

Revendications

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

ledit procédé comprenant, dans l'ordre :

- la succession des étapes suivantes, répétée de $q=1$ à Q :
 - une première action effectuée par l'émetteur (C_1) comprenant la préparation par l'émetteur (C_1) d'un photon dans un état quantique de départ $|u\rangle$ d'une base d'encodage B_a orthonormée de dimension d et d'états de base $|e_0\rangle$, $|e_1\rangle$, ... $|e_{d-1}\rangle$, avec a choisi au hasard entre 0 et 1,
 - transmission du photon préparé dans la chaîne de communication,
 - une deuxième action effectuée par le premier participant (C_i) sur ledit photon, de décision de transformation ou non de l'état quantique du photon transmis, en un état quantique de base orthogonal dans la base d'encodage B_0 et dans la base d'encodage B_1
 - une troisième action effectuée par le second participant (C_j) sur ledit photon, de décision de transformation ou non de l'état quantique du photon reçu du participant immédiatement précédent (C_{j-1}) en un état quantique orthogonal correspondant dans la base d'encodage B_0 et dans la base d'encodage B_1
 - une quatrième action effectuée par le récepteur (C_N) comprenant la mesure, dans la base standard B_0 ou dans la base B_1 , de l'état final $|\alpha_{\text{final}}\rangle$ du photon transmis dans la chaîne de communication par le récepteur (C_N),
 - échange sur un canal de communication classique entre au moins une partie des participants, d'au moins une partie des décisions parmi celles de la base de départ a , de l'état de départ $|u\rangle$, de la base de mesure choisie par ledit récepteur (C_N) et du résultat de la mesure de $|\alpha_{\text{final}}\rangle$ dans cette base de mesure,

- obtention, entre les premier et second participants (C_i) et (C_j), d'une description de l'état quantique transmis q_q correspondant à l'un des états de base $|e_0\rangle, |e_1\rangle, \dots |e_{d-1}\rangle$, grâce à ladite partie des décisions et dudit résultat de la mesure ;
- puis, la reconstitution, par les premier et second participants (C_i) et (C_j), par concaténation, d'une séquence des descriptions des Q états quantiques transmis q_q , pour q allant de 1 à Q .

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

- La première action, effectuée par l'émetteur (C_1), comprend les étapes suivantes :
 - Choisir une valeur s_q égale à 0 ou 1
 - Choisir une valeur l comprise entre 0 et $d-1$
 - Appliquer une transformation $P^{s_q}X_l$ à un photon de référence créé par l'émetteur au début de la chaîne de communication
- la deuxième action, effectuée par le premier participant (C_i), comprend les étapes suivantes :
 - Choisir une valeur m comprise entre 0 et $d-1$
 - Appliquer une transformation X_m au photon reçu à travers la chaîne de communication,
- la troisième action, effectuée par le deuxième participant (C_j), comprend les étapes suivantes :
 - Choisir une valeur n comprise entre 0 et $d-1$
 - Appliquer une transformation X_n au photon reçu à travers la chaîne de communication,
- la quatrième action, effectuée par le récepteur (C_N), comprend les étapes suivantes :
 - Choisir une valeur t_q égale à 0 ou 1
 - Appliquer une transformation $P^{(-1)t_q}$ au photon reçu à travers la chaîne de communication,

dans lequel :

la notation P^1 signifie que la transformation P a lieu,

la notation P^0 signifie que la transformation P n'a pas lieu,

la notation $P^{(-1)1}$ signifie que la transformation $P^{(-1)}$ a lieu,

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

la notation X_m désigne une transformation permettant de passer de l'état quantique de base $|t\rangle$, t étant un entier compris entre 0 et $d-1$, à l'état orthogonal $c|(t+m) \bmod d\rangle$ dans la base B_0 ou la transformation permettant de passer d'un état $|e_t\rangle$ à $d|e_t+m \bmod d\rangle$ dans la base B_1 , pour m un entier compris entre 0 et $d-1$, et c et d des phases globales induites par ces transformations.

[Revendication 3] Procédé de transmission sécurisée selon la revendication 1, dans lequel, pour chaque répétition de $q=1$ à Q de la succession d'étapes :

- la première action, comprend la préparation par l'émetteur (C_1) d'un photon dans un état quantique de base de référence $|0\rangle$ d'une base d'encodage B_0 orthonormée, nommée base standard de dimension d ,
- la deuxième action effectuée par le premier participant (C_i), comprend les étapes suivantes :
 - o Choisir une valeur s_q égale à 0 ou 1
 - o Choisir une valeur m comprise entre 0 et $d-1$
 - o Appliquer une transformation $P^{s_q} X_m$ au photon reçu à travers la chaîne de communication, ou dans le cas où i est égal à 1, au photon au début de la chaîne de communication,
- la troisième action, effectuée par le second participant (C_j), comprend les étapes suivantes :
 - o Choisir une valeur t_q égale à 0 ou 1
 - o Choisir une valeur n comprise entre 0 et $d-1$
 - o Appliquer une transformation $X_n P^{(-1)^{t_q}}$ au photon reçu à travers la chaîne de communication,

dans lequel :

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

[Revendication 4] Procédé de transmission sécurisée selon l'une des revendications 1 à 3, dans lequel ladite dimension d est égale à 2.

[Revendication 5] Procédé selon l'une des revendications précédentes, dans lequel ledit photon est transmis à travers un filtre fréquentiel et une porte temporelle.

[Revendication 6] Procédé de transmission sécurisée selon l'une des revendications 1 à 5, dans lequel i est différent de 1 et N , et j est différent de 1 et N , la séquence des Q photons encodant la séquence des Q états quantiques q_q présente une puissance lumineuse donnée P_{seq} et N est un entier supérieur ou égal à 4, et dans lequel :

- Ladite deuxième action comprend :
 - une étape (G_5) de prélèvement d'une première portion (P_{seq1}) de la puissance lumineuse (P_{seq}) du flux de photons reçu du participant (C_{i-1}) précédant immédiatement le premier participant (C_i),
 - une étape (G_6) de comparaison de la première portion (P_{seq1}) avec une seconde portion ($P_{seq1'}$) de la puissance lumineuse (P_{seq}) du flux de photons envoyé par l'émetteur (C_1) afin de détecter une potentielle injection de photons espions avant le premier participant (C_i),
- ladite troisième action comprend :
 - une étape (G_7) de prélèvement d'une troisième portion (P_{seq2}) de la puissance lumineuse du flux de photons reçu du participant (C_{j-1}) précédant immédiatement le second participant (C_j),
 - une étape (G_8) de comparaison de la troisième portion (P_{seq2}) avec une quatrième portion ($P_{seq2'}$) de la différence entre la puissance lumineuse du flux de photons envoyé par l'émetteur (P_{seq}) et la première portion (P_{seq1}) afin de détecter une potentielle injection de photons espions avant le second participant (C_j).

[Revendication 7] Procédé de transmission sécurisée, selon l'une des revendications 1 à 6 dans lequel chaque état quantique q_q est codé dans un degré de liberté du photon choisi parmi la phase, la différence de phase, la localisation temporelle, la polarisation ou la fréquence du photon.

[Revendication 8] Procédé de transmission sécurisée selon l'une des revendications 1 à 7 dans lequel la séquence de Q états quantiques q_q est choisie de manière aléatoire dans le but d'établir une clé quantique.

[Revendication 9] Dispositif pour la mise en œuvre du procédé de transmission

sécurisée selon l'une des revendications 1 à 6, ou 8, comprenant :

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

dans lequel :

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

[Revendication 10] Dispositif selon la revendication 9 pour la mise en œuvre d'un procédé de transmission sécurisée comprenant en outre, dans le cas où le premier participant (C_i) et le second participant (C_j) sont tous les deux distincts de l'émetteur (C_1) et du récepteur (C_N) :

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

dans lequel :

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

- le deuxième séparateur de faisceau (S_j) est apte à séparer un flux de photons reçu du participant précédant immédiatement le second participant dans la chaîne de communication (C_{j-1}) dans deux directions distinctes, l'une en direction du modulateur du second participant (C_j) puis vers la suite de la chaîne de communication, l'autre en direction de la deuxième photodiode (PD_j), dans le but de mettre en œuvre le procédé de transmission sécurisée selon la revendication 6.

[Revendication 11] Dispositif pour la mise en œuvre d'un procédé de transmission sécurisée selon la revendication 9 ou 10, dans lequel :

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

[Revendication 12] Dispositif pour la mise en œuvre du procédé de transmission sécurisée selon la revendication 9 ou 10, dans lequel :

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

[Revendication 13] Dispositif pour la mise en œuvre d'un procédé de transmission sécurisée selon la revendication 9 ou 10, dans lequel :

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