

Revendications

[Revendication 1] Procédé pour calculer un ET logique entre deux bits choisis, x_i , x_j détenus par un premier et un second participants, C_i , C_j respectivement, connectés entre eux et à un serveur (C_1), par au moins un canal de communication quantique (L_q) et un canal de communication conventionnel (L_c), comportant

une première phase utilisant ledit canal de communication quantique et comprenant

une première étape (S1) dans laquelle lesdits premier et second participants déterminent aléatoirement, respectivement, une première α et seconde β variable de corrélation ; déterminent chacun un bit aléatoire, respectivement p et q , et transmettent audit serveur (C_1), une valeur dépendante dudit bit aléatoire respectif p , q ;

une deuxième étape (S2) dans laquelle ledit serveur (C_1) prépare un photon dans un premier état dans une base orthonormée, et le transmet audit premier participant (C_i) ;

une troisième étape (S3) dans laquelle ledit premier participant (C_i) applique une première transformation $V^\alpha U^p$ audit photon, et le transmet audit second participant (C_j), la porte logique V transformant un état dans un état orthogonal et la porte logique U étant une racine carrée de la porte logique V ;

une quatrième étape (S4) dans laquelle ledit second participant (C_j) applique une seconde transformation $V^\beta U^q$ audit photon, et le transmet audit serveur ;

une cinquième étape (S5) dans laquelle le serveur C_1 effectue une troisième transformation $(U^*)^{p+q}$, mesure l'état dudit photon et détermine une troisième variable de corrélation γ en fonction dudit état, de sorte à former une corrélation entre lesdites variables de corrélation ; et,

une seconde phase comportant

une sixième étape (S6) dans laquelle lesdits premier et second participants s'échangent une valeur u_1, u_2 dépendant de la somme entre le bit aléatoire, p, q , et le bit choisi, x_i, x_j , qu'ils détiennent, respectivement ;

une septième étape (S7) dans laquelle ledit premier participant calcule et fournit une première valeur $a = \alpha + x_i \wedge u_2$, ledit second participant calcule et fournit une seconde valeur $b = \beta + x_j \wedge u_1 + u_1 \wedge u_2$ et ledit serveur fournit la troisième variable de corrélation γ ,

de sorte que l'on puisse obtenir le résultat du calcul du « et » logique entre lesdits bits choisis en sommant lesdites première et seconde valeur et ladite troisième variable de corrélation.

[Revendication 2] Procédé selon la revendication précédente, dans lequel ladite première phase est effectuée avant que lesdits bits choisis ne soient connus desdits participants

[Revendication 3] Procédé selon l'une des revendications précédentes, dans lequel, lors de ladite première étape (S1), lesdits premier et second participant transmettent des valeurs respectives $t_1 = p + r$ et $t_2 = q + r$, où r est un bit partagé secrètement par lesdits premier et second participants ;

[Revendication 4] Procédé selon l'une des revendications précédentes, dans lequel ledit premier état est l'état $|+\rangle$

[Revendication 5] Procédé selon l'une des revendications précédentes, dans lequel ledit canal de communication conventionnel (L_c) est un canal sécurisé.

[Revendication 6] Dispositif pour calculer un ET logique entre deux bits choisis, x_i, x_j détenus par un premier et un second participants (C_i, C_j respectivement), connectés entre eux et à un serveur (C_1), par au moins un canal de communication quantique (L_q) et un canal de communication conventionnel (L_c), comportant des moyens pour mettre en œuvre le procédé selon l'une des revendications précédentes.

[Revendication 7] Dispositif selon la revendication précédente dans lequel lesdits premier et second participants appartiennent à une chaîne de

participants, dans laquelle les deux participants aux extrémités (C_1 , C_N respectivement) mettent en œuvre ledit serveur un participant amont étant apte à émettre un photon, et un participant aval (C_N) étant apte à recevoir un photon et à mesurer son état.

[Revendication 8] Dispositif selon la revendication 6, dans lequel lesdits premier et second participants appartiennent à un anneau de participants, de sorte qu'un participant donné (C_1) mette en œuvre ledit serveur et soit apte à émettre un photon, à recevoir un photon et à mesurer son état.

[Revendication 9] Dispositif selon l'une des revendications 6 à 8, dans lequel ledit serveur comporte un laser apte à générer des photons et un modulateur initial apte à moduler un degré de liberté d'un photon généré par ledit laser.

[Revendication 10] Dispositif selon l'une des revendications 6 à 8, dans lequel lesdits premier et second participants comportent des modulateurs aptes à moduler un champ électromagnétique dans lequel passent les photons afin de modifier un degré de liberté de ceux-ci.]