

Client simplifié et architectures associées pour la délégation de calculs quantiques à un serveur quantique

[0001] DOMAINE DE L'INVENTION

- 5 [0002] La présente invention est relative à l'informatique quantique en général, et en particulier à la délégation d'un calcul quantique d'un client vers un serveur distant.

[0003] CONTEXTE DE L'INVENTION

- 10 [0004] L'informatique quantique (« *quantum computing* » en anglais) est un domaine qui s'est beaucoup développé au fil de la dernière décennie, du fait de ses nombreuses promesses. Elle utilise les propriétés quantiques de la matière, telle que la superposition et l'intrication afin d'effectuer des opérations sur des données. À la différence d'un ordinateur classique travaillant sur des données binaires (codées sur des bits, valant 0 ou 1), le calculateur quantique travaille sur des « qubits » dont l'état quantique peut posséder une infinité de valeurs.

- 15 [0005] Néanmoins, tout comme le calcul haute-performance (HPC pour « *High Performance Computing* », en anglais), l'informatique quantique nécessite le déploiement de dispositifs spécifiques pour manipuler ces propriétés quantiques de la matière. Il en résulte que les calculateurs, ou ordinateurs, quantiques devraient rester des systèmes coûteux et qu'une évolution envisagée repose sur un paradigme
20 client/serveur.

[0006] Selon ce modèle, des clients peuvent déléguer tout ou partie des calculs quantiques à des serveurs, de sorte que les ressources quantiques les plus coûteuses peuvent ainsi être mutualisées pour plusieurs clients.

- 25 [0007] Il est également envisagé que de tels serveurs soient accessibles via des réseaux de télécommunication de vaste échelle, tels Internet, sous la forme d'un service : « quantum as a Service », QaaS (ou « calcul quantique à la demande » selon une traduction française). Ainsi, le serveur quantique peut être accessible via une architecture d'informatique en nuage, ou « *cloud* ».

[0008] Les clients souhaitant déléguer un calcul quantique auprès de ce serveur doivent donc établir un canal de communication (qui peut être, selon différentes modalités, quantique et/ou classique) avec ce serveur.

5 [0009] Des mécanismes de sécurisation ont été proposés afin d'éviter que des tiers puissent prendre connaissance des calculs effectués. Également, des mécanismes de « calcul aveugle » (ou « *blind computing* » en anglais) ont été proposés afin d'éviter que le serveur lui-même (qui peut être corrompu) puisse connaître les calculs effectués : dès lors, le serveur effectue des calculs sans en connaître ni les opérations ni le résultat ni même les valeurs d'entrées. Il est ainsi possible de déléguer à un
10 serveur des calculs sur des données sans communiquer ces données, par exemple dans le cas où elles ne pourraient pas être légalement rendues publiques (données médicales, données d'entraînement pour l'apprentissage machine, etc.). Il est aussi possible de se prémunir d'une éventuelle corruption du serveur.

15 [0010] Également, des mécanismes de calcul vérifiable ont été proposés afin de permettre au client de s'assurer que le serveur effectue bien les calculs demandés.

[0011] Ces propositions sont notamment décrites dans « *Secure Assisted Quantum Computation* » d'Andrew M. Childs, in *Quantum Information and Computation* 5, 456 (2005), <https://arxiv.org/abs/quant-ph/0111046> ou « *Universal Blind Quantum Computation* » d'Anne Broadbent, Joseph Fitzsimmons et Elham Kashefi, in
20 *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009)*, pp. 517-526, <https://arxiv.org/abs/0807.4154v3>

[0012] D'une façon générale, ces mécanismes de calculs délégués aveugles reposent sur un mécanisme de calcul basé sur la mesure. Ce mécanisme a été décrit dans une série d'articles fondateurs, dont « *Measurement-based quantum computation* » de
25 Briegel, H. J., Browne, D. E., Dür, W., Raussendorf, R. & Van den Nest, M. in *Nature Physics* 5, 19 (2009), arXiv:0910.1116v2, ou « *Unconditionally verifiable blind computation* » de Joseph F. Fitzsimmons et Elham Kashefi in *Phys. Rev. A* 96, 012203 (2017), <https://arxiv.org/abs/1203.5217> qui présente en outre comment obtenir la propriété de vérifiabilité qui permet de repérer un serveur cherchant à modifier le calcul
30 délégué par le client.

[0013] Le calcul basé sur la mesure, MBQC (pour « *Measurement-Based Quantum Computation* » en anglais), repose sur une séquence de mesures, dans un ordre précis, d'un qubit précis dans une ressource d'états quantiques intriqués prédéfinis.

[0014] La communication entre les clients et le serveur peut se baser sur des schémas
5 types comme, par exemple une procédure de type « préparer et envoyer » ou une procédure de type « recevoir et mesurer ».

[0015] Dans les protocoles de type *préparer-et-envoyer*, le client génère des états quantiques et les envoie au serveur qui est capable de les enregistrer pour les utiliser dans un calcul.

10 [0016] Dans les protocoles de type *recevoir-et-mesurer*, le client reçoit un état quantique du serveur et le mesure dans une base de mesure arbitraire. Le serveur ayant préalablement intriqué l'état quantique envoyé au client avec un état de sa mémoire interne, la mesure par le client provoque une préparation à distance de l'état dans la mémoire du serveur.

15 [0017] Quoique le paradigme du calcul quantique délégué permet (et a même pour but) de prévoir des clients nettement plus légers que les serveurs, ces deux types de procédure nécessitent que le client dispose, dans le premier cas, d'un émetteur de qubits (par exemple une source de photons uniques) pour coder les états quantiques, et dans le deuxième cas, d'un dispositif pour mesurer les qubits reçus du serveur (par
20 exemple un détecteur de photons uniques).

[0018] De tels dispositifs (sources et détecteurs) sont généralement des équipements complexes et coûteux. Ces coûts forment un frein au développement de l'informatique quantique, et en particulier, à un vaste déploiement de clients adaptés à la délégation de calculs quantiques vers un serveur, par exemple déployé sur un nuage.

25 [0019] D'autres mécanismes ont été proposés, comme par exemple Qin Li et al., « *Blind quantum computation for a user who only performs single-qubit gates* ». Toutefois, il peut être démontré qu'un tel mécanisme est vulnérable à certaines attaques et n'offre donc pas la caractéristique de vérifiabilité.

[0020] RESUME DE L'INVENTION

30 [0021] Un objectif de la présente invention est de fournir une solution palliant au moins partiellement les inconvénients précités.

[0022] Plus particulièrement, selon des modes de réalisation, elle vise à simplifier l'architecture des clients, afin d'en abaisser le coût et permettre, ainsi, un plus grand déploiement des clients quantiques pouvant déléguer des calculs quantiques à des serveurs, notamment accessibles via des réseaux de télécommunication quantiques à grande distance, tout en conservant les caractéristiques importantes des architectures de délégations citées ci-dessus, notamment le calcul aveugle et sécurisé et la vérifiabilité du calcul délégué.

[0023] À cette fin, selon un premier aspect, la présente invention peut être mise en œuvre par un procédé de délégation d'un calcul quantique par au moins un client vers un serveur, comprenant au moins :

- une première étape comprenant la transmission au serveur d'une description d'intrications à effectuer dans une mémoire quantique ;
- une deuxième étape comprenant l'émission d'une séquence d'états quantiques par une source, distincte de ce serveur, vers ledit au moins un client ;
- une troisième étape comprenant une modification d'un état quantique de ladite séquence ;
- une quatrième étape comprenant la transmission de ladite séquence vers ledit serveur ;
- une cinquième étape comprenant l'application d'une séquence de mesures selon une base donnée, au sein de ladite mémoire quantique dont le contenu a été intriqué selon ladite description, et la transmission du résultat de chaque mesure audit au moins un client.

[0024] 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 :

- les états quantiques fournis par la source sont une superposition d'états orthogonaux, et la modification effectuée par le client est de la forme $Z^{\theta+c.\pi}$ dans laquelle Z est une porte de Pauli selon l'axe Z, θ est choisi de façon aléatoire parmi une liste $\{0; \pi/4; \pi/2; 3\pi/4\}$ et c est choisi aléatoirement parmi les valeurs 0 et 1 ;

- 5 - les états quantiques fournis par la source sont une superposition d'états orthogonaux, et le procédé comporte en outre une étape de détermination d'un sous-ensemble de qubits pièges et dans la troisième étape comprend une modification de qubits voisins desdits qubits pièges selon ladite description d'intrications, de la forme $X^d H$, dans laquelle H est la transformation de Hadamard, X est une porte de Pauli selon l'axe X et d est choisi parmi les valeurs 0 et 1, et le client met en œuvre une étape de comparaison entre un résultat d'une mesure d'un desdits qubits pièges avec un résultat attendu pour ledit qubit piège, permettant de déterminer une honnêteté dudit serveur ;
- 10 - chacun des au moins un client ne peut modifier qu'une partie des états quantiques qui lui est alloué, et transmet ladite séquence vers un client subséquent d'une chaîne de clients le liant au serveur ;
- cette partie des états quantiques peut être déterminée par une allocation d'une fenêtre temporelle ;
- 15 - plusieurs clients peuvent modifier successivement un même état quantique de ladite séquence.

[0025] Selon un autre aspect, l'invention peut également être mise en œuvre par un système pour la délégation d'un calcul quantique d'au moins un client (10) vers un serveur (20), comportant :

- 20 - au moins une source adaptée pour émettre une séquence d'états quantiques,
- et dans lequel ledit serveur comporte un dispositif de mesure d'états quantiques reçus, et au moins un composant quantique permettant de réaliser ledit calcul quantique ; et
- ledit au moins un client comportant une interface d'entrée pour recevoir ladite
- 25 séquence, un dispositif de transformation adapté pour modifier un état quantique de ladite séquence et une interface de sortie pour transmettre ladite séquence vers ledit dispositif de mesure.

[0026] Suivant des modes de réalisation préférés, le système selon l'invention comprend une ou plusieurs des caractéristiques suivantes qui peuvent être utilisées

30 séparément ou en combinaison partielle entre elles ou en combinaison totale entre elles :

- ce dispositif de transformation comporte un premier dispositif pour appliquer une première transformation visant à préparer des états quantiques pour effectuer un calcul quantique aveugle, et un second dispositif pour appliquer une seconde transformation visant à préparer des états quantiques pour vérifier une honnêteté dudit serveur ;
- ledit premier équipement et ledit second équipement sont répartis en des localisations physiques distinctes ;
- une pluralité de clients sont connectés audit serveur par une ligne de communication unique en formant une chaîne, de sorte que lesdits états quantiques sont transmis de proche en proche depuis ladite source vers ledit dispositif de mesure ;
- chacun desdits clients est configuré pour ne pouvoir modifier que la partie des états quantiques qui lui est alloué ;
- les états quantiques sont des photons et le dispositif de transformation est un modulateur optique ;
- la source est adaptée pour fournir des états quantiques sous la forme d'une superposition d'états orthogonaux, et le dispositif de transformation est adapté pour effectuer une modification de la forme $Z^{\theta+c.\pi}$ dans laquelle Z est une porte de Pauli selon l'axe Z, θ est choisi de façon aléatoire parmi une liste $\{0; \pi/4; \pi/2; 3\pi/4\}$ et c est choisi aléatoirement parmi les valeurs 0 et 1.

[0027] D'une façon générale, un système selon l'invention est configuré pour mettre en œuvre le procédé précédemment défini, selon ses différents modes de réalisation.

[0028] D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui suit d'un mode de réalisation préféré de l'invention, donnée à titre d'exemple et en référence aux dessins annexés

[0029] BREVE DESCRIPTION DES FIGURES

[0030] Les dessins annexés illustrent l'invention :

[0031] La figure 1 représente schématiquement un exemple de système selon un mode de réalisation de l'invention.

[0032] La figure 2 illustre un organigramme d'un procédé selon un mode de réalisation de l'invention

Les figures 3a, 3b illustrent des modes de réalisation avec une pluralité de clients.

[0033] DESCRIPTION DETAILLÉE DE MODES DE RÉALISATION DE L'INVENTION

5 [0034] L'invention repose notamment sur un principe que le client ne dispose que d'un moyen de transformer l'information quantique mais ni de moyen de générer, ni de mesurer celle-ci, dans la mesure où la génération et la mesure sont des étapes nécessitant des composants plus complexes et coûteux.

10 [0035] Ces étapes, ou fonctions, sont déportées vers un serveur et une source, ce qui permet de mutualiser les ressources puisqu'un grand nombre de clients peut exister et se connecter à un serveur unique et à une source unique. En outre, cela permet d'abaisser le coût des clients et donc de permettre un plus large accès aux technologies quantiques via des serveurs accessibles via le « cloud » (informatique en nuage).

15 [0036] Également, il devient possible d'alléger et de simplifier l'architecture générale en permettant de raccorder une pluralité de clients à un même serveur et à une même source quantique au moyen d'une ligne de communication unique.

20 [0037] Ainsi qu'illustré sur la Figure 1, un client 10 possède une interface d'entrée 11 adaptée à la réception d'une séquence d'états quantiques, un dispositif de transformation 12 adapté à la modification des états quantiques reçus, et une interface de sortie 13 adaptée à l'émission des états quantiques (éventuellement modifiés par le dispositif de transformation 12).

25 [0038] Le client 10 peut ne posséder que ces trois composants comme composants quantiques. Il peut en outre disposer, bien sûr, de composants classiques (au sens de « non quantiques »), notamment afin de piloter le dispositif de transformation de façon connue en soi.

[0039] Ainsi, le client ne dispose ni de source d'états quantiques, ni de dispositifs de mesures d'états quantiques.

30 [0040] En dehors de ces deux éléments supprimés, le client 10 peut être conforme aux clients décrits dans la littérature relative à la délégation de calcul quantique. Notamment, le client peut être du type décrit dans les articles susmentionnés :

- « *Secure Assisted Quantum Computation* » d'Andrew M. Childs, in Quantum Information and Computation 5, 456 (2005), <https://arxiv.org/abs/quant-ph/0111046> ou
- « *Universal Blind Quantum Computation* » d'Anne Broadbent, Joseph Fitzsimmons et Elham Kashefi, in Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), pp. 517-526, <https://arxiv.org/abs/0807.4154v3>

[0041] Il est à noter qu'un tel client peut être une sous-partie d'un ordinateur ou d'un équipement généraliste, ou bien un équipement autonome pouvant être raccordé à un tel équipement généraliste ou ordinateur. Différents modes de réalisation sont envisageables dans le cadre de la présente invention.

[0042] Selon l'invention, une source 40 est prévue pour générer et émettre une séquence d'états quantiques vers le client, au travers d'une ligne de communication 31.

[0043] Les états quantiques peuvent être portés par différentes technologies. Selon une mise en œuvre préférentielle, les états quantiques sont portés par des photons.

[0044] D'une façon générale, le calcul quantique repose sur la manipulation de données sous forme de bits quantiques ou "qubits". Alors que dans le calcul classique, un bit d'information est utilisé pour représenter seulement un des deux états logiques possibles, à savoir "1" ou "0", dans le calcul quantique, un qubit peut représenter les deux états logiques simultanément comme une superposition d'états quantiques.

[0045] En pratique, les qubits peuvent être codés en utilisant les degrés de liberté de différentes particules physiques. Les degrés de liberté sont une propriété physique des systèmes physiques, qui peut être décrite par la mécanique quantique.

[0046] En particulier, les qubits peuvent être physiquement mis en œuvre par divers supports, notamment les photons, l'état cohérent de la lumière, les électrons, le noyau d'un atome, les réseaux optiques, les jonctions Josephson pour les qubits supraconducteurs, etc. Une liste non exhaustive peut être trouvée, par exemple, sur Wikipedia : <https://en.wikipedia.org/wiki/Qubit>

[0047] En conséquence, les degrés de liberté dépendent du support physique et comprennent la phase, les différences de phase, la fréquence, la polarisation, la

localisation temporelle des photons. On peut également utiliser les spins des électrons, la charge supraconductrice, le nombre d'électrons, etc.

[0048] Les qubits peuvent être écrits comme un vecteur dans un espace vectoriel de Hilbert de dimension d .

- 5 Dans une dimension $d=2$, le qubit peut être défini par une base composée de deux états, qui sont dénommés $|0\rangle$ et $|1\rangle$. Ainsi, l'état $|\alpha\rangle$ du qubit peut être représenté par :

$$|\alpha\rangle = a|0\rangle + b|1\rangle$$

où a et b sont des coefficients de nombres complexes.

- [0049] Le qubit peut stocker des informations sous la forme d'une combinaison de 0 et 1, en utilisant différentes valeurs de a et b . Cependant, une mesure du qubit l'amènera à se projeter sur l'état $|0\rangle$ ou $|1\rangle$ et à renvoyer le résultat 0 ou 1 respectivement. Les probabilités de renvoyer ces valeurs sont respectivement de $|a|^2$ et $|b|^2$

- [0050] Selon un mode de réalisation de l'invention, on utilise le photon comme support de qubit. 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.

- 20 [0051] La source 40 peut alors être un laser apte à générer des photons, combiné avec un modulateur initial apte à moduler un degré de liberté d'un photon généré afin de générer des états quantiques souhaités (comme on le verra plus bas, une superposition d'états notée $|+\rangle$).

- [0052] Selon un mode de réalisation, la source et le dispositif de transformation 12 du client effectuent des modulations sur l'intervalle de temps pour lequel on veut générer/transformer un photon, dont l'énergie globale correspond à un quantum d'énergie du photon.

- [0053] Selon un autre mode de réalisation, on utilise la différence de phase comme degré de liberté pour encoder les qubits. Aussi, la source 40 génère les photons en effectuant une modulation selon deux pics, chacun dans un demi-intervalle de l'intervalle correspondant au photon que l'on souhaite générer. L'énergie globale de

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.

5 [0054] 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 télécommunication.

10 [0055] Les dispositifs de transformation 12 peuvent alors être des modulateurs optiques. 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. Comme il sera vu plus tard, chaque dispositif de transformation peut, selon un mode de réalisation, comporter au moins deux modulateurs optiques, chacun prévu pour moduler les photons selon un axe différent de la sphère de Bloch représentant le degré de liberté retenu.

15 [0056] Au travers du lien de communication 32, le client 10 est en communication avec un serveur 20. La ligne 32 peut être une fibre optique.

20 [0057] Un serveur est également prévu, pour effectuer du calcul quantique en délégation d'un client. Ce serveur 20 est un équipement distinct de la source. Préférentiellement, il appartient à une entité distincte de cette source, afin d'éviter tout collusion fonctionnelle. Préférentiellement, même, il peut être prévu que le serveur n'ait aucune connaissance de la source.

[0058] Le serveur 20 dispose de circuits quantiques et éventuellement de circuits conventionnels (permettant notamment le contrôle de ces circuits quantiques). Il comporte notamment un dispositif 21 de mesure d'états quantiques reçus.

25 [0059] Le serveur 20 peut outre comporter un ou plusieurs élément(s) quantique(s) 22 permettant d'effectuer les calculs quantiques qui sont délégués au serveur. Ces composants quantiques peuvent notamment comprendre une mémoire quantique permettant de stocker des qubits reçus, des moyens pour effectuer des opérations sur un ou plusieurs qubits, etc. La nature de ces éléments quantiques dépend de la technologie retenue et de différents modes de réalisation possibles.

30 [0060] Le dispositif de mesure 21 du serveur 20 peut être un détecteur de photons uniques, c'est-à-dire pouvant mesurer l'état quantique d'un photon individuel et non

pas un flux, ou une énergie, lumineuse. Différents mécanismes existent dans l'état de la technique. On peut par exemple citer par exemple les détecteurs basés sur des photodiodes à avalanches (APD pour « *Avalanche PhotoDiode* » en anglais).

[0061] Plus généralement, selon différents modes de réalisation de l'invention et en fonction du type de degré de liberté, différents types de modulateurs et de détecteurs peuvent être utilisés.

[0062] 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 utilisé.

[0063] 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.

[0064] 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. Afin de réaliser un calcul aveugle, on peut démontrer qu'il faut et qu'il suffit de savoir encoder des états dans des bases incompatibles entre elles. La superposition de localisations temporelles à réaliser pour encoder un qubit dans une base parmi un ensemble de bases incompatibles peut être obtenue en programmant les lames séparatrices.

[0065] D'une façon générale, les modulateurs de photon sont des dispositifs de télécommunication standards, et donc peu coûteux et produits à grande échelle.

[0066] D'autres mises en œuvre sont possibles, y compris des mises en œuvre non basés sur le photon.

[0067] Dans le cas où les qubits manipulés par le serveur sont couplés au domaine micro-onde (par exemple qubit supraconducteur), la communication avec le client pourra se faire :

- 5 - Soit par la transduction de l'information quantique dans le domaine optique tel que décrite par exemple dans l'article « *Superconducting qubit to optical photon transduction* » de Mohammad Mirhosseini, Alp Sipahigil, Mahmoud Kalaei & Oskar Painter in *Nature* 588, 599–603 (2020). <https://doi.org/10.1038/s41586-020-3038-6>. Ceci permet d'appliquer les méthodes décrites précédemment pour manipuler des photons.
- 10 - Soit par l'utilisation par le client d'un système quantique auxiliaire tel qu'un qubits supraconducteur, ou un qubit semi-conducteur, par exemple à base de silicium. En particulier, le couplage entre un qubit supraconducteur (qui peut être utilisé par le serveur) et un qubit semi-conducteur (qui peut être utilisé par le client) est décrit dans l'article « *Coherent microwave-photon-mediated coupling between a semiconductor and a superconducting qubit* » de Scarlino, P., van Woerkom, D.J., Mendes, U.C. et al. in *Nat Commun* 10, 3011 (2019). <https://doi.org/10.1038/s41467-019-10798-6>. Après réception et stockage du
- 15 qubit par le client, celui-ci pourra appliquer une transformation en utilisant les techniques standards de manipulation de l'information quantique avant de renvoyer le qubit ainsi obtenu par le serveur.

[0068] Dans le dernier cas, le client est donc équipé d'un système quantique complexe, mais limité à un seul qubit. Il s'ensuit que le client est considérablement plus simple

20 que le serveur qui a la capacité de manipuler un nombre plus important de qubits.

[0069] L'invention est ainsi indépendante du type de technologies pour encoder et transformer les qubits (états quantiques).

[0070] Protocole avec un client simplifié

[0071] La figure 2 illustre un procédé selon un mode de réalisation de l'invention. Ce

25 mode de réalisation se base sur les mécanismes de calcul délégué basé sur la mesure tels que décrits dans les articles suscités de Childs, et de Broadbent, Fitzsimmons et Kashefi. Selon ces mécanismes, le serveur comporte une mémoire quantique qui est d'abord préparée dans un état intriqué. Cet état, appelé « *cluster state* », ou « *graph state* » en anglais, est universel, au sens où il ne dépend pas du calcul quantique à

30 effectuer. Il forme un « substrat » sur lequel peut opérer une phase subséquente de calcul propre dit.

[0072] Dans cette phase de calcul, le client indique une séquence de mesures à effectuer individuellement sur certains qubits de la mémoire quantique du serveur, ou graphe d'état. Ces mesures spécifient véritablement l'algorithme de calcul quantique à effectuer sur le serveur. L'algorithme quantique correspond donc à un traitement
5 ordonné de corrélations quantiques. Il peut donc consister en une séquence d'identifiants de qubit à mesurer associés à une base de mesure.

[0073] Dans le cadre d'un calcul aveugle, le graphe d'état et l'algorithme (définissant l'ordonnancement des mesures à effectuer) peuvent être connus de l'ensemble des parties. Le « secret », rendant le calcul aveugle, réside dans l'état individuel des qubits
10 fournis au serveur.

[0074] Plus précisément, dans une phase de préparation, une étape S1 consiste en la transmission au serveur d'une description de la ressource de calcul, c'est-à-dire d'intrications à effectuer dans une mémoire quantique du serveur. Cette étape définit le graphe d'état au sein du serveur.

15 [0075] Pour ce faire, le client envoie au serveur la description (classique) de la ressource de calcul. Cette ressource est en général un état quantique composé de plusieurs qubits intriqués les uns avec les autres. La description envoyée par le client consiste en les relations d'intrications entre les qubits, mais pas dans la description des qubits eux-mêmes. Celle-ci reste en effet cachée au serveur et est, selon
20 l'invention, fournit ultérieurement au serveur par le client lors de l'étape S4.

[0076] Dans une étape S2, une source 40 émet une séquence d'état sur l'interface d'entrée 11 du client. Ces états quantiques sont transmis via un lien de communication 31. Typiquement, ce lien de communication 31 est une fibre optique permettant la transmission de photons, mais d'autres mises en œuvre sont
25 évidemment possibles dans le cadre de l'invention.

[0077] Dans une étape S3, un moyen, ou dispositif, de transformation 12 applique les transformations nécessaires à chaque état, l'un après l'autre. Les états quantiques peuvent être ainsi modifiés, de façon aveugle pour le serveur.

[0078] Dans un procédé de calcul délégué aveugle classique, le masquage de
30 l'information au serveur provient d'un choix très spécifique des états envoyés par le client au serveur. Dans le processus selon l'invention, le masquage de l'information

est assuré par la combinaison d'un choix des états quantiques initiaux générés par la source 40, et par les transformations appliquées par le client.

[0079] En particulier, la source 40 peut générer une séquence d'états quantiques $|+\rangle$

[0080] Ces états sont, chacun, une superposition d'états orthogonaux, de sorte que :

$$5 \quad |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

[0081] Le dispositif de transformation 12 peut appliquer des transformations, de manière à ce que le serveur ne puisse pas les identifier avec certitude.

[0082] Pour ce faire, ces transformations peuvent être de la forme :

$$Z^{\theta+c.\pi}$$

10 dans laquelle

- Z est une porte de Pauli selon l'axe Z,
- θ est choisi de façon aléatoire parmi une liste $\{0; \pi/4; \pi/2; 3\pi/4\}$
- c est choisi aléatoirement parmi les valeurs 0 et 1

[0083] La porte Pauli-Z agit sur un seul qubit. Cela équivaut à une rotation autour de
15 l'axe Z de la sphère de Bloch par π radians. Elle laisse l'état $|0\rangle$ inchangé et transforme l'état $|1\rangle$ en $-|1\rangle$. Elle peut être représentée par la matrice Pauli-Z :

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

[0084] Ainsi, en appliquant la transformation $Z^{\theta+c.\pi}$, on obtient en sortie l'état quantique suivant :

$$20 \quad |0\rangle + e^{\theta+c.\pi}|1\rangle$$

[0085] Cet état est habituellement noté $|+_{\theta+c.\pi}\rangle$

[0086] L'envoi de tels états au serveur suffit à masquer entièrement le calcul qu'il effectue. Les clés permettant de déchiffrer le calcul et son résultat sont les valeurs θ et c choisies pour chaque qubit

25 [0087] Dans une étape S4, les états transmis au client sont envoyés au serveur après que les transformations ont été appliquées.

[0088] Le reste du protocole peut être conforme à ceux décrits dans la littérature. Ainsi, dans une étape S5, le serveur applique une séquence de mesure sur chacun des qubits dans un ordre prédéterminé ainsi qu'évoqué précédemment. La base de mesure de chaque qubit est choisie de manière interactive en communiquant au client le résultat de chaque mesure. Le client spécifie alors au serveur la base dans laquelle mesurer le qubit suivant, et ainsi de suite.

[0089] La dernière mesure donne le résultat du calcul de manière chiffrée. Son résultat est transmis au client qui peut le déchiffrer afin de lire le résultat du calcul.

[0090] Le choix de la transformation $Z^{\theta+c.\pi}$ permet de masquer les informations au serveur. D'autres choix de transformation sont également possibles.

[0091] Notamment, d'autres transformations peuvent être utilisées afin de rendre le protocole vérifiable, c'est-à-dire de s'assurer (pour le client) que le serveur applique bien le protocole convenu, sans en altérer les opérations. Cela peut notamment être intéressant pour vérifier si le serveur n'a pas été corrompu et/ou si celui-ci est digne de confiance. En effet, notamment dans le cadre d'un déploiement d'un serveur sur une plateforme publique, telle qu'un « cloud », il peut être important, voire essentiel, de pouvoir assurer de la légitimité, ou honnêteté, du serveur.

[0092] Un mécanisme permettant la vérifiabilité par le client des calculs effectués par le serveur a été proposé dans l'article « *Unconditionally verifiable blind computation* » précédemment cité. Celui repose sur l'idée de faire faire un calcul au serveur dont le résultat est prévisible afin de comparer le résultat obtenu du serveur avec celui escompté. Pour ce faire, il est nécessaire d'isoler les qubits sur lesquels portent le calcul au sein du graphe d'état, c'est-à-dire de s'assurer qu'ils ne sont pas intriqués avec leurs voisins, afin que le calcul soit effectivement prévisible.

[0093] Selon un mode de réalisation, lors de la phase de préparation, le client choisit un certain nombre de qubit qui seront des « pièges » pour le serveur. Le nombre de qubit choisi est un paramètre de sécurité : plus il est élevé, plus il sera difficile pour le serveur de tricher.

[0094] Le sous-ensemble des qubits pièges peut être choisi de façon masquée au serveur, selon donc un schéma qui lui est inconnu. Il faut par contre isoler chacun de ces qubits pièges, c'est-à-dire faire en sorte qu'ils ne soient pas, au moment de la

mesure, encore intriqués avec d'autres qubits de la mémoire quantique du serveur, afin que le résultat de la mesure soit prédictible.

[0095] Ainsi, pour chaque qubit lié avec un qubit piège dans le graphe d'état (qui décrit les intrications à effectuer entre qubits au sein de la mémoire quantique du serveur),
 5 le client prépare un état avec une transformation X^dH sur l'état $|+\rangle$ reçu. Ces qubits sont dits « factices » et ne sont pas utilisés par le calcul en tant que tel.

[0096] H représente la transformation de Hadamard, X est une porte de Pauli selon l'axe X et d est choisi parmi les valeurs 0 et 1.

[0097] La transformation de Hadamard agit sur un seul qubit et transforme un état $|0\rangle$
 10 en une superposition d'états équiprobables $|+\rangle$ et un état $|1\rangle$ en une superposition $|-\rangle$. Elle correspond à la combinaison d'une rotation de π selon l'axe X et d'une rotation de $\pi/2$ sur l'axe Y, selon la sphère de Bloch. Elle peut être représentée par la matrice de Hadamard :

$$H = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

15 [0098] La porte Pauli-X agit sur un seul qubit. Cela équivaut à une rotation autour de l'axe X de la sphère de Bloch par π radians. Elle équivaut à une porte « NON » en logique conventionnelle puisqu'elle échange les états $|0\rangle$ et $|1\rangle$. Elle peut être représentée par la matrice Pauli-X :

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

20 [0099] Le nombre d indique si la transformation selon la porte Pauli X a lieu (d=1) ou n'a pas lieu (d=0).

[0100] Les qubits de pièges sont préparés en appliquant une transformation $Z^{\theta+c.\pi}$ sur l'état $|+\rangle$ reçu.

[0101] Lorsque, toujours dans la phase de préparation, le serveur va appliquer le
 25 graphe d'état pour établir les intrications entre qubits adjacents, l'opération d'intrication effectuée par le serveur entre un qubit de piège et un qubit factice sera sans effet, du fait de la préparation basée sur la transformation X^dH appliquée à l'état $|+\rangle$.

[0102] Ainsi, le client peut ordonner au serveur d'effectuer, sur chaque qubit de piège, une mesure dont il peut prédire le résultat. Si les résultats de mesure sont conformes

aux prédictions, alors il sait que le serveur n'a pas dévié du calcul ordonné par le client. Inversement, en cas d'erreurs trop nombreuses dans les résultats de mesure des qubits de piège, le client saura que le serveur n'a pas réalisé les opérations conformes à ses instructions. Le client peut ainsi s'assurer de l'honnêteté du serveur.

- 5 [0103] Cette propriété de vérifiabilité, consistant à vérifier l'honnêteté ou intégrité du serveur, est ainsi atteinte par le procédé et le système selon l'invention, notamment par la séparation physique et fonctionnelle entre la source et le serveur.

[0104] On peut ainsi résoudre un problème posé par les mécanismes de l'état de la technique, par exemple, comme évoqué précédemment, une architecture dans
10 laquelle le serveur fournit lui-même les séquences d'états quantiques, comme par exemple l'architecture décrite dans Qin Li et al, « *Blind quantum computation for a user who only performs single-qubit gates* ».

[0105] Il est en effet possible de démontrer la vulnérabilité d'une telle architecture.

- [0106] Une faille possible est l'attaque décrit dans l'article « *Delegating Multi-Party Quantum Computations vs. Dishonest Majority in Two Quantum Rounds* »
15 (<https://arxiv.org/abs/2102.12949>), Appendice I, page 48.

[0107] Cette attaque consiste pour le serveur à appliquer une opération spécifique, la transformation Z, sur chacun des qubits avant et après transmission au client. Cette opération a pour effet de modifier les qubits utilisés dans les calculs quantiques. Dans
20 le cadre du protocole décrit, l'effet de ces modifications ne peut pas être détecté par le client.

[0108] Le mécanisme de l'invention permet au contraire de s'assurer que l'attaque décrite plus haut est impossible sans une collusion entre la source des qubits et le serveur. Ceci permet facilement de mettre en œuvre un protocole vérifiable.

- 25 [0109] On peut remarquer que les portes logiques mises en œuvre à l'étape S3, qui correspond à la seule manipulation quantique opérée par les clients, correspondent à des rotations selon des axes différents dans le cas d'un calcul quantique et dans le cas d'une vérification de l'honnêteté du serveur.

[0110] Selon un mode de réalisation de l'invention, le dispositif de transformation
30 comporte deux (ou plus) dispositifs distincts, chacun adapté pour une transformation particulière. Ainsi, un premier dispositif peut appliquer une première transformation

visant à préparer les qubits nécessaires pour effectuer un calcul quantique, et un second dispositif peut appliquer une seconde transformation visant à préparer les qubits nécessaires pour vérifier une honnêteté dudit serveur. Par exemple, un premier dispositif (par exemple un modulateur optique) est adapté à la transformation $Z^{\theta+c.\pi}$,
 5 et un second dispositif (par exemple un second modulateur optique) est adapté à la transformation X^dH .

[0111] Architectures N clients / 1 serveur

[0112] Comme il a été vu précédemment, un des avantages d'un client selon l'invention consiste en sa simplicité permettant d'en abaisser le coût et de faciliter le
 10 déploiement à grande échelle. En particulier, l'architecture permet d'assurer le passage à l'échelle du déploiement d'une infrastructure de « cloud » (ou nuage) quantique

[0113] Selon un mode de réalisation illustré par la figure 3a, il est ainsi possible de connecter un grand nombre de clients $10_1, 10_2, 10_3 \dots 10_N$ à un unique serveur 20, via
 15 autant de lignes de communication, respectivement $30_1, 30_2, 30_3 \dots 30_N$. Sur la figure 3a, la source d'états quantiques n'est pas représentée.

[0114] Le serveur 20 peut alors posséder un commutateur lui permettant de recevoir les séquences d'états quantiques émis par les différents clients vers ses ressources quantiques mutualisées (notamment le dispositif de mesure).

20 [0115] Dans le cas où le client est unique, on est ramené à la situation illustrée en figure 1 et le serveur ne nécessite évidemment pas l'utilisation d'un commutateur.

[0116] Le client simplifié selon l'invention permet également de connecter plusieurs clients à un même serveur via une ligne de communication unique, ainsi qu'illustré en figure 3b.

25 [0117] Ainsi, sur la figure 3b, une ligne 30 unique connecte la source 40, les clients $30_1, 30_2, 30_3 \dots 30_N$, et le serveur 20

[0118] Les clients forment ainsi une chaîne selon laquelle chaque client 10_i peut posséder un client précédent 10_{i-1} dans la chaîne (sauf le premier client 10_1 connecté directement à la source 40) et un client subséquent 10_{i+1} (sauf le dernier client 10_N
 30 connecté directement au serveur 20), de sorte que les états quantiques sont transmis de proche en proche depuis la source 40 vers le dispositif de mesure 21.

[0119] Ainsi, le serveur n'a qu'une seule ligne de communication entrante mais ses capacités de calcul sont néanmoins mutualisées entre tous les clients, ceux-ci pouvant être très nombreux.

[0120] Une telle architecture est rendue possible par le fait que les clients simplifiés
5 selon l'invention ne disposent que d'un dispositif de transformation quantique. Celui-ci peut transformer ou pas les états quantiques qui lui sont transmis, de sorte que les états quantiques ne sont modifiés que par le, ou les, clients souhaités.

[0121] Selon l'invention, les dispositifs constructeur (source) et destructeur (mesure)
d'états quantiques sont relégués en bout de chaîne et ne perturbent donc pas la
10 transmission de bout en bout via une pluralité de clients intermédiaires.

[0122] Selon un mode de réalisation, la ligne de communication peut être partagée, ou mutualisée, entre les différents clients qui y sont connectés, en leur allouant une partie des états quantiques fournis par la source 40.

[0123] Ainsi, chaque client de la chaîne ne peut modifier que la partie des états
15 quantiques qui lui est alloué, et transmet l'ensemble de la séquence vers le client subséquent dans la chaîne (ou vers le serveur pour le dernier).

[0124] Cette partie peut par exemple être déterminée par une allocation d'une fenêtre temporelle. Ainsi, chaque client se voit allouer une fenêtre disjointe des autres clients de la chaîne et ne modifie (éventuellement) que les états quantiques reçus dans la
20 fenêtre qui lui a été allouée. Chaque état quantique émis par la source peut donc n'être modifié que par un unique client de la chaîne.

[0125] Ces fenêtres temporelles peuvent être périodiques, c'est-à-dire que l'axe du temps peut être subdivisé en périodes, et chaque période subdivisée en une séquence ordonnée de fenêtres temporelles allouées individuellement à un client et dont l'ordre
25 est préférentiellement identique d'une période à l'autre.

[0126] Ainsi, un simple démultiplexage temporel peut permettre au serveur 20 de savoir, à chaque instant, avec quel client il est en interaction.

[0127] 21Ainsi qu'évoqué précédemment, le serveur 20 et la source 40 sont distincts afin d'assurer la propriété de vérifiabilité.

30 [0128] Ils peuvent être mis en œuvre par des équipements physiques distincts et autonomes. En particulier, ils peuvent posséder chacun des microprocesseurs

indépendants, et une source d'alimentation indépendantes. Ils peuvent en outre être localisés en des lieux géographiques distincts.

[0129] Préférentiellement, la source et le serveur sont fonctionnellement indépendants et sont adaptés pour ne pas pouvoir interagir hormis par la transmission des états quantiques depuis la source vers le serveur via les clients. On peut ainsi garantir l'absence de collusion, ou ententes, entre ces deux entités.

[0130] Toutefois, ils peuvent néanmoins appartenir à une même entité légale, si celle-ci peut être considérée comme digne de confiance. Cela peut par exemple être le cas d'une entité légale disposant d'un certificat spécifique garantissant un comportement honnête, par exemple d'un opérateur de télécommunication : celui-ci peut prévoir un équipement pour générer les états quantiques en une première localisation, et un autre équipement pour les mesurer (et effectuer le traitement quantique) en une seconde localisation distincte, sans que ceux-ci communiquent fonctionnellement (hors éventuels besoin de gestion et d'administration)..

[0131] Selon un mode de réalisation, plusieurs clients peuvent interagir avec un même qubit généré par la source. Plusieurs clients peuvent ainsi modifier, successivement, un même état quantique de la séquence d'états générés par la source.

[0132] Ainsi, un premier client peut modifier une partie des états quantiques transmis, et au moins un second client peut modifier à nouveau tout ou partie de ces états quantiques. Ces premiers et seconds clients peuvent ne représenter qu'une partie de la chaîne de clients et ne sont pas nécessairement successifs.

[0133] Selon un mode de réalisation, une sous-partie de la séquence d'états quantiques, correspondant par exemple à une fenêtre temporelle, peut être allouée à une telle pluralité de clients.

[0134] Cette possibilité de modifications successives par plusieurs clients d'un même état quantique permet de réaliser des calculs multipartites, c'est-à-dire de préparer un état à destination du serveur dont les entrées dépendent de plusieurs clients.

[0135] Ainsi, l'invention permet de nouveaux types de calculs qui n'étaient pas possibles avec les mécanismes conventionnels de calcul délégué d'un client unique vers un serveur.

[0136] En particulier, cette tâche peut être utile pour réaliser un calcul multipartite sécurisé, c'est-à-dire un calcul qui dépend des entrées de plusieurs clients, mais effectué de manière à ne pas révéler lesdites entrées. Ce type de calcul est par exemple décrit dans « *Multiparty Delegated Quantum Computing* » de Elham Kashefi et Anna Pappa, *in Cryptography 2017*, 1(2), 12, <https://arxiv.org/abs/1606.09200v2> ou bien « *Actively Secure Two-Party Evaluation of any Quantum Operation* » de Frédéric Dupuis, Jesper Buus Nielsen et Louis Savail, *in Proceedings of the 32nd Annual Cryptology Conference on Advances in Cryptology*, vol. 7417, Août 2012, https://doi.org/10.1007/978-3-642-32009-5_46

10 [0137] Selon une mise en œuvre basée sur celle de l'article d'Elham Kashefi et Anna Pappa susmentionné, on peut modifier les protocoles décrits afin de les appliquer au contexte d'un client simplifié.

[0138] Ainsi, dans le protocole 1 décrit en page 8, chaque client impliqué dans le calcul multipartite envoie un état de la forme $|+\theta_i\rangle$. Ensuite, le serveur qui a reçu tous ces états réalise une opération qui lui permet de préparer l'état $|+\theta\rangle$, où θ est la somme de tous les θ_i (protocole 3). Cet état forme la ressource qui permet au serveur de réaliser un calcul délégué multipartite (protocole 4).

[0139] Grace aux avantages combinés d'un client simplifié et d'une architecture en ligne d'une chaîne de clients, il est possible de préparer directement cet état $|+\theta\rangle$

20 [0140] Il suffit pour cela que, partant de l'état $|+\rangle$ généré par la source, chaque client impliqué dans le calcul réalise la rotation Z^{θ_i} correspondant à son entrée θ_i . Le cumul, des rotations effectués successivement par chacun des clients impliqués permet de préparer l'état $|+\theta\rangle$ en sortie du dernier client (et donc en entrée du serveur).

25 [0141] Cette architecture simplifie donc largement la phase de préparation de l'état initial du calcul.

[0142] Bien entendu, la présente invention n'est pas limitée aux exemples et au mode de réalisation décrits et représentés, mais est défini par les revendications. Elle est notamment susceptible de nombreuses variantes accessibles à l'homme de l'art.

Revendications

[Revendication 1] Procédé de délégation d'un calcul quantique par au moins un client vers un serveur, comprenant

- une première étape (S1) comprenant la transmission au serveur d'une description d'intrications à effectuer dans une mémoire quantique;
- une deuxième étape (S2) comprenant l'émission d'une séquence d'états quantiques par une source, distincte dudit serveur, vers ledit au moins un client ;
- une troisième étape (S3) comprenant une modification d'un état quantique de ladite séquence,
- une quatrième étape (S4) comprenant la transmission de ladite séquence vers ledit serveur ;
- une cinquième étape (S5) comprenant l'application d'une séquence de mesures selon une base donnée, au sein de ladite mémoire quantique dont le contenu a été intriqué selon ladite description, et la transmission du résultat de chaque mesure audit au moins un client.

[Revendication 2] Procédé selon la revendication précédente, dans lequel les états quantiques fournis par ladite source sont une superposition d'états orthogonaux, et la modification effectuée par ledit client est de la forme $Z^{\theta+c.\pi}$ dans laquelle Z est une porte de Pauli selon l'axe Z, θ est choisi de façon aléatoire parmi une liste $\{0; \pi/4; \pi/2; 3\pi/4\}$ et c est choisi aléatoirement parmi les valeurs 0 et 1

[Revendication 3] Procédé selon la revendication 1, dans lequel les états quantiques fournis par ladite source sont une superposition d'états orthogonaux, et comportant une étape de détermination d'un sous-ensemble de qubits pièges et dans lequel ladite troisième étape comprend une modification de qubits voisins desdits qubits pièges selon ladite description d'intrications, de la forme X^dH , dans laquelle H est la transformation de Hadamard, X est une porte de Pauli selon l'axe X et d est choisi parmi les valeurs 0 et 1, et ledit client met en œuvre une étape de comparaison entre un

résultat d'une mesure d'un desdits qubits pièges avec un résultat attendu pour ledit qubit piège, permettant de déterminer une honnêteté dudit serveur.

[Revendication 4] Procédé selon l'une des revendications précédentes, dans lequel chacun desdits au moins un client ne peut modifier qu'une partie des états quantiques qui lui est alloué, et transmet ladite séquence vers un client subséquent d'une chaîne de clients le liant audit serveur.

[Revendication 5] Procédé selon la revendication précédente, dans lequel ladite partie est déterminée par une allocation d'une fenêtre temporelle.

[Revendication 6] Procédé selon l'une des revendications précédentes, dans lequel plusieurs clients peuvent modifier successivement un même état quantique de ladite séquence.

[Revendication 7] Système pour la délégation d'un calcul quantique d'au moins un client (10) vers un serveur (20), comportant

- au moins une source (40) adaptée pour émettre une séquence d'états quantiques,
- dans lequel le serveur comporte un dispositif (21) de mesure d'états quantiques reçus, et au moins un composant quantique (22) permettant de réaliser ledit calcul quantique ; et
- ledit au moins un client comportant une interface d'entrée (11) pour recevoir ladite séquence, un dispositif de transformation (12) adapté pour modifier un état quantique de ladite séquence et une interface de sortie (13) pour transmettre ladite séquence vers ledit dispositif de mesure.

[Revendication 8] Système selon la revendication précédente, dans lequel ledit dispositif de transformation (12) comporte un premier dispositif pour appliquer une première transformation visant à préparer des états quantiques pour effectuer un calcul quantique aveugle, et un second dispositif pour

appliquer une seconde transformation visant à préparer des états quantiques pour vérifier une honnêteté dudit serveur.

[Revendication 9] Système selon la revendication précédente, dans lequel ledit premier équipement et ledit second équipement sont répartis en des localisations physiques distinctes.

[Revendication 10] Système selon la revendication précédente, dans lequel une pluralité de clients sont connectés audit serveur par une ligne de communication unique (30) en formant une chaîne, de sorte que lesdits états quantiques sont transmis de proche en proche depuis ladite source vers ledit dispositif de mesure.

[Revendication 11] Système selon la revendication précédente, lequel chacun desdits clients est configuré pour ne pouvoir modifier que la partie des états quantiques qui lui est alloué.

[Revendication 12] Système selon l'une des revendications 7 à 11, dans lequel lesdits états quantiques sont des photons et ledit dispositif de transformation est un modulateur optique.

[Revendication 13] Système selon l'une des revendications 7 à 12, dans lequel ladite source est adaptée pour fournir des états quantiques sous la forme d'une superposition d'états orthogonaux, et ledit dispositif de transformation est adapté pour effectuer une modification de la forme $Z^{\theta+c.\pi}$ dans laquelle Z est une porte de Pauli selon l'axe Z, θ est choisi de façon aléatoire parmi une liste $\{0; \pi/4; \pi/2; 3\pi/4\}$ et c est choisi aléatoirement parmi les valeurs 0 et 1

[Revendication 14] Système selon l'une des revendications 7 à 13, adapté pour la mise en œuvre d'un procédé selon l'une des revendications 1 à 6.]