

Procédé de calcul d'un ET logique entre deux bits de manière sécurisée par l'utilisation de la communication quantique

[0001] La présente invention concerne de manière générale le domaine du calcul sécurisé utilisant des communications quantiques et plus particulièrement le calcul d'un ET logique entre plusieurs participants connectés à un réseau de communication.

[0002] Contexte de l'invention

[0003] D'une façon générale, l'invention concerne le domaine du calcul multipartite sécurisé, qui est une branche de la cryptographie dont l'objectif est de permettre à des participants d'obtenir le résultat d'une fonction commune sans qu'aucun d'entre eux ne puisse connaître les entrées des autres participants.

[0004] Ce type de problématique semble avoir été évoqué dans les années 1970 dans l'article d'A. Shamir, R. Rivest, and L. Adleman, "*Mental Poker*", Technical Report LCS/TR-125, Massachusetts Institute of Technology, avril 1979. Dans les années 1980, la problématique fut appliquée au problème théorique des milliardaires qui consiste à déterminer la personne la plus riche dans un ensemble de milliardaire sans qu'aucun ne divulgue sa fortune à quiconque. On peut notamment citer l'article d'Andrew C. Yao, « *Protocols for secure computations* » qui présente le problème et un protocole permettant de le résoudre.

[0005] D'autres applications du calcul multipartite sécurisé comprennent les mécanismes d'enchères, ou de votes, les statistiques sur des données médicales, etc. Dans ces applications, d'une façon générale, on veut parvenir à un résultat basé sur l'ensemble des données d'entrées tout en gardant celles-ci privées, c'est-à-dire secrètes vis-à-vis des autres parties. Dans le cas des données médicales, par exemple, il peut être intéressant de construire des données statistiques, ou agrégées, mais pour des raisons légales, les données individuelles ne peuvent pas être accessibles à quiconque. De même, dans les systèmes d'enchère, sur un marché de gros de produits agricoles par exemple, l'enjeu est de déterminer la partie qui a emporté l'enchère mais sans que les différentes parties n'aient à dévoiler leurs offres.

[0006] S'il existe des travaux théoriques sur le calcul multipartite sécurisé, fort peu de développements industriels existent. En effet, la protection de la vie privée est une

préoccupation relativement neuve : la première implémentation à grande échelle datant de 2009, et les premières solutions pratiques arrivent sur le marché avec, nécessairement, un temps de retard.

5 [0007] En outre, les propositions existantes induisent généralement un surcoût en termes de temps de calcul qui les rendent réductibles pour des utilisations pratiques.

[0008] Un autre inconvénient des propositions existantes est leur haut niveau de technicité, lié aux techniques cryptographiques, qui les rendent difficiles à intégrer dans les produits et systèmes existants.

10 [0009] Le but de l'invention est d'au moins améliorer la situation en offrant un procédé efficace et sécurisé de calcul multipartite sécurisé faisant usage d'un canal de communication quantique.

[0010] Plus particulièrement, l'invention concerne le sous-problème d'un calcul distribué d'un ET logique, ce calcul permettant la réalisation de toutes fonctions logiques multipartites.

15 [0011] À cette fin, la présente invention propose un 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 par au moins un canal de communication quantique L_q et un canal de communication conventionnel L_c , comportant

20 une première phase utilisant ledit canal de communication quantique et comprenant

25 une première étape 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, une valeur dépendante dudit bit aléatoire respectif p, q ;

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

5 une troisième étape dans laquelle ledit premier participant applique une première transformation $V^{\alpha}U^p$ audit photon, et le transmet audit second participant, 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 dans laquelle ledit second participant applique une seconde transformation $V^{\beta}U^q$ audit photon, et le transmet audit serveur ;

une cinquième étape dans laquelle le serveur effectue une troisième transformation $(U^*)^{p+q}$, mesure l'état dudit photon et détermine une

10 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 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 ;

15

une septième étape 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 ,

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

[0012] Suivant des modes de réalisation préférés, l'invention comprend une ou plusieurs des caractéristiques suivantes qui peuvent être utilisées séparément ou en

25 combinaison partielle entre elles ou en combinaison totale entre elles :

- ladite première phase est effectuée avant que lesdits bits choisis ne soient connus desdits participants
- lors de ladite première étape, 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

30 par lesdits premier et second participants ;

- ledit premier état est l'état $|+\rangle$
- ledit canal de communication conventionnel (Lc) est un canal sécurisé

[0013] Un autre aspect de l'invention est relatif à un 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, par au moins un canal de communication quantique et un canal de communication conventionnel, comportant des moyens pour mettre en œuvre le procédé précédemment décrit.

[0014] Suivant des modes de réalisation préférés, l'invention comprend une ou plusieurs des caractéristiques suivantes qui peuvent être utilisées séparément ou en combinaison partielle entre elles ou en combinaison totale entre elles :

- lesdits premier et second participants appartiennent à une chaîne de participants, dans laquelle les deux participants aux extrémités respectivement mettent en œuvre ledit serveur, un participant amont étant apte à émettre un photon, et un participant aval étant apte à recevoir un photon et à mesurer son état.
- lesdits premier et second participants appartiennent à un anneau de participants, de sorte qu'un participant donné mette en œuvre ledit serveur et soit apte à émettre un photon, à recevoir un photon et à mesurer son état.
- 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.
- 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

[0015] L'utilisation de la communication quantique permet un excellent niveau de sécurité pour un surcoût en temps de calcul modeste. La sécurité est perpétuelle car ne repose pas sur la résolution de problème de calcul. Ainsi, il n'est pas possible d'enregistrer la communication pour briser le protocole plus tard, dans le futur. Le surcoût en temps de calcul pour un ET est peu important : quelques échanges de qubits.

[0016] Description des figures

[0017] Les figures 1a et 1b illustrent deux variantes d'un exemple d'architecture d'un dispositif pour le calcul multipartite sécurisé selon un mode de réalisation de l'invention.

[0018] La figure 2 illustre sous forme de tableau plusieurs exemples de degrés de liberté pour l'encodage de bits quantiques.

- 5 [0019] La figure 3 illustre un mode de réalisation du procédé, ou protocole, permettant le calcul sécurisé multipartite du « ET » logique dans lequel les étapes principales sont représentées.

[0020] Description de mises en œuvre de l'invention

- 10 [0021] Comme il a été vu en introduction, un des buts de l'invention est de permettre d'effectuer du calcul multipartite sécurisé entre un ensemble de participants.

[0022] Selon un mode de réalisation, ces participants peuvent être organisés selon une chaîne tel qu'illustré en figure 1b ou selon un anneau, tel qu'illustré en figure 1a.

- 15 [0023] Les N participants $C_1, C_2, C_3 \dots C_N$ peuvent communiquer avec leurs voisins immédiats uniquement et par au moins deux canaux de communication : un canal de communication quantique L_q et un canal de communication classique, ou conventionnel, L_c .

- 20 [0024] Ce canal de communication classique L_c peut être sécurisé. La sécurisation peut être réalisée par exemple grâce au canal de communication quantique qui permet l'échange de clé de chiffrement avec sécurité inconditionnelle. Il peut être de différentes natures, selon les modes de réalisation. Typiquement, il peut s'agir d'un canal de communication numérique conforme à la pile protocolaire TCP/IP. Il peut s'agir d'un canal filaire (Ethernet...) ou sans-fil (WiFi, cellulaire...).

- 25 [0025] Selon un autre mode de réalisation, le canal de communication classique L_c peut être de type « diffusion », ou *broadcast* selon la terminologie anglaise commune. Ainsi, tous les participants reçoivent les données de tous les participants. Toutefois, la sécurisation par échange de clés de chiffrement peut se faire de pair à pair, de sorte que le canal de communication classique L_c « physique » supporte un ensemble de canaux de communication « logique » pair-à-pair, connectant chacun des participants à ses voisins.

[0026] En pratique, les participants peuvent être de types variés : il peut s'agir d'ordinateurs connectés à un réseau de communication, ou de machines virtuelles déployées sur un serveur ou sur une ferme de serveurs, etc.

5 [0027] Le canal de communication quantique L_q peut être mis en œuvre de différentes façons également.

[0028] Selon un mode de réalisation, le canal de communication quantique L_q est prévu pour permettre la transmission de signaux lumineux permettant le transport de bits quantiques, généralement appelés « qubits ». Il s'agit typiquement d'une fibre optique.

10 [0029] Les bits quantiques peuvent être codés avec des photons selon un degré de liberté de ceux-ci. Par degré de liberté de photon, on entend une propriété physique décrite par la mécanique quantique et utilisable pour des communications quantiques. Des exemples de degrés de liberté des photons sont la phase, la différence de phase, la fréquence, la polarisation ou encore la localisation temporelle. Dans cette
15 description, on utilise le formalisme qui représente un état quantique sous la forme d'un vecteur $|\alpha\rangle$ dans un espace vectoriel hilbertien de dimension d . Le concept d'espace vectoriel hilbertien étend les méthodes de l'algèbre linéaire en généralisant les notions d'espace euclidien (comme le plan euclidien ou l'espace usuel de dimension 3) et d'espace hermitien à des espaces de dimension quelconque (finie ou
20 infinie). Un vecteur $|\alpha\rangle$ d'un espace vectoriel hilbertien de dimension d peut être décrit par l'intermédiaire d'une base de l'espace vectoriel hilbertien de dimension d .

[0030] La figure 2 donne des exemples de degrés de liberté de photon, dans un espace vectoriel hilbertien de dimension 2.

25 [0031] Un premier participant C_1 est prévu pour émettre les photons, qui vont être transmis de proche en proche le long de la chaîne.

[0032] Selon un mode de réalisation en chaîne, tel qu'illustré par la figure 1b, cette transmission est effectuée jusqu'au participant C_N le plus en aval de la chaîne qui peut être prévu pour effectuer des mesures des états des photons et ainsi lire les états des qubits associés. Ce participant C_N est prévu pour communiquer avec le participant C_1
30 par un canal de communication sécurisé L_s .

[0033] Selon un mode de réalisation en anneau, tel qu'illustré par la figure 1a, la transmission est effectuée jusqu'au premier participant C_1 . Comme on le verra, ce premier participant joue donc les rôles d'émetteur et récepteur.

5 [0034] Le premier participant C_1 peut être appelé « émetteur ». De façon pratique, il peut être mis en œuvre de différentes façons. Par exemple, il peut comporter un laser apte à générer des photons et un modulateur initial apte à moduler un degré de liberté d'un photon généré.

10 [0035] Selon un mode de réalisation, on effectue une modulation sur l'intervalle de temps pour lequel on veut générer un photon, dont l'énergie globale correspond à un quantum d'énergie du photon.

[0036] Selon un autre mode de réalisation, on utilise la différence de phase comme degré de liberté pour encoder les qubits. Aussi, l'émetteur C_1 génère les photons en effectuant une modulation selon deux pics, chaque dans un demi-intervalle de l'intervalle correspondant au photon que l'on souhaite générer. L'énergie globale de
15 cette modulation étant, par configuration, égale au quantum d'énergie d'un photon, chaque photon ainsi généré est une superposition d'un photon entre ces deux demi-intervalles.

[0037] Le laser peut être prévu avec une longueur d'onde de 1550 nm qui correspond à l'atténuation minimale dans les fibres optiques communément utilisés en
20 télécommunication.

[0038] Les $N-2$ participants en dehors de participants les plus extrêmes C_1 , C_N sont des modulateurs. Ils ne sont pas prévus pour émettre des photons mais uniquement pour moduler un champ électromagnétique dans lequel passent les photons afin de modifier un degré de liberté de ceux-ci.

25 [0039] Selon un mode de réalisation (figure 1b), le participant C_N le plus en aval de la chaîne peut être appelé récepteur. Selon un autre mode de réalisation (figure 1a), le participant C_1 est à la fois émetteur et récepteur.

[0040] Le participant récepteur, C_1 , C_N , peut comprendre un détecteur de photons uniques. Différents mécanismes existent dans l'état de la technique. On peut par
30 exemple citer par exemple les détecteurs basés sur des photodiodes à avalanches (APD pour « *Avalanche PhotoDiode* » en anglais).

[0041] Il est possible de mettre en place des canaux de communication bidirectionnels, de sorte que les bits quantiques (ou qubits) puissent être émis dans les deux sens de la chaîne. Dans un tel cas, l'émetteur C_1 peut également être un récepteur, c'est-à-dire disposer des moyens de mesure (détecteur de photon unique).

- 5 [0042] En fonction du type de degré de liberté, différents types de modulateurs et de détecteurs peuvent être utilisés par les participants $C_1, C_2, C_3 \dots C_N$.

[0043] Lorsque le degré de liberté des photons pour encoder les bits quantiques est la phase, les modulateurs peuvent être des modulateurs de phase. Par exemple, le modèle LN53S-FC ou LN65S-FC commercialisé par la société Thorlabs peut être
10 utilisé.

[0044] Lorsque le degré de liberté des photons pour encoder les bits quantiques est la polarisation des photons, les modulateurs peuvent être des modulateurs de polarisation. Par exemple, un modèle de la série de produits PSC-LN series commercialisé par la société iXblue Photonics peut être utilisé.

- 15 [0045] Lorsque le degré de liberté des photons pour encoder les bits quantiques est la localisation temporelle des photons, les modulateurs peuvent comprendre chacun un nombre d de lignes à retard et un nombre $2d$ de lames séparatrices, où d représente la dimension de l'espace vectoriel hilbertien de représentation des états quantiques. La superposition de localisations temporelles à réaliser pour créer une
20 base incompatible peut être obtenue en programmant les lames séparatrices.

[0046] Le même principe peut être utilisé pour la détection par le récepteur C_N . Celui-ci peut ne disposer que d'un seul détecteur de photon unique, en aval d'un dispositif similaire permettant de séparer les faisceaux et retarder les faisceaux différemment pour qu'après recombinaison des faisceaux, l'instant de la détection du photon
25 permette de déterminer la localisation temporelle de ce photon.

[0047] Cette architecture peut être utilisée pour le calcul multipartite sécurisé entre les participants.

- [0048] Il est connu que tout calcul portant sur des données binaires peut être réduit en combinaison d'opérateurs logiques universels. Ces opérateurs logiques universelles
30 sont « NON ET » (ou « NAND » pour « Not And » en anglais) et « NON OU » (ou NOR » pour « Not Or » en anglais).

[0049] La réalisation d'un opérateur « NON » logique ne pose pas de problème particulier de sécurisation puisqu'il s'agit d'un opérateur local. Par contre, les opérateurs logiques ET et OU peuvent impliquer plusieurs participants et impliquent donc un problème de sécurité pour permettre d'obtenir le résultat de l'opération sans qu'aucun des participants n'ait connaissance de la valeur détenue par les autres participants.

[0050] Il est plus commun d'utiliser l'opérateur « NON ET ». Aussi, l'invention porte sur le sous-problème particulier du calcul d'un ET logique entre plusieurs participants. Plus spécifiquement, elle porte sur le calcul d'un ET logique entre deux participants, étant entendu que le passage à plus de deux participants revient à combiner plusieurs opérateurs « ET ».

[0051] Dans la suite on notera $x_i \wedge x_j$ l'opération du « et » logique entre les bits x_i et x_j .

[0052] L'invention vise donc à calculer un ET logique entre des bits x_i et x_j détenus par deux participants, respectivement C_i et C_j avec $1 < i < N$ et $1 < j < N$ et, bien sûr, $i \neq j$, avec pour contraintes que

- Le participant C_i ne doit pas pouvoir apprendre davantage d'information que les valeurs du bit x_i et de $x_i \wedge x_j$ (*a fortiori*, il ne doit pas pouvoir connaître la valeur du bit x_j),
- le participant C_j ne doit pas pouvoir apprendre davantage d'information que les valeurs du bit x_j et de $x_i \wedge x_j$ (*a fortiori*, il ne doit pas pouvoir connaître la valeur du bit x_i), et
- aucune autre partie au calcul ne doit pouvoir connaître ni x_i ni x_j .

[0053] On appellera ces deux bits x_i et x_j , « bits choisis ».

[0054] Notamment, le procédé selon l'invention fait intervenir un tiers-partie, appelé serveur dans la suite. Ce serveur peut connaître le résultat final $x_i \wedge x_j$ mais ne doit pas connaître ni la valeur de x_i ni la valeur de x_j . Ce serveur a aussi pour fonction de créer et émettre un photon dans un état donné, et peut donc être mise en œuvre, au moins partiellement, par l'émetteur C_1 .

[0055] Selon un premier mode de réalisation basé sur une architecture en anneau (figure 1a), le participant C_1 est également récepteur, de sorte que le serveur dispose directement de toutes les informations en tant qu'émetteur et récepteur.

5 [0056] Selon un second mode de réalisation basé sur une architecture en chaîne (figure 1b), le serveur peut disposer des informations reçues par le récepteur C_N via un canal de communication sécurisé L_S . En quelque sorte, le serveur est alors mis en œuvre par le couple C_1/C_N formé par les deux participants situés aux extrémités de la chaîne de participants.

10 [0057] D'autres mises en œuvre sont encore envisageables. Dans la suite, par simplicité, on attribuera la référence C_1 au serveur.

[0058] D'une façon très générale, ce calcul repose sur corrélation, dite « magique », entre trois variables binaires α, β, γ déterminées chacune, respectivement, par les deux participants C_i, C_j et le serveur C_1 et correspondant à un « et » logique entre deux bits b_1, b_2 détenus par les participants de sorte que $\alpha + \beta + \gamma = b_1 \wedge b_2$. En outre, les
15 distribution marginales des trois variables α, β, γ doivent répondre au critère d'uniformité : lorsqu'on le regarde individuellement, chaque bit peut prendre pour valeur 0 ou 1 de façon équiprobable. Dans la suite, on appellera ces trois variables, « variables de corrélation »

[0059] Une première phase consiste à établir une corrélation magique correspondant
20 au « et » logique entre deux bits aléatoires et en utilisant le canal de communication quantique L_q et le calcul quantique. A l'issue de cette première phase, on détermine donc les trois variables α, β, γ formant la corrélation magique.

[0060] Une seconde phase consiste à utiliser cette corrélation magique (α, β, γ) pour calculer le « et » logique entre les deux bits choisis x_i, x_j , c'est-à-dire le résultat final
25 recherché, en utilisant un canal de communication classique sécurisé, L_c .

[0061] Dans la première phase, les participants C_i et C_j vont appliquer des portes quantiques, U et V , à des qubits d'entrées pour générer des qubits de sortie.

[0062] La porte quantique V transforme l'état (ou qubit) d'un photon en un état orthogonal, dans une base orthonormée quelconque. La porte quantique U
30 correspond à une racine carrée de la transformation effectuée par la porte quantique V .

[0063] Sur la sphère de Bloch, ces opérations reviennent donc à dire toute la partie quantique est définie à une rotation près.

[0064] Le qubit est généré par le serveur C₁, dans un premier état, dans une base orthonormée.

- 5 [0065] Selon un mode de réalisation, ce premier état est noté $|+\rangle$. Cette notation est toutefois arbitraire, dans la mesure où il suffit, selon l'invention, de disposer de deux états orthogonaux quelconque, mais permet la clarté de l'exposé.

[0066] On notera dans la suite $|0\rangle$ et $|1\rangle$ deux états orthogonaux (c'est-à-dire parfaitement distinguables) parmi les degrés de liberté quantiques du photon émis
10 dans cette base orthonormée.

[0067] On note $|+\rangle$ et $|-\rangle$ deux états formés par la superposition de ces deux qubits orthogonaux. On peut écrire :

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

[0068] On peut également écrire

15 $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

[0069] La porte V est une porte de Pauli-Z qui équivaut à une rotation autour de l'axe Z de la sphère de Bloch par π radians. Elle peut être représentée par la matrice Pauli-Z :

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- 20 [0070] Autrement dit, une telle porte V transforme l'état $|+\rangle$ en l'état $|-\rangle$, et, réciproquement l'état $|-\rangle$ en l'état $|+\rangle$

[0071] Comme dit précédemment, la porte U est une racine carrée de la porte V. Selon un mode de réalisation, il peut s'agir d'une rotation autour de l'axe Z de la sphère de Bloch par $\pi/2$ radians. Autrement dit, en appliquant deux fois la porte U, on obtient
25 l'équivalent d'une porte V.

[0072] Dans un mode de réalisation consistant à encoder l'information sur la différence de phases, le qubit $|+\rangle$ peut correspondre à un photon en superposition uniforme sur

ces deux demi-intervalles. Dans ce cas, les rotations U et V correspondent à un déphasage du 2e demi-intervalle de π et $\pi/2$, respectivement.

[0073] Dans tous les cas décrits plus haut et d'une façon générale, les implémentations sont réalisées en appliquant une modulation adéquate.

- 5 [0074] On peut également citer l'article de Marco Clementi, Anna Pappa, Andreas Eckstein, Ian Walmsley, Elham Kashefi, et al., « *Classical multiparty computation using quantum resources* » in Physical Review A, American Physical Society, 2017, 96 (6), pp.062317. (10.1103/PhysRevA.96.062317). (hal-02164423). Dans cet article, les états $|+\rangle$ et $|-\rangle$ sont implémentés en utilisant des polarisations verticales et
- 10 horizontales. Les rotations U et V sont implémentées avec des lames à demi-retard ou « *half-wave plates* » en anglais.

- [0075] La figure 3 illustre un mode de réalisation du procédé, ou protocole, permettant le calcul sécurisé multipartite du « ET » logique dans lequel les étapes principales sont représentées. La figure 3 est un organigramme purement illustratif et l'enchaînement
- 15 des étapes peut se comprendre sans le recours à cet organigramme, de même que d'autres enchaînements, ou d'autres divisions en étapes, sont possibles et accessibles à l'homme du métier.

- [0076] Dans cet exemple, on suppose que deux participants C_i et C_j disposent, à un moment donné, de deux bits, respectivement x_i et x_j dont on souhaite calculer le « et »
- 20 logique.

- [0077] Dans une étape S1, chaque participant C_i , C_j détermine, par exemple de façon aléatoire, une valeur pour sa variable de corrélation respective α , β destiné à former une corrélation magique. Chaque participant détermine également la valeur de deux autres bits, respectivement p et q , également de façon aléatoire. Ces 4 bits aléatoires
- 25 α , β , p , q peuvent être déterminés dans cette préliminaire S1 ou bien plus tard, avant que ces bits ne soient nécessaires dans les calculs exigées par les étapes subséquentes du protocole.

[0078] Dans une étape S2, le serveur C_1 prépare et envoie un photon dans un état de superposition d'états orthogonaux dans une base orthonormée donnée.

- 30 [0079] Selon un mode de réalisation, le serveur C_1 prépare et émet un état $|+\rangle$ qui est une superposition uniforme de deux états $|0\rangle$ et $|1\rangle$, au premier participant C_i . Selon

un autre mode de réalisation, le serveur C_1 prépare et émet un état $|->$. Comme dit plus haut, l'état initial est en soi indifférent, il est uniquement important que la transformation V transforme cet état en un état orthogonal.

[0080] Il est à noter que les deux participants sont interchangeables, puisque le « et »
 5 logique est une opération commutative. Aussi les termes de « premier » et « second » participants permettent uniquement de les distinguer, pour la clarté de la description, sans établir d'ordre ou de hiérarchie entre eux.

[0081] Dans une étape S3, le premier participant C_i reçoit cet état du photon et y applique une première transformation quantique formée de la succession de portes
 10 quantiques effectuant l'une une rotation d'angle π autour de l'axe Z et l'autre une rotation d'angle $\pi/2$ autour de l'axe Z, cette transformation dépendant des deux bits aléatoires déterminés par ce premier participants, c'est-à-dire α et p .

[0082] Plus précisément, cette première transformation peut s'écrire $V^\alpha U^p$.

[0083] Cette notation T^e signifie que si l'exposant e est égal à 1, on applique la
 15 transformation T et s'il est égal à 0, on ne l'applique pas.

[0084] Le premier participant C_i peut alors envoyer le qubit résultat de cette transformation dans le canal de communication quantique L_q à destination du second participant C_j .

[0085] Dans une étape S4, le second participant C_j effectue une transformation
 20 similaire mais basée sur les deux bits aléatoires dont il dispose : β et q . Cette seconde transformation peut s'écrire $V^\beta U^q$. Le qubit résultat de cette transformation peut alors être envoyé dans le canal de communication quantique L_q à destination du serveur C_1 .

[0086] Dans une étape S5, le serveur C_1 effectue une troisième transformation qui peut s'écrire $(U^*)^{p+q}$, où U^* est la transformation inverse de U .

[0087] Selon l'invention, la valeur $p+q$ est transmise au serveur C_1 , sans communiquer
 25 les valeurs individuelles de p et de q .

[0088] Selon un mode préférentiel de réalisation de l'invention, on sécurise le protocole en partageant secrètement un bit r entre les deux participants C_i et C_j afin d'encoder la communication des bits p et q vers le serveur C_1 . Aussi, lors de l'étape
 30 S1 (qui peut se prolonger jusqu'à cette étape S4),

- le participant C_i envoie au serveur C_1 le bit $t_1=p+r$ sur un canal sécurisé ;
- le participant C_j envoie au serveur C_1 le bit $t_2=q+r$ sur un canal sécurisé.

[0089] D'autres méthodes sécurisées peuvent permettre de transmettre la valeur de t_1+t_2 au serveur C_1 , comme il sera vu plus loin.

- 5 [0090] Le signe « + » désigne l'addition binaire. Dans la mesure où l'on ne s'intéresse qu'à un unique bit, cette opération équivaut à un « ou exclusif »

[0091] Le serveur C_1 peut alors calculer la troisième transformation $(U^*)^{t_1+t_2}$.

[0092] Après cette transformation, l'état du qubit vaut : $(U^*)^{t_1+t_2} \cdot V^\beta U^q V^\alpha U^p |+\rangle$

- 10 [0093] Cette expression peut se simplifier, en fonction des différentes valeurs que peuvent prendre les bits aléatoires p et q (du fait de la commutativité des ports U , V et U^*) en:

- $V^\beta V^\alpha |+\rangle$ si $p=0$ et $q=0$
- $V^\beta V^\alpha |+\rangle$ si $p=0$ et $q=1$
- $V^\beta V^\alpha |+\rangle$ si $p=1$ et $q=0$
- 15 - $V^\beta V^\alpha |-\rangle$ si $p=1$ et $q=1$

[0094] On peut ici rappeler que la porte V revient à intervertir les états $|+\rangle$ et $|-\rangle$, de sorte que le nombre d'interversions dépend de la valeur des valeurs de corrélations α et β .

[0095] On peut donc écrire la table de vérité suivante :

α	β	$V^\beta V^\alpha +\rangle$	$\alpha + \beta$
0	0	$ +\rangle$	0
0	1	$ -\rangle$	1
1	0	$ -\rangle$	1
1	1	$ +\rangle$	0

- 20 [0096] Le serveur C_1 mesure alors le qubit reçu dans la base $\{|+\rangle, |-\rangle\}$, et détermine la valeur de sa variable de corrélation γ de la façon suivante :

- si la mesure vaut $|+\rangle$, alors $\gamma=0$

- si la mesure vaut $|->$, alors $\gamma=1$

[0097] Dès lors, on peut remarquer que $\gamma = \alpha + \beta + (p \wedge q)$.

[0098] Autrement dit, $\alpha + \beta + \gamma = p \wedge q$

5 [0099] Cette expression est celle d'une corrélation magique entre les trois variables de corrélation α , β , γ , dont la somme binaire permet de calculer le « et » logique des deux bits p et q .

[0100] Cette corrélation une fois établie, elle permet de calculer, dans une seconde phase, le « et » logique pour d'autres bits, et notamment les bits choisis x_i , x_j .

10 [0101] On peut remarquer que cette première phase est indépendante des bits choisis x_i , x_j .

[0102] Selon un mode de réalisation, les premières étapes $S1$, $S2$, $S3$, $S4$, $S5$ constituant une première phase, peuvent être effectués en amont du moment où les participants C_i et C_j disposent des bits respectifs x_i , x_j dont on souhaite calculer le « et » logique. Autrement dit, cette première phase peut faire l'objet d'un précalcul, de sorte à alléger les calculs à effectuer entre le moment où les bits x_i et x_j sont connus et la mise à disposition du résultat, $x_i \wedge x_j$.

15

[0103] Ce mode de réalisation permet des gains de performance et de sécurité conséquents.

20 [0104] Dans une étape $S6$, les participants C_i , C_j s'échange une valeur dépendant de la somme entre le bit aléatoire, respectivement p , q , et le bit choisi, respectivement x_i , x_j .

[0105] Par exemple,

- le premier participant C_i calcule $u1 = p + x_i$ et l'envoie au second participant C_j .
- le second participant C_j calcule $u2 = q + x_j$ et l'envoie au premier participant C_i .

25 [0106] Dans une étape $S7$, les deux participants C_i , C_j et le serveur C_1 fournissent chacun séparément une valeur, respectivement a , b , c , de sorte que $a+b+c = x_i \wedge x_j$.

[0107] Plus précisément,

- le premier participant calcule et fournit $a = \alpha + x_i \wedge u2$

- le second participant calcule et fournit $b = \beta + x_j \wedge u_1 + u_1 \wedge u_2$
- le serveur fournit $c = \gamma$

[0108] Les valeurs de u_1 et u_2 sont aléatoires et sont partagées préalablement entre les participants. Ce partage peut être effectué par le canal de communication classique L_c sécurisé.

[0109] On peut alors vérifier que $a+b+c = x_i \wedge x_j$, soit le résultat recherché.

[0110] En effet, $a+b+c = \alpha + x_i \wedge u_2 + \beta + x_j \wedge u_1 + u_1 \wedge u_2 + \gamma$

$$= \alpha + x_i \wedge (q+x_j) + \beta + x_j \wedge (p+x_i) + (p+x_i) \wedge (q+x_j) + \gamma$$

$$= \alpha + \beta + \gamma + x_i \wedge q + x_i \wedge x_j + x_j \wedge p + x_j \wedge x_i + p \wedge q + p \wedge x_j + x_j \wedge q + x_i \wedge x_j$$

$$= p \wedge q + x_i \wedge q + x_i \wedge x_j + x_j \wedge p + x_j \wedge x_i + p \wedge q + p \wedge x_j + x_j \wedge q + x_i \wedge x_j$$

[0111] Les termes identiques s'annulent deux à deux puisqu'il s'agit d'additions binaires sur un unique bit (sans retenue), donc équivalentes à un « ou » exclusif. Dès lors, cette expression peut se simplifier, effectivement, en $a+b+c = x_i \wedge x_j$

[0112] On peut ainsi donc obtenir, par cette simple somme binaire de termes indépendants, la valeur du « et » logique entre les bits x_i et x_j choisis respectivement par le premier participant C_i , et le second participant C_j sans que leur valeur ne soit connue par une autre entité que celui qui l'a choisi. Ainsi, donc, on assure bien la propriété recherchée de calcul multipartite sécurisé.

[0113] En outre, dans le cas où la première phase (quantique) est effectuée en avance, la phase de calcul effectif de ce « et logique » (seconde phase) est très efficace puisque ne comporte qu'un double échange entre les deux participants (étape S6), des additions de bit et la mise à disposition des valeurs a , b , c qu'il suffit de sommer pour obtenir le résultat.

[0114] Selon un mode de réalisation de l'invention, la sécurité du procédé peut être renforcée de différentes manières.

[0115] Le canal de communication conventionnel L_c peut notamment être sécurisé selon des moyens conventionnels ou quantiques.

[0116] Ainsi que précédemment décrit, un bit r peut être partagé secrètement entre les participants et le serveur. Ce bit peut être partagé en utilisant une distribution de clé quantique, par exemple.

5 [0117] Les mécanismes de sécurisation par clés quantiques sont connus en soi, et il existe différents dispositifs commerciaux pour réaliser cette étape. On peut notamment citer les dispositifs les dispositifs « Cerberis3 QKD System » commercialisé par la société ID Quantique, « QKD system » commercialisé par la société Toshiba, ou « Quantum Key Distribution (QKD) » de la société Quintessence Labs.

10 [0118] On peut également citer la demande de brevet FR1909839 intitulée « Procédé de transmission sécurisée de séquences d'états quantiques entre plusieurs participants en ligne sur un canal de communication quantique ».

[0119] Egalement, un bit différent, r_1, r_2, r_3 peut être partagé entre chaque couple de l'ensemble constitué par les participants et le serveur. Ainsi, le premier participant C_i
 15 et le serveur C_1 s'échangent un premier bit r_1 ; le second participant C_j et le serveur C_1 s'échangent un deuxième bit r_2 , et les premier et second participant s'échangent un troisième bit r_3 .

[0120] Lors de la phase d'initialisation S_1 , on peut alors avoir :

- Le premier participant C_i envoie au serveur C_1 la valeur $t_1' = p + r_1 + r_3$
- 20 - Le second participant C_j envoie au serveur C_1 la valeur $t_2' = q + r_2 + r_3$
- Le serveur C_1 peut alors former les valeurs $t_1 = t_1' + r_1$ et $t_2 = t_2' + r_2$

[0121] Le calcul d'un « et » logique binaire peut être appliqué pour résoudre quel problème de calcul distribué entre les deux participants C_i, C_j .

[0122] Dans le cas d'une application à un mécanisme d'enchères, on suppose que
 25 chacun des participants C_i, C_j détient deux nombres, respectivement x_i, x_j , de n bits chacun et représentant une valeur d'enchère : $x_{ij} \in \{0, 1\}^n$

[0123] Pour deux entrées binaires a, b , on définit la fonction $f(a, b) = 1 + a \wedge (1 + b)$. Cette fonction prend pour valeur 1 si $b \geq a$, et 0 sinon.

[0124] Cette fonction peut se calculer, pour un bit, selon le procédé précédemment décrit. En effet, en remarquant que $1+b$ revient à un NON logique, cette fonction se calcule donc comme $f(a,b)=\text{NON}(a \text{ et } (\text{NON } b))$

5 [0125] On peut alors déterminer le vainqueur entre deux offres de l'enchère en effectuant la comparaison des bits des deux valeurs x_i , x_j bit par bit en partant du bit de poids le plus fort, et en utilisant cette fonction f de comparaison pour chaque bit.

[0126] Si f renvoie 0 pour un bit, alors $x_i > x_j$ et C_i emporte l'enchère sur C_j ; sinon $x_j \geq x_i$ et l'enchère est soit emportée par C_j soit les deux participants ont fait la même offre.

10 [0127] En faisant ce calcul dans les deux sens, c'est-à-dire également en intervertissant x_i et x_j pour le second calcul, on peut déterminer, dans toutes les situations, lequel des participants a emporté l'enchère.