12}$$

et $E_n^\pm = \omega_c(n+1) \pm \sqrt{g^2(n+1) + \delta^2}$. Ensuite, dans la limite $g/\delta \ll 1$, nous pouvons approximer les états propres comme $|+, n\rangle = |e, n-1\rangle$, $|-, n\rangle = |g, n\rangle$. Ainsi, si la cavité commence dans un état de Fock, l'évolution sera la suivante

$$c_g |g, n\rangle + c_e |e, n\rangle \to c_g |g, n\rangle + e^{-i(E_{n+1}^+ - E_n^-)t} c_e |e, n\rangle = |n\rangle \otimes (c_g |g\rangle + e^{-i(E_{n+1}^+ - E_n^-)t} c_e |e\rangle). \tag{5.13}$$

Ainsi, la phase acquise pertinente est

$$E_{n+1}^+ - E_n^- = \omega + \sqrt{g^2(n+2) + \delta^2} + \sqrt{g^2(n+1) + \delta^2} \simeq \omega + 2\delta + \frac{g^2}{2\delta}(2n+3). \tag{5.14}$$

Ainsi, nous voyons que si nous pouvons déterminer avec précision ω et δ, nous pouvons distinguer la rotation causée par le terme dépendant du photon. Précisément signifie que notre incertitude

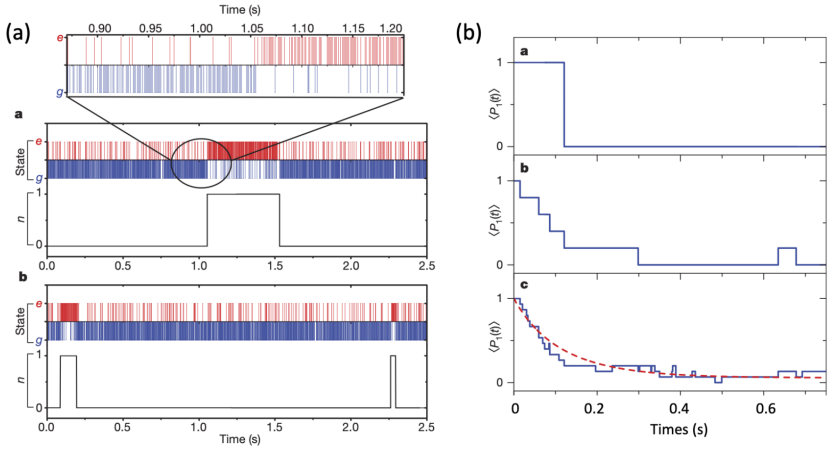


Figure 15: (a) Deux exemples de séquence expérimentale correspondant chacun à plusieurs centaines d'atomes envoyés dans la cavité : les atomes sont soit détectés dans e, soit dans g dans D, et n est le nombre de photons déduit de la mesure des états atomiques. (b) Probabilité de trouver un seul photon dans C pour respectivement 1, 5 et 15 trajectoires.

concernant ω et δ est bien plus petite que $g^2/2\delta$. Naturellement, pour que cette description soit exacte, nous voulons que g/δ soit aussi petit que possible, mais cela rend également la caractérisation plus difficile, il y a donc un compromis, et en pratique, il faudra trouver un point optimal.

Q3. Représentez l'effet de R_1 et de la cavité C sur le vecteur de Bloch représentant le qubit atomique.

A3. Il suffit de faire un schéma.

Q4. Similairement à R_1, la cavité R_2 réalise $R(\pi/2, \pi/2, \Phi)$. Calculez l'état après R_2 et montrez que la probabilité de détecter l'atome dans g, e lorsque la cavité contient n photons est $P(g, \Phi|n) = (1 + \cos(\beta n t - \Phi)/2$, et $P(e, \Phi, n) = (1 - \cos(\beta n t - \Phi)/2$.

A4. En passant dans le référentiel du qubit qui tourne autour de l'axe z à la fréquence $\omega + \delta + 3g^2/2\delta$, on isole la rotation dépendant du nombre de photons βn ($\beta \equiv g^2/2\delta$). Ensuite, il suffit de réaliser le schéma de la sphère de Bloch.

5.2 Naissance et mort d'un photon

Q5. Nous souhaitons enregistrer les trajectoires quantiques des photons dans la cavité. Expliquez pourquoi une mesure QND est nécessaire pour les observer.

Q6. On fixe $\Phi = 0$. Quelle devrait être la valeur de βt pour pouvoir associer la présence d'un photon à la détection de l'atome dans e ?

Q7. fig. 15 montre les états d'un flux d'atomes envoyés dans une cavité initialement presque vide. Expliquez le signal.

Q8. La température de la cavité C est $T = 0.8$ K. Expliquez pourquoi un photon peut apparaître et calculez le nombre moyen de photons $\bar{n}$ pour $\omega_0 = 2\pi \times 51$ GHz.

Q9. Pour préparer un seul photon dans la cavité de manière déterministe, un atome est initialement préparé dans $|e\rangle$ et envoyé dans la cavité. Contrairement à la situation discutée ci-dessus, la cavité C et l'atome sont en résonance pour cette préparation. Expliquez comment cela permet de préparer un seul photon (pas besoin de refaire les calculs connus).

Q10. Expliquez ce que signifie la durée de vie T_c du photon dans la cavité. Basez votre explication sur l'approche par trajectoire, montrée dans fig. 15 (b).

5.3 Effondrement du champ photonique sous une mesure QND

Q11. Nous supposons maintenant que la cavité contient un état cohérent correspondant à une distribution de Poisson du nombre de photons $P_0(n)$. La moyenne est $\bar{n} \simeq 4$. Nous fixons le décalage de phase pour un photon unique $\beta t = \pi/2q$, avec q un entier. Tracez les différentes probabilités $P(e, \Phi|n)$

```
j 11011111111100111011011111
i ddcbccabcdaadaabadddbadbc

j 01010011010101011011011111
i dababbaacbccdadccdcbaaacc
```

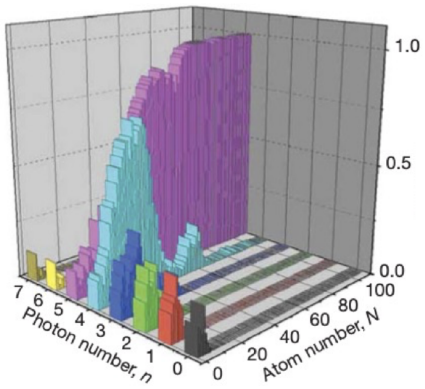


Figure 16: À gauche. Enregistrement des mesures et des phases. À droite. Évolution de la distribution du nombre de photons en fonction du nombre d'atomes envoyés dans la cavité.

pour obtenir l'atome dans e sur un cercle trigonométrique pour $q = 0$ et $\Phi = 0$. Expliquez pourquoi vous ne seriez pas capable de distinguer plus de $2q$ photons.

Q12. Nous voulons calculer la probabilité $P(n|e, \Phi)$ que la cavité contienne n photons conditionnée à la mesure de l'atome dans e pour une phase particulière Φ. Justifiez que

$$P(n|e, \Phi) \propto P(e, \Phi, n)P_0(n). \tag{5.15}$$

Q13. Nous fixons maintenant $\Phi = p\pi/q$, avec p également un entier. Expliquez l'effet de la mesure d'un atome dans e sur la distribution $P(n|e, \Phi)$.

Q14. Supposez maintenant que vous envoyez un flux de N atomes à travers C. L'atome k est mesuré soit dans g soit dans e pour un choix de phase $\Phi(k)$. Écrivez (il suffit d'indiquer que c'est le cas, pas besoin de donner une expression sous forme fermée) la distribution de probabilité du nombre de photons $P_N(n)$ comme un produit de $P(j(k), \Phi(k)|n)$ et $P_0(n)$. $\mathbf{j}$ est la chaîne de bits du registre des mesures $g(0)$ et $e(1)$, et $\mathbf{\Phi}$ est le vecteur des phases utilisées pour préparer et lire chaque atome.

Q15. Le résultat de l'expérience pour une séquence particulière de détections d'atomes associée à un choix particulier de la phase Φ (à gauche) parmi 4 valeurs a, b, c, d est montré dans Figure 16 (à droite). Décrivez les résultats et interprétez-les qualitativement.

5.4 Correlations of quadratures

Nous avons vu en cours que le calcul des corrélations entre le signal à mesurer et la sonde permet de quantifier à quel point une mesure est QND. Prenons l'exemple concret de la lame séparatrice vue en cours Fig.X. L'idée est ici de voir s'il est possible d'utilise un deuxéme faisceau (sonde) pour mesurer le signal sans le détruire. En termes d'opérateurs le mode du signal est donné a et celui de la sonde par b. En terme de mesure, il n'est pas possible de mesurer directement a, b, il est alors utile de définir les quadratures,

$$q^a = a + a^\dagger,\ p^a = i(a^\dagger - a). \tag{5.16}$$

L'opération réalisée par la lame séparatirce est donnée par

$$\begin{pmatrix} q^a_{out} \\ p^b_o ut \end{pmatrix} = \begin{pmatrix} \sqrt{1-\eta^2} & -\eta \\ \eta & \sqrt{1-\eta^2} \end{pmatrix} \begin{pmatrix} q^a_{in} \\ p^b_{in} \end{pmatrix}. \tag{5.17}$$

Q16. Montrez que les corrélation entre amplitude du signal en entrée (q^a_{in}) et amplitude du signal en sortie (q^a_{out}) sont données par

$$C^2_{q^a_{in}, q^a_{out}} \equiv C^2_{qq} = \frac{|\langle q^a_{in} q^a_{out}\rangle - \langle q^a_{in}\rangle\langle q^a_{out}\rangle|}{\mathrm{Var}[q^a_{in}]\mathrm{Var}[q^a_{out}]} = \frac{(1-\eta^2)\mathrm{Var}[q^a_{in}]}{(1-\eta^2)\mathrm{Var}[q^a_{in}] + \eta^2\mathrm{Var}[p^b_{in}]}. \tag{5.18}$$

Q17. Montrez que les corrélation entre amplitude du signal en entrée (q^a_{in}) et amplitude du signal en sortie (p^b_{out}) sont données par

$$C^2_{q^a_{in},p^b_{out}} \equiv C^2_{qp} = \frac{|\langle q^a_{in} p^b_{out}\rangle - \langle q^a_{in}\rangle\langle p^b_{out}\rangle|}{\mathrm{Var}[q^a_{in}]\mathrm{Var}[p^b_{out}]} = \frac{\eta^2 \mathrm{Var}[q^a_{in}]}{\eta^2\mathrm{Var}[q^a_{in}] + (1-\eta^2)\mathrm{Var}[p^b_{in}]}. \tag{5.19}$$

Q18. Show that for any input coherent states $|\alpha\rangle$, $|\beta\rangle$ $C^2_{qq} + C^2_{qp} = 1$. En vous basant sur des arguments simples, expliquez pourquoi cette valeur de 1 est typique d'une mesure qui n'est past QND.

À l'inverse, si une système de mesure permet d'obtenir une mesure QND parfaite $C^2_{qq} + C^2_{qp} = 2$, quelle est selon vous la valeur des corrélations C^2_{qp}?

Q19. Considerons maintenant un état du vide parfaitement comprimé pour la sonde p^b_{in}, c'est-à-dire que la variance d'une des quadratures tends vers 0 alors que l'autre diverge. Laquelle des deux quadratures est-il important de minimiser pour améliorer la mesure obtenue avec la lame séparatrice? Est-il théoretiquement possible d'obtenir une mesure QND parfaite?

Q20. Finalement, considérons simplement le Hamiltonien libre d'un seul mode décrit par l'opérateur a, $H_0 = \omega a^\dagger a$. En utilisant le paradigme de Heisenberg, montrez qu'une mesure de le quadrature $a^\dagger + a$ n'est pas un bon choix d'observable.

6 Further references

First demonstration of coherent control in the time domain in cQED [22]. Metrology of qubit frequencies beyond Ramsey limit [23]. For understanding spectral densities and quantum noise see the great review [24]. Excellent introductory book to quantum optics [25].

References

[1] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[2] Jun John Sakurai and Jim Napolitano. *Modern quantum mechanics*. Cambridge University Press, 2020.

[3] *python.org*. https://www.python.org/downloads/. [Accessed 16-09-2024].

[4] *Getting started with Visual Studio Code — code.visualstudio.com*. https://code.visualstudio.com/docs/introvideos/basics. [Accessed 16-09-2024].

[5] *GitHub - LautaroLabarcaG/optique-quantique: optique-quantique 2024 UdeS — github.com*. https://github.com/LautaroLabarcaG/optique-quantique/tree/main. [Accessed 16-09-2024].

[6] Christopher M Dawson et al. "Quantum computing and polynomial equations over the finite field Z_2". In: *arXiv preprint quant-ph/0408129* (2004).

[7] Albert Einstein, Boris Podolsky, and Nathan Rosen. "Can quantum-mechanical description of physical reality be considered complete?" In: *Physical review* 47.10 (1935), p. 777.

[8] Alain Aspect, Jean Dalibard, and Gérard Roger. "Experimental test of Bell's inequalities using time-varying analyzers". In: *Physical review letters* 49.25 (1982), p. 1804.

[9] Stuart J Freedman and John F Clauser. "Experimental test of local hidden-variable theories". In: *Physical review letters* 28.14 (1972), p. 938.

[10] John S Bell. "On the einstein podolsky rosen paradox". In: *Physics Physique Fizika* 1.3 (1964), p. 195.

[11] Simon Storz et al. "Loophole-free Bell inequality violation with superconducting circuits". In: *Nature* 617.7960 (2023), pp. 265–270.

[12] Andrea Aiello. *Against Bell's Theorem*. 2024. arXiv: 2406.03028 [quant-ph]. URL: https://arxiv.org/abs/2406.03028.

[13] Akash V Dixit et al. "Searching for dark matter with a superconducting qubit". In: *Physical review letters* 126.14 (2021), p. 141302.

[14] *Topical on quantum gravity tests with atoms*. https://smd-cms.nasa.gov/wp-content/uploads/2023/05/45_e8d91f69e93d0cf59de3959b6bb25b55_BiedermannGrantW.pdf. [Accessed 16-09-2024].

[15] Claude Elwood Shannon. "A mathematical theory of communication". In: *The Bell system technical journal* 27.3 (1948), pp. 379–423.

[16] Jordan Cotler and Frank Wilczek. "Quantum overlapping tomography". In: *Physical review letters* 124.10 (2020), p. 100401.

[17] Flavio Del Santo and Nicolas Gisin. *Which features of quantum physics are not fundamentally quantum but are due to indeterminism?* 2024. arXiv: 2409.10601 [quant-ph]. URL: https://arxiv.org/abs/2409.10601.

[18] Brian Pigott et al. *Eavesdropping on the BB84 Protocol using Phase-Covariant Cloning: Experimental Results*. 2024. arXiv: 2409.16284 [quant-ph]. URL: https://arxiv.org/abs/2409.16284.

[19] Carlton M Caves et al. "On the measurement of a weak classical force coupled to a quantum-mechanical oscillator. I. Issues of principle". In: *Reviews of Modern Physics* 52.2 (1980), p. 341.

[20] Sebastien Gleyzes et al. "Quantum jumps of light recording the birth and death of a photon in a cavity". In: *Nature* 446.7133 (2007), pp. 297–300.

[21] Christine Guerlin et al. "Progressive field-state collapse and quantum non-demolition photon counting". In: *Nature* 448.7156 (2007), pp. 889–893.

[22] Yasunobu Nakamura, Yu A Pashkin, and JS Tsai. "Coherent control of macroscopic quantum states in a single-Cooper-pair box". In: *nature* 398.6730 (1999), pp. 786–788.

[23] M. O. Hecht et al. *Beating the Ramsey limit on sensing with deterministic qubit control*. 2024. arXiv: 2408.15926 [quant-ph]. URL: https://arxiv.org/abs/2408.15926.

[24] Aashish A Clerk et al. "Introduction to quantum noise, measurement, and amplification". In: *Reviews of Modern Physics* 82.2 (2010), pp. 1155–1208.

[25] Ulf Leonhardt. *Essential quantum optics: from quantum measurements to black holes*. Cambridge University Press, 2010.