(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 100 642**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **19 09839**

(51) Int Cl[8] : ***G 06 N 10/00*** *(2022.01), H 04 B 10/70, H 04 L 9/12*

(12) **BREVET D'INVENTION** **B1**

(54) PROCEDE DE TRANSMISSION SECURISEE DE SEQUENCES D'ETATS QUANTIQUES ENTRE PLUSIEURS PARTICIPANTS EN LIGNE SUR UN CANAL DE COMMUNICATION QUANTIQUE.

(22) **Date de dépôt :** 06.09.19.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 12.03.21 Bulletin 21/10.

(45) **Date de la mise à disposition du public du brevet d'invention :** 12.08.22 Bulletin 22/32.

(56) **Liste des documents cités dans le rapport de recherche :**

Se reporter à la fin du présent fascicule

(60) **Références à d'autres documents nationaux apparentés :**

(○) **Demande(s) d'extension :**

(71) **Demandeur(s) :** *VERIQLOUD Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** KAPLAN Marc et HARDER George.

(73) **Titulaire(s) :** VERIQLOUD Société par actions simplifiée.

(74) **Mandataire(s) :** NOVAGRAAF TECHNOLOGIES.

FR 3 100 642 - B1

Description

Titre de l'invention : PROCEDE DE TRANSMISSION SECURISEE DE SEQUENCES D'ETATS QUANTIQUES ENTRE PLUSIEURS PARTICIPANTS EN LIGNE SUR UN CANAL DE COMMUNICATION QUANTIQUE

[0001] La présente invention concerne de manière générale le domaine de la communication quantique et plus particulièrement une méthode et un dispositif pour échanger des séquences d'états quantiques entre plusieurs participants d'un même canal de communication quantique.

[0002] La communication quantique consiste à échanger des états quantiques, encodés sur des bits quantiques ou qubits, entre plusieurs participants. Lorsque les états quantiques à échanger doivent l'être de manière secrète, la communication quantique est couplée à des méthodes de cryptographie quantique, ces dernières consistant à utiliser les propriétés de la physique quantique pour établir des protocoles de cryptographie, c'est-à-dire qui assurent la confidentialité des données échangées, permettant de sécuriser la communication quantique.

[0003] Un exemple de protocole de communication quantique bien connu est la distribution de clé quantique (QKD, « quantum key distribution »), qui permet à deux participants reliés par un canal de communication quantique non-sécurisé d'établir une clé aléatoire qui peut être utilisée pour chiffrer une communication classique standard. Dans un protocole de distribution de clé quantique, il y a deux participants jouant en général un rôle différent : un émetteur, qui envoie de l'information quantique sous la forme de qubits, et un récepteur, qui décode cette information grâce à un dispositif adéquat.

[0004] Il est connu de l'homme de l'art, dans les protocoles de distribution de clé quantique utilisés en pratique, d'encoder les qubits constituant la clé à distribuer dans des photons. La génération des photons est réalisée par un laser, l'encodage des photons est réalisé par un modulateur de propriétés optiques, et le décodage par le récepteur par un montage impliquant un détecteur de photons. A la fin du protocole, l'émetteur et le récepteur partagent une chaîne de qubits aléatoires secrète.

[0005] Un problème technique que se propose de résoudre l'invention est de proposer une méthode sécurisée pour l'échange d'un flux d'états quantiques entre deux participants parmi un nombre de participants d'un même canal de communication quantique supérieur ou égal à trois et formant une chaîne de communication quantique, les deux participants échangeant un flux d'états quantiques pouvant être différents des participants dits émetteur et récepteur dans un protocole de distribution de clé quantique de l'art antérieur, ainsi qu'un dispositif pour mettre en œuvre cette méthode, ledit

dispositif utilisant un matériel simple et très limité.

[0006] Afin de résoudre ce problème, le demandeur a mis au point un procédé de transmission sécurisée d'une séquence de Q états quantiques encodée sous la forme d'une séquence de Q photons, entre un premier participant et un second participant, choisis parmi une pluralité de N participants distincts d'un même canal de communication quantique formant une chaîne de communication entre un émetteur et un récepteur, où N est un entier supérieur ou égal à 3, dans lequel le premier participant est situé en amont du second participant dans la chaîne de communication,

ledit procédé comprenant, dans l'ordre :

- la succession des étapes suivantes, répétée de q=1 à Q :

■ préparation par l'émetteur d'un photon dans un état quantique de base de référence |0> d'une base d'encodage B_0 orthonormée nommée base standard de dimension d et d'états de base |0>, |1>,… |d-1>,

■ transmission du photon préparé dans la chaîne de communication,

■ une première action effectuée par le premier participant sur ledit photon, comprenant deux première et deuxième étapes consécutives:

○ une première étape de décision de transformation ou non de l'état quantique du photon transmis, en un état quantique de base orthogonal dans la base d'encodage B_0,

○ une deuxième étape de décision d'appliquer ou non une transformation P permettant d'effectuer un changement de base d'encodage, depuis la base standard B_0 vers une base d'encodage B_1 incompatible avec la base standard B_0, d'états de base $|e_0>$, $|e_1>$,… $|e_{d-1}>$

■ une deuxième action effectuée par le second participant sur ledit photon, comprenant deux troisième et quatrième étapes consécutives:

○ une troisième étape de décision d'appliquer ou non la transformation inverse $P^{(-1)}$ de ladite transformation P, permettant d'effectuer un changement de base d'encodage, depuis la base incompatible B_1 vers la base standard B_0,

○ une quatrième étape de décision de transformation ou non de l'état quantique du photon reçu en un état quantique orthogonal correspondant dans la base d'encodage résultant de la troisième étape

■ mesure, dans la base standard B_0, de l'état final du photon transmis dans la chaîne de communication par le récepteur,

■ échange sur un canal de communication classique entre les premier et second participants, des décisions des deuxième et troisième étapes,

■ obtention, entre les premier et second participants, d'une description de l'état quantique transmis correspondant à l'un des états de base |0>, |1>,… |d-1>, grâce aux informations de décisions des deuxième et troisième étapes et à la mesure de l'état final ;

- puis, la reconstitution, par les premier et second participants, par concaténation, d'une séquence des descriptions des Q états quantiques transmis, pour q allant de 1 à Q.

[0007] Par l'expression chaîne de communication, il doit être entendu une succession de participants connectés entre eux. Plus spécifiquement, le participant C_1 est connecté au participant C_2 ; pour i compris entre 2 et N-1, le participant C_i succède et est connecté au participant C_{i-1}, et précède et est connecté au participant C_{i+1} ; le participant C_{N-1} précède et est connecté au dernier participant C_N.

[0008] En particulier, la première action, effectuée par le premier participant, comprend les étapes suivantes :

- Choisir une valeur sq égale à 0 ou 1
- Choisir une valeur m comprise entre 0 et d-1
- Appliquer une transformation $P^{sq}X_m$ au photon reçu à travers la chaîne de communication, ou dans le cas où i est égal à 1, au photon au début de la chaîne de communication, ladite transformation $P^{sq}X_m$ correspondant à la succession des première et deuxième étapes

dans laquelle :

- la notation P^1 signifie que la transformation P a lieu,
- la notation P^0 signifie que la transformation P n'a pas lieu
- la notation X_m désigne une transformation permettant de passer de l'état quantique de base $|t\rangle$, t étant un entier compris entre 0 et d-1, à l'état orthogonal $|(t+m) \bmod d\rangle$ dans la base B_0 ou la transformation permettant de passer d'un état $|e_t\rangle$ à $|e_{t+m} \bmod d\rangle$ dans la base B_1, pour m un entier compris entre 0 et d-1.

[0009] En particulier, la deuxième action, effectuée par le second participant, comprend les étapes suivantes :

- choisir une valeur tq égale à 0 ou 1
- choisir une valeur n comprise entre 0 et d-1
- appliquer une transformation $X_nP^{(-1)tq}$ au photon reçu à travers la chaîne de communication, ladite transformation $X_nP^{(-1)tq}$ correspondant à la succession des troisième et quatrième étapes

dans laquelle :

- la notation $P^{(-1)1}$ signifie que la transformation $P^{(-1)}$ a lieu,
- la notation $P^{(-1)0}$ signifie que la transformation $P^{(-1)}$ n'a pas lieu.

[0010] Un mode de réalisation particulier est celui où la dimension d de la base d'encodage est égale à 2.

[0011] Dans un autre mode de réalisation du procédé de transmission sécurisée décrit dans cette demande, où le nombre de participants N est supérieur ou égal à 4, où le premier et le second participants ne sont ni l'émetteur, ni le récepteur, et où la séquence de Q photons encodant la séquence des Q états quantiques présente une puissance lumineuse

donnée, la deuxième étape de décision d'appliquer ou non une transformation P permettant d'effectuer un changement de base d'encodage, depuis la base standard B_0 vers une base d'encodage B_1 incompatible avec la base standard B_0 est immédiatement suivie de :

- une cinquième étape de prélèvement d'une première portion de la puissance lumineuse du flux de photons reçu du participant précédant immédiatement le premier participant,
- une sixième étape de comparaison de la première portion avec une seconde portion de la puissance lumineuse du flux de photons envoyé par l'émetteur afin de détecter une potentielle injection de photons espions avant le premier participant.

[0012] Dans ce même mode de réalisation du procédé de transmission sécurisée, la quatrième étape de décision de transformation ou non de l'état quantique du photon reçu en un état quantique orthogonal correspondant dans la base d'encodage résultant de la troisième étape est immédiatement suivie de :

- une septième étape de prélèvement d'une troisième portion de la puissance lumineuse du flux de photons reçu du participant précédant immédiatement le second participant,
- une huitième étape de comparaison de la troisième portion avec une quatrième portion de la différence entre la puissance lumineuse du flux de photons envoyé par l'émetteur et la première portion afin de détecter une potentielle injection de photons espions avant le second participant.

[0013] Avantageusement, chaque état quantique est codé dans un degré de liberté du photon choisi parmi la phase, la différence de phase, la localisation temporelle, la polarisation ou la fréquence du photon.

[0014] Avantageusement, dans le procédé de transmission sécurisé selon l'invention, la séquence de Q états quantiques est choisie de manière aléatoire dans le but d'établir une clé quantique.

[0015] La présente invention a également pour objet un dispositif pour la mise en œuvre du procédé de transmission sécurisée précédemment décrit, comprenant :

- un laser apte à générer des photons et un modulateur initial apte à moduler un degré de liberté d'un photon généré,
- N-2 modulateurs intermédiaires aptes à moduler un degré de liberté d'un photon reçu,
- un détecteur de photons apte à détecter des photons uniques et un modulateur final apte à moduler un degré de liberté d'un photon reçu.

[0016] Avantageusement, le laser et le modulateur initial sont associés à l'émetteur et aptes à être commandés par l'émetteur. Avantageusement, chacun des N-2 modulateurs intermédiaires est associé à un participant intermédiaire parmi les N-2 participants inter-

médiaires distincts de l'émetteur et du récepteur et apte à être commandé par ledit participant intermédiaire. Avantageusement, le détecteur de photons et le modulateur final sont associés au récepteur et sont aptes à être commandés par le récepteur.

[0017] Ainsi, la connexion entre les N participants de la chaîne de communication peut être réalisée par la transmission d'un photon généré par le laser associé à l'émetteur à travers le modulateur initial, les N-2 modulateurs intermédiaires, le modulateur final, jusqu'au détecteur de photons associé au récepteur.

[0018] Dans une variante du dispositif précédemment décrit, celui-ci peut comprendre en outre, dans le cas où le premier participant et le second participant sont tous les deux distincts de l'émetteur et du récepteur :

- un premier séparateur de faisceau positionné en amont du modulateur associé au premier participant,
- une première photodiode associée au premier participant et apte à mesurer une puissance lumineuse d'un flux de photons,
- un deuxième séparateur de faisceau positionné en amont du modulateur associé au second participant,
- une deuxième photodiode associée au second participant et apte à mesurer une puissance lumineuse d'un flux de photons.

[0019] Cette variante du dispositif permet de mettre en œuvre le mode de réalisation du procédé de transmission sécurisée dans lequel les cinquième, sixième et septième étapes ont lieu.

[0020] Avantageusement, le premier séparateur de faisceau est apte à séparer le flux de photons reçu du participant précédant immédiatement le premier participant dans la chaîne de communication dans deux directions distinctes, l'une en direction du modulateur associé au premier participant puis vers la suite de la chaîne de communication, l'autre en direction de la première photodiode. Avantageusement, le deuxième séparateur de faisceau est apte à séparer le flux de photons reçu du participant précédant immédiatement le second participant dans la chaîne de communication dans deux directions distinctes, l'une en direction du modulateur associé au second participant puis vers la suite de la chaîne de communication, l'autre en direction de la deuxième photodiode.

[0021] Dans le cas où le degré de liberté du photon encodant l'état quantique est la phase de ce photon, le modulateur initial, les N-2 modulateurs intermédiaires et le modulateur final peuvent être des modulateurs de phase.

[0022] Dans le cas où le degré de liberté du photon encodant l'état quantique est la polarisation de ce photon, le modulateur initial, les modulateurs intermédiaires et le modulateur final peuvent être des modulateurs de polarisation.

[0023] Dans le cas où le degré de liberté du photon encodant l'état quantique est la loca-

lisation temporelle de ce photon, le modulateur initial, les modulateurs intermédiaires et le modulateur final peuvent comprendre chacun un nombre de lignes à retard égal à la dimension d de la base d'encodage des bits quantiques et un nombre de lames séparatrices égal au double du nombre de lignes à retard

[0024] D'autres avantages et particularités de la présente invention résulteront de la description détaillée qui va suivre, donnée à titre d'exemple non limitatif et faite en référence aux figures annexées :

[0025] - La figure 1 illustre plusieurs exemples de degrés de liberté pour l'encodage de bits quantiques ainsi que des exemples de bases incompatibles associées.

- La figure 2 est un synoptique du procédé de transmission sécurisée d'un état quantique entre deux participants d'une chaîne de communication comprenant N participants en ligne selon un premier mode de réalisation.

- La figure 3 illustre un exemple d'effet de transformations pouvant être appliquées sur un état quantique de référence dans le cadre du procédé de transmission sécurisée de séquences d'états quantiques.

- La figure 4 illustre un exemple de réalisation d'attaque par canaux cachés dans un dispositif de communication quantique optique.

- La figure 5 illustre une étape supplémentaire réalisée dans un deuxième mode de réalisation du procédé de transmission sécurisée d'un état quantique.

- La figure 6 illustre une réalisation de dispositif pour la mise en œuvre du procédé de transmission sécurisée d'une séquence, pour une chaîne de communication quantique de 4 participants.

- La figure 7 illustre un dispositif modulateur de localisation temporelle

- La figure 8 est un exemple de bases incompatibles dans un espace vectoriel hilbertien de dimension 4.

DESCRIPTION DETAILLEE

[0026] La présente invention présente un procédé de transmission sécurisée pour envoyer des séquences d'états quantiques, codés sur des bits quantiques, entre plusieurs participants en ligne sur un canal de communication quantique. Dans les modes de réalisation et exemples présentés ci-dessous, les bits quantiques sont codés avec des photons dans un degré de liberté de ceux-ci. Par degré de liberté de photon, on entend une propriété physique décrite par la mécanique quantique et utilisable pour des communications quantiques. Des exemples de degrés de liberté des photons sont la phase, la différence de phase, la fréquence, la polarisation ou encore la localisation temporelle. Dans cette description, on utilise le formalisme qui représente un état quantique sous la forme d'un vecteur $|\alpha\rangle$ dans un espace vectoriel hilbertien de dimension d. Le concept d'espace vectoriel hilbertien étend les méthodes de l'algèbre

linéaire en généralisant les notions d'espace euclidien (comme le plan euclidien ou l'espace usuel de dimension 3) et d'espace hermitien à des espaces de dimension quelconque (finie ou infinie). Un vecteur $|\alpha\rangle$ d'un espace vectoriel hilbertien de dimension d peut être décrit par l'intermédiaire d'une base de l'espace vectoriel hilbertien de dimension d. Pour la suite de la description des modes de réalisation et exemples qui suivront, le concept de bases incompatibles va être utilisé. Deux bases d'un même espace vectoriel hilbertien sont dites incompatibles si chaque vecteur d'une des deux bases a des projections de longueurs égales sur chacun des vecteurs de l'autre base. La figure 1 donne des exemples de bases incompatibles pour différents degrés de liberté de photon, dans un espace vectoriel hilbertien de dimension 2.

[0027] On décrit ici un premier mode de réalisation de l'invention dans le cas particulier d'un espace vectoriel hilbertien de dimension d, d étant un entier supérieur ou égal à 2, et dans le cas d'une chaîne de communication comprenant N participants en ligne C_1, … C_i,…C_j… et C_N, où C_1 est le participant émetteur et C_N est le participant récepteur, et où N est un entier supérieur ou égal à 3. La figure 2 illustre ce premier mode de réalisation. Les participants intermédiaires C_2 à C_{N-1} sont appelés transformateurs. Par le terme « émetteur », on désigne un participant muni d'un dispositif adéquat capable d'envoyer de l'information quantique, en particulier des bits quantiques encodant des états quantiques. Ici, puisqu'il est considéré que les bits quantiques sont codés dans des photons, le dispositif dont dispose l'émetteur est un laser générant des photons. Par le terme « récepteur », on désigne un participant muni d'un dispositif adéquat capable de décoder l'information quantique envoyée par un émetteur, notamment mesurer un état quantique lié à un bit quantique reçu. Dans le cas où les bits quantiques sont codés dans des photons, le dispositif dont dispose le récepteur peut être un détecteur de photon unique SPD. Par le terme « transformateur », dans le cas où les bits quantiques sont codés dans de photons, on désigne un participant muni d'un matériel lui permettant de moduler le signal optique qu'il reçoit. On considère qu'un transformateur dispose d'un matériel limité et qu'il ne peut que moduler le signal optique qu'il reçoit, mais ni créer de signal lui-même, ni mesurer l'état quantique d'un photon qu'il reçoit.

[0028] Dans le procédé de transmission sécurisée décrit dans cette demande, deux participants distincts C_i et C_j parmi les participants C_1 à C_N de la chaîne de communication, C_i étant le participant le plus en amont dans la chaîne de communication, C_j celui le plus en aval dans la chaîne de communication, décident de partager une séquence de Q états quantiques q_q, pour q un entier compris entre 1 et Q, ladite séquence présentant une puissance lumineuse P_{seq} en nombre de photons par seconde. Selon la nature des participants C_i et C_j, le procédé de transmission sécurisée peut présenter des étapes ordonnées de manière différente. Aussi, les participants C_i et C_j

sont connus de tous, c'est-à-dire des autres participants de la chaîne de communication mais aussi du public.

[0029] On envisage ici un premier cas de procédé de transmission sécurisée d'une séquence d'états quantiques où les participants C_i et C_j sont des participants différents des participants C_1 et C_N, c'est-à-dire qu'ils ne sont ni émetteur, ni récepteur, mais simplement des transformateurs. N est alors un entier supérieur ou égal à 4. La figure 2 donne une illustration générale de ce procédé de transmission sécurisée d'une séquence d'états quantiques. Les étapes du procédé de transmission sécurisée de la séquence d'états quantiques peuvent alors consister en la répétition des étapes suivantes, pour q étant un entier compris entre 1 et Q :

- le participant émetteur C_1 envoie à travers la chaîne de communication d'un photon préparé dans un état quantique de base de référence $|0\rangle$ d'une base d'encodage B_0 de travail nommée base standard, orthonormée, de dimension d, et d'états de base orthogonaux $|0\rangle$, $|1\rangle$,... $|d-1\rangle$:
- le premier participant C_i effectue une première action composée de deux étapes G_1 et G_2 successives à réception du photon transmis dans la chaîne de communication, plus précisément :

■ dans une première étape G_1, le premier participant C_i décide ou non de transformer l'état quantique du photon reçu, ou généré, en un état quantique de base $|m\rangle$ orthogonal à l'état $|0\rangle$ dans la base d'encodage B_0,

■ dans une deuxième étape G_2, le premier participant C_i décide ou non d'appliquer une transformation P permettant d'effectuer un changement de base d'encodage, depuis la base standard B_0 vers en une base d'encodage B_1 orthonormée et de dimension d, incompatible avec la base standard B_0, d'états de base orthogonaux $|e_0\rangle$, $|e_1\rangle$,... $|e_{d-1}\rangle$;

- le photon issu de la deuxième étape G_2 est propagé dans la chaîne de communication ;
- le second participant C_j effectue une deuxième action composée de deux étapes G_3 et G_4 successives à réception du photon transmis dans la chaîne de communication, plus précisément :

■ dans une troisième étape G_3, le second participant C_j décide ou non d'appliquer la transformation inverse de la transformation P, notée $P^{(-1)}$, permettant d'effectuer un changement de base d'encodage, depuis la base d'encodage B_1 vers la base standard B0 ;

■ dans une quatrième étape G_4, le second participant C_j décide ou non de transformer l'état quantique du photon reçu du participant C_{j-1} en un état quantique orthogonal correspondant dans la base d'encodage résultant de l'étape G_3 ;

- le photon issu de la quatrième étape G_4 est propagé dans la chaîne de commu-

nication ;

- le récepteur C_N détecte et mesure dans la base standard B_0 l'état $|alpha_{final}>$ du photon transmis dans la chaîne de communication.
- les premier et second participants C_i et C_j échangent entre eux sur un canal de communication classique leurs décisions de transformation de bases d'encodage résultant des deuxième et troisième étapes G_2 et G_3 ;
- les premier et second participants C_i et C_j obtiennent une description de l'état quantique q_q correspondant à l'un des états de base |0>, |1>,... |d-1>, grâce aux informations de bases d'encodage échangées entre et à la mesure de l'état final $|alpha_{final}>$.

[0030] Des exemples de canaux de communication classiques sont les connexions Ethernet, Wifi, ou encore les protocoles TCP/IP.

[0031] Après que les Q répétitions ont été effectuées, les premier et second participants C_i et C_j reconstituent, par concaténation, une séquence des descriptions des Q états quantiques q_q.

[0032] Il va maintenant être décrit d'une part, ce qui est entendu par le terme « description d'un état quantique q_q », et d'autre part comment est réalisée la sécurisation de la transmission de la séquence d'états quantiques par le protocole décrit dans le précédent cas. Les première et deuxième actions effectuées par les premier et second participants C_i et C_j transcrivent une méthode d'application du principe du codage conjugué. Le codage conjugué consiste à encoder une information dans un état quantique en gardant secrète la base dans laquelle cette information est codée. Ce principe repose en particulier sur l'utilisation de deux bases d'encodage d'un espace vectoriel hilbertien incompatibles entre elles. Prenant en compte un état quantique dans une des deux bases, celui-ci, s'il est mesuré dans une base incompatible correspondante, va se comporter de manière complètement aléatoire. En effet, la définition donnée plus haut de deux bases incompatibles, c'est-à-dire, que la projection de chaque vecteur d'une des deux bases a des projections de longueurs égales sur chacun des vecteurs de l'autre base peut être formulée mathématiquement de la manière suivante, en prenant l'exemple de bases B_0 et B_1 précédemment évoquées :

[0033] Pour m et n des entiers compris entre 0 et d-1 :

[0034] [Math.1]

$$\langle m|e_n \rangle = 1/\sqrt{d}$$

[0035] et

[0036] $$\langle e_m|n \rangle = 1/\sqrt{d}$$

[0037] où <..|..> désigne le produit scalaire de l'espace vectoriel hilbertien de définition des vecteurs d'état.

[0038] En mécanique quantique, les quantités $|\langle m \mid e_n\rangle|^2$ et $|\langle e_m \mid n\rangle|^2$ représentent respectivement les probabilités de trouver un système dans un état initial $|e_n\rangle$ dans l'état $|m\rangle$, si on effectuait une mesure dans la base standard B_0, et de trouver un système dans un état initial $|n\rangle$ dans l'état $|e_m\rangle$, si on effectuait une mesure dans la base incompatible B_1. Ainsi, ces probabilités sont toutes égales. Il peut donc en être conclu que la mesure, dans la base incompatible correspondante, d'un état préparé dans l'une ou l'autre des bases B_0 ou B_1 donnerait un résultat de mesure complètement aléatoire.

[0039] Ainsi, dans le procédé de transmission sécurisée d'une séquence de Q états quantiques, seules deux configurations permettent une transmission d'état quantique fournissant une information pertinente, c'est-à-dire, un résultat de la mesure par le récepteur C_N pouvant être utilisé par les premier et second participants C_i et C_j : il s'agit soit du cas où les premier et second participants C_i et C_j décident tous les deux lors des deuxième et troisième étapes G_2 et G_3 d'appliquer respectivement les transformations P et $P^{(-1)}$, soit du cas où aucun des deux ne décide lors des deuxième et troisième étapes G_2 et G_3 d'appliquer la transformation P, respectivement $P^{(-1)}$. En effet, dans ces deux cas, la troisième étape G_3 permet de défaire la transformation effectuée lors de la deuxième étape G_2 et de revenir à la base B_0, dans laquelle la mesure faite par le récepteur C_N donnera un résultat de mesure non aléatoire. L'état mesuré par le récepteur C_N sera celui résultant des transformations issues des première et quatrième étapes G_1 et G_4. Ainsi, la sécurisation du procédé de transmission de la séquence d'états quantiques provient du fait que l'état mesuré par le récepteur C_N est celui de la succession des transformations issues des première et quatrième étapes G_1 et G_4, mais ne permet pas de déterminer l'état, choisi par le premier participant C_i lors de la sous-étape G_1, transmis au deuxième participant C_j. Celui-ci est masqué par la combinaison des première et deuxième actions effectuées respectivement par le premier participant C_i et le second participant C_j.

[0040] Dans le cas où le premier participant C_i décide d'appliquer la transformation P lors de la deuxième étape G_2, et que le second participant C_j décide de ne pas appliquer la transformation $P^{(-1)}$ lors de la sous-étape G_3, ou inversement, dans le cas où le premier participant C_i décide de ne pas appliquer la transformation P lors de la sous-étape G_2, et que le second participant C_j décide d'appliquer la transformation $P^{(-1)}$ lors de la troisième étape G_3, l'information qui aura circulé dans la chaîne de communication et mesurée par le récepteur C_N ne sera pertinente, c'est-à-dire, que le résultat de la mesure effectuée par le récepteur C_N ne pourra pas être exploité par les premier et second participants C_i et C_j. En effet, elle correspondra à une mesure d'un état d'une base B_0 ou B_1 dans la base incompatible correspondante, et, comme expliqué précédemment, à un résultat complètement aléatoire. En pratique, ce résultat de la transmission du bit

quantique correspondant sera jeté et mis à l'écart.

[0041] C'est pourquoi le terme «description d'un état quantique q_q » est utilisé pour généraliser le résultat de la mesure faite par le récepteur C_N car l'information quantique déduite de cette mesure n'est pas forcément pertinente et ne correspond pas nécessairement à la nature de l'état q_q.

[0042] Ainsi, selon les décisions prises par les premier et second participants C_i et C_j, une information codée dans un bit quantique peut être transmise du premier participant C_i vers le second participant C_j de manière sécurisée car les autres participants, différents de C_i et C_j, n'ont accès, lorsque le récepteur C_N annonce la mesure de l'état final qu'à l'information portant sur l'état $|alpha_{final}>$ du photon transmis dans la chaîne de communication. D'un point de vue statistique, en moyenne, et du fait des configurations où l'information quantique portant sur l'état $|alpha_{final}>$ est aléatoire et donc non pertinente, un état quantique sur deux peut être transmis par le premier participant C_i au second participant C_j de manière cachée aux autres participants de la chaîne de communication.

[0043] On envisage ici un deuxième cas où le premier participant C_i est le participant émetteur C_1 mais que le participant C_j n'est qu'un transformateur, différent du récepteur C_N. N est alors un entier supérieur ou égal à 3. Les étapes du procédé de transmission sécurisée de la séquence d'états quantiques peuvent alors consister en la répétition des étapes suivantes, pour q étant un entier compris entre 1 et Q :

- l'émetteur C_1 effectue la première action décrite dans le premier cas et composée des première et deuxième étapes successives G_1 et G_2;
- le photon issu de la deuxième étape G_2 est propagé dans la chaîne de communication ;
- le second participant C_j effectue la deuxième action décrite dans le premier cas et composée des troisième et quatrième étapes successives G_3 et G_4 ;
- le photon issu de la quatrième étape G_4 est propagé dans la chaîne de communication ;
- le récepteur C_N détecte et mesure dans la base standard B_0 l'état $|alpha_{final}>$ du photon transmis dans la chaîne de communication.
- l'émetteur C_1 et le second participant C_j échangent entre eux sur un canal de communication classique les bases d'encodage résultant des étapes G_2 et G_3 ;
- l'émetteur C_1 et le second participant C_j obtiennent une description de l'état quantique q_q correspondant à l'un des états de base $|0>$, $|1>$,… $|d-1>$, grâce aux informations de bases d'encodage échangées entre et à la mesure de l'état final $|alpha_{final}>$.

[0044] Après que les Q répétitions ont été effectuées, l'émetteur C_1 et le second participant C_j reconstituent, par concaténation, une séquence des descriptions des Q états

quantiques q_q, jetant, si nécessaire, les descriptions non pertinentes et non exploitables.

[0045] On envisage ici un troisième cas où le premier participant C_i est un transformateur, différent de l'émetteur C_1, et le participant C_j est le récepteur C_N, et où N est un entier supérieur ou égal à 3. Les étapes du procédé de transmission sécurisée de la séquence d'états quantiques peuvent alors consister en la répétition des étapes suivantes, pour q étant un entier compris entre 1 et Q :

- l'émetteur C_1 envoie à travers la chaîne de communication d'un photon préparé dans un état quantique de base de référence |0> d'une base d'encodage B_0 de travail nommée base standard, orthonormée et de dimension d, et d'états de base orthogonaux |0>, |1>,... |d-1> :
- le premier participant C_i effectue la première action décrite dans le premier cas et composée des première et deuxième étapes successives G_1 et G_2 ;
- le photon issu de la deuxième étape G_2 est propagé dans la chaîne de communication ;
- le récepteur C_N détecte le photon qu'il reçoit, effectue la deuxième action décrite dans le premier cas et composée des troisième et quatrième étapes successives G_3 et G_4 , puis mesure dans la base standard B0 l'état $|alpha_{final}>$ du photon issu de la quatrième étape G_4 ;

le premier participant C_i et le récepteur C_N échangent entre eux sur un canal de communication classique crypté les bases d'encodage résultant des deuxième et troisième étapes G_2 et G_3 ;

- le premier participant C_i et le récepteur C_N obtiennent une description de l'état quantique q_q correspondant à l'un des états de base |0>, |1>,... |d-1>, grâce aux informations de bases d'encodage échangées entre et à la mesure de l'état final $|alpha_{final}>$.

[0046] Après que les Q répétitions ont été effectuées, le premier participant C_i et le récepteur C_N reconstituent, par concaténation, une séquence des descriptions des Q états quantiques q_q, en jetant, si nécessaire, les descriptions non pertinentes et non exploitables.

[0047] On envisage ici un quatrième et dernier cas où le premier participant C_i est l'émetteur C_1 et le second participant C_j est le récepteur C_N, et où N est un entier supérieur ou égal à 3. Les étapes du procédé de transmission sécurisée de la séquence d'états quantiques peuvent alors consister en la répétition des étapes suivantes, pour q étant un entier compris entre 1 et Q :

- l'émetteur C_1 effectue la première action décrite dans le premier cas et composée des première et deuxième étapes successives G_1 et G_2;
- le photon issu de la deuxième étape G_2 est propagé dans la chaîne de communication ;

- le récepteur C_N détecte le photon qu'il reçoit, effectue la deuxième action décrite dans le premier cas et composée des troisième et quatrième étapes successives G_3 et G_4, puis mesure dans la base standard B_0 l'état lalpha$_{final}$> du photon issu de l'étape G_4 ;
- l'émetteur C_1 et le récepteur C_N échangent entre eux sur un canal de communication classique crypté les bases d'encodage résultant des étapes G_2 et G_3 ;
- l'émetteur C_1 et le récepteur C_N obtiennent une description de l'état quantique q_q correspondant à l'un des états de base |0>, |1>,... |d-1>, grâce aux informations de bases d'encodage échangées entre et à la mesure de l'état final lalpha$_{final}$>.

[0048] Après que les Q répétitions ont été effectuées, l'émetteur C_1 et le récepteur C_N reconstituent, par concaténation, une séquence des descriptions des Q états quantiques q_q , en jetant, si nécessaire, les descriptions non pertinentes et on exploitables.

[0049] Pour les deuxième, troisième et quatrième cas précédemment décrits, le principe de sécurisation de la transmission de séquences d'états quantiques à travers la chaîne de communication des N participants et le concept de descriptions d'états quantiques sont les mêmes que ceux décrits pour le premier cas de transmission sécurisée.

[0050] Les première et deuxième actions réalisées respectivement par les premier et second participants distincts C_i et C_j dans les quatre différents cas de transmission sécurisée de séquences d'états quantiques vont maintenant être décrites de manière formelle.

[0051] On considère un espace vectoriel hilbertien d'encodage d'états quantiques de dimension d. La première action réalisée, lors de la q-ième répétition de la succession d'étapes précédemment décrites par le participant C_i peut ainsi consister en les étapes suivantes :

- le premier participant C_i choisit une valeur s_q égale à 0 ou 1
- le premier participant C_i choisit une valeur entière m comprise entre 0 et d-1
- le premier participant C_i applique une transformation $P^{sq}X_m$ au photon reçu à travers la chaîne de communication, ou dans le cas où i est égal à 1, au photon au début de la chaîne de communication,

où, il est rappelé, la notation P désigne une transformation permettant d'effectuer un changement de base d'encodage, depuis la base standard B_0 vers une base d'encodage B_1 orthonormée, i.e. pour m un entier compris entre 0 et d-1 :

[0052] [Math.3]

$$P|\ m\ \rangle = e_m$$

[0053] et où la notation X_m désigne les transformations suivantes, respectivement dans la base B_0 et la base B_1, pour m et t deux entiers compris entre 0 et d-1 :

[0054] [Math.4]

$$X_m|t> = |t + m \bmod d>$$

[0055] et $X_m|e_t> = |e_{t+m \bmod d}>$

[0056] où l'abréviation mod désigne la fonction mathématique modulo.

[0057] La transformation X_m correspond à la première étape G_1, et la transformation P^{sq} correspond à la deuxième G_2. L'effet de la première action effectuée par le premier participant Ci, $P^{sq}X_m$, sur un état de référence |0> est illustrée sur la figure 3. Les états |+> et |-> sont définis comme suit :

[0058] $$|+> = \frac{1}{\sqrt{2}}(|0> + |1>)$$

[0059] [Math.6]

$$|-> = \frac{1}{\sqrt{2}}(|0> - |1>)$$

[0060] La deuxième action réalisée, lors de la q-ième répétition de la succession d'étapes précédemment décrites par le second participant C_j peut ainsi consister en les étapes suivantes :

- le second participant C_j choisit une valeur t_q égale à 0 ou 1 ;
- le second participant C_j choisit une valeur n comprise entre 0 et d-1 ;
- le second participant C_j applique une transformation $X_nP^{(-1)tq}$ au photon reçu à travers la chaîne de communication

où la notation $P^{(-1)}$ désigne la transformation permettant d'effectuer un changement de base d'encodage, depuis la base incompatible B_1 vers la base standard B_0, i.e. pour m un entier compris entre 0 et d-1 :

[0061] $P^{(-1)}|e_m> = |m>$ et où :

- la notation $P^{(-1)0}$ signifie que la transformation $P^{(-1)}$ n'a pas lieu ;
- la notation $P^{(-1)1}$ signifie que la transformation $P^{(-1)}$ a lieu,

[0062] La transformation $P^{(-1)tq}$ correspond à la troisième étape G_3, et la transformation X_n correspond à la quatrième étape G_4.

[0063] Ainsi, dans les deux configurations permettant une transmission d'état quantique fournissant une information pertinente, c'est-à-dire soit la configuration où les participants C_i et C_j décident tous les deux lors des deuxième et troisième étapes G_2 et G_3 d'appliquer respectivement les transformations P et $P^{(-1)}$, soit la configuration où aucun des deux ne décide lors des deuxième et troisième étapes G_2 et G_3 d'appliquer respectivement les transformations P et $P^{(-1)}$, la base d'encodage résultante à l'étape G_4 est la base standard B_0. L'état final $|alpha_{final}>$ est égal à |m+n mod d> et peut être mesuré dans la base standard B_0 par le récepteur C_N. Le résultat de la mesure annoncé par le récepteur est m+n mod d. Tous les participants ignorant la valeur de m et n, c'est-à-dire tous les participants sauf les premier et second participants C_i et C_j n'apprennent rien de la valeur m+n mod d. La transformation X_n a pour effet de masquer l'état transmis par le premier participant C_i lorsqu'il est mesuré et annoncé par le récepteur C_N. Du fait de la divulgation du résultat de la mesure par le récepteur C_N,

m+n mod d, le participant C_j peut ainsi déduire l'état |m> que lui a transmis le participant C_i. La transmission de l'état quantique par le premier participant C_i au second participant C_j a bien été effectuée de manière sécurisée, car tous les autres participants de la chaîne connaissent seulement le résultat m+n mod d de la mesure effectuée par le récepteur C_n.

[0064] Ainsi, l'application du codage conjugué par l'intermédiaire de l'utilisation de bases d'encodage incompatibles permet une transmission sécurisée d'un état quantique, ou information quantique, entre deux premier et second participants Ci et Cj, dans laquelle l'état quantique transmis est inconnu des autres participants de la chaîne de communication.

[0065] De manière plus générale, il peut être envisagé que la transmission d'états quantiques par le premier participant C_i au second participant C_j soit répétée pour transmettre une pluralité de messages. Dans ce cas, C_i peut envoyer a posteriori à C_j les décisions qu'il a prises aux différentes deuxième étapes répétées, et C_j peut sélectionner les informations issues de mesures pour lesquelles il a pris des décisions correctes lors des différentes troisièmes étapes G3 répétées.

[0066] Plus théoriquement, derrière l'utilisation du codage conjugué se cache l'utilisation du principe d'incertitude de la physique quantique. L'utilisation de bases conjuguées a pour effet que la lecture dans une base d'une information codée dans une autre base donne une valeur complètement aléatoire. Il s'agit là d'une incompatibilité maximale, car on parle d'incompatibilité dès qu'il y a incertitude sur la valeur envoyée.

[0067] Dans les deux autres configurations ne permettant pas une transmission d'état quantique fournissant une information pertinente, c'est-à-dire, comme expliqué plus haut, dans le cas où le participant C_i décide d'appliquer la transformation P lors de la sous-étape G_2, et que le participant C_j décide de ne pas appliquer la transformation $P^{(-1)}$ lors de la sous-étape G_3, ou inversement, dans le cas où le participant C_i décide de ne pas appliquer la transformation P lors de la sous-étape G_2, et que le participant C_j décide d'appliquer la transformation $P^{(-1)}$ lors de la sous-étape G_3, le résultat de la mesure annoncé par le récepteur C_N sera aléatoire et jeté et mis à l'écart.

[0068] Selon un mode de réalisation du procédé de transmission sécurisée d'une séquence d'états quantiques, la dimension d de l'espace vectoriel hilbertien de codage des vecteurs d'états est égale à 2.

[0069] Un autre mode de réalisation du premier cas de transmission sécurisée, où les premier et second participants C_i et C_j sont des participants différents des participants C_1 et C_N, c'est-à-dire qu'ils ne sont ni émetteur, ni récepteur, mais simplement des transformateur et que la chaîne de communication comprend un nombre N de participants supérieur ou égal à 4, va être décrit, où les deuxième et quatrième étapes G_2 et G_4 peuvent être suivies d'étapes complémentaires visant à prévenir d'attaques

d'espions de la transmission d'états quantiques par canaux cachés.

[0070] Lors de la q-ième répétition de la succession d'étapes du procédé de transmission sécurisée d'une séquence de Q états quantiques q_q, l'étape G_2 peut être suivie des étapes successives suivantes :

- lors d'une cinquième étape G_5, une portion P_{seq1} de la puissance lumineuse provenant du participant C_{i-1} peut être prélevée ;
- lors d'une sixième étape G_6, la portion P_{seq1} peut être comparée avec une portion $P_{seq1'}$ de la puissance lumineuse P_{seq} de la séquence de photons envoyée par l'émetteur C_1, afin de détecter une potentielle injection de photons espions entre le participant C_{i-1} et le premier participant C_i.

L'étape G_4 peut elle aussi être suivie des étapes successives suivantes :

- lors d'une septième étape G_7, une portion P_{seq2} de la puissance lumineuse provenant du participant C_{j-1} peut être prélevée ;
- lors d'une huitième étape G_8, la portion P_{seq2} peut être comparée avec une portion $P_{seq2'}$ de la puissance lumineuse P_{seq}-P_{seq1}, afin de détecter une potentielle injection de photons espions entre le participant C_{j-1} et le second participant C_j.

[0071] En effet, il peut être envisagé que, puisque les premier et second participants C_i et C_j sont des transformateurs ne pouvant mesurer de puissance lumineuse, un espion applique l'attaque suivante : dans le cas de bits quantiques encodés dans la phase de photons, l'espion pourrait injecter entre l'émetteur C_1 et le participant C_i des photons de polarisation différente de ceux émis par l'émetteur C_1, qui est un participant légitime. La figure 4 montre un exemple de réalisation de cette attaque par canaux cachés sur un premier participant C_i par un espion dans un dispositif de communication quantique optique. Il suffirait à l'espion de combiner ses photons espions aux photons émis légitimement par l'émetteur C_1, en utilisant par exemple un combinateur de polarisation, et de récupérer juste après le participant C_i les photons espions qu'il aura introduits. Ainsi, l'espion pourrait mesurer la modulation appliquée par le premier participant C_i, et apprendre par exemple les valeurs de s_q et m choisies par le premier participant C_i. La même attaque d'injection de photons espions en amont du second participant C_j et récupération de photons modulés par le second participant C_j juste après le second participant C_j pourrait être appliquée. Une condition nécessaire pour réaliser ce type d'attaque est pour l'espion de pouvoir se positionner juste avant et juste après un participant. Ainsi, ce type d'attaque n'est pas possible sur les participants émetteur C_1 et récepteur C_N. La figure 4 illustre schématiquement le principe d'attaque par canal caché tel que décrit précédemment.

[0072] Les prélèvements de puissance lumineuse effectué lors des cinquième et septième étapes G_5 et G_7 en permettent la mesure ainsi que la vérification de la conformité de ces mesures, par les comparaisons effectuées lors des sixième et huitième étapes G_6 et

G_8, avec la puissance lumineuse P_{seq} envoyée par l'émetteur C_1. Ces prélèvements et comparaisons constituent ainsi des contre-mesures effectuées respectivement par le premier participant C_i et le second participant C_j. La figure 5 illustre schématiquement le principe de contre-mesure qui peut être effectuée par l'un des premier ou second participants C_i ou C_j lors des sixième et huitième étapes G_6 ou G_8.

[0073] Les cinquième, sixième, septième et huitième étapes G_5 à G_8 constituent donc une sécurité additionnelle du procédé de transmission d'une séquence d'états quantiques entre les premier et deuxième participants C_i et C_j, car elles permettent de détecter d'éventuelles attaques par canaux cachés par des espions. Cette sécurité additionnelle peut être mise en œuvre avec un matériel simple et peu coûteux.

[0074] Dans ce mode de réalisation, le principe d'incertitude assure également la sécurité. Supposons qu'un espion mesure les photons le premier participant C_i et le réémet un photon identique à celui qu'il a mesuré. S'il a mesuré dans une base d'encodage différente de celle choisie par le premier participant C_i, ce qui arrive une fois sur deux, alors l'espion va modifier le photon, du fait de l'équiprobabilité sur les résultats de mesure qu'il pourra obtenir. Les statistiques seront modifiées en conséquence de manière visible pour le premier participant C_i et le second participant C_j. En comparant une petite portion des photons reçus avec ceux envoyés, les premier et second participants C_i et C_j, peuvent ainsi repérer un espion qui écoute leur conversation.

[0075] Préférentiellement, le degré de liberté des photons encodant les bits quantiques est choisi parmi la phase, la différence de phase, la localisation temporelle, la polarisation ou la fréquence du photon.

[0076] Avantageusement, la séquence des Q états quantiques q_q pour q entier compris entre 1 et q est choisie de manière aléatoire dans le but d'établir une clé quantique distribuée entre les participants Ci et Cj. Dans ce cas particulier, l'étape d'échange des décisions de transformation des étapes G_2 et G_3 correspondant à l'opération de « key sifting » effectuée de manière standard dans un protocole de distribution de clé quantique.

[0077] La mise en œuvre du procédé de transmission sécurisée d'une séquence de Q états quantiques q_q, q étant un entier compris entre 1 et Q peut être réalisée à l'aide d'un dispositif comprenant :

- un laser apte à générer des photons et un modulateur initial apte à moduler un degré de liberté d'un photon généré, ledit laser et ledit modulateur initial étant associé à l'émetteur C_1
- N-2 modulateurs intermédiaires aptes à moduler un degré de liberté d'un photon reçu, chacun des N-2 modulateurs intermédiaires étant associé à un participant intermédiaire C_k, parmi les N-2 participants intermédiaires C_2 à C_{N-1} distincts de l'émetteur C_1 et du récepteur C_N
- un détecteur de photons apte à détecter des photons uniques et un modulateur final

apte à moduler un degré de liberté d'un photon reçu ; ledit détecteur de photons et ledit modulateur final étant associé au récepteur C_N

La figure 6 illustre une réalisation de ce dispositif pour une chaîne de communication à quatre participants.

[0078] Le dispositif précédemment décrit peut être utilisé de la manière suivante. Une fois les premier et second participants C_i et C_j choisis, un laser associé à l'émetteur C_1 génère, suite à une commande de l'émetteur C_1, un flux de photons encodant une séquence bits quantiques. Le flux de photons est transmis dans la chaîne de communication par l'intermédiaire du modulateur initial, des N-2 modulateurs intermédiaires, du modulateur final, et jusqu'au détecteur de photons.

[0079] Dans le cadre de la transmission d'une séquence de Q états quantiques codés sur Q photons, pour chaque photon :

- au cours de la transmission dudit photon à travers la chaîne de communication, le premier participant C_i effectue sur ledit photon une première action, comprenant une première étape G_1 de décision et une deuxième étape de décision G_2, en commandant un modulateur lui étant associé, c'est-à-dire soit le modulateur initial, soit l'un des N-2 modulateurs,
- suite à la première action du premier participant C_i sur ledit photon, la transmission du photon est poursuivie jusqu'au second participant C_j, qui effectue sur le photon, après réception de celui-ci, une deuxième action, comprenant une troisième étape G_3 de décision et une quatrième étape de décision G_4, en commandant un modulateur lui étant associé, c'est-à-dire soit l'un des N-2 modulateurs intermédiaires, soit le modulateur final. Suite à la deuxième action du second participant C_j sur le photon, la transmission dudit photon est poursuivie jusqu'à la réception de celui-ci par le détecteur de photons associé au récepteur C_N,
- le récepteur C_N mesure l'état final du bit quantique codé dans le photon qu'il reçoit et partage le résultat de la mesure avec les autres participants de la chaîne de communication,
- les premier et second participants C_i et C_j échangent sur un canal de communication classique les décisions prises au cours des deuxième et troisième étapes G_2 et G_3,
- les premier et second participants C_i et C_j déduisent une description de l'état quantique à l'aide des décisions échangées et de la mesure par le récepteur C_N de l'état final du bit quantique codé dans le photon détecté par le détecteur de photons associé au récepteur C_N.

[0080] Ainsi, le premier participant C_i et le second participant C_j reconstituent, par concaténation, une séquence des descriptions des Q états quantiques transmis, en jetant, si nécessaire, les descriptions non pertinentes et non exploitables, dans les cas précédemment décrits.

[0081] L'avantage du procédé de transmission séquences d'états quantiques entre plusieurs participants présenté dans cette demande est donc de pouvoir être mis en œuvre par un dispositif ne comprenant qu'un seul laser et qu'un seul détecteur de photons. Ces derniers composants étant en général les éléments matériels les plus coûteux, le protocole présenté ici permet donc de réaliser une transmission de séquences d'états quantiques avec un coût par participant moindre.

[0082] Dans le cas précédemment décrit où les premier et second participants C_i et C_j sont des participants différents des participants C_1 et C_N, le dispositif précédemment décrit peut être complété par :

- un premier séparateur de faisceau S_i positionné en amont du modulateur associé au premier participant C_i,
- une première photodiode PD_i associée au premier participant C_i et apte à mesurer une puissance lumineuse,
- un deuxième séparateur de faisceau S_j positionné en amont du modulateur associé au second participant C_j,
- une deuxième photodiode PD_j associée au second participant C_j et apte à mesurer une puissance lumineuse.

[0083] Le séparateur de faisceau S_i sépare le flux de photons reçu du participant C_{i-1} dans deux directions distinctes, l'une en direction du modulateur du premier participant C_i puis vers la suite de la chaîne de communication, l'autre en direction de la photodiode PD_i . Le deuxième séparateur de faisceau S_j sépare le flux de photons reçu du participant C_{j-1} dans deux directions distinctes, l'une en direction du modulateur du second participant C_j puis vers la suite de la chaîne de communication, l'autre en direction de la deuxième photodiode PD_j.

Ces composants supplémentaires permettent la mise en œuvre de la sécurisation du procédé de transmission de séquences d'états quantiques vis-à-vis des attaques par canaux cachés. Ils permettent en particulier la réalisation des cinquième, sixième, septième et huitième étapes G_5 à G_8 précédemment décrites. Les cinquième et septième étapes G_5 et G_7 sont réalisées respectivement par la mesure de la puissance lumineuse P_{seq1} par la photodiode PD_i et par la mesure de la puissance lumineuse P_{seq2}. Les sixième et huitième étapes de comparaison G_6 et G_8 sont réalisées en utilisant les mesures des puissances lumineuses P_{seq1} et P_{seq2} et des valeurs de prédiction de puissance lumineuses $P_{seq1'}$ et $Ps_{eq2'}$. Par exemple, lorsque l'une des comparaisons, entre P_{seq1} et $P_{seq1'}$ d'une part, et entre P_{seq2} et $P_{seq2'}$ d'autre part, a pour résultat une inégalité, une attaque par un espion, par exemple par injection de photons, peut être détectée.

Dans cette configuration, les premier et deuxième séparateurs de faisceau S_i et S_j sont configurés de manière à ce qu'avec une probabilité p, les photons qui les traversent soient dirigés vers respectivement les première et deuxième photodiodes PD_i et PD_j.

Les photodiodes PD_i et PD_j peuvent mesurer la puissance lumineuse moyenne sur une période de temps donnée.

Ainsi, ces composants supplémentaires sont également beaucoup plus simples et moins coûteux en comparaison avec du matériel classiquement utilisé dans les dispositifs de communication quantique tels que par exemple des détecteurs de photon unique.

[0084] Lorsque le degré de liberté des photons pour encoder les bits quantiques est la phase, le modulateur initial, les N-2 modulateurs intermédiaires et le modulateur peuvent être des modulateurs de phase. Par exemple, le modèle LN53S-FC ou LN65S-FC commercialisé par la société Thorlabs peut être utilisé.

[0085] Lorsque le degré de liberté des photons pour encoder les bits quantiques est la polarisation des photons, le modulateur initial, les N-2 modulateurs intermédiaires et le modulateur peuvent être des modulateurs de polarisation. Par exemple, un modèle de la série de produits PSC-LN series commercialisé par la société iXblue Photonics peut être utilisé.

[0086] Lorsque le degré de liberté des photons pour encoder les bits quantiques est la localisation temporelle des photons, le modulateur initial, les N-2 modulateurs intermédiaires et le modulateur peuvent comprendre chacun un nombre d de lignes à retard et un nombre 2d de lames séparatrices, où d représente la dimension de l'espace vectoriel hilbertien de représentation des états quantiques. La superposition de localisations temporelles à réaliser pour créer une base incompatible peut être obtenue en programmant les lames séparatrices. La figure 7 illustre un dispositif modulateur de localisation temporelle, dans le cas où d est égal à 2.

[0087] La figure 8 montre un exemple de couple de bases incompatibles conçues dans le cas où le degré de liberté des photons est la localisation pour un espace vectoriel hilbertien de dimensions 4. Les quatre localisations temporelles correspondant aux états de la base $|t_0\rangle$, $|t_1\rangle$, $|t_2\rangle$ et $|t_3\rangle$ sont t_0, t_1 égale à $t_0+\tau$, t_2 égale à $t_0+2\tau$ et t_3 égale à $t_0+3\tau$. Un exemple de base incompatible peut-être alors la base $|\tau_0\rangle$, $|\tau_1\rangle$, $|\tau_2\rangle$ et $|\tau_3\rangle$ telle que représentée à la figure 8. Une utilisation de ces deux bases est retrouvée dans l'article « *Provably secure and high-rate quantum key distribution with time-bin qubits* » (Islam et *al.*, Sci. Adv. 2017 ;3).

[0088] Des post-traitements tels que la correction d'erreur ou l'amplification de confidentialité standard dans des protocoles de distribution de clé quantique peuvent être également appliqués suite à la mise en œuvre des différents modes de réalisation de procédé de transmission sécurisée de séquences d'états quantiques.

[0089] Selon certains modes de réalisation, l'invention peut présenter plusieurs avantages :

- le procédé de transmission d'états quantiques peut être doublement sécurisé, d'une part de manière intrinsèque par l'application du principe de codage conjugué, d'autre part de manière extrinsèque par la contre-mesure mise en œuvre pour détecter des

attaques par canaux cachés ;
- le matériel utilisé pour la mise en œuvre du procédé de transmission présenté est simple est peu coûteux car il ne nécessite que deux composants coûteux, un laser et un détecteur de photon unique, ainsi que d'autres composants beaucoup plus accessibles, modulateurs, lignes à retard, lames séparatrices, photodiodes classiques.

Revendications

[Revendication 1] Procédé de transmission sécurisée d'une séquence de Q états quantiques q_q encodée sous la forme d'une séquence de Q photons, q étant un entier compris entre 1 et Q, entre un premier participant (C_i) et un second participant (C_j), choisis parmi une pluralité de N participants distincts (C_1), …(C_i), …(C_j), …(C_N) d'un même canal de communication quantique formant une chaîne de communication entre un émetteur (C_1) et un récepteur (C_N), où N est un entier supérieur ou égal à 3, dans lequel le premier participant (C_i) est situé en amont du second participant (C_j) dans la chaîne de communication,
ledit procédé comprenant, dans l'ordre :

– la succession des étapes suivantes, répétée de q=1 à Q :

- préparation par l'émetteur (C_1) d'un photon dans un état quantique de base de référence |0> d'une base d'encodage B_0 orthonormée nommée base standard de dimension d et d'états de base |0>, |1>,… |d-1>,
- transmission du photon préparé dans la chaîne de communication,
- une première action effectuée par le premier participant (C_i) sur ledit photon, comprenant deux première et deuxième étapes (G_1) et (G_2) consécutives :

○ une première étape (G_1) de décision de transformation ou non de l'état quantique du photon transmis, en un état quantique de base orthogonal dans la base d'encodage B_0,
○ une deuxième étape (G_2) de décision d'appliquer ou non une transformation P permettant d'effectuer un changement de base d'encodage, depuis la base standard B_0 vers une base d'encodage B_1 incompatible avec la base standard B_0, d'états de base $|e_0>$, $|e_1>$,… $|e_{d-1}>$

- une deuxième action effectuée par le second participant (C_j) sur ledit photon, comprenant deux troisième et quatrième (G_3) et (G_4) étapes consécutives :

○ une troisième étape (G_3) de décision d'appliquer ou non la trans-

formation inverse $P^{(-1)}$ de ladite transformation P, permettant d'effectuer un changement de base d'encodage, depuis la base incompatible B_1 vers la base standard B_0,

○ une quatrième étape (G_4) de décision de transformation ou non de l'état quantique du photon reçu du participant immédiatement précédent (C_{j-1}) en un état quantique orthogonal correspondant dans la base d'encodage résultant de la troisième étape (G_3)

- mesure, dans la base standard B_0, de l'état final $|alpha_{final}\rangle$ du photon transmis dans la chaîne de communication par le récepteur (C_N),
- échange sur un canal de communication classique entre les premier et second participants (C_i) et (C_j) des décisions des deuxième et troisième étapes (G_2) et (G_3),
- obtention, entre les premier et second participants (C_i) et (C_j), d'une description de l'état quantique transmis q_q correspondant à l'un des états de base $|0\rangle$, $|1\rangle$,… $|d-1\rangle$, grâce aux informations de décisions des deuxième et troisième étapes (G_2) et (G_3) et à la mesure de l'état final $|alpha_{final}\rangle$,

– puis, la reconstitution, par les premier et second participants (C_i) et (C_j), par concaténation, d'une séquence des descriptions des Q états quantiques transmis q_q, pour q allant de 1 à Q, et,

dans lequel i est différent de 1 et N, et j est différent de 1 et N, la séquence des Q photons encodant la séquence des Q états quantiques q_q présente une puissance lumineuse donnée P_{seq} et N est un entier supérieur ou égal à 4, et dans lequel :

– La deuxième étape (G_2) est immédiatement suivie de :

- une cinquième étape (G_5) de prélèvement d'une première portion (P_{seq1}) de la puissance lumineuse (P_{seq}) du flux de photons reçu du participant (C_{i-1}) précédant immédiatement le premier participant (C_i),
- une sixième étape (G_6) de comparaison de la première portion (P_{seq1}) avec une seconde portion ($P_{seq1'}$) de la puissance

lumineuse (P_{seq}) du flux de photons envoyé par l'émetteur (C_1) afin de détecter une potentielle injection de photons espions avant le premier participant (C_i),

– La quatrième étape (G_4) est immédiatement suivie de :

• une septième étape (G_7) de prélèvement d'une troisième portion (P_{seq2}) de la puissance lumineuse du flux de photons reçu du participant (C_{j-1}) précédant immédiatement le second participant (C_j),

– une huitième étape (G_8) de comparaison de la troisième portion (P_{seq2}) avec une quatrième portion ($P_{seq2'}$) de la différence entre la puissance lumineuse du flux de photons envoyé par l'émetteur (P_{seq}) et la première portion (P_{seq1}) afin de détecter une potentielle injection de photons espions avant le second participant (C_j)..

[Revendication 2] Procédé de transmission sécurisée selon la revendication 1, dans lequel, pour chaque répétition de q=1 à Q de la succession d'étapes selon la revendication 1 :

– la première action, effectuée par le premier participant (C_i), comprend les étapes suivantes :

• Choisir une valeur sq égale à 0 ou 1
• Choisir une valeur m comprise entre 0 et d-1
• Appliquer une transformation $P^{sq}X_m$ au photon reçu à travers la chaîne de communication, ou dans le cas où i est égal à 1, au photon au début de la chaîne de communication, ladite transformation $P^{sq}X_m$ correspondant à la succession des première et deuxième étapes (G_1) et (G_2)

– la deuxième action, effectuée par le second participant (C_j),

comprend les étapes suivantes :

- Choisir une valeur tq égale à 0 ou 1
- Choisir une valeur n comprise entre 0 et d-1
- Appliquer une transformation $X_nP^{(-1)tq}$ au photon reçu à travers la chaîne de communication, ladite transformation $X_nP^{(-1)tq}$ correspondant à la succession des troisième et quatrième étapes (G3) et (G4)

dans lequel :

- la notation P^1 signifie que la transformation P a lieu,
- la notation P^0 signifie que la transformation P n'a pas lieu,
- la notation $P^{(-1)1}$ signifie que la transformation $P^{(-1)}$ a lieu,
- la notation $P^{(-1)0}$ signifie que la transformation $P^{(-1)}$ n'a pas lieu,
- la notation X_m désigne une transformation permettant de passer de l'état quantique de base $|t>$, t étant un entier compris entre 0 et d-1, à l'état orthogonal $|(t+m) \bmod d>$ dans la base B_0 ou la transformation permettant de passer d'un état $|e_t>$ à $|e_{t+m \bmod d}>$ dans la base B_1, pour m un entier compris entre 0 et d-1.

[Revendication 3] Procédé de transmission sécurisée selon l'une des revendications 1 ou 2, dans lequel ladite dimension d est égale à 2.

[Revendication 4] Procédé de transmission sécurisée, selon l'une des revendications 1 à 3 dans lequel chaque état quantique q_q est codé dans un degré de liberté du photon choisi parmi la phase, la différence de phase, la localisation temporelle, la polarisation ou la fréquence du photon.

[Revendication 5] Procédé de transmission sécurisée selon l'une des revendications 1 à 4 dans lequel la séquence de Q états quantiques q_q est choisie de manière aléatoire dans le but d'établir une clé quantique.

[Revendication 6] Dispositif pour la mise en œuvre du procédé de transmission sécurisée selon l'une des revendications 1 à 5, comprenant :
- un laser apte à générer des photons et un modulateur initial apte à moduler un degré de liberté d'un photon généré,
- N-2 modulateurs intermédiaires aptes à moduler un degré de liberté d'un photon reçu,
- un détecteur de photons apte à détecter des photons uniques et un mo-

dulateur final apte à moduler un degré de liberté d'un photon reçu, dans lequel :

- le laser et le modulateur initial sont associés à l'émetteur (C_1) et sont aptes à être commandés par l'émetteur (C_1),
- chacun des N-2 modulateurs intermédiaires est associé à un participant intermédiaire (C_k) parmi les N-2 participants intermédiaires (C_2) à (C_{N-1}) distincts de l'émetteur (C_1) et du récepteur (C_N) et est apte à être commandé par ledit participant intermédiaire (C_k),
- le détecteur de photons et le modulateur final sont associés au récepteur (C_N) et sont aptes à être commandés par le récepteur (C_N), et

comprenant en outre, dans le cas où le premier participant (C_i) et le second participant (C_j) sont tous les deux distincts de l'émetteur (C_1) et du récepteur (C_N) :
- un premier séparateur de faisceau (S_i) positionné en amont du modulateur associé au premier participant (C_i),
- une première photodiode (PD_i) associée au premier participant (C_i) et apte à mesurer une puissance lumineuse d'un flux de photons,
- un deuxième séparateur de faisceau (S_j) positionné en amont du modulateur associé au second participant (C_j),
- une deuxième photodiode (PD_j) associée au second participant (C_j) et apte à mesurer une puissance lumineuse d'un flux de photons,

dans lequel :

- le premier séparateur de faisceau (S_i) est apte à séparer un flux de photons reçu du participant précédant immédiatement le premier participant dans lachaîne de communication (C_{i-1}) dans deux directions distinctes, l'une en direction du modulateur du premier participant (C_i) puis vers la suite de la chaîne de communication, l'autre en direction de la première photodiode (PD_i),
- le deuxième séparateur de faisceau (S_j) est apte à séparer un flux de photons reçu du participant précédant immédiatement le second participant dans la chaîne de communication (C_{j-1}) dans deux directions distinctes, l'une en direction du modulateur du second participant (C_j) puis vers la suite de la

chaîne de communication, l'autre en direction de la deuxième photodiode (PD_j).

[Revendication 7] Dispositif pour la mise en œuvre d'un procédé de transmission sécurisée selon la revendication 6, dans lequel :

- Le degré de liberté du photon choisi est la phase
- Le modulateur initial, les modulateurs intermédiaires et le modulateur final sont des modulateurs de phase.

[Revendication 8] Dispositif pour la mise en œuvre du procédé de transmission sécurisée selon la revendication 6, dans lequel :

- Le degré de liberté du photon choisi est la polarisation
- Le modulateur initial, les modulateurs intermédiaires et le modulateur final sont des modulateurs de polarisation.

[Revendication 9] Dispositif pour la mise en œuvre d'un procédé de transmission sécurisée selon la revendication 6, dans lequel :

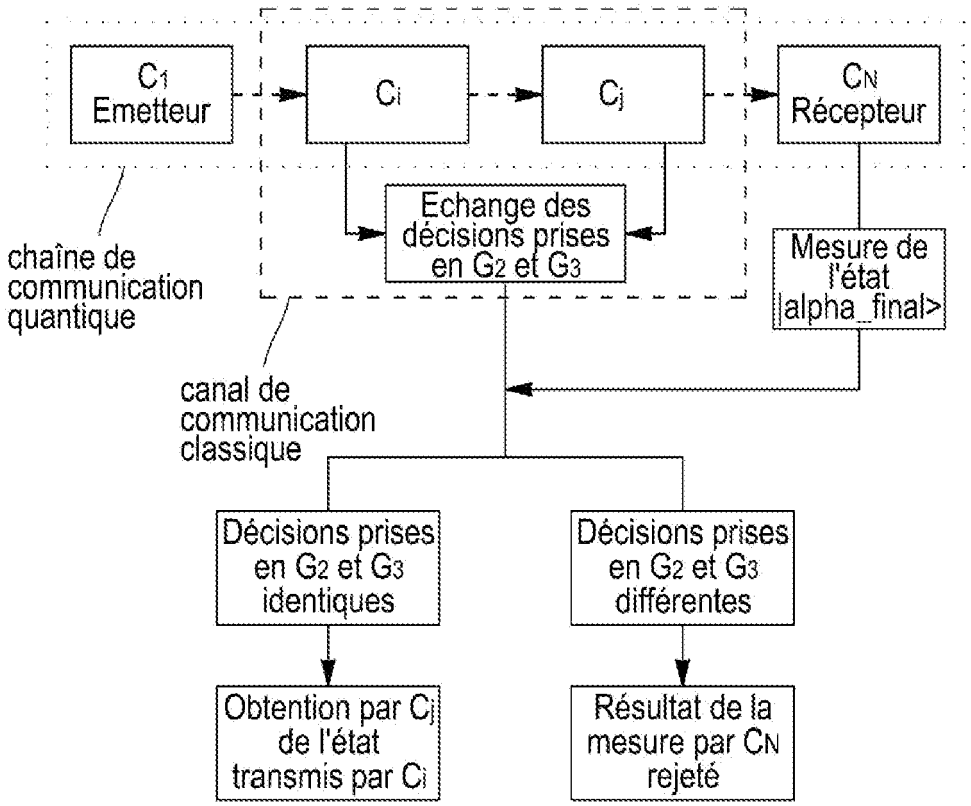
- Le degré de liberté du photon choisi est la localisation temporelle
- Le modulateur initial, les modulateurs intermédiaires et le modulateur final comprennent chacun un nombre de lignes à retard égal à la dimension de la base d'encodage des bits quantiques et un nombre de lames séparatrices égal au double du nombre de lignes à retard.

[Fig. 1]

Degré de liberté	|0>	|1>	Bases incompatibles
Phase	Phase fixe P_0	P_0+pi	Phase décalée de pi/2
Différence de phase	0	Pi	Phase décalée de pi/2
Localisation temporelle	Temps t_0	t_0+delta	Base de Hadamard
Polarisation	Horizontale	Verticale	Base diagonale
Fréquence	f_1	f_2	Base de Hadamard

La base HV (à gauche) et la base diagonale (à droite) pour la polarisation

[Fig. 2]

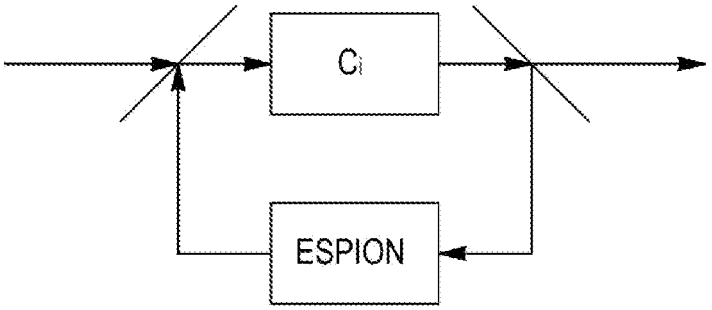


[Fig. 3]

$P^{Sq}X_m$ |0>
d=2

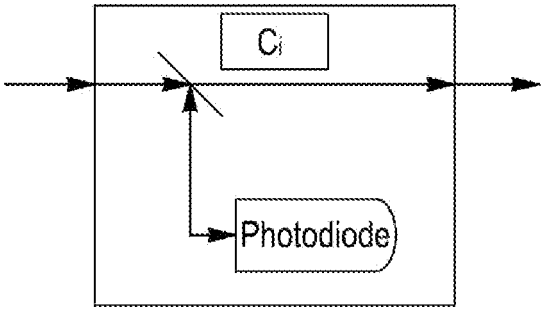
S_q	m	état
0	0	|0>
0	1	|1>
1	0	|+>
1	1	|->

[Fig. 4]



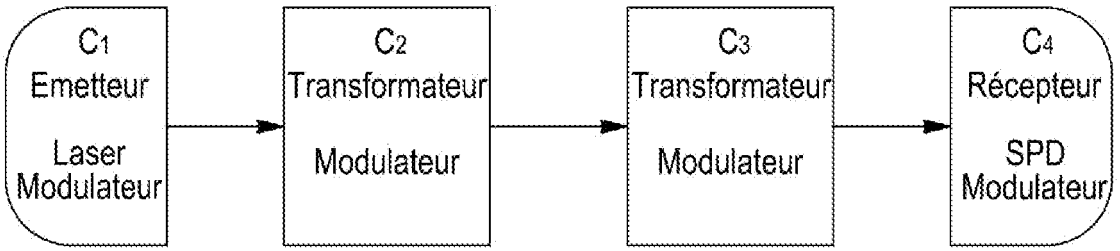
Injection de lumière par l'espion

[Fig. 5]

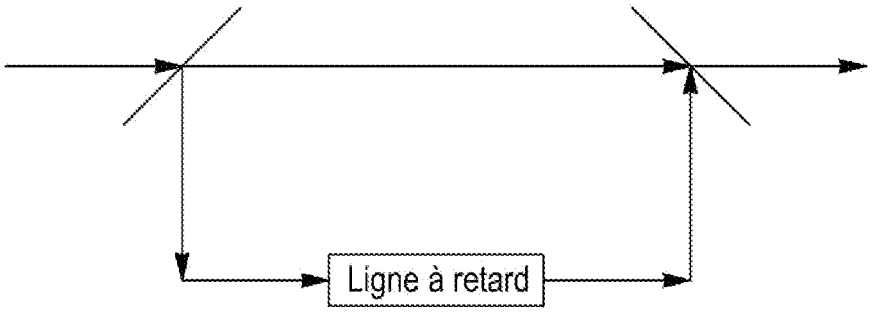


Contre mesure: Ci prélève des photons
pour mesurer l'intensité lumineuse moyenne

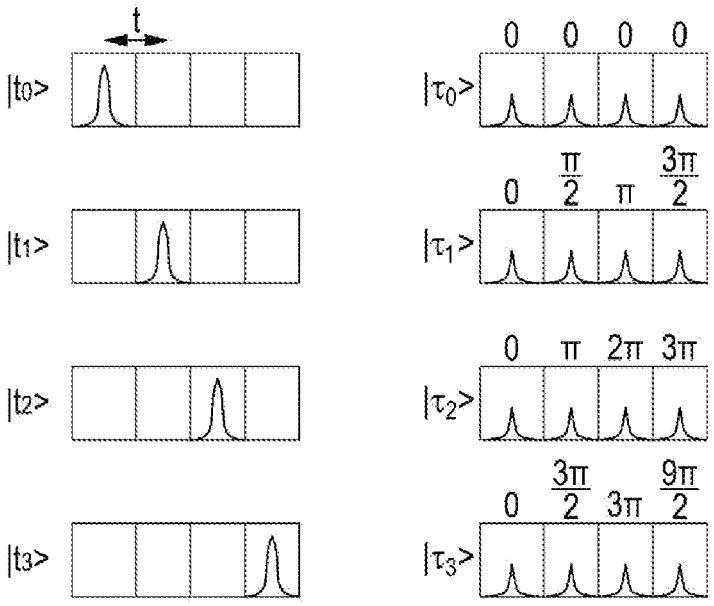
[Fig. 6]



[Fig. 7]



[Fig. 8]



RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

[x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

☐ Le demandeur a maintenu les revendications.

[x] Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

[x] Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

☐ Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION

US 5 764 765 A (PHOENIX SIMON JAMES [GB] ET AL) 9 juin 1998 (1998-06-09)

A. R. DIXON ET AL: "Quantum key distribution with hacking countermeasures and long term field trial", SCIENTIFIC REPORTS, vol. 7, no. 1, 16 mai 2017 (2017-05-16), XP055707051, DOI: 10.1038/s41598-017-01884-0

US 2007/076883 A1 (KUANG RANDY [CA]) 5 avril 2007 (2007-04-05)

2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL

NEANT

3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES

NEANT