

⑫

BREVET D'INVENTION

B1

⑤④ Système et procédé de détermination de clés de cryptage utilisant l'encodage de phase d'un signal.

②② Date de dépôt : 02.06.22.

③③ Priorité :

⑥⑥ Références à d'autres documents nationaux
apparentés :

☐ Demande(s) d'extension :

⑦① Demandeur(s) : *THALES Société anonyme* — FR.

④③ Date de mise à la disposition du public
de la demande : 08.12.23 Bulletin 23/49.

④⑤ Date de la mise à disposition du public du
brevet d'invention : 07.06.24 Bulletin 24/23.

⑤⑥ Liste des documents cités dans le rapport de
recherche :

Se reporter à la fin du présent fascicule

⑦② Inventeur(s) : BERTRAND Mathieu et VAN DEN
BOSSCHE Mathias.

⑦③ Titulaire(s) : *THALES Société anonyme*.

⑦④ Mandataire(s) : ATOUT PI LAPLACE.



Description

Titre de l'invention : Système et procédé de détermination de clés de cryptage utilisant l'encodage de phase d'un signal

Domaine technique

- [0001] La présente invention concerne de manière générale le domaine des communications quantiques, et en particulier un système et un procédé de détermination de clés de cryptage quantique.
- [0002] La détermination de clés de cryptage quantique (ou QKD, acronyme pour l'expression anglo-saxonne correspondante 'Quantum Key Distribution' signifiant 'distribution de clés quantiques' en français) est une technologie de détermination de clés secrètes (encore appelée technologie d'établissement de clés secrètes) entre des utilisateurs distants dans le cadre de communications optiques hautement sécurisées. Cette technologie utilise des protocoles cryptographiques basés sur des lois de la mécanique quantique. En particulier, on distingue la classe des protocoles « prépare et mesure » (P&M, acronyme pour l'expression anglo-saxonne correspondante 'Prepare and Measure') des protocoles basés sur l'intrication quantique.
- [0003] Dans le domaine de la cryptographie, les utilisateurs distants sont classiquement nommés Alice (dispositif émetteur) et Bob (dispositif récepteur). Un protocole P&M de détermination quantique utilisant un « encodage en phase » comporte une étape d'émission, une étape de réception, et une étape de réconciliation.
- [0004] La première étape d'émission est effectuée par l'émetteur Alice et consiste à préparer une information quantique (appelé aussi « qubit ») encodée sur la phase d'un signal optique impulsionnel S possédant en moyenne moins d'un photon par impulsion, puis à émettre ce signal S par un canal de transmission quantique. L'émetteur Alice comprend notamment un interféromètre optique composé de deux bras optique asymétriques. L'information quantique est alors un signal quantique (i.e. photon unique) modulé selon une phase α dans un des bras de l'interféromètre de l'émetteur Alice.
- [0005] Dans la deuxième étape effectuée par le récepteur Bob, une estimation de l'information quantique sur le signal reçu est effectuée. Le récepteur Bob comprend également un interféromètre optique, sensiblement identique à l'interféromètre de l'émetteur Alice. Une modulation de phase β (indépendante de α) est alors appliquée, au signal quantique reçu, dans un des bras de l'interféromètre du récepteur Bob.
- [0006] Dans la troisième étape de réconciliation, l'émetteur Alice et le récepteur Bob se communiquent les modulations de phase identiques, c'est-à-dire telles que $\alpha = \beta$, via un canal public authentifié.
- [0007] Selon ce protocole P&M de détermination de clé quantique qui utilise un encodage

en phase, toute fluctuation de phase indésirable générée par l'un ou l'autre des interféromètres du système de distribution de clés de cryptage quantique conduit à des incertitudes de probabilité de mesure des photons uniques en réception et donc à des erreurs sur les qubits mesurés et sur l'établissement de la clé secrète.

- [0008] Des fluctuations de phase possibles sont des fluctuations de phase aléatoires qui peuvent être d'un ordre thermique, vibrationnel, ou issues de toute autre source de bruit influant sur la qualité du signal se propageant dans chacun des interféromètres. Il en résulte des variations de phase propres à chacun des interféromètres optiques du système qui ne peuvent pas être parfaitement identiques.
- [0009] D'autres fluctuations de phase possibles sont des fluctuations de phase déterministes présentent dans des systèmes comprenant un émetteur Alice et un récepteur Bob en mouvement relatif l'un par rapport à l'autre. Elles induisent des variations de phase dues au changement de la géométrie de transmission du signal au cours du temps, comme décrit dans l'article "Interference at the Single Photon Level Along Satellite-Ground Channels" de G. Vallone et al. 2016, Phys. Rev. Lett. 116, 253601.
- [0010] Pour résoudre les problèmes de fluctuations de phase aléatoires, les systèmes de détermination de clés de cryptage quantique connus utilisent deux solutions distinctes. La première solution consiste à effectuer une stabilisation passive des interféromètres optiques, en les isolant thermiquement et en les plaçant dans un environnement dépourvu de vibrations, comme décrit dans l'article "Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate" de A. R. Dixon et al. 2008, Optics Express Vol. 16, Issue 23, pp. 18790-18797. Cette solution, bien qu'efficace pour les applications en environnements contrôlés selon une communication fibrée au sol, n'est pas adaptée aux applications ayant des conditions extrêmes d'utilisation. En particulier dans le domaine spatial, dans lequel au moins un des utilisateurs distants est un satellite, cette solution implique l'utilisation d'une boucle d'asservissement à bord du satellite, augmentant ainsi les facteurs de coût, de poids et de puissance de sa charge utile.
- [0011] La seconde solution consiste à effectuer un multiplexage temporel du signal quantique avec un signal de contrôle impulsif possédant un grand nombre de photons, comme décrit dans l'article "10-Mb/s Quantum Key Distribution" de Z. Yuan et al. 2018, Journal of Lightwave Technology, Volume:36 Issue:16. Cette solution entraîne une réduction du débit d'informations quantiques transmises et nécessite l'utilisation d'une électronique de compensation en temps réel qui peut se révéler difficile à mettre en place. De plus, le phénomène d'atténuation en intensité des impulsions du signal de contrôle, dû à des variations du taux de transmission atmosphérique, pourrait être interprétée comme une baisse de contraste engendrée par les fluctuations de phase dans les interféromètres, et conduire ainsi à une correction

erronée des fluctuations de phase.

[0012] Les systèmes de détermination de clés de cryptage quantique existants ne sont ainsi pas capables de résoudre les problèmes de fluctuations de phase déterministes.

[0013] Il existe ainsi un besoin pour un système et un procédé de détermination de clés de cryptage quantique amélioré, qui soit notamment capable de corriger les fluctuations de phase aléatoires induites par les interféromètres servant à l'encodage et au décodage de la phase, ainsi que les fluctuations de phase déterministes présentes lorsque le transmetteur et le récepteur sont en mouvement l'un par rapport à l'autre.

Résumé de l'invention

[0014] La présente invention vient améliorer la situation en proposant un émetteur (Alice) configuré pour transmettre un signal interférométrique encodé S_2 à travers un canal de transmission, l'émetteur comprenant un module de génération de signal configuré pour générer un signal quantique intermédiaire $|\Psi_1\rangle$ et un signal de contrôle intermédiaire S_c , le module de génération de signal étant en outre configuré pour effectuer un décalage fréquentiel $\Delta\omega$ entre le signal quantique intermédiaire $|\Psi_1\rangle$ et le signal de contrôle intermédiaire S_c . L'émetteur comprend également un module interférométrique d'encodage configuré pour déterminer le signal interférométrique encodé S_2 comprenant un signal quantique interférométrique encodé $|\Psi_A\rangle$ et un signal de contrôle interférométrique S_{cA} parcourant un chemin optique sensiblement similaire, le module interférométrique d'encodage comprenant un dispositif d'encodage configuré pour appliquer une modulation de phase α uniquement à une composante du signal quantique intermédiaire $|\Psi_1\rangle$.

[0015] Dans des modes de réalisation, le module interférométrique d'encodage peut être implémenté sous la forme d'un interféromètre optique asymétrique comprenant un premier bras interférométrique et un deuxième bras interférométrique, le premier bras interférométrique étant plus court que le deuxième bras interférométrique. Le dispositif d'encodage peut alors comprendre au moins une unité de séparation fréquentielle positionnée sur le deuxième bras interférométrique, l'unité de séparation fréquentielle étant configurée pour effectuer un découplage fréquentiel du signal quantique intermédiaire $|\Psi_1\rangle$ et du signal de contrôle intermédiaire S_c .

[0016] Avantageusement, le module de génération de signal peut comprendre en outre une unité de décalage temporel configurée pour décaler temporellement le signal quantique intermédiaire $|\Psi_1\rangle$ et le signal de contrôle intermédiaire S_c .

[0017] La présente invention propose de plus un récepteur (Bob) configuré pour recevoir un signal quantique interférométrique encodé $|\Psi_A\rangle$ et un signal de contrôle interférométrique S_{cA} à travers un canal de transmission (50), le récepteur comprenant un module interférométrique de transcodage configuré pour générer un signal quantique

interférométrique transcodé $|\Psi_B\rangle$ et un signal de contrôle interférométrique modulé en phase S_{cB} , le module interférométrique de transcodage comprenant un dispositif de transcodage et de modulation de phase configuré pour appliquer une modulation de phase β_{eff} uniquement à une composante du signal quantique interférométrique encodé $|\Psi_A\rangle$ et une modulation de phase Φ_m uniquement à une composante du signal de contrôle interférométrique S_{cA} . Le récepteur comprend également un module de traitement configuré pour effectuer la mesure interférométrique du signal quantique interférométrique transcodé $|\Psi_B\rangle$ et du signal de contrôle interférométrique modulé en phase S_{cB} , le module de traitement étant en outre configuré pour déterminer la modulation de phase β_{eff} à partir de la modulation de phase Φ_m et de la mesure interférométrique du signal de contrôle interférométrique modulé en phase S_{cB} .

- [0018] Dans des modes de réalisation, le module interférométrique de transcodage peut être implémenté sous la forme d'un interféromètre optique asymétrique comprenant un premier bras interférométrique et un deuxième bras interférométrique, le premier bras interférométrique étant plus court que le deuxième bras interférométrique. Le dispositif de transcodage et de modulation de phase peut alors comprendre au moins une unité de séparation fréquentielle positionnée sur le deuxième bras interférométrique, l'unité de séparation fréquentielle étant configurée pour effectuer un découplage fréquentiel du signal quantique interférométrique encodé $|\Psi_A\rangle$ et du signal de contrôle interférométrique S_{cA} .
- [0019] Avantageusement, le module interférométrique de transcodage peuvent comprendre deux chemins optiques en sortie de l'interféromètre, et le module de traitement peut comprendre deux parties de traitement comprenant chacune une unité de séparation fréquentielle configurée pour effectuer la mesure interférométrique du signal quantique interférométrique transcodé $|\Psi_B\rangle$ et du signal de contrôle interférométrique modulé en phase S_{cB} , provenant des deux chemins optiques.
- [0020] Les modes de réalisation de l'invention fournissent ainsi un système de détermination de clé de cryptage quantique comprenant un émetteur (Alice) et un récepteur (Bob).
- [0021] Il est en outre proposé un procédé d'émission d'un signal interférométrique encodé S_2 , mis en œuvre par l'émetteur (Alice), le procédé comprenant les étapes consistant à :
- [0022] - générer un signal quantique intermédiaire $|\Psi_1\rangle$ de fréquence ω_q et un signal de contrôle intermédiaire S_c de fréquence ω_c ayant un décalage fréquentiel égal à $\omega_q - \omega_c$
- [0023] - appliquer une modulation de phase α à une composante du signal quantique intermédiaire $|\Psi_1\rangle$ passant à travers un interféromètre,
- [0024] - générer le signal interférométrique encodé S_2 comprenant un signal quantique interférométrique encodé $|\Psi_A\rangle$ et un signal de contrôle interférométrique S_{cA} .

- [0025] Le procédé d'émission comprend en outre une étape consistant à appliquer un retard temporel entre le signal quantique intermédiaire $|\Psi_I\rangle$ et le signal de contrôle intermédiaire S_c .
- [0026] Il est également proposé un procédé de réception d'un signal quantique interférométrique encodé $|\Psi_A\rangle$ et d'un signal de contrôle interférométrique S_{cA} , mis en œuvre par le récepteur (Bob), le procédé comprenant les étapes consistant à :
- [0027] - appliquer une modulation de phase Φ_m à la composante du signal de contrôle interférométrique S_{cA} et générer un signal de contrôle interférométrique modulé en phase S_{cB} ,
- [0028] - effectuer une mesure interférométrique du signal de contrôle interférométrique modulé en phase S_{cB} ,
- [0029] - déterminer une modulation de phase β_{eff} à partir de la modulation de phase Φ_m et de la mesure interférométrique du signal de contrôle interférométrique modulé en phase S_{cB} ,
- [0030] - appliquer la modulation de phase β_{eff} à la composante du signal quantique interférométrique encodé $|\Psi_A\rangle$ et générer un signal quantique interférométrique transcodé $|\Psi_B\rangle$,
- [0031] - effectuer une mesure interférométrique du signal quantique interférométrique transcodé $|\Psi_B\rangle$.
- [0032] Le système et le procédé d'établissement de clés de cryptage quantique selon les modes de réalisation de l'invention permettent de corriger les fluctuations de phase aléatoires induites par les interféromètres servant à l'encodage et au décodage de la phase et les fluctuations de phase déterministes présentes lorsque le transmetteur et le récepteur sont en mouvement l'un par rapport à l'autre, afin d'établir la clé quantique.

Description des figures

- [0033] D'autres caractéristiques, détails et avantages de l'invention ressortiront à la lecture de la description faite en référence aux dessins annexés donnés à titre d'exemple.
- [0034] [Fig.1] La [Fig.1] est un schéma représentant un système de détermination de clés de cryptage quantique, selon des modes de réalisation de l'invention.
- [0035] [Fig.2] La [Fig.2] est un schéma représentant un module de génération de signal d'un émetteur, selon des modes de réalisation de l'invention.
- [0036] [Fig.3] La [Fig.3] est un schéma représentant un module interférométrique d'encodage d'un émetteur, selon des modes de réalisation de l'invention.
- [0037] [Fig.4] La [Fig.4] est un schéma représentant un module interférométrique de transcodage d'un récepteur, selon des modes de réalisation de l'invention.
- [0038] [Fig.5] La [Fig.5] est un schéma représentant un module de traitement d'un récepteur, selon des modes de réalisation de l'invention.

- [0039] [Fig.6] La [Fig.6] est un schéma représentant une unité de correction du module de traitement d'un récepteur, selon des modes de réalisation de l'invention.
- [0040] [Fig.7] La [Fig.7] est un organigramme représentant un procédé de détermination de clés de cryptage quantique réalisé par un émetteur, selon des modes de réalisation de l'invention.
- [0041] [Fig.8] La [Fig.8] est un organigramme représentant un procédé de détermination de clés de cryptage quantique réalisé par un récepteur, selon des modes de réalisation de l'invention.
- [0042] Des références identiques sont utilisées dans les figures pour désigner des éléments identiques ou analogues. Pour des raisons de clarté, les éléments représentés ne sont pas à l'échelle.

Description détaillée

- [0043] La [Fig.1] représente schématiquement un système de détermination de clés de cryptage quantique 1 comprenant deux dispositifs 10 et 30 communiquant entre eux. Les deux dispositifs comprennent un émetteur 10, encore appelé 'Alice', et un récepteur 30, encore appelé 'Bob'.
- [0044] Le système de détermination de clés de cryptage quantique 1 peut être utilisé par exemple dans le domaine spatial, lorsque l'émetteur Alice (ou réciproquement le récepteur Bob) est monté à bord d'un satellite et que le récepteur Bob (ou réciproquement l'émetteur Alice) est un module terrestre. Le système de détermination de clés de cryptage quantique 1 peut en outre être utilisé dans une application de l'invention où l'un des dispositifs ou les deux dispositifs Alice et Bob sont des modules avioniques. Selon des modes de réalisation, le système de détermination de clés de cryptage quantique 1 peut également être utilisé dans une application de l'invention où l'un des dispositifs ou les deux dispositifs Alice et Bob sont des modules pour fibres optiques intégrés dans des réseaux au sol.
- [0045] Un dispositif Alice et/ou Bob peut être fixe ou en mouvement par rapport à l'autre dispositif communiquant.
- [0046] L'émetteur Alice comprend un module de génération de signal 100 et un module interférométrique d'encodage 200. Le récepteur Bob comprend un module interférométrique de transcodage 300 et un module de traitement 400. Avantageusement, l'émetteur Alice et le récepteur Bob sont des dispositifs tout-optique fibrés.
- [0047] Tel qu'utilisé ici, un 'signal' ou 'signal optique' fait référence à une impulsion de lumière cohérente issue par exemple d'un faisceau laser. Un faisceau laser peut notamment être caractérisé par sa cadence d'impulsions f et par une impulsion laser (i.e. le signal) définie par son intensité I , sa phase et sa fréquence ω . La 'fréquence ω ' du faisceau laser désigne la 'fréquence optique de l'impulsion laser multipliée par 2π '

définie en fonction de la longueur d'onde du faisceau λ , telle que $\lambda \times \frac{\omega}{2\pi} = c$, c désignant la vitesse de la lumière.

- [0048] Un 'signal quantique' fait référence à un signal optique ayant en moyenne moins d'un photon par impulsion. La mesure d'un signal quantique fournit une mesure de détection d'un photon dépendant d'une « probabilité de détection » de ce photon.
- [0049] Tel qu'utilisé ici, un 'encodage' fait référence à une ou plusieurs opérations consistant à générer une représentation d'informations suivant un certain code. Par exemple et sans limitation, un encodage peut comprendre l'application d'une première modulation de phase à un signal quantique.
- [0050] Un 'transcodage' fait référence à une ou plusieurs opérations consistant à transformer une représentation d'informations suivant un certain code en une autre représentation selon un autre code différent. Par exemple et sans limitation, un transcodage peut comprendre l'application d'une deuxième modulation de phase à signal quantique modulé en phase.
- [0051] L'émetteur Alice est configuré pour générer et transmettre, à travers un canal de transmission 50 (encore appelé 'canal quantique'), un signal encodé.
- [0052] Le canal de transmission 50 peut être par exemple un espace libre ou un dispositif fibré de transport d'informations, en fonction de l'application de l'invention. Le canal de transmission 50 peut comprendre un dispositif espion, appelé 'Eve' (non représenté sur les figures), configuré pour intercepter le signal transmis par l'émetteur Alice.
- [0053] Le module interférométrique d'encodage 200 de l'émetteur Alice et le module interférométrique de transcodage 300 du récepteur Bob peuvent avoir des architectures sensiblement identiques. Un module interférométrique comprend un interféromètre, l'interféromètre comprenant un premier bras interférométrique et un deuxième bras interférométrique.
- [0054] Dans des modes de réalisation, le premier bras interférométrique du module interférométrique d'encodage 200 et le premier bras interférométrique du module interférométrique de transcodage 300 ne comprennent pas d'élément optique capable de modifier la phase d'un signal qui le traverse. En outre, le premier bras interférométrique du module interférométrique d'encodage 200 et le premier bras interférométrique du module interférométrique de transcodage 300 peuvent ne pas comprendre de fluctuation de phase, induisant de décalage de phase à un signal qui les traverse, et sont qualifiés de « bras de référence ». Dans ces modes de réalisation, le deuxième bras interférométrique du module interférométrique d'encodage 200 et le deuxième bras interférométrique du module interférométrique de transcodage 300 comprennent chacun un ou plusieurs éléments optiques et peuvent être configurés pour modifier la phase de un ou de plusieurs signaux qui les traverse. En outre, le deuxième bras interférométrique du module interférométrique d'encodage 200 peut comprendre des fluc-

tuations de phase induisant un décalage de phase, noté Φ_A , à tout signal qui le traverse. Par ailleurs, le deuxième bras interférométrique du module interférométrique de transcodage 300 peut comprendre des fluctuations de phase induisant un décalage de phase, noté Φ_B , à tout signal qui le traverse.

- [0055] Le récepteur Bob est configuré pour recevoir le signal encodé du canal de transmission 50, transmis par l'émetteur Alice, et effectuer une estimation du signal reçu (ce qui fournit un signal reçu estimé). Le récepteur Bob est en outre configuré pour déterminer et effectuer une correction différentielle des fluctuations de phase entre les décalages de phase Φ_A et Φ_B induits respectivement sur le signal encodé et sur le signal reçu estimé par les modules interférométriques compris dans le système de détermination de clés de cryptage quantique 1.
- [0056] Par ailleurs, l'émetteur Alice et le récepteur Bob sont configurés pour déterminer (i.e. établir) une clé de cryptage quantique, en utilisant le signal encodé et le signal reçu estimé.
- [0057] Le module de génération de signal 100 de l'émetteur Alice est configuré pour générer, à partir d'un signal initial noté S_0 de fréquence ω_0 et d'intensité I_0 , un signal intermédiaire noté S_1 comprenant :
- [0058] - un signal quantique intermédiaire notée S_q (ou selon la notation d'état quantique $|\Psi_1\rangle$) de fréquence ω_q et d'intensité I_q , et
- [0059] - un signal de contrôle intermédiaire notée S_c de fréquence ω_c et d'intensité I_c .
- [0060] En particulier, le module de génération de signal 100 de l'émetteur Alice est configuré pour produire un décalage fréquentiel noté $\Delta\omega$ entre le signal quantique intermédiaire $|\Psi_1\rangle$ et le signal de contrôle intermédiaire S_c , le décalage fréquentiel $\Delta\omega$ pouvant être défini selon l'équation (01) suivante :
- [0061] $\Delta\omega = \omega_q - \omega_c$ (01)
- [0062] Le module interférométrique d'encodage 200 de l'émetteur Alice est configuré pour générer, à partir du signal intermédiaire S_1 , un signal interférométrique encodé noté S_2 comprenant :
- [0063] - un signal quantique interférométrique encodé noté $|\Psi_A\rangle$, et
- [0064] - un signal de contrôle interférométrique noté S_{cA} .
- [0065] En particulier, le module interférométrique d'encodage 200 de l'émetteur Alice peut comprendre une unité de séparation fréquentielle positionnée sur le deuxième bras interférométrique du module interférométrique d'encodage 200. Une composante du signal quantique intermédiaire $|\Psi_1\rangle$ et une composante du signal de contrôle intermédiaire S_c traversent le deuxième bras interférométrique du module interférométrique d'encodage 200. L'unité de séparation fréquentielle du module interférométrique d'encodage est alors configurée pour séparer (i.e. sélectionner fréquentiellement) la

composante du signal quantique intermédiaire $|\Psi_i\rangle$ de la composante du signal de contrôle intermédiaire S_c selon le décalage fréquentiel $\Delta\omega$. Le module interférométrique d'encodage 200 est alors configuré pour appliquer une modulation de phase α , permettant l'encodage d'une clé de cryptage quantique, à la composante du signal quantique intermédiaire $|\Psi_i\rangle$ traversant le deuxième bras interférométrique du module interférométrique d'encodage 200.

[0066] Le module interférométrique de transcodage 300 du récepteur Bob est configuré pour générer, à partir du signal interférométrique encodé S_2 , un signal interférométrique transcodé S_3 comprenant :

[0067] - un signal quantique interférométrique transcodé noté $|\Psi_B\rangle$, et

[0068] - un signal de contrôle interférométrique modulé en phase noté S_{cB} .

[0069] L'homme du métier comprendra que le module interférométrique de transcodage 300 du récepteur Bob est configuré pour :

[0070] - projeter le signal quantique interférométrique encodé $|\Psi_A\rangle$ sur un état quantique interférométrique transcodé noté $|\Psi_{B+}\rangle$ sur un « premier port de sortie » de l'interféromètre du module 300, et sur l'état quantique interférométrique transcodé noté $|\Psi_B\rangle$ sur un « second port de sortie » de l'interféromètre du module 300, et

[0071] - pour générer un signal de contrôle interférométrique modulé en phase noté S_{cB} .

[0072] En particulier, le module interférométrique de transcodage 300 du récepteur Bob peut comprendre une unité de séparation fréquentielle positionnée sur le deuxième bras interférométrique du module interférométrique de transcodage 300. Une composante du signal quantique interférométrique encodée $|\Psi_A\rangle$ et une composante du signal de contrôle interférométrique S_{cA} traversant le deuxième bras interférométrique du module interférométrique de transcodage 300. L'unité de séparation fréquentielle du module interférométrique de transcodage et alors configurée pour séparer (i.e. sélectionner fréquemment) la composante du signal quantique interférométrique encodée $|\Psi_A\rangle$ de la composante du signal de contrôle interférométrique S_{cA} . Le module interférométrique de transcodage 300 est alors configuré pour appliquer une modulation de phase β_{eff} , permettant de transcoder la clé de cryptage quantique, et une modulation de phase Φ_m , respectivement, à la composante de signal quantique interférométrique encodée $|\Psi_A\rangle$ et à la composante de signal de contrôle interférométrique S_{cA} traversant le deuxième bras interférométrique du module interférométrique de transcodage 300.

[0073] Le module de traitement 400 du récepteur Bob est configuré pour :

[0074] – mesurer le signal de contrôle modulé en phase S_{cB} issu du module interférométrique de transcodage 300,

[0075] – déterminer une correction différentielle ϵ des fluctuations de phase entre les

- décalages de phase φ_A et φ_B (ou signal d'erreur discret ε) à partir de la mesure du signal de contrôle modulé en phase S_{cB} et de la modulation de phase φ_m ,
- [0076] – déterminer la ou les valeurs de la modulation de phase β_{eff} à partir de la correction différentielle ε et d'une modulation de phase β , et transmettre la ou les valeurs de la modulation de phase β_{eff} au module interférométrique de transcodage 300, et
- [0077] – estimer le signal quantique interférométrique transcodé $|\Psi_B\rangle$, (c'est-à-dire, estimer la projection du signal quantique interférométrique encodé $|\Psi_A\rangle$ sur les états quantiques interférométriques transcodés $|\Psi_{B+}\rangle$ et $|\Psi_{B-}\rangle$).
- [0078] Il est à noter que, dans ces modes de réalisation, le signal de contrôle interférométrique S_{cA} n'est pas modulé par le module interférométrique d'encodage 200 de l'émetteur Alice alors qu'une composante du signal de contrôle interférométrique S_{cB} est modulée en phase dans le module interférométrique de transcodage 300 du récepteur Bob. Cette configuration permet au module de traitement 400 de déterminer la correction différentielle les fluctuations de phase entre les décalages de phase φ_A et φ_B des modules interférométriques de l'émetteur Alice et du récepteur Bob, sans compromettre la sécurité de la clé secrète établie (c'est-à-dire sans modifier la modulation de phase α), et ainsi de déduire la modulation de phase β_{eff} par une rétroaction électronique rapide.
- [0079] Similairement, une composante de chacun des signaux quantiques interférométrique $|\Psi_A\rangle$ et $|\Psi_B\rangle$, est modulée en phase respectivement dans l'un des deux bras interférométriques du module interférométrique d'encodage 200, ainsi que dans l'un des deux bras interférométrique du module interférométrique de transcodage 300. Cette double modulation α et β permet à l'émetteur Alice et au récepteur Bob de produire la ou les informations nécessaires à l'établissement d'une clé de cryptage sécurisée.
- [0080] La [Fig.2] représente schématiquement le module de génération de signal 100 de l'émetteur Alice, selon des modes de réalisation de l'invention.
- [0081] Le module de génération de signal 100 comprend une unité laser 120, une unité de séparation de faisceau 140, et une unité de recombinaison de faisceau 160.
- [0082] Dans des modes de réalisation, l'unité laser 120 peut comprendre un laser de transmission émettant un faisceau laser ayant une fréquence ω_0 (équivalent à une longueur d'onde λ_0) et caractérisé par une longueur de cohérence noté L_c .
- [0083] La longueur d'onde λ_0 d'émission du laser peut se situer dans le visible ou l'infrarouge. Par exemple et de façon non limitative, l'unité laser 120 peut comprendre une diode laser DFB (acronyme pour l'expression anglo-saxonne correspondante 'Distributed Feedback', signifiant à rétroaction distribuée) utilisant un réseau de Bragg permettant de choisir la longueur d'onde d'émission λ_0 . La longueur d'onde λ_0 d'émission choisie de la diode laser peut être égale à 1550 nm. Une telle diode laser

émet notamment un faisceau laser continue. Alternativement, l'unité laser 120 peut comprendre une source laser impulsionnel.

- [0084] Ainsi, dans des modes de réalisation, l'unité laser 120 peut comprendre en outre une unité de modulation d'intensité (non représenté sur les figures) permettant de générer, à partir d'un faisceau laser continu (ou impulsionnel), des impulsions laser définies selon une cadence d'impulsions f_0 et une intensité d'impulsions I_0 , et une largeur temporelle d'impulsion τ_0 allant jusqu'à quelques nanosecondes. La cadence f_0 du train d'impulsions peut être de l'ordre de quelques kilohertz jusqu'à quelques dizaines de gigahertz.
- [0085] Le faisceau laser peut être polarisé selon toute polarisation adaptée. Par exemple, le faisceau laser peut être polarisé linéairement.
- [0086] Par conséquent, l'unité laser 120 peut être configurée pour générer un signal initial S_0 pouvant être défini selon l'équation (02) suivante :
- [0087] $S_0 = s_0 \times e^{i\omega_0 t}$, tel que $I_0 \propto s_0^2$ (02)
- [0088] L'unité de séparation de faisceau 140 est configurée pour séparer le faisceau laser transmis par l'unité laser 120 en deux composantes du signal initial (notées par exemple S_{0-1} et S_{0-2}) parcourant deux voies optiques distinctes 140-1 et 140-2.
- [0089] Dans des modes de réalisation, l'unité de séparation de faisceau 140 peut être un coupleur optique (par exemple en Y fibré) à maintien de polarisation, typiquement disposé en sortie de l'unité laser 120. L'unité de séparation de faisceau 140 peut en outre être asymétrique, de manière à fournir une composante du signal initial (par exemple S_{0-1}) composée d'impulsions à faible intensité parcourant la voie optique 140-1 et une composante du signal initial (par exemple S_{0-2}) composée d'impulsions de forte intensité parcourant la voie optique 140-2. Avantageusement, le coupleur est du type 90/10, c'est-à-dire délivrant 90% de la puissance optique pour la composante S_{0-2} du signal initial parcourant la voie optique 140-2 et 10% de la puissance optique pour la composante S_{0-1} du signal initial parcourant la voie optique 140-1. L'unité de séparation de faisceau 140 peut ainsi générer les deux composantes de signal S_{0-1} et S_{0-2} . Les composantes de signal S_{0-1} et S_{0-2} peuvent être définies selon les équations (03) et (04) suivantes :
- [0090] $S_{0-1} = \sqrt{t} \times S_0$, tel que par exemple $t = 90\%$ et (03)
- [0091] $S_{0-2} = \sqrt{1-t} \times S_0$ (04)
- [0092] Le module de génération de signal 100 comprend en outre une unité 142 configurée pour générer un 'signal quantique' à partir de la composante S_{0-1} du signal initial parcourant la voie optique 140-1.
- [0093] Dans les modes de réalisation de l'invention, l'unité de génération de signal quantique 142 peut être un atténuateur optique permettant de former le signal

quantique ayant une amplitude I_q équivalent en moyenne à moins d'un photon par impulsion. L'unité de génération de signal quantique 142 est ainsi configurée pour générer le signal quantique $S_q(I_q, \omega_0)$ appelé signal quantique intermédiaire et désigné également selon la notation d'état quantique $|\Psi_i\rangle$.

[0094] Par ailleurs, l'unité de génération de signal quantique 142 peut comprendre une autre unité de modulation d'intensité (non représentée sur les figures) configurée pour effectuer une modulation additionnelle d'impulsion du signal quantique et/ou de la composante S_{0-1} du signal initial parcourant la voie optique 140-1. Par exemple, une telle unité peut être utilisée pour implémenter un protocole appliquant des états leurs quantiques.

[0095] Dans certains modes de réalisation, en particulier si l'unité laser 120 comprend une source laser continue, l'unité de génération de signal quantique 142 peut également comprendre une unité de modification de phase (non représentée sur les figures) configurée pour modifier la phase de chacune des impulsions quantiques parcourant la voie optique 140-1. Avantagusement, l'unité de modification de phase peut être configurée pour rendre aléatoire (i.e. randomiser) la phase de chacune de ces impulsions quantiques, de manière à ce que les phases de deux impulsions quantiques consécutives soient indépendantes l'une par rapport à l'autre. Il est à noter que la randomisation de phase peut permettre de se prémunir de certaines attaques de la clé quantique, pouvant être effectuées par un dispositif espion, appelé 'Eve', disposé sur le canal de transmission 50 interceptant le signal de contrôle transmis par l'émetteur Alice et prenant en compte la cohérence de phase entre impulsions. Une telle unité de modification de phase peut être par exemple un modulateur de phase.

[0096] Le module de génération de signal 100 comprend en outre une unité 144 configurée pour générer un 'signal de contrôle' à partir de la composante S_{0-2} du signal initial parcourant la voie optique 140-2.

[0097] Dans des modes de réalisation de l'invention, l'unité de génération de signal de contrôle 144 peut être une unité de décalage en fréquence configurée pour former le signal de contrôle ayant une fréquence ω_c décalée par rapport à la fréquence ω_0 du signal initial et de la composante S_{0-2} du signal initial parcourant la voie optique 140-2, selon un décalage $\Delta\omega = \omega_0 - \omega_c$. L'unité de génération de signal de contrôle 141 génère alors un signal $S_c(I_c, \omega_c)$, appelé signal de contrôle intermédiaire et pouvant être défini selon l'équation (05) suivante :

[0098]
$$S_c(\omega_c) = s_c \times e^{i(\omega_0 - \Delta\omega)t} = s_c \times e^{i\omega_c t}, \text{ tel que } s_c = \sqrt{t} \times s_0 \quad (05)$$

[0099] L'unité de génération de signal de contrôle 144 peut être par exemple un modulateur acousto-optique (AOM, acronyme pour l'expression anglo-saxonne 'acousto-optic modulator') ou un dispositif de décalage de fréquence acousto-optique (AOFS)

acronyme pour l'expression anglo-saxonne 'acousto-optic frequency shifters') ou un modulateur de phase. Le module de génération de signal 100 peut ainsi comprendre, par exemple et sans limitation, un générateur de tension 146 permettant de contrôler le décalage $\Delta\omega$. Il est à noter que le décalage $\Delta\omega$ à appliquer est choisi de manière à obtenir un découplage spectral entre le signal de contrôle intermédiaire S_c et le signal quantique intermédiaire $|\Psi_1\rangle$ adapté, afin d'éviter que le dispositif espion 'Eve' disposé sur le canal de transmission 50 interceptant le signal de contrôle transmis par l'émetteur Alice, puisse en déduire les fluctuations de phase à corriger et ainsi les qubits transmis. Selon un exemple non limitatif, pour une longueur d'onde λ_0 d'émission choisie égale à 1550 nm, un décalage $\Delta\omega$ entre 1 GHz et 130 GHz peut permettre une variation de quelques picomètres à 1 nm entre la longueur d'onde du signal de contrôle intermédiaire S_c et la longueur d'onde du signal quantique intermédiaire $|\Psi_1\rangle$.

- [0100] Dans certains modes de réalisation, l'unité de génération de signal de contrôle 144 (ou l'unité de génération de signal quantique 142) peut comprendre en outre une unité de décalage temporel (non représentée sur les figures) configurée pour décaler temporellement les composantes de faisceaux entre elles. La composante portée par la voie optique 140-1 (i.e. le signal quantique $|\Psi_1\rangle$) peut être retardée d'une durée $\Delta\tau$ par rapport à la composante de faisceaux portée par la voie optique 140-2 (i.e. le signal de contrôle S_c). Cette durée $\Delta\tau$ peut être définie par exemple en fonction de la cadence d'impulsions f_s du faisceau et/ou de la largeur temporelle τ_s d'impulsion, telles que $\frac{1}{f_s} > \Delta\tau > \tau_s$. Cette durée $\Delta\tau$ peut aussi être définie en fonction de la durée τ_r de mise en œuvre de la rétroaction électronique pour pouvoir déduire au sein de l'émetteur Bob la modulation de phase β_{eff} et corriger les fluctuations de phase, telles que $\Delta\tau < \tau_r$.
- [0101] L'unité de recombinaison de faisceau 160, en extrémité des deux voies optiques distinctes 140-1 et 140-2, permet de recombinaison les deux composantes de signaux sur un unique chemin optique en un signal intermédiaire S_1 transmis au module interférométrique d'encodage 200 et pouvant être défini selon l'équation (06) suivante :
- [0102] $S_1 = S_c + |\Psi_1\rangle$ (06)
- [0103] L'unité de recombinaison fréquentielle 160 du signal quantique avec le signal de contrôle peut être par exemple, et en fonction des modes de réalisation utilisés, un multiplexeur de fréquence (communément noté MUX) dont la technologie dépend du décalage fréquentiel $\Delta\omega$ entre le signal de contrôle intermédiaire S_c et le signal quantique intermédiaire $|\Psi_1\rangle$.
- [0104] La [Fig.3] représente schématiquement un module interférométrique d'encodage 200 de l'émetteur Alice, selon des modes de réalisation de l'invention.
- [0105] Le module interférométrique d'encodage 200 comprend un séparateur de faisceau

240 configuré pour séparer le signal intermédiaire S_1 transmis en deux composantes de faisceaux, notées par exemple S_{1-1} et S_{1-2} , parcourant chacune un premier bras interférométrique noté 240-1 ou un deuxième bras interférométrique noté 240-2. Le signal intermédiaire S_1 comprend le signal de contrôle intermédiaire S_c et le signal quantique intermédiaire $|\Psi_1\rangle$ et chacune des composantes S_{1-1} et S_{1-2} du signal intermédiaire comprend une composante du signal de contrôle intermédiaire S_c (par exemple S_{c-1} ou S_{c-2}) et un état quantique (ou de façon simplifiée appelé ‘composante’) du signal quantique intermédiaire $|\Psi_1\rangle$ (par exemple $|\Psi_{1-1}\rangle$ ou $|\Psi_{1-2}\rangle$). L’unité de séparation de faisceau 240 peut être un coupleur optique symétrique (par exemple en Y fibré de type 50/50) à maintien de polarisation, configuré pour fournir deux composantes S_{1-1} et S_{1-2} du signal intermédiaire composées d’impulsions à intensité égale.

- [0106] Selon des modes de réalisation, le module interférométrique d’encodage 200 peut être un interféromètre de Michelson, comme l’exemple illustré sur la [Fig.3]. Avantageusement, un tel module interférométrique d’encodage 200 peut comprendre des miroirs de Faraday 242 et 248, disposés en extrémités des bras interférométriques 240-1 et 240-2, configurés pour compenser certaines variations en polarisation subies par les composantes S_{1-1} et S_{1-2} du signal intermédiaire lors de leur parcours respectif le long d’un des deux bras de l’interféromètre 240-1 ou 240-2.
- [0107] Par ailleurs, comme représenté sur la [Fig.3], dans ces modes de réalisation, le séparateur de faisceau 240 du module interférométrique d’encodage 200 peut être configuré pour recombinaison, en un signal interférométrique encodé résultant S_2 , les composantes de faisceaux S_{1-1} et S_{1-2} du signal intermédiaire, à la suite de leur parcours respectif le long d’un des deux bras interférométriques 240-1 ou 240-2.
- [0108] Alternativement, le module interférométrique d’encodage 200 peut être un interféromètre de Mach-Zehnder (configuration non représentée sur les figures). Dans ces modes de réalisation, le module interférométrique d’encodage 200 comprend un coupleur de faisceau disposé en extrémité des bras interférométriques 240-1 et 240-2 et configuré pour recombinaison les composantes de faisceaux S_{1-1} et S_{1-2} du signal intermédiaire, en un signal interférométrique résultant S_2 .
- [0109] Le premier bras interférométrique 240-1 ne comprend aucun élément optique supplémentaire. En outre, le premier bras interférométrique 240-1 est le bras de référence de phase, tel que la composante S_{1-1} du signal intermédiaire parcourant le premier bras interférométrique 240-1 ne subit pas de fluctuation de phase.
- [0110] Dans des modes de réalisation, les deux bras interférométriques 240-1 et 240-2 peuvent avoir des longueurs de bras différentes, tel que l’interféromètre comprend un bras interférométrique court et un bras interférométrique long. La différence de longueur entre les deux bras interférométriques est notée ΔL . L’interféromètre du

module d'encodage 200 et l'interféromètre du module de transcodage 300 (ayant des architectures sensiblement identiques) peuvent avoir la même différence de longueur ΔL . Par exemple et sans limitation, cette différence de longueur ΔL peut être inférieure à la longueur de cohérence L_c de l'unité laser 120, et supérieure à la taille de l'impulsion L_0 définie à partir de la largeur temporelle d'une impulsion $L_0 = c \times \tau_0$, c désignant la vitesse de la lumière et τ_0 la largeur temporelle d'impulsion. Cette différence de longueur ΔL induit une séparation temporelle entre les composantes S_{1-1} et S_{1-2} du signal intermédiaire, parcourant chacun un des deux bras interférométriques 240-1 ou 240-2, après recombinaison en un signal interférométrique encodé S_2 . De façon générale, pour un interféromètre, cette séparation temporelle est définie tel que les composantes de signal sont retardées d'une durée Δt , calculée à partir de la différence ΔL . En outre, une composante en sortie d'un interféromètre comporte un retard appelé « retard interférométrique » et noté t , tel que :

- [0111] - une composante parcourant le bras interférométrique court comporte un retard interférométrique $t = 0$; et
- [0112] - la composante parcourant le bras interférométrique long comporte un retard interférométrique $t = \Delta t$ par rapport à la composante parcourant le bras interférométrique court.
- [0113] Dans une première variante de l'invention, le premier bras interférométrique 240-1 peut être le bras interférométrique court. Dans cette variante de l'invention, le deuxième bras interférométrique 240-2 peut être le bras interférométrique long selon la différence de longueur ΔL entre les deux bras. Alternativement, dans une seconde variante de l'invention, le premier bras interférométrique 240-1 peut être le bras interférométrique long, alors que le deuxième bras interférométrique 240-2 peut être le bras interférométrique court.
- [0114] Le module interférométrique d'encodage 200 comprend en outre un dispositif d'encodage 240D configurée pour appliquer une modulation de phase α uniquement à une composante du signal quantique intermédiaire $|\Psi_1\rangle$. En particulier, le dispositif d'encodage 240D peut être disposé (i.e. positionné) sur le deuxième bras interférométrique 240-2.
- [0115] Le dispositif d'encodage 240D peut comprendre unité de séparation fréquentielle 244 configurée pour séparer (i.e. sélectionner fréquentiellement ou spectralement) la composante S_{1-2} du signal intermédiaire parcourant le deuxième bras interférométrique 240-2, de manière à obtenir les composantes de faisceaux suivantes :
- [0116] - la composante S_{c-2} du signal de contrôle intermédiaire S_c parcourant une voie dite « voie de signal de contrôle de l'émetteur Alice » 244-1, et
- [0117] - l'état quantique $|\Psi_{1-2}\rangle$ correspondant au photon du signal quantique inter-

médiaire parcourant une voie dite « voie de signal quantique de l'émetteur Alice » 244-2.

- [0118] Par ailleurs, le dispositif d'encodage 240D peut comprendre une unité de recombinaison fréquentielle 246 configurées pour recombinaison fréquentielle, sur le deuxième bras interférométrique 240-2, les composantes S_{c-2} et $|\Psi_{t-2}\rangle$ parcourant les voies de signal 244-1 et 244-2.
- [0119] L'unité de recombinaison fréquentielle 246 peut être identique à l'unité de séparation fréquentielle 244 du module de génération de signal 100. Par exemple, ces deux unités peuvent être des démultiplexeurs de fréquence (dénomé DEMUX) reposant sur une technologie qui dépend du décalage fréquentiel $\Delta\omega$ entre le signal de contrôle intermédiaire S_c et le signal quantique intermédiaire S_q .
- [0120] Comme représenté sur la [Fig.3], la voie de signal de contrôle 244-1 de l'émetteur Alice ne présente aucun élément optique supplémentaire.
- [0121] Avantagusement, le dispositif d'encodage 240D peut comprendre une unité de modulation de phase 2442 configurée pour moduler, selon un paramètre α (également appelé 'modulation de phase α '), la phase du photon (d'état quantique $|\Psi_{t-2}\rangle$) du signal quantique intermédiaire parcourant la voie de signal quantique 244-2 de l'émetteur Alice. L'unité de modulation de phase 2442 peut aussi être appelée 'unité d'encodage' 2442 (permettant l'encodage d'une clé de cryptage quantique).
- [0122] Par exemple et de manière non limitative, une unité d'encodage 2442 peut être un modulateur électro-optique constitué de cristaux électro-optiques auxquels sont appliqués un signal électrique défini à partir d'une unité de contrôle 2444. L'unité de contrôle peut être par exemple un générateur de tension configuré pour contrôler le paramètre α . La phase du photon (d'état quantique $|\Psi_{t-2}\rangle$) du signal quantique intermédiaire traversant l'unité 2442 est alors modulée de manière à encoder une information quantique.
- [0123] Avantagusement, le paramètre α peut être choisi dans un ensemble des deux bases orthogonales comme par exemple $[0, \pi]$ et $[\pi/2, 3\pi/2]$. Il est à noter que ce choix de paramètre α et l'encodage en phase de l'information quantique constituent une nouvelle alternative à l'approche classique d'un protocole nommé BB84 (comme décrit dans l'article "Quantum cryptography: Public key distribution and coin tossing" de C. Bennett et G. Brassard, 1984, Theoretical Computer Science, vol. 560, 1984, p. 7–11). Dans le protocole BB84 l'encodage de l'information quantique s'effectue sur la polarisation des photons (et non sur leur phase). L'implémentation classique du protocole BB84 d'encodage en polarisation est limitée à des contraintes systèmes relatives à la correction d'erreurs sur la polarisation du signal quantique. Cette correction étant de type mécanique (par exemple en utilisant des lames demi-onde mo-

torisées), l'implémentation classique du protocole BB84 est donc limitée en termes de bande-passante du signal quantique par rapport à une solution d'encodage en phase utilisant des dispositifs électro-optiques (par exemple un modulateur électro-optique) permettant une mise en œuvre à haut débit. Le haut débit obtenu avec les modes de réalisation de l'invention est également plus important par rapport à un encodage utilisant le multiplexage temporel qui nécessite plus de corrections d'erreurs de fluctuations et permet ainsi de réduire le débit d'encodage et de transfert des qubits. Dans une application de l'invention au domaine spatial, le débit d'encodage et de transfert des qubits est par exemple limité au temps de passage d'un satellite. Le nombre de qubits échangés lors d'un passage est donc réduit dans ce cas. Par ailleurs, si les fluctuations deviennent trop importantes, le seuil critique d'erreurs corrigibles (égale environ à 10%) peut être dépassé de sorte que l'établissement de la clé deviendrait impossible. Le haut débit du procédé d'encodage en phase présente ainsi l'avantage d'augmenter le nombre de qubits échangés dans une communication quantique limitée en temps, ce qui permet d'établir une clé secrète entre deux utilisateurs distants.

[0124] L'unité de contrôle 2444 de l'unité d'encodage 2442 de l'émetteur Alice peut avantageusement comprendre un générateur de nombre aléatoire quantique plus sûr que les générateurs de nombres pseudo-aléatoires logiciels classiquement utilisés dans les ordinateurs pour générer des nombres aléatoires. De tels générateurs de nombres pseudo-aléatoires classiques utilisent un algorithme déterministe pour produire des séquences de nombres aléatoires prédites. Au contraire, un générateur de nombre aléatoire quantique permet d'obtenir une séquence de paramètres α à encoder sur la phase du signal quantique, de manière aléatoire selon une probabilité statistique quantique qui n'est pas prévisible, ce qui permet de fournir un plus haut niveau de sécurité de clé secrète.

[0125] Par ailleurs, les composantes $|\Psi_{i-2}\rangle$ du signal quantique intermédiaire et S_{c-2} du signal de contrôle intermédiaire parcourant le deuxième bras interférométrique 240-2 peuvent subir des fluctuations de phase. Cependant, ces deux composantes $|\Psi_{i-2}\rangle$ et S_{c-2} suivent des chemins optiques similaires de sorte qu'en sortie de l'interféromètre du module interférométrique d'encodage 200, les composantes $|\Psi_{i-2}\rangle$ et S_{c-2} portent le même décalage de phase Φ_A par rapport aux composantes $|\Psi_{i-1}\rangle$ et S_{c-1} parcourant le premier bras interférométrique 240-1. Ceci n'est pas le cas dans les dispositifs de l'état de la technique où le signal quantique et le signal de contrôle suivent des chemins optiques différents, par exemple si le signal de contrôle emprunte un premier bras interférométrique court et le signal quantique « emprunte » un deuxième bras interférométrique long. Il est à noter que le terme « emprunter » dans le cas du signal quantique est utilisé par souci de simplification. En effet, en pratique le signal

quantique n' « emprunte » pas un chemin optique spécifique ou l'autre mais plus précisément l'équivalent d'une superposition des deux chemins optiques.

[0126] En sortie de l'interféromètre du module interférométrique d'encodage 200, le signal de contrôle interférométrique résultant, noté S_{cA} , peut être défini en fonction du signal de contrôle intermédiaire S_c et du décalage de phase Φ_A , selon l'équation (07) suivante :

$$[0127] \quad S_{cA} = \frac{1}{2} \times (1 + e^{i\Phi_A}) \times S_c \quad (07)$$

[0128] En particulier, le signal de contrôle interférométrique S_{cA} est constitué de deux impulsions lumineuses classiques de même intensité, séparées temporellement de la quantité Δt , définie à partir de la différence ΔL .

[0129] En sortie de l'interféromètre du module interférométrique d'encodage 200, le signal quantique interférométrique encodé résultant, noté $|\Psi_A\rangle$, peut être défini en fonction de la modulation de phase α et du décalage de phase Φ_A , selon l'équation (08) suivante :

$$[0130] \quad |\Psi_A\rangle = \frac{1}{\sqrt{2}} \times (|\Psi_{I-1}\rangle + e^{i(\alpha+\Phi_A)} |\Psi_{I-2}\rangle) \quad (08)$$

[0131] Il est à noter que l'état quantique $|\Psi_A\rangle$ peut être représenté par une superposition des états $|\Psi_{I-1}\rangle$ et $|\Psi_{I-2}\rangle$, tels que l'état $|\Psi_{I-1}\rangle$ correspond au photon du signal quantique intermédiaire ayant emprunté le premier bras interférométrique 240-1 et l'état $|\Psi_{I-2}\rangle$ correspond au photon du signal quantique intermédiaire ayant emprunté le premier bras interférométrique 240-2.

[0132] Par conséquent, en sortie de l'interféromètre du module interférométrique d'encodage 200, le signal interférométrique encodé S_2 comprend le signal de contrôle interférométrique S_{cA} et le signal quantique interférométrique encodé $|\Psi_A\rangle$, et peut être défini selon l'équation (09) suivante :

$$[0133] \quad S_2 = S_{cA} + |\Psi_A\rangle \quad (09)$$

[0134] Comme représenté sur la [Fig.3], dans des modes de réalisation utilisant un interféromètre de Michelson, le signal interférométrique encodé S_2 peut se propager alors d'une part vers le module de génération de signal 100 et d'autre part vers le récepteur Bob, selon le chemin optique 240-3. Dans ces modes de réalisation, le module interférométrique d'encodage 200 de l'émetteur Alice peut comprendre en outre une unité de déviation de signal 220 configurée pour dévier (i.e. rediriger) le signal interférométrique encodé S_2 vers une unité de contrôle 222 du signal interférométrique. Par exemple, l'unité de contrôle 222 peut être une photodiode de contrôle permettant de contrôler le signal interférométrique encodé S_2 transmis par l'émetteur Alice au récepteur Bob. L'unité de déviation de signal 320 peut être un circulateur optique. L'unité de déviation de signal 220 permet d'empêcher le transfert du signal interférométrique

métrique encodé S_2 dans le module de génération de signal 100.

- [0135] Lors de la propagation dans le canal de transmission 50 entre l'émetteur Alice et le récepteur Bob, le signal quantique et le signal de contrôle du signal interférométrique encodé S_2 peuvent aussi subir des fluctuations de phase de propagation. La propagation dans le canal de transmission 50 étant commune pour les deux composantes du signal interférométrique encodé S_2 , ces fluctuations de phase de propagation n'ont pas d'influence sur le résultat de la mesure des interférences quantiques effectuée par le récepteur Bob.
- [0136] La [Fig.4] représente schématiquement un module interférométrique de transcodage 300 du récepteur Bob, selon des modes de réalisation de l'invention.
- [0137] Le module interférométrique de transcodage 300 a une architecture d'interféromètre optique dissymétrique similaire au module interférométrique d'encodage 200 de l'émetteur Alice. Ainsi, le module interférométrique de transcodage 300 comprend un séparateur de faisceau 340 (par exemple un coupleur optique symétrique en Y, fibré de type 50/50 à maintien de polarisation) configuré pour séparer le faisceau du signal interférométrique S_2 transmis par l'émetteur Alice en deux composantes de faisceaux, notées S_{2-1} et S_{2-2} . Les composantes S_{2-1} et S_{2-2} (composées d'impulsions à intensité égale par exemple) parcourent chacune un premier bras interférométrique noté 340-1 ou un deuxième bras interférométrique noté 340-2. Le signal interférométrique encodé S_2 comprenant un signal de contrôle et un signal quantique, chacune des composantes S_{2-1} et S_{2-2} du signal intermédiaire comprend une composante du signal de contrôle interférométrique (par exemple noté S_{cA-1} ou S_{cA-2}) et un état quantique (ou de façon simplifiée appelé une « composante ») du signal quantique interférométrique (par exemple noté $|\Psi_{A-1}\rangle$ ou $|\Psi_{A-2}\rangle$).
- [0138] Dans un mode de réalisation où le module interférométrique d'encodage 200 de l'émetteur Alice est un interféromètre de Mach-Zhender le module interférométrique de transcodage 300 peut être un interféromètre de Mach-Zhender. Dans un autre mode de réalisation où le module interférométrique d'encodage 200 est un interféromètre de Michelson, le module interférométrique de transcodage 300 peut être avantageusement un interféromètre de Michelson comprenant des miroirs de Faraday 342 et 348, disposés chacun à l'extrémité de l'un des deux bras interférométriques 340-1 et 340-2 de manière à compenser les variations en polarisation subies par les composantes de faisceaux S_{2-1} et S_{2-2} .
- [0139] Similairement au module interférométrique d'encodage 200 de l'émetteur Alice, le premier bras interférométrique 340-1 ne comprend aucun élément optique supplémentaire. En outre, le premier bras interférométrique 340-1 est le bras de référence de phase, tel que la composante S_{2-1} du signal interférométrique encodé S_2 ne subit pas de fluctuation de phase. Le premier bras interférométrique 340-1 peut être le bras le plus

court tandis que le deuxième bras interférométrique 340-2 est le bras le plus long, les deux bras présentant entre eux une différence de longueur ΔL . Alternativement, le premier bras interférométrique 340-1 peut être le bras le plus long tandis que le deuxième bras interférométrique 340-2 est le bras le plus court.

- [0140] Le module interférométrique de transcodage 300 du récepteur Bob comprend en outre un dispositif 340D de transcodage et de modulation de phase configuré pour appliquer une modulation de phase β_{eff} uniquement à une composante du signal quantique interférométrique encodé $|\Psi_A\rangle$ et une modulation de phase Φ_m uniquement à une composante du signal de contrôle interférométrique S_{cA} . Le dispositif de transcodage et de modulation de phase 340D peut être disposé (i.e. positionné) sur le deuxième bras interférométrique 340-2.
- [0141] Le dispositif de transcodage et de modulation de phase 340D peut comprendre une unité de séparation fréquentielle 344 configurée pour séparer (i.e. sélectionner fréquemment) la composante S_{cA-2} du signal intermédiaire parcourant le deuxième bras interférométrique 340-2, de manière à obtenir les composantes de faisceaux suivantes :
- [0142] - la composante S_{cA-2} du signal de contrôle interférométrique S_{cA} parcourant la voie de signal de contrôle du récepteur Bob 344-1, et
- [0143] - l'état quantique $|\Psi_{A-2}\rangle$ correspondant au photon du signal quantique intermédiaire parcourant la voie de signal quantique du récepteur Bob 244-2.
- [0144] Le dispositif de transcodage et de modulation de phase 340D peut comprendre une unité de recombinaison fréquentielle 346 configurées pour recombinaison fréquemment, sur le deuxième bras interférométrique 340-2, les composantes S_{cA-2} et $|\Psi_{A-2}\rangle$ parcourant les voies de signal 344-1 et 344-2.
- [0145] L'unité de séparation fréquentielle 344 et l'unité de recombinaison fréquentielle 346 du récepteur Bob peuvent être identiques respectivement à l'unité de séparation fréquentielle 244 et à l'unité de recombinaison fréquentielle 246 de l'émetteur Alice. Elles peuvent ainsi être mises en œuvre sous la forme d'un démultiplexeur et d'un multiplexeur en fréquence reposant sur une technologie qui dépend du décalage fréquentiel $\Delta\omega$ entre le signal de contrôle intermédiaire S_c et le signal quantique intermédiaire S_q .
- [0146] A la différence du dispositif d'encodage 240D de l'émetteur Alice, le dispositif de transcodage et de modulation de phase 340D du récepteur Bob peut comprendre une unité de modulation de phase 3446 configurée pour moduler, selon un paramètre Φ_m , la phase de la composante S_{cA-2} du signal de contrôle interférométrique S_{cA} se propageant sur la voie de signal de contrôle du récepteur Bob 344-1.
- [0147] Le paramètre Φ_m de modulation de phase de l'unité de modulation de phase 3446 peut être contrôlé par une unité de contrôle 3448 qui peut être par exemple un générateur de tension configuré pour émettre un signal radiofréquence permettant de

générer une modulation de phase sinusoïdale. Ce signal radiofréquence peut avoir une phase nulle et dépendre d'une fréquence ω_m . Une telle modulation de phase notée Φ_m peut être définie, en fonction d'un paramètre $\Delta\phi$ correspondant à la profondeur de modulation, selon l'équation (10) suivante :

[0148] $\Phi_m(t) = \Delta\phi \times \cos(\omega_m t)$ (10)

[0149] De manière similaire au dispositif d'encodage 240D de l'émetteur Alice, le dispositif de transcodage et de modulation de phase 340D du récepteur Bob peut comprendre une unité de modulation de phase 3442 configurée pour moduler, selon un paramètre β_{eff} , la phase du photon (d'état quantique $|\Psi_{A-2}\rangle$) du signal quantique intermédiaire parcourant la voie de signal quantique 344-2 du récepteur Bob. Par exemple, et de façon non limitative, l'unité de modulation de phase 3442 peut être similaire à l'unité de modulation de phase 2442. L'unité de modulation de phase 3442 peut aussi être appelée unité de transcodage 3442 (permettant de transcoder l'information encodée de la clé de cryptage quantique).

[0150] Les composantes $|\Psi_{A-2}\rangle$ du signal quantique interférométrique et S_{cA-2} du signal de contrôle interférométrique parcourant le deuxième bras interférométrique 340-2 peuvent subir des fluctuations de phase. Cependant, ces deux composantes suivant des chemins optiques similaires de sorte qu'en sortie de l'interféromètre du module interférométrique de transcodage 300, les composantes $|\Psi_{A-2}\rangle$ et S_{cA-2} portent le même décalage de phase Φ_B .

[0151] En sortie de l'interféromètre du module interférométrique de transcodage 300, le signal de contrôle interférométrique modulé en phase, noté S_{cB} , peut être défini en fonction du signal de contrôle interférométrique S_{cA} et des décalages de phase Φ_m et Φ_B , selon l'équation (11) suivante :

[0152] $S_{cB} = \frac{1}{2} \times (1 + e^{i(\Phi_m + \Phi_B)}) \times S_{cA}$ (11)

[0153] En particulier, le signal de contrôle interférométrique S_{cA} est constitué de trois impulsions lumineuses classiques, séparées temporellement de la quantité Δt (i.e. impulsions de retard interférométrique égal à 0, Δt et $2 \times \Delta t$), définie à partir de la différence de longueur ΔL des interféromètres de l'émetteur Alice et du récepteur Bob.

[0154] Dans des modes de réalisation, le module de traitement 400 est configuré pour déterminer la correction différentielle des fluctuations de phase entre les décalages de phase Φ_A et Φ_B des modules interférométriques 200 et 300, à partir de mesures des fluctuations d'intensité prédéfinies sur le signal de contrôle interférométrique S_{cA} , en sortie du module interférométrique de transcodage 300. Les fluctuations d'intensité correspondent notamment aux interférences entre les photons du signal de contrôle, constituant des impulsions lumineuses classiques ayant un retard interférométrique Δt , et ayant donc emprunté:

- [0155] – d’une part, le premier bras interférométrique 240-1 de l’émetteur Alice puis le deuxième bras interférométrique 340-2 du récepteur Bob, et
- [0156] – d’autre part, le deuxième bras interférométrique 240-2 de l’émetteur Alice puis le premier bras interférométrique 340-1 du récepteur Bob.
- [0157] Selon des modes de réalisation de l’invention, le paramètre β_{eff} de modulation de phase de l’unité de transcodage 3442 peut être directement contrôlé par le module de traitement 400 du récepteur Bob tel que représenté sur la figure 4. En particulier, le paramètre β_{eff} peut alors être défini à partir d’un paramètre β de modulation de phase obtenu de façon similaire au paramètre α , mais comprenant une correction différentielle des fluctuations de phase entre les décalages de phase φ_A et φ_B des modules interférométriques 200 et 300, définie à partir de la mesure du signal de contrôle interférométrique S_{cB} .
- [0158] A titre de simplification, en sortie de l’interféromètre du module interférométrique de transcodage 300, le signal quantique interférométrique transcodé résultant, noté $|\Psi_B\rangle$, peut être défini en fonction du signal quantique interférométrique encodé $|\Psi_A\rangle$, de la modulation de phase β_{eff} et du décalage de phase φ_B .
- [0159] Par conséquent, en sortie de l’interféromètre du module interférométrique de transcodage 300, le signal interférométrique transcodé S_3 comprend le signal de contrôle interférométrique S_{cB} et le signal quantique interférométrique transcodé $|\Psi_B\rangle$, et peut être défini selon l’équation (12) suivante :
- [0160] $S_3 = S_{\text{cB}} + |\Psi_B\rangle$ (12)
- [0161] Comme représenté sur la [Fig.4], dans des modes de réalisation utilisant un interféromètre de Michelson, le signal interférométrique transcodé S_3 peut se propager d’une part vers l’émetteur Alice et d’autre part vers le module de traitement 400, selon le chemin optique 340-3 (qui correspond au premier port de sortie de l’interféromètre du module 300). Dans de tels modes de réalisation, le module interférométrique de transcodage 300 peut comprendre en outre une unité de déviation de signal 320 configurée pour dévier (i.e. rediriger) le signal interférométrique transcodé S_3 vers le module de traitement 400 selon le chemin optique 340-4 (qui correspond au second port de sortie de l’interféromètre du module 300). Par exemple, l’unité de déviation de signal 320 peut être un circulateur optique. L’unité de déviation de signal 320 permet d’empêcher le transfert du signal interférométrique transcodé S_3 vers le canal de transmission 50.
- [0162] La [Fig.5] représente schématiquement le module de traitement 400 du récepteur Bob, selon des modes de réalisation de l’invention.
- [0163] Le module de traitement 400 comprend deux parties de traitement, chacune associée à l’un des deux chemins optiques 340-3 et 340-4 obtenus en sortie du module interférométrique.

métrique 300 du récepteur Bob.

- [0164] Chaque partie de traitement 420 (respectivement 440) comprend une unité de séparation fréquentielle 422 (respectivement 442) configurée pour séparer (i.e. sélectionner fréquemment) le signal de contrôle interférométrique modulé en phase S_{cB} du signal quantique interférométrique transcodé résultant $|\Psi_B\rangle$ de manière à ce qu'ils parcourent un des deux bras de mesure 422-1 ou 422-2 (respectivement 442-1 ou 442-2) associés à la partie de traitement 420 (respectivement 440). Par exemple et sans limitation, le bras de mesure 422-1 pour la partie de traitement 420 et le bras de mesure 442-1 pour la partie de traitement 440 peuvent être les bras de mesure quantique, tandis que le bras de mesure 422-2 pour la partie de traitement 420 et le bras de mesure 442-2 pour la partie de traitement 440 peuvent être les bras de mesure de contrôle. Par conséquent, le signal quantique interférométrique transcodé $|\Psi_B\rangle$ parcourt le bras de mesure quantique 422-1 (respectivement 442-1), et le signal de contrôle interférométrique modulé en phase S_{cB} parcourt le bras de mesure de contrôle 422-2 (respectivement 442-2). Les unités de séparation fréquentielle 422 et 442 peuvent être des démultiplexeurs en fréquence reposant sur une technologie qui dépend du décalage fréquentiel $\Delta\omega$ entre le signal de contrôle intermédiaire S_c et le signal quantique intermédiaire S_q .
- [0165] Chaque partie de traitement 420 (respectivement 440) comprend une unité de détection de photon unique 4222 (respectivement 4422) positionnée sur le bras de mesure quantique 422-1 (respectivement 442-1). Une unité de détection de photon unique peut comprendre une surface de détection et être configurée pour détecter la « présence » de photons uniques à sa surface de détection (i.e. par interaction photon/surface). Cette détection de la présence de photons uniques est définie selon une efficacité quantique de détection donnée. Par exemple et sans limitation, l'unité de détection de photon unique 4222 (respectivement 4422) peut être une photodiode à avalanche (APD, acronyme pour l'expression anglo-saxonne correspondante 'Avalanche Photodiode Detector') ou encore un détecteur de photon unique à nanofil supraconducteur (SNSPD, acronyme pour l'expression anglo-saxonne correspondante 'Superconducting Nanowire Single Photon Detector'). En particulier, l'unité de détection de photon unique 4222 (respectivement 4422) peut comprendre un mécanisme d'amplification interne configuré pour délivrer une tension, lorsque qu'un photon est détecté.
- [0166] Chaque unité de détection de photons 4222 et 4422 peut mesurer le résultat d'une interférence entre photons à partir de la projection de l'état quantique associé au signal quantique intermédiaire $|\Psi_A\rangle$ sur l'état quantique associé au signal quantique interférométrique transcodé $|\Psi_B\rangle$.

[0167] L'homme du métier comprendra que le module de traitement 400 est configuré pour effectuer une sélection temporelle du signal quantique interférométrique transcodé $|\Psi_B\rangle$, le signal quantique interférométrique encodé $|\Psi_A\rangle$ étant alors projeté :

[0168] - au niveau du module de réception 4222, sur un état quantique noté $|\Psi_{B+}\rangle$ tel que :

$$[0169] \quad |\Psi_{B+}\rangle = \frac{1}{\sqrt{2}} \times (|\Psi_{A-1}\rangle + e^{i(\beta+\varphi_B)} |\Psi_{A-2}\rangle) \quad (13)$$

[0170] - au niveau du module de réception 4422, sur un état quantique noté $|\Psi_{B-}\rangle$ tel que :

$$[0171] \quad |\Psi_{B-}\rangle = \frac{1}{\sqrt{2}} \times (|\Psi_{A-1}\rangle - e^{i(\beta+\varphi_B)} |\Psi_{A-2}\rangle) \quad (14)$$

[0172] Les états quantiques $|\Psi_{B+}\rangle$ et $|\Psi_{B-}\rangle$ sont aussi appelés « états quantiques transcodés ». Comme présenté dans les équations (13) et (14), les états quantiques $|\Psi_{B+}\rangle$ et $|\Psi_{B-}\rangle$ peuvent être représentés par une superposition des états $|\Psi_{A-1}\rangle$ et $|\Psi_{A-2}\rangle$, tels que l'état $|\Psi_{A-1}\rangle$ correspond au photon du signal quantique interférométrique encodé ayant emprunté le premier bras interférométrique 340-1 et l'état $|\Psi_{A-2}\rangle$ correspond au photon du signal quantique interférométrique encodé ayant emprunté le premier bras interférométrique 340-2.

[0173] Une « probabilité de détection », notée P_+ (ou P_-), de l'unité de détection de photon unique 4222 (ou 4422) peut être définie, à partir de l'équation (15) suivante :

$$[0174] \quad P_{\pm} = |\langle \Psi_{B\pm} | \Psi_A \rangle|^2 \quad (15)$$

[0175] Selon l'équation (15), le signal quantique interférométrique transcodé, résultant du module interférométrique de transcodage 300, peut être décomposé sur une base de quatre modes temporels définis tels que :

[0176] - le premier mode temporel (correspondant à un état $|\Psi_{A-1}\Psi_{I-1}\rangle$) correspond au photon ayant emprunté le premier bras interférométrique 240-1 de l'émetteur Alice puis le premier bras interférométrique 340-1 du récepteur Bob. Dans ce cas, le retard interférométrique du photon est nul ($t=0$) et la probabilité de détection d'un photon, possédant par convention une phase nulle, ne dépend pas des modulations de phases α et β_{eff} ;

[0177] - le deuxième mode temporel (correspondant à un état $|\Psi_{A-2}\Psi_{I-2}\rangle$) correspond au photon ayant emprunté le deuxième bras interférométrique 240-2 de l'émetteur Alice (comprenant la modulation de phase α) puis le deuxième bras interférométrique 340-2 du récepteur Bob (comprenant la modulation de phase β_{eff}). Dans ce cas, le retard interférométrique est de $2 \times \Delta t$. Bien que la phase du photon soit égale à $\alpha + \beta_{\text{eff}}$, la probabilité de détecter le photon est alors proportionnelle au module carré du champ

électrique et n'est donc pas affectée par les deux paramètres de modulation de phase α et β_{eff} ;

[0178] - le troisième mode temporel (correspondant à un état $|\Psi_{A-1}\Psi_{I-2}\rangle$) correspond au photon ayant emprunté le deuxième bras interférométrique 240-2 de l'émetteur Alice (comprenant la modulation de phase α) puis le premier bras interférométrique 340-1 du récepteur Bob. Dans ce cas, le retard interférométrique du photon est de Δt et le photon acquiert une phase α et subit des fluctuations de phase induisant un décalage de phase φ_A associé notamment au bras interférométrique 240-2 du module interférométrique d'encodage 200 ; et

[0179] - le quatrième mode temporel (correspondant à un état $|\Psi_{A-2}\Psi_{I-1}\rangle$) correspond au photon ayant emprunté le premier bras interférométrique 240-1 de l'émetteur Alice puis le deuxième bras interférométrique 340-2 du récepteur Bob (comprenant la modulation de phase β_{eff}). Dans ce cas, le retard interférométrique du photon est de Δt et le photon acquiert une phase β_{eff} et subit des fluctuations de phase induisant un décalage de phase φ_B associée au bras interférométrique 340-2 du module interférométrique de transcodage 300.

[0180] En particulier, seuls les photons ayant le même retard interférométrique, c'est-à-dire $t = \Delta t$, peuvent interférer entre eux. Par conséquent, le résultat de cette interférence correspond à une probabilité de détection des photons par l'unité 4222 (ou 4422) reçus avec un retard Δt (i.e. troisième et quatrième modes temporels). Les « probabilités de détection » P_+ et P_- peuvent être définies selon l'équation (16) suivante :

$$[0181] \quad P_{\pm}(\alpha, \beta_{\text{eff}}) = \frac{1 \pm \cos(\alpha - \beta_{\text{eff}} + \varphi_A - \varphi_B)}{2} \quad (16)$$

[0182] Il est à noter que l'attribution du signe + ou - à la probabilité de détection P_+ ou P_- est effectuée (par réglage) de façon arbitraire au niveau du séparateur de faisceau 340 puis est fixée selon le parcours du photon sur l'un des deux chemins optiques 340-3 ou 340-4, puis 422-1 ou 442-1.

[0183] Le module de traitement 400 peut comprendre en outre une unité de stockage 460 des valeurs de probabilités de détection $P_{\pm}$.

[0184] Le système de détermination de clés de cryptage quantique 1 peut comprendre en outre un dispositif d'affichage (non représenté sur les figures) configuré pour générer un affichage des probabilités stockées sur une interface homme-machine.

[0185] Chaque partie de traitement 420 (respectivement 440) peut en outre comprendre une unité de détection auxiliaire 4226 (respectivement 4426) positionnée sur l'autre bras de mesure, c'est à dire le bras de mesure de contrôle 422-2 (respectivement 442-2). L'unité de détection auxiliaire 4226 (respectivement 4426) peut être configurée pour détecter des signaux d'impulsions lumineuses classiques (c'est-à-dire non quantiques). Par exemple et sans limitation, l'unité de détection auxiliaire 4226 (respectivement

4426) peut être une photodiode configurée pour délivrer un photo-courant, en fonction de la mesure du signal de contrôle interférométrique modulé en phase S_{cB} .

[0186] Chaque bras de mesure 422-1 et 422-2, 442-1 et 442-2 du module de traitement 400 peut comprendre en outre une unité de filtrage électronique (notée respectivement 4224, 4228, 4424 et 4428) et positionnée après l'unité de détection de photon unique ou après l'unité de détection auxiliaire. Ces unités de filtrage peuvent correspondre à des signaux créneaux et être configurées pour extraire les composantes temporelles centrales équivalentes au retard interférométrique Δt des probabilités de détection (i.e. tensions mesurées) ou des photo-courants mesurés par les unités de détection 4224, 4228, 4424 et 4428.

[0187] Dans certains modes de réalisation, l'unité de détection auxiliaire 4226 (respectivement 4426) et l'unité de détection de photons uniques 4222 (respectivement 4422) de la partie de traitement 420 (respectivement 440) peuvent comprendre chacune un filtre fréquentiel (non représenté sur les figures) associé respectivement aux fréquences ω_c et ω_q de manière à optimiser la détection des signaux équivalents (i.e. signal de contrôle et signal quantique).

[0188] Comme indiqué par l'équation (18) définissant les probabilités de détection $P_{\pm}$, la qualité du contraste des interférences au niveau des photons uniques peut être affectée par les fluctuations de phase induisant les décalages de phase Φ_A et Φ_B reliées aux modules interférométriques 200 et 300, brouillant le signal quantique à mesurer. Ces paramètres conduisent en effet à des probabilités de détection moins bien marquées entre les deux unités de détection de photon unique 4222 et 4422, qui peuvent être corrigées via la modulation de phase β_{eff} afin d'en déduire des probabilités de détection selon l'équation (17) suivante :

[0189]
$$P_{\pm}(\alpha, \beta) = \frac{1 \pm \cos(\alpha - \beta)}{2} \quad (17)$$

[0190] Le système de détermination de clés de cryptage quantique 1 selon les modes de l'invention peut ainsi être configuré pour corriger les fluctuations de phase parasites induisant les décalages de phase Φ_A et Φ_B en appliquant une modulation de phase β_{eff} déterminée par rétroaction sur le signal quantique, à partir des mesures du signal de contrôle. Dans un mode de réalisation, le module de traitement 400 peut comprendre en outre une unité de correction 480 configurée pour déterminer une correction différentielle des fluctuations de phase entre les décalages de phase Φ_A et Φ_B des modules interférométriques 200 et 300, sans compromettre la sécurité de la clé secrète établie.

[0191] Les unités de détection auxiliaires des parties de traitement 420 et 440 sont configurées avantageusement pour mesurer le résultat d'une interférence entre les différents bras interférométriques possibles du signal de contrôle au travers des modules interférométriques 200 et 300, le signal de contrôle interférométrique modulé

en phase S_{CB} comportant trois impulsions lumineuses de différentes intensités, séparées temporellement de la quantité Δt . Seule la composante temporelle centrale Δt est filtrée par les unités de filtrage 4228 et 4428 qui délivrent à l'unité de correction 480 deux photo-courants (notées par exemple I_{420} et I_{440}) issus de la mesure interférométrique du signal de contrôle provenant des deux chemins optiques 340-3 et 340-4 en sortie du module interférométrique 300 du récepteur Bob.

[0192] La [Fig.6] représente schématiquement l'unité de correction 480 du module de traitement 400, selon des modes de réalisation de l'invention.

[0193] L'unité de correction 480 peut être un module électronique.

[0194] Dans des modes de réalisation, l'unité de correction 480 peut comprendre un moyen de soustraction 482 configuré pour effectuer une soustraction $\delta = |I_{420} - I_{440}|$ entre les deux photo-courants I_{420} et I_{440} , ce qui fournit un signal électronique δ proportionnel au terme $\cos(\varphi_A - \varphi_B - \varphi_m)$.

[0195] L'unité de correction 480 peut comprendre en outre un moyen de multiplication 484 configuré pour effectuer le produit $\delta_m = \delta * \varphi_m$ entre le signal électronique δ et le signal de modulation sinusoïdal φ_m , qui dépend de l'unité de contrôle 3448 du module interférométrique 300 du récepteur Bob. L'unité de correction 480 peut comprendre un filtre passe-bas 486 de fréquence de coupure inférieure à ω_m configuré pour déterminer un signal électronique ε , dit signal d'erreur discret, à partir du produit δ_m . Le signal d'erreur discret ε est alors indépendant de la modulation de phase φ_m et peut être défini par l'équation (18) suivante :

$$[0196] \quad \varepsilon \propto -J_1(\Delta\varphi) \times \sin(\varphi_A - \varphi_B) \quad (18)$$

[0197] Dans l'équation (20) du signal d'erreur discret ε , la composante J_1 correspond à la fonction de Bessel d'ordre 1. Le signal d'erreur discret ε peut ainsi correspondre à la « correction différentielle ε des fluctuations de phase entre les décalages de phase φ_A et φ_B ».

[0198] L'unité de correction 480 peut comprendre enfin un additionneur 488 configuré pour additionner le signal d'erreur discret ε et une modulation de phase β définie à partir d'une unité de contrôle 4882, ce qui fournit la modulation β_{eff} qui permet d'annuler (de façon analogique ou numérique) les décalages de phase φ_A et φ_B .

[0199] Avantagusement, le paramètre β peut être obtenu de manière similaire au paramètre α défini à partir d'une unité de contrôle 2444. Par exemple, le paramètre β peut être choisi par exemple dans un ensemble de deux bases orthogonales comme $[0, \pi]$ et $[\pi/2, 3\pi/2]$ dépendant d'un générateur de nombre aléatoire quantique.

[0200] Les coïncidences mesurées sur les détecteurs de photons uniques les probabilités $P_{\pm}$ définies par l'équation (17) sont ainsi uniquement données par α et β . Avantagusement, selon les modes de réalisation de l'invention, l'unité de correction 480

utilise une rétroaction de la modulation β_{eff} en utilisant des éléments électroniques permettant d'effectuer une compensation (ou rétroaction) électronique plus rapide et continue, contrairement à l'état de la technique.

- [0201] La [Fig.7] est un organigramme représentant le procédé de détermination de clés de cryptage quantique réalisé par l'émetteur Alice (i.e. procédé d'émission d'un signal interférométrique encodé S_2), selon des modes de réalisation de l'invention.
- [0202] A l'étape 700, un signal intermédiaire S_1 est généré par le module 100 de l'émetteur Alice. Le signal intermédiaire S_1 comprend un signal quantique intermédiaire S_q (noté $|\Psi_1\rangle$) et un signal de contrôle intermédiaire S_c modulé en fréquence, selon un décalage de fréquence $\Delta\omega$ par rapport au signal quantique $|\Psi_1\rangle$.
- [0203] A l'étape 702, le signal quantique intermédiaire $|\Psi_1\rangle$ et le signal de contrôle intermédiaire S_c passent par un interféromètre (ayant deux bras interférométriques) du module interférométrique d'encodage 200 de l'émetteur Alice. Par conséquent, le signal $|\Psi_1\rangle$ et le signal S_c se séparent chacun en deux composantes interférométriques qui traversent ensuite un des deux bras interférométriques du module interférométrique d'encodage 200.
- [0204] A l'étape 704, la modulation de phase α est appliquée par le module interférométrique d'encodage 200 de l'émetteur Alice à une des deux composantes interférométriques du signal quantique $|\Psi_1\rangle$ dans l'interféromètre.
- [0205] A l'étape 706, un signal interférométrique encodé S_2 est généré en sortie de l'interféromètre par le module interférométrique d'encodage 200 de l'émetteur Alice. Le signal interférométrique encodé S_2 comprend le signal quantique interférométrique encodé $|\Psi_A\rangle$, modulé en phase, et le signal de contrôle interférométrique S_{cA} (modulée en fréquence).
- [0206] A l'étape 708, le signal interférométrique encodé S_2 est alors transmis par l'émetteur Alice au récepteur Bob.
- [0207] La [Fig.8] est un organigramme représentant le procédé de détermination de clés de cryptage quantique réalisé par le récepteur Bob (i.e. procédé de réception d'un signal interférométrique encodé S_2), selon des modes de réalisation de l'invention.
- [0208] A l'étape 800, le signal quantique interférométrique encodé $|\Psi_A\rangle$ et le signal de contrôle interférométrique S_{cA} passent par un interféromètre (ayant deux bras interférométriques) du module interférométrique de transcodage 300 du récepteur Bob. Le signal $|\Psi_A\rangle$ et le signal S_{cA} se séparent alors chacun en deux composantes interférométriques qui traversent ensuite un des deux bras interférométriques du module interférométrique de transcodage 300.
- [0209] A l'étape 802, la modulation de phase Φ_m est appliquée par le module interférométrique de transcodage 300 du récepteur Bob à une des deux composante du signal de

contrôle interférométrique S_{cA} , ce qui fournit le signal de contrôle interférométrique modulé en phase S_{cB} en sortie du module interférométrique 300.

[0210] A l'étape 804, la mesure interférométrique du signal de contrôle interférométrique modulé en phase S_{cB} est effectuée par le module de traitement 400 du récepteur Bob.

[0211] A l'étape 806, une opération de détermination du signal d'erreur discret ϵ de correction différentielle des fluctuations de phase entre les décalages de phase Φ_A et Φ_B des modules interférométriques 200 et 300, est effectuée à partir de la modulation de phase Φ_m et de la mesure interférométrique du signal de contrôle interférométrique modulé en phase S_{cB} .

[0212] A l'étape 808, une opération de détermination de la modulation de phase β_{eff} (prenant en compte la correction différentielle des fluctuations de phase entre les décalages de phase Φ_A et Φ_B) est effectuée à partir du signal d'erreur discret ϵ et d'une modulation de phase β .

[0213] A l'étape 810, la modulation de phase β_{eff} est appliquée par le module interférométrique de transcodage 300 du récepteur Bob, à une des deux composantes du signal quantique interférométrique encodé $|\Psi_A\rangle$, ce qui fournit le signal quantique interférométrique transcodé $|\Psi_B\rangle$ (i.e. ce qui fournit la projection du signal $|\Psi_A\rangle$ sur les états quantiques transcodés $|\Psi_{B+}\rangle$ et $|\Psi_{B-}\rangle$), en sortie du module interférométrique 300.

[0214] A l'étape 812, la mesure interférométrique du signal quantique interférométrique transcodé $|\Psi_B\rangle$ (i.e. la mesure interférométrique de la projection du signal quantique interférométrique encodé $|\Psi_A\rangle$ sur les états $|\Psi_{B+}\rangle$ et $|\Psi_{B-}\rangle$) est effectuée par le module de traitement 400 du récepteur Bob, en sortie du module interférométrique 300, pour en déduire la clé de quantique.

[0215] Le procédé de détermination de clés de cryptage quantique peut en outre comprendre à l'étape 700, une sous-étape 701 dans laquelle est implémenté un retard temporel du signal quantique intermédiaire S_q par rapport au signal de contrôle intermédiaire S_c pour générer le signal intermédiaire S_l .

[0216] Les modes de réalisation de l'invention permettent ainsi la mesure et la compensation en temps réel des décalages de phase Φ_A et Φ_B induits par les modules interférométriques 200 et 300, et par suite permettent une augmentation du rapport signal sur bruit de la composante quantique générée et encodée. Il en résulte une capacité maximale en termes de vitesse de modulation. En outre, le système de détermination de clés de cryptage quantique 1 a l'avantage d'être robuste aux fluctuations d'intensité des impulsions laser émises, notamment par rapport au signal de contrôle.

[0217] L'homme du métier comprendra que le système de détermination de clés de cryptage quantique 1 ou des sous-systèmes du système de détermination de clés de cryptage

quantique 1, selon les modes de réalisation de l'invention, peuvent être mis en œuvre de diverses manières par matériel (« hardware »), logiciel, ou une combinaison de matériel et de logiciels, notamment sous la forme de code de programme pouvant être distribué sous la forme d'un produit de programme, sous diverses formes. Le code de programme peut être distribué à l'aide de supports lisibles par ordinateur, qui peuvent inclure des supports de stockage lisibles par ordinateur et des supports de communication. Les procédés décrits dans la présente description peuvent être notamment implémentés sous la forme d'instructions de programme d'ordinateur exécutables par un ou plusieurs processeurs dans un dispositif informatique d'ordinateur. Ces instructions de programme d'ordinateur peuvent également être stockées dans un support lisible par ordinateur.

[0218] L'invention n'est pas limitée aux modes de réalisation décrits ci-avant à titre d'exemple non limitatif. Elle englobe toutes les variantes de réalisation qui pourront être envisagées par l'homme du métier. En particulier, l'homme du métier comprendra que l'invention n'est pas limitée aux différents modules de l'émetteur Alice et du récepteur Bob décrits à titre d'exemples non limitatif.

Revendications

[Revendication 1] Emetteur configuré pour transmettre un signal interférométrique encodé S_2 à travers un canal de transmission (50), caractérisé en ce que ledit émetteur comprend :

- un module de génération de signal (100) configuré pour générer un signal quantique intermédiaire $|\Psi_1\rangle$ et un signal de contrôle intermédiaire S_c , ledit module de génération de signal (100) étant en outre configuré pour effectuer un décalage fréquentiel $\Delta\omega$ entre le signal quantique intermédiaire $|\Psi_1\rangle$ et le signal de contrôle intermédiaire S_c ,
- un module interférométrique d'encodage (200) configuré pour recevoir ledit signal quantique intermédiaire $|\Psi_1\rangle$ et ledit signal de contrôle intermédiaire S_c , et pour déterminer un signal interférométrique encodé S_2 comprenant un signal quantique interférométrique encodé $|\Psi_A\rangle$ et un signal de contrôle interférométrique S_{cA} à partir dudit signal quantique intermédiaire $|\Psi_1\rangle$ et dudit signal de contrôle intermédiaire S_c parcourant un chemin optique sensiblement similaire, ledit module interférométrique d'encodage (200) comprenant un dispositif d'encodage (240D) configuré pour appliquer une modulation de phase α uniquement à une composante du signal quantique intermédiaire $|\Psi_1\rangle$.

[Revendication 2] Emetteur, selon la revendication précédente, dans lequel le module interférométrique d'encodage (200) est implémenté sous la forme d'un interféromètre optique asymétrique comprenant un premier bras interférométrique (240-1) et un deuxième bras interférométrique (240-2), le premier bras interférométrique (240-1) étant plus court que le deuxième bras interférométrique (240-2), et dans lequel ledit dispositif d'encodage (240D) comprend au moins une unité de séparation fréquentielle (244) positionnée sur ledit deuxième bras interférométrique (240-2), ladite unité de séparation fréquentielle (244) étant configurée pour effectuer un découplage fréquentiel du signal quantique intermédiaire $|\Psi_1\rangle$ et du signal de contrôle intermédiaire S_c .

[Revendication 3] Emetteur, selon l'une des revendications 1 ou 2, dans lequel le module de génération de signal (100) comprend en outre une unité de décalage

temporel configurée pour décaler temporellement le signal quantique intermédiaire $|\Psi_i\rangle$ et le signal de contrôle intermédiaire S_c .

[Revendication 4]

Récepteur configuré pour recevoir un signal quantique interférométrique encodé $|\Psi_A\rangle$ et un signal de contrôle interférométrique S_{cA} à travers un canal de transmission (50), caractérisé en ce que ledit récepteur comprend :

- un module interférométrique de transcodage (300) configuré pour générer un signal quantique interférométrique transcodé $|\Psi_B\rangle$ et un signal de contrôle interférométrique modulé en phase S_{cB} à partir dudit signal quantique interférométrique encodé $|\Psi_A\rangle$ et dudit signal de contrôle interférométrique S_{cA} parcourant un chemin optique sensiblement similaire, ledit module interférométrique de transcodage (300) comprenant un dispositif de transcodage et de modulation de phase (340D) étant configuré pour appliquer une modulation de phase β_{eff} uniquement à une composante du signal quantique interférométrique encodé $|\Psi_A\rangle$ et une modulation de phase φ_m uniquement à une composante du signal de contrôle interférométrique S_{cA} ,
- un module de traitement (400) configuré pour effectuer au moins une mesure du signal quantique interférométrique transcodé $|\Psi_B\rangle$ et au moins une mesure du signal de contrôle interférométrique modulé en phase S_{cB} , ledit module de traitement (400) étant en outre configuré pour déterminer la modulation de phase β_{eff} à partir de la modulation de phase φ_m et de ladite au moins une mesure du signal de contrôle interférométrique modulé en phase S_{cB} .

[Revendication 5]

Récepteur, selon la revendication 4, dans lequel le module interférométrique de transcodage (300) est implémenté sous la forme d'un interféromètre optique asymétrique comprenant un premier bras interférométrique (340-1) et un deuxième bras interférométrique (340-2), le premier bras interférométrique (340-1) étant plus court que le deuxième bras interférométrique (340-2), et dans lequel ledit dispositif de transcodage et de modulation de phase (340D) comprend au moins une unité de séparation fréquentielle (344) positionnée sur ledit deuxième

bras interférométrique (340-2), ladite unité de séparation fréquentielle (244) étant configurée pour effectuer un découplage fréquentiel du signal quantique interférométrique encodé $|\Psi_A\rangle$ et du signal de contrôle interférométrique S_{cA} .

[Revendication 6] Récepteur, selon d'une des revendications 4 ou 5, dans lequel le module interférométrique de transcodage (300) comprend deux chemins optiques (340-3, 340-4) en sortie dudit interféromètre, et dans lequel le module de traitement (400) comprend deux parties de traitement (420, 440), chaque partie de traitement comprenant une unité de séparation fréquentielle (422, 442) et étant configurée pour effectuer une mesure parmi ladite au moins une mesure du signal quantique interférométrique transcodé $|\Psi_B\rangle$ et une mesure parmi ladite au moins une mesure du signal de contrôle interférométrique modulé en phase S_{cB} , provenant des deux chemins optiques (340-3 et 340-4)

[Revendication 7] Système de détermination de clé de cryptage quantique (1) comprenant un émetteur défini selon l'une des revendications 1 à 3 et un récepteur défini selon l'une des revendications 4 à 6.

[Revendication 8] Procédé d'émission d'un signal interférométrique encodé S_2 , mis en œuvre par l'émetteur selon les revendications 1 à 3, le procédé comprenant les étapes consistant à :

- générer (700) un signal quantique intermédiaire $|\Psi_1\rangle$ de fréquence ω_q et un signal de contrôle intermédiaire S_c de fréquence ω_c ayant un décalage fréquentiel égal à $\omega_q - \omega_c$
- appliquer (704) une modulation de phase α uniquement à une composante du signal quantique intermédiaire $|\Psi_1\rangle$ passant à travers un interféromètre, ledit signal quantique intermédiaire $|\Psi_1\rangle$ et ledit signal de contrôle intermédiaire S_c parcourant un chemin optique sensiblement similaire pour générer un signal interférométrique encodé S_2 comprenant un signal quantique interférométrique encodé $|\Psi_A\rangle$ et un signal de contrôle interférométrique S_{cA} ,
- générer (706) un signal interférométrique encodé S_2 comprenant ledit signal quantique interférométrique encodé $|\Psi_A\rangle$ et ledit signal de contrôle interférométrique S_{cA} .

[Revendication 9] Procédé d'émission d'un signal interférométrique encodé S_2 , selon la re-

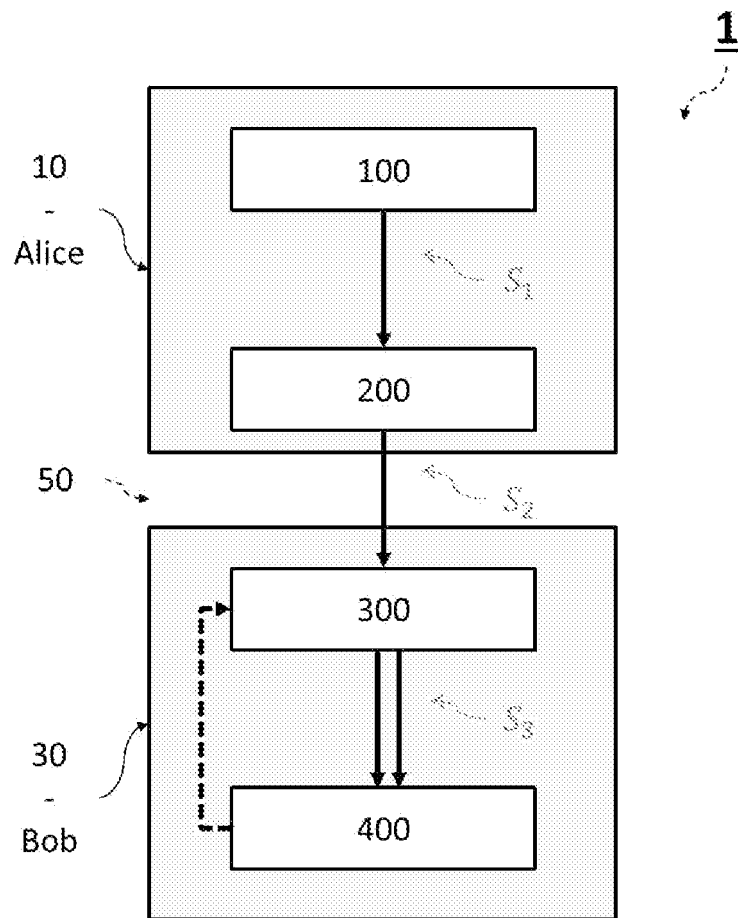
vention 8, dans lequel le procédé comprend en outre une étape consistant à appliquer (701) un retard temporel entre ledit signal quantique intermédiaire $|\Psi_1\rangle$ et ledit signal de contrôle intermédiaire S_c .

[Revendication 10]

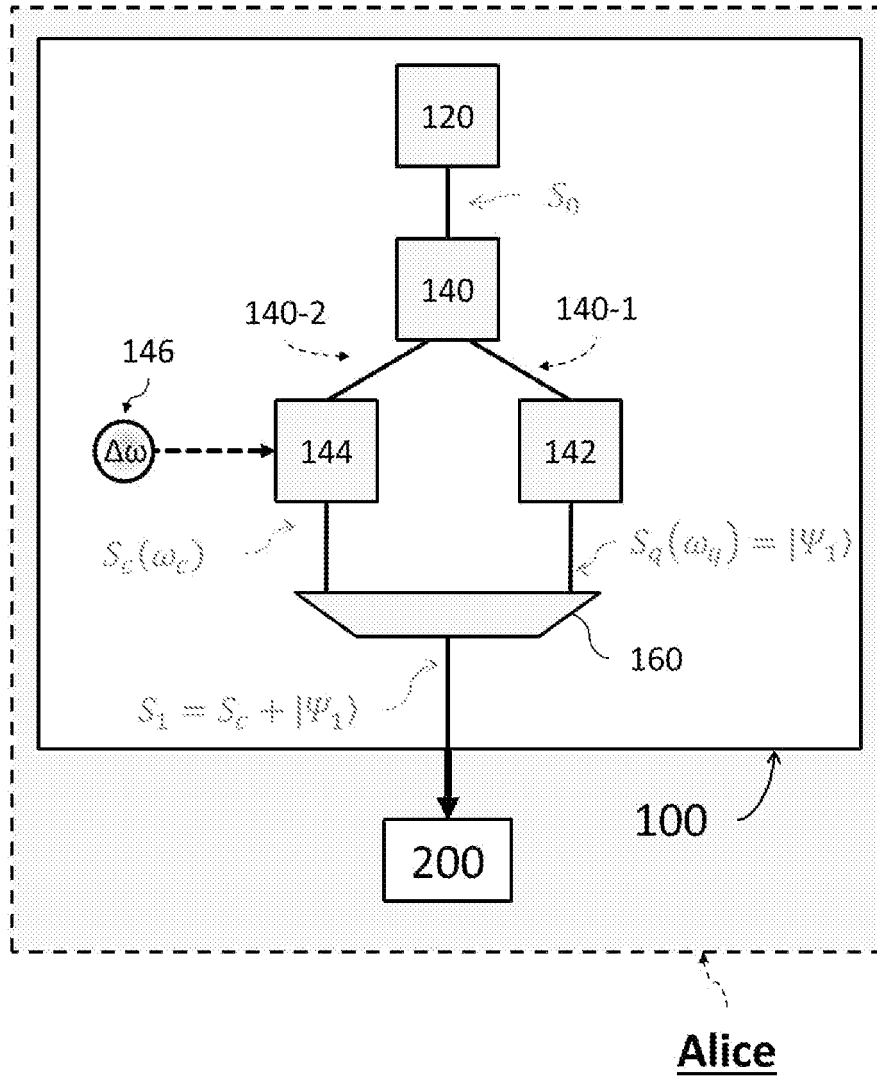
Procédé de réception d'un signal quantique interférométrique encodé $|\Psi_A\rangle$ et d'un signal de contrôle interférométrique S_{cA} , mis en œuvre par le récepteur selon les revendications 4 à 6, le procédé comprenant les étapes consistant à :

- appliquer (802) une modulation de phase Φ_m à la composante du signal de contrôle interférométrique S_{cA} et générer un signal de contrôle interférométrique modulé en phase S_{cB} ,
- effectuer (804) au moins une mesure du signal de contrôle interférométrique modulé en phase S_{cB} ,
- déterminer (808) une modulation de phase β_{eff} à partir de ladite modulation de phase Φ_m et de la mesure du signal de contrôle interférométrique modulé en phase S_{cB} ,
- appliquer (810) la modulation de phase β_{eff} à la composante du signal quantique interférométrique encodé $|\Psi_A\rangle$ et générer un signal quantique interférométrique transcodé $|\Psi_B\rangle$, ledit signal quantique interférométrique encodé $|\Psi_A\rangle$ et ledit signal de contrôle interférométrique S_{cA} parcourant un chemin optique sensiblement similaire,
- effectuer (812) au moins une mesure du signal quantique interférométrique transcodé $|\Psi_B\rangle$.

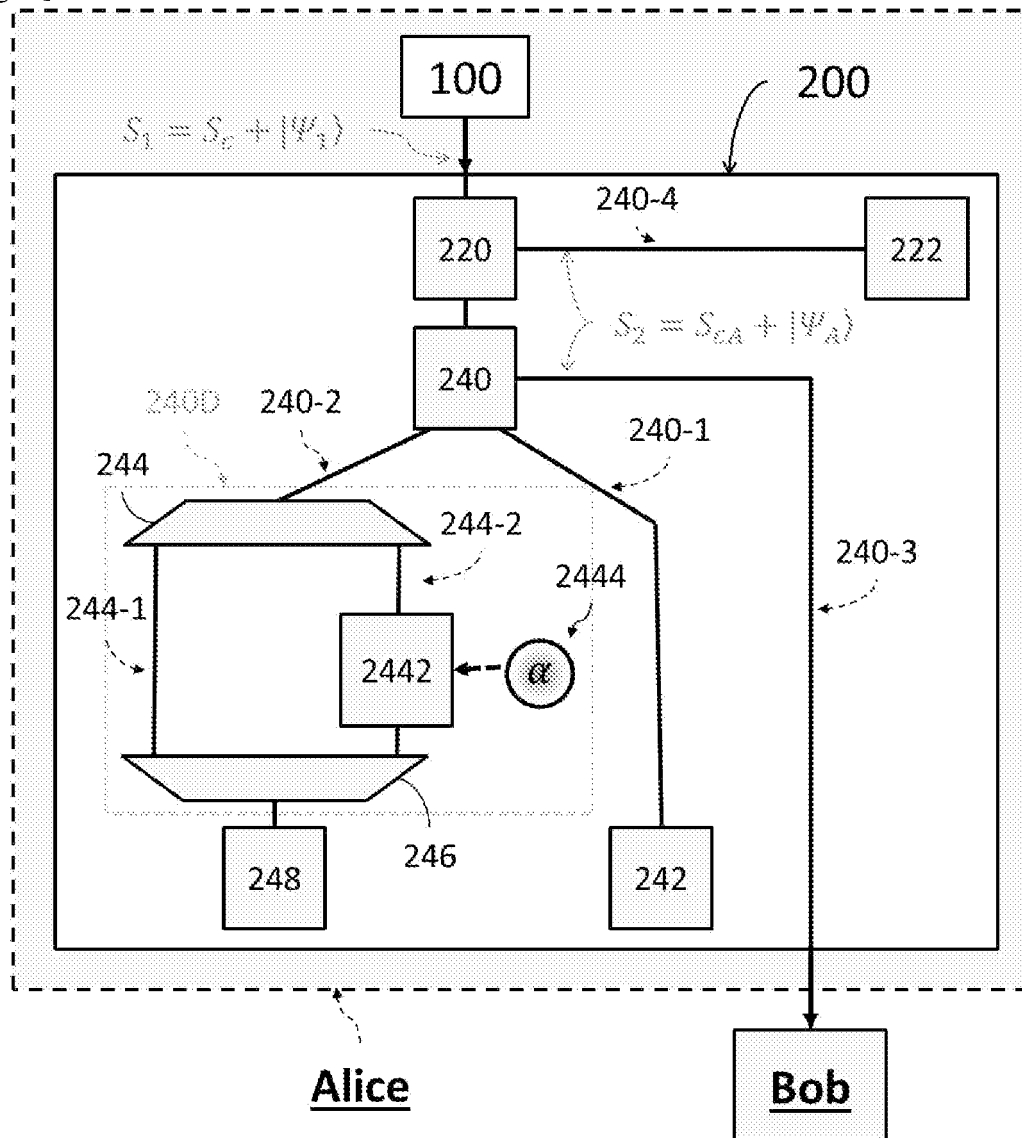
[Fig. 1]

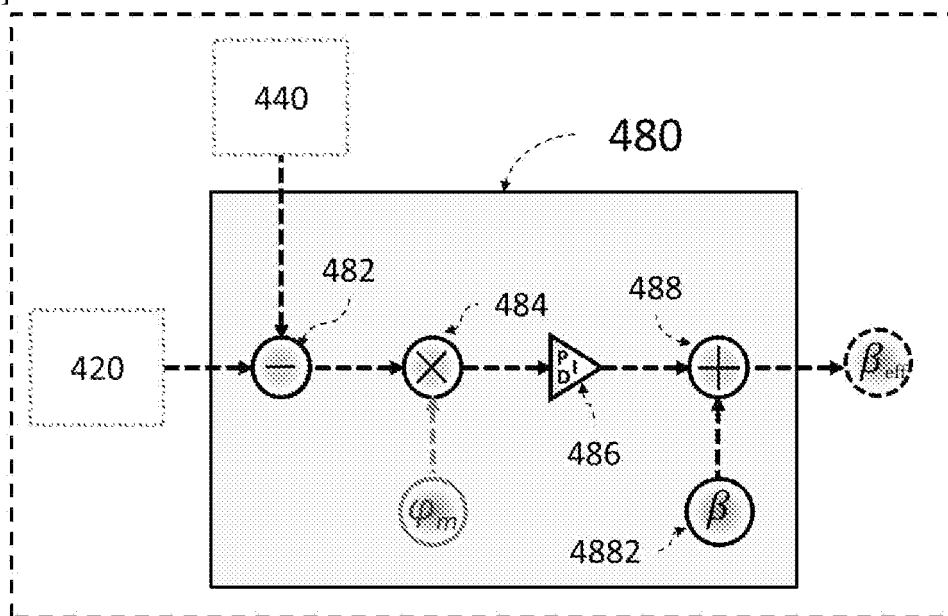


[Fig. 2]



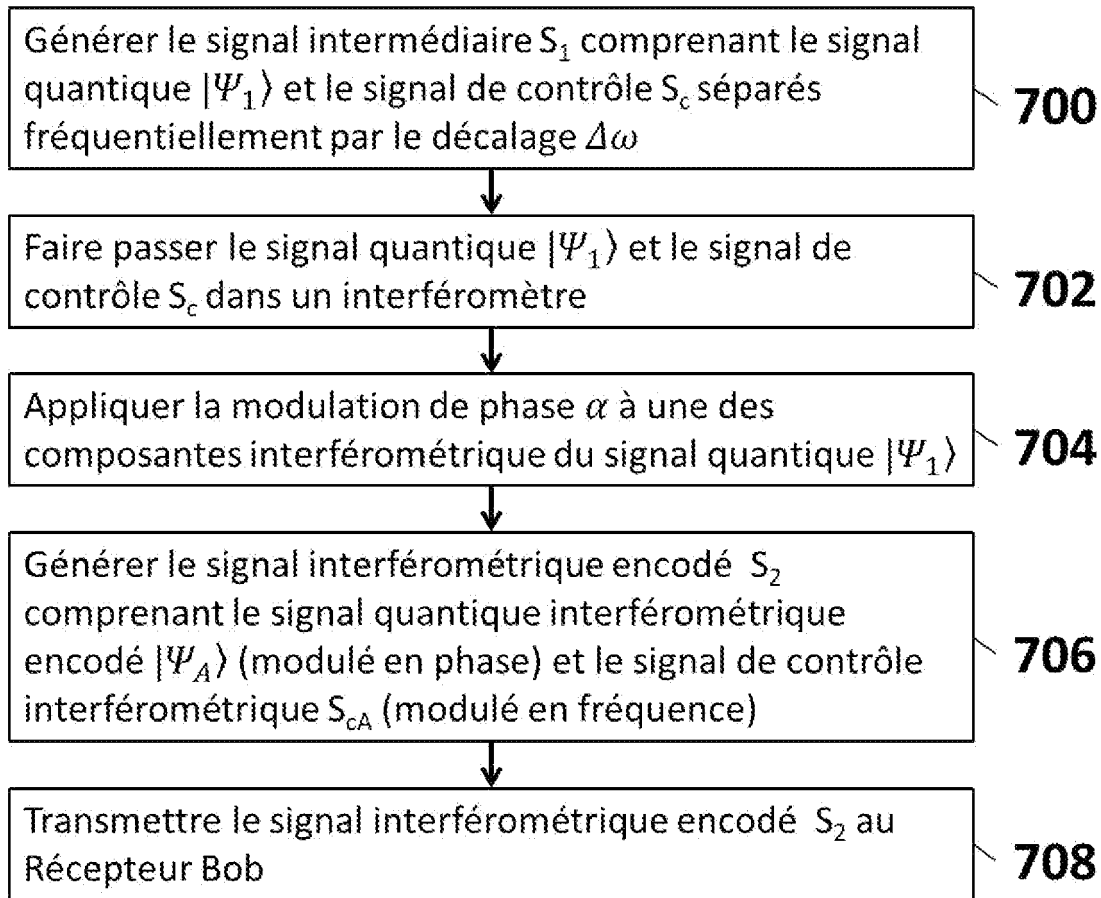
[Fig. 3]





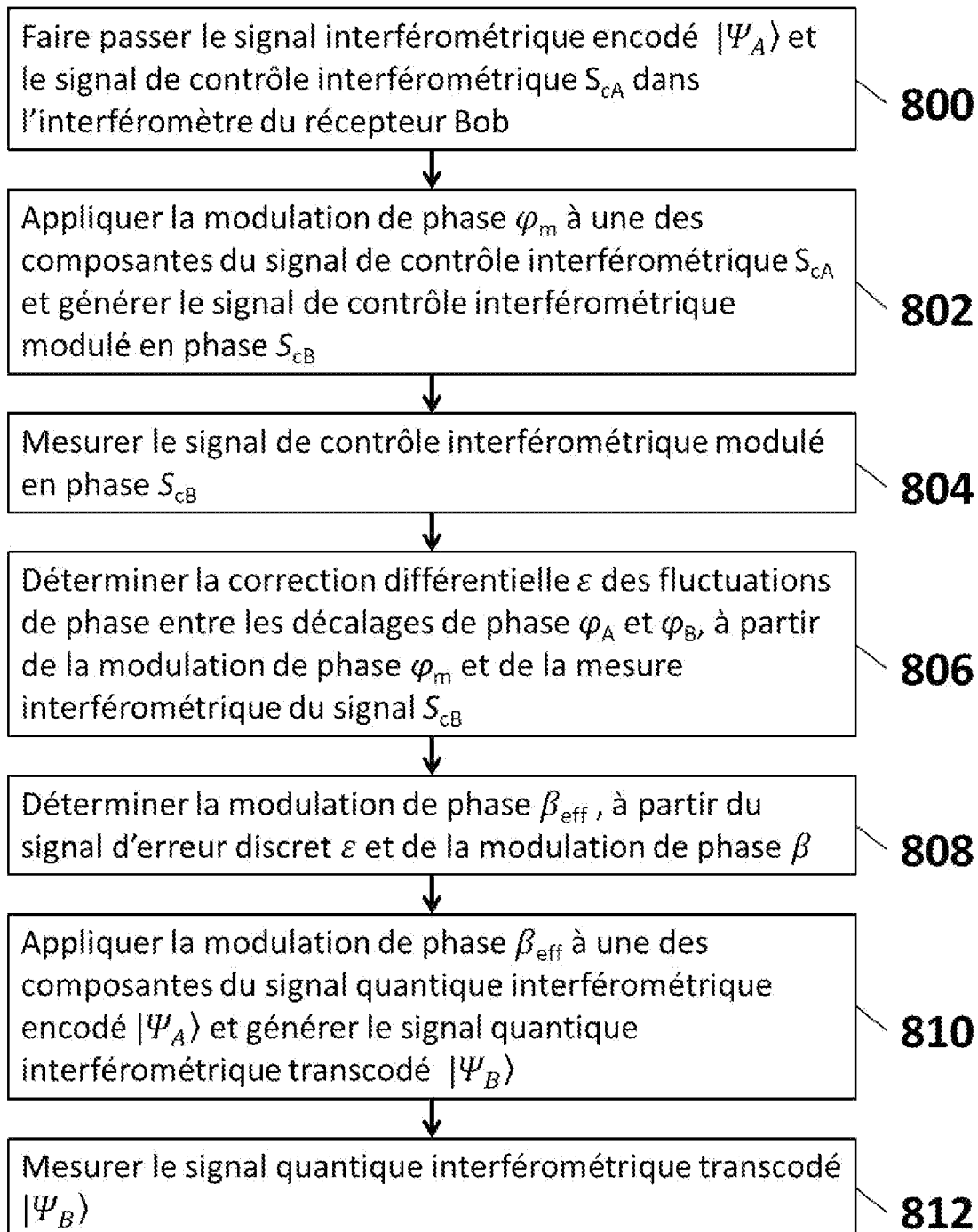
[Fig. 7]

Émetteur Alice



[Fig. 8]

Récepteur Bob



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 (nouveau) 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

☒ Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

☐ Le demandeur a maintenu les revendications.

☒ 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.

☐ 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**

NEANT

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

EP 1 499 040 A2 (TOSHIBA KK [JP])
19 janvier 2005 (2005-01-19)

GB 2 430 124 A (TOSHIBA RES EUROP LTD
[GB]) 14 mars 2007 (2007-03-14)

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

NEANT