

METHOD FOR SECURELY COMPUTING A LOGICAL AND BETWEEN TWO BITS USING QUANTUM COMMUNICATION

5 [0001] The present invention relates generally to the field of secure computing using quantum communications and more particularly to the computation of a logical AND between multiple participants connected to a communication network.

10 [0002] Background of the invention

[0003] Generally speaking, the invention relates to the field of secure multi-party computation, which is a branch of cryptography whose objective is to allow participants to obtain the result of a common function without any of them being able to know the inputs of the other participants.

15 [0004] This type of problem seems to have been raised in the 1970s in the article by A. Shamir, R. Rivest, and L. Adleman, "*Mental Poker*", Technical Report LCS/TR-125, Massachusetts Institute of Technology, April 1979. In the 1980s, the problem was applied to the theoretical problem of billionaires which
20 consisted of determining the richest person in a set of billionaires without any of them disclosing their fortune to anyone. A notable example is the article by Andrew C. Yao, "*Protocols for secure computations*" which presents the problem and a protocol to solve it.

25 [0005] Other applications of secure multi-party computation include auction or voting mechanisms, statistics on medical data, etc. In these applications, generally speaking, one wants to achieve a result based on all the input data while keeping it private, that is secret from other parties. In the case of medical data, for example, it may be interesting to construct statistical or aggregate
30 data, but for legal reasons, individual data cannot be accessible to anyone. Similarly, in auction systems, for example in a wholesale market for agricultural

products, the issue is to determine which party has won the auction but without the different parties having to reveal their bids.

5 [0006] While there is theoretical work on secure multi-party computation, very few industrial developments exist. Indeed, privacy protection is a relatively new concern: the first large-scale implementation dates back to 2009, and the first practical solutions are necessarily coming to market with some delay.

10 [0007] Furthermore, existing proposals generally induce an additional cost in terms of computation time which makes them prohibitive for practical uses.

[0008] Another drawback of existing proposals is their high level of technicality, linked to cryptographic techniques, which makes them difficult to integrate into existing products and systems.

15 [0009] The purpose of the invention is to at least improve the situation by providing an efficient. secure multi-party computation method making use of a quantum communication channel.

20 [0010] More particularly, the invention concerns the sub-problem of a distributed computation of a logical AND, as this computation allows any multi-party logic functions to be carried out.

25 [0011] To this end, the present invention proposes a method for calculating a logical AND between two chosen bits, x_i , x_j held by a first and a second participant, C_i , C_j respectively, connected to each other and to a server by at least one quantum communication channel L_q and one conventional communication channel L_c , comprising

30 a first phase using said quantum communication channel and comprising a first step in which said first and second participants randomly determine, respectively, a first α and second β correlation variable; each determine a random bit, respectively p and q , and

transmit to said server, a value dependent on said respective random bit p, q ;

a second step in which said server prepares a photon in a first state in an orthonormal basis, and transmits it to said first participant;

a third step in which said first participant applies a first transformation $V^\alpha U^p$ to said photon, and transmits it to said second participant, the logic gate V transforming a state into an orthogonal state and the logic gate U being a square root of the logic gate V ;

a fourth step in which said second participant applies a second transformation $V^\beta U^q$ to said photon, and transmits it to said server;

a fifth step in which the server performs a third transformation $(U^*)^{p+q}$, measures the state of said photon and determines a third correlation variable γ based on said state, so as to form a correlation between said correlation variables; and,

a second phase comprising

a sixth step in which said first and second participants exchange a value u_1, u_2 depending on the sum between the random bit, p, q , and the chosen bit, x_i, x_j , they hold, respectively;

a seventh step in which said first participant calculates and provides a first value $a = \alpha + x_i \wedge u_2$, said second participant calculates and provides a second value $b = \beta + x_j \wedge u_1 + u_1 \wedge u_2$ and said server provides the third correlation variable γ , so that the result of the computation of the logical "AND" between said chosen bits may be obtained by summing said first and second values and said third correlation variable.

[0012] According to preferred embodiments, the invention comprises one or several of the following features which may be used separately or in partial combination with each other or in total combination with each other:

- said first phase is performed before said chosen bits are known to said participants
- in said first step, said first and second participants transmit respective values $t_1=p+r$ and $t_2=q+r$, where r is a bit secretly shared by said first and second participants;
- said first state is the $|+\rangle$ state
- said conventional communication channel (L_c) is a secure channel

[0013] Another aspect of the invention relates to a device for calculating a logical AND between two chosen bits, x_i , x_j held by a first and a second participants, C_i , C_j respectively, connected to each other and to a server by at least one quantum communication channel and one conventional communication channel, comprising means for implementing the previously described method.

15

[0014] According to preferred embodiments, the invention comprises one or several of the following features which may be used separately or in partial combination with each other or in total combination with each other:

- said first and second participants belong to a chain of participants, wherein the two participants at the ends respectively implement said server, an upstream participant being able to emit a photon, and a downstream participant being able to receive a photon and measure its state.
- said first and second participants belong to a ring of participants, such that a given participant implements said server and is able to emit a photon, receive a photon, and measure its state.
- said server comprises a laser capable of generating photons and an initial modulator capable of modulating a degree of freedom of a photon generated by said laser.
- said first and second participants comprise modulators capable of modulating an electromagnetic field through which the photons pass in order to modify a degree of freedom thereof.

[0015] The use of quantum communication allows an excellent level of security for a modest computational overhead. The security is perpetual because it does not rely on the solving of computational problems. Thus, it is not possible
5 to record the communication to break the protocol later, in the future. The computational overhead for an AND is not very large: a few qubit exchanges.

[0016] Description of the figures

10 [0017] Figures 1a and 1b show two variations of an example architecture of a device for secure multi-party computation according to an embodiment of the invention.

[0018] Figure 2 shows in table form several examples of degrees of freedom
15 for quantum bit encoding.

[0019] Figure 3 shows an embodiment of the method, or protocol, for secure multi-party computation of the logical "AND" in which the main steps are shown.

20

[0020] Description of implementations of the invention

[0021] As discussed in the introduction, one of the purposes of the invention is to enable secure multi-party computation between a set of participants.

25

[0022] According to one embodiment, these participants can be organized in a chain as shown in Figure 1b or in a ring as shown in Figure 1a.

[0023] The N participants $C_1, C_2, C_3 \dots C_N$ can communicate with their
30 immediate neighbors only and through at least two communication channels: a quantum communication channel L_q and a classical, or conventional, communication channel L_c .

[0024] This conventional communication channel L_c can be secured. The security can be achieved for example through the quantum communication channel which allows the exchange of encryption keys with unconditional security. It can be of different types, depending on the embodiments. Typically, it can be a digital communication channel compliant with the TCP/IP protocol stack. It can be a wired channel (Ethernet, etc.) or wireless (WiFi, cellular, etc).

[0025] According to another embodiment, the conventional communication channel L_c can be of the "broadcast" type. Thus, all participants receive data from all participants. However, the security by exchanging encryption keys can be peer-to-peer, so that the conventional "physical" communication channel L_c supports a set of peer-to-peer "logical" communication channels, connecting each of the participants to its neighbors.

[0026] In practice, the participants can be of various types: they can be computers connected to a communication network, or virtual machines deployed on a server or on a server farm, etc.

[0027] The quantum communication channel L_q can be implemented in different ways as well.

[0028] According to one embodiment, the quantum communication channel L_q is provided to allow the transmission of light signals enabling the transport of quantum bits, generally called "qubits". It is typically an optical fiber.

[0029] Quantum bits can be encoded with photons according to their degree of freedom. "Photon degree of freedom" refers to a physical property described by quantum mechanics and usable for quantum communications. Examples of photon degrees of freedom are phase, phase difference, frequency, polarization or temporal location. In this description, we use the formalism that represents a quantum state as a vector $|\alpha\rangle$ in a d -dimensional Hilbert vector

space. The concept of Hilbert vector space extends the methods of linear algebra by generalizing the notions of Euclidean space (like the Euclidean plane or the usual space of dimension 3) and Hermitian space to spaces of any dimension (finite or infinite). A vector $|\alpha\rangle$ of a d-dimensional Hilbert vector space can be described via a basis of the d-dimensional Hilbert vector space.

[0030] Figure 2 gives examples of photon degrees of freedom, in a 2-dimensional Hilbert vector space.

10 [0031] A first participant C_1 is intended to emit the photons, which will be transmitted from one to the next along the chain.

[0032] According to a chain embodiment, as shown in Figure 1b, this transmission is performed to the most downstream participant C_N in the chain which may be provided to perform measurements of the photon states and thus read the states of the associated qubits. This participant C_N is intended to communicate with participant C_1 through a secure communication channel L_s .

20 [0033] According to a ring embodiment, as shown in Figure 1a, the transmission is performed up to the first participant C_1 . As we shall see, this first participant thus plays the roles of sender and receiver.

[0034] The first participant C_1 can be called the "sender". In practice, it can be implemented in different ways. For example, it may comprise a laser capable of generating photons and an initial modulator capable of modulating a degree of freedom of a generated photon.

[0035] According to one embodiment, a modulation is carried out on the time interval for which a photon is to be generated, the overall energy of which corresponds to a photon energy quantum.

[0036] According to another embodiment, the phase difference is used as a degree of freedom to encode the qubits. Also, the sender C_1 generates the photons by modulating them according to two peaks, each in a half-interval of the interval corresponding to the photon to be generated. The total energy of this modulation being, by configuration, equal to the energy quantum of a photon, each photon thus generated is a superposition of a photon between these two half-intervals.

[0037] The laser can be provided with a wavelength of 1550 nm which corresponds to the minimum attenuation in optical fibers commonly used in telecommunications.

[0038] The $N-2$ participants besides the endpoint participants C_1 , C_N are modulators. They are not designed to emit photons but only to modulate an electromagnetic field in which the photons pass in order to modify one of their degrees of freedom.

[0039] According to one embodiment (Figure 1b), the most downstream participant C_N in the chain can be called a receiver. According to another embodiment (Figure 1a), the participant C_1 is both a sender and a receiver.

[0040] The receiving participant, C_1 , C_N , may comprise a single photon detector. Different mechanisms exist in the prior art. For example, there are detectors based on avalanche photodiodes (APDs).

[0041] It is possible to set up bidirectional communication channels, so that quantum bits (or qubits) can be transmitted in both directions of the chain. In such a case, the sender C_1 can also be a receiver, that is it can have measuring means (single photon detector).

[0042] Depending on the type of degree of freedom, different types of modulators and detectors can be used by the participants C_1 , C_2 , C_3 ... C_N .

[0043] When the degree of freedom of photons to encode quantum bits is the phase, the modulators can be phase modulators. For example, the LN53S-FC or LN65S-FC model marketed by Thorlabs can be used.

5

[0044] When the degree of freedom of photons to encode quantum bits is photon polarization, the modulators can be polarization modulators. For example, a model from the PSC-LN series of products marketed by iXblue Photonics can be used.

10

[0045] When the degree of freedom of the photons to encode the quantum bits is the temporal location of the photons, the modulators may each comprise a number d of delay lines and a number $2d$ of splitter plates, where d represents the dimension of the Hilbert vector space of representation of the quantum states. The superposition of temporal locations to be realized to create an incompatible base can be obtained by programming the splitter plates.

15

[0046] The same principle can be used for detection by the receiver C_N . This can have only one single photon detector, downstream of a similar device allowing to separate the beams and to delay the beams differently so that after recombination of the beams, the instant of the detection of the photon makes it possible to determine the temporal location of that photon.

20

[0047] This architecture can be used for secure multi-party computation between participants.

25

[0048] It is known that any computation on binary data can be reduced to a combination of universal logical operators. These universal logical operators are "NAND" (for "Not And") and "NOR" (for "Not Or").

30

[0049] Carrying out a logical "NOT" operator does not pose any particular problem of security since it is a local operator. On the other hand, the logical

operators AND OR can involve several participants and thus imply a security problem to make it possible to obtain the result of the operation without any of the participants knowing the value held by the other participants.

- 5 [0050] It is more common to use the "NOT AND" operator. Also, the invention addresses the particular sub-problem of computing a logical AND between multiple participants. More specifically, it deals with the computation of a logical AND between two participants, it being understood that switching to more than two participants amounts to combining several "AND" operators.

10

[0051] In the following we will denote $x_i \wedge x_j$ the logical "and" operation between the bits x_i and x_j .

- [0052] The invention thus aims to calculate a logical AND between bits x_i and x_j held by two participants, C_i and C_j respectively, where $1 < i < N$ and $1 < j < N$ and, of course, $i \neq j$, with the constraints that

- 15 - Participant C_i should not be able to learn more information than the values of bit x_i and $x_i \wedge x_j$ (indeed, it should not be able to know the value of bit x_j),
- participant C_j should not be able to learn more information than the values of
20 bit x_j and of $x_i \wedge x_j$ (indeed, it should not be able to know the value of bit x_i),
- no other party to the computation should be able to know either x_i or x_j .

[0053] We will call these two bits x_i and x_j , "chosen bits".

- 25 [0054] Especially, the method according to the invention involves a third party, called server in the following. This server may know the final result $x_i \wedge x_j$ but must not know the value of x_i nor the value of x_j . This server also has the function of creating and emitting a photon in a given state, and can therefore be implemented, at least partially, by the sender C_1 .

30

[0055] According to a first embodiment based on a ring architecture (Figure 1a), participant C_1 is also a receiver, so that the server has all the information directly at its disposal as sender and receiver.

- 5 [0056] According to a second embodiment based on a chain architecture (Figure 1b), the server can have the information received by the receiver C_N via a secure communication channel L_s . In a way, the server is then implemented by the pair C_1/C_N formed by the two participants located at the ends of the chain of participants.

10

[0057] Even more implementations are possible. In the following, for simplicity, we will assign the reference C_1 to the server.

- 15 [0058] In a very general way, this computation is based on correlation, known as "magic", between three binary variables α , β , γ each determined, respectively, by the two participants C_i , C_j and the server C_1 and corresponding to a logical "and" between two bits b_1 , b_2 held by the participants so that $\alpha + \beta + \gamma = b_1 \wedge b_2$. Furthermore, the marginal distributions of the three variables α , β , γ must satisfy the uniformity criterion: when viewed individually, each bit can
- 20 equiprobably take the value 0 or 1. In the following, we will call these three variables "correlation variables".

- [0059] A first phase consists of establishing a magic correlation corresponding to the logical "and" between two random bits and using the quantum
- 25 communication channel L_q and quantum computation. At the end of this first phase, we therefore determine the three variables α , β , γ forming the magic correlation.

- [0060] A second phase is to use this magic correlation (α, β, γ) to compute the
- 30 logical "and" between the two chosen bits x_i , x_j , that is, the final result sought, using a conventional secure communication channel, L_c .

[0061] In the first phase, participants C_i and C_j will apply quantum gates, U and V , to input qubits in order to generate output qubits.

5 [0062] The quantum gate V transforms the state (or qubit) of a photon into an orthogonal state, in any orthonormal basis. The quantum gate U corresponds to a square root of the transformation performed by the quantum gate V .

10 [0063] On the Bloch sphere, these operations are therefore equivalent to saying that the whole quantum part is defined to within one rotation.

[0064] The qubit is generated by the server C_1 , in a first state, in an orthonormal basis.

15 [0065] According to an embodiment, this first state is denoted $|+\rangle$. This notation is, however, arbitrary, since it is sufficient, according to the invention, to have any two orthogonal states, but it allows for clearer description.

20 [0066] In the following, we will denote as $|0\rangle$ and $|1\rangle$ two orthogonal states (that is perfectly distinguishable) among the quantum degrees of freedom of the emitted photon in this orthonormal basis.

[0067] We denote as $|+\rangle$ and $|-\rangle$ two states formed by the superposition of these two orthogonal qubits. We can write:

25
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

[0068] We can also write

30
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

[0069] The gate V is a Pauli-Z gate which is equivalent to a rotation around the Z-axis of the Bloch sphere by π radians. It can be represented by the Pauli-Z matrix:

5
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

[0070] In other words, such a gate V transforms the state $|+\rangle$ into the state $|-\rangle$, and, reciprocally the state $|-\rangle$ into the state $|+\rangle$

10 [0071] As said before, the gate U is a square root of the gate V. According to one embodiment, it may be a rotation about the Z axis of the Bloch sphere by $\pi/2$ radians. In other words, by applying the U gate twice, we obtain the equivalent of a V gate.

15 [0072] In an embodiment of encoding phase difference information, the qubit $|+\rangle$ may correspond to a photon in uniform superposition over these two half-intervals. In this case, the rotations U and V correspond to a phase shift of the 2nd half-interval of π and $\pi/2$, respectively.

20 [0073] In all the cases described above and in general, the implementations are carried out by applying an appropriate modulation.

[0074] Also of interest is the paper by 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, 25 2017, 96 (6), pp.062317. (10.1103/PhysRevA.96.062317). (hal-02164423). In this paper, the states $|+\rangle$ and $|-\rangle$ are implemented using vertical and horizontal polarizations. The rotations U and V are implemented with half-wave plates.

30 [0075] Figure 3 shows an embodiment of the method, or protocol, for secure multi-party computation of the logical "AND" in which the main steps are

shown. Figure 3 is a purely illustrative flowchart and the sequence of steps can be understood without recourse to this flowchart, just as other sequences, or other divisions into steps, are possible and accessible to the skilled person.

- 5 [0076] In this example, it is assumed that two participants C_i and C_j have, at a given time, two bits, respectively x_i and x_j whose logical "and" is to be calculated.

10 [0077] In a step S1, each participant C_i , C_j determines, for example randomly, a value for its respective correlation variable α , β intended to form a magic correlation. Each participant also determines the value of two other bits, p and q respectively, also at random. These 4 random bits α , β , p , q can be determined in this preliminary step S1 or later, before these bits are needed in the computations required by the subsequent steps of the protocol.

15

[0078] In a step S2, the server C_1 prepares and sends a photon in a superposition state of orthogonal states in a given orthonormal basis.

20 [0079] According to one embodiment, the server C_1 prepares and transmits a $|+\rangle$ state which is a uniform superposition of two $|0\rangle$ and $|1\rangle$ states, to the first participant C_i . According to another embodiment, the server C_1 prepares and sends a $|-\rangle$ state. As said above, the initial state itself does not matter, it is only important that the transformation V transforms this state into an orthogonal state.

25

[0080] Note that the two participants are interchangeable, since the logical "and" is a commutative operation. Therefore, the terms "first" and "second" participants are only used to distinguish them, for the clarity of the description, without establishing any order or hierarchy between them.

30

[0081] In a step S3, the first participant C_i receives this state of the photon and applies to it a first quantum transformation formed by the succession of

quantum gates performing a rotation of angle π around the Z-axis and the other a rotation of angle $\pi/2$ around the Z-axis, this transformation depending on the two random bits determined by this first participant, that is α et p .

5 [0082] More precisely, this first transformation can be written $V^\alpha U^p$.

[0083] This notation T^e means that if the exponent e is equal to 1, we apply the transformation T and if it is equal to 0, we do not apply it.

10 [0084] The first participant C_1 can then send the qubit resulting from this transformation in the quantum communication channel L_q to the second participant C_j .

[0085] In a step S4, the second participant C_j performs a similar transformation
15 but based on the two random bits at its disposal: β and q . This second transformation can be written $V^\beta U^q$. The qubit resulting from this transformation can then be sent in the quantum communication channel L_q to the server C_1 .

20 [0086] In a step S5, the server C_1 performs a third transformation which can be written as $(U^*)^{p+q}$, where U^* is the inverse transformation of U .

[0087] According to the invention, the value $p+q$ is transmitted to the server C_1 , without communicating the individual values of p and q .

25

[0088] According to a preferred mode of implementation of the invention, the protocol is secured by secretly sharing a bit r between the two participants C_i and C_j in order to encode the communication of bits p and q to the server C_1 . Also, during step S1 (which can be extended to this step S4),

30 - the participant C_i sends to the server C_1 the bit $t_1 = p+r$ over a secure channel;

- the participant C_j sends to the server C_1 the bit $t_2=q+r$ over a secure channel.

[0089] Other secure methods can be used to transmit the value of $t_1 + t_2$ to the server C_1 , as will be seen later.

[0090] The sign "+" indicates binary addition. Since we are only interested in a single bit, this operation is equivalent to an "exclusive or"

[0091] The server C_1 can then calculate the third transformation $(U^*)^{t_1+t_2}$

[0092] After this transformation, the state of the qubit is: $(U^*)^{t_1+t_2} V^\beta U^q V^\alpha U^p |+\rangle$

[0093] This expression can be simplified, depending on the different values that the random bits p and q can take (due to the commutativity of the ports U , V and U^*) into:

- $V^\beta V^\alpha |+\rangle$ if $p=0$ and $q=0$
- $V^\beta V^\alpha |+\rangle$ if $p=0$ and $q=1$
- $V^\beta V^\alpha |+\rangle$ if $p=1$ and $q=0$
- $V^\beta V^\alpha |-\rangle$ if $p=1$ and $q=1$

[0094] Here we can recall that the gate V amounts to swapping the $|+\rangle$ and $|-\rangle$ states, so that the number of swaps depends on the value of the correlation values α and β .

[0095] We can therefore write the following truth table:

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

[0096] The server C_1 then measures the received qubit in the $\{|+\rangle, |-\rangle\}$ base, and determines the value of its correlation variable γ as follows:

- if the measure is $|+\rangle$, then $\gamma=0$

5 - if the measure is $|-\rangle$, then $\gamma=1$

[0097] From then on, we can notice that $\gamma = \alpha + \beta + (p \wedge q)$.

[0098] In other words, $\alpha + \beta + \gamma = p \wedge q$

10

[0099] This expression is that of a magic correlation between the three correlation variables α , β , γ , the binary sum of which is used to calculate the logical "and" of the two bits p and q .

15 [0100] Once this correlation is established, it allows us to calculate, in a second phase, the logical "and" for other bits, and in particular the chosen bits x_i , x_j .

[0101] It is noteworthy that this first phase is independent of the chosen bits x_i , x_j .

20

[0102] According to one embodiment, the first steps S_1 , S_2 , S_3 , S_4 , S_5 constituting a first phase, can be carried out upstream of the moment when the participants C_i and C_j have the respective bits x_i , x_j whose logical "and" is to be calculated. In other words, this first phase can be precomputed, so as to
25 reduce the computations to be performed between the moment when the bits x_i and x_j are known and the result is made available, $x_i \wedge x_j$.

[0103] This type of implementation allows significant gains in performance and security.

30

[0104] In a step S6, the participants C_i , C_j exchange a value depending on the sum between the random bit, respectively p , q , and the chosen bit, respectively x_i , x_j .

5 [0105] For example,

- the first participant C_i calculates $u1 = p + x_i$ and sends it to the second participant C_j .
- the second participant C_j calculates $u2 = q + x_j$ and sends it to the first participant C_i .

10

[0106] In a step S7, both participants C_i , C_j and the server C_1 each separately provide a value, a , b , c , respectively, such that $a+b+c = x_i \wedge x_j$.

[0107] More precisely,

15

- the first participant computes and provides $a = \alpha + x_i \wedge u2$
- the second participant computes and provides $b = \beta + x_j \wedge u1 + u1 \wedge u2$
- the server provides $c = \gamma$

20

[0108] The values of $u1$ and $u2$ are random and are shared among the participants beforehand. This sharing can be done through the conventional secure communication channel L_c .

25 [0109] It may then be verified that $a+b+c = x_i \wedge x_j$, which is the desired result.

[0110] Indeed, $a+b+c = \alpha + x_i \wedge u2 + \beta + x_j \wedge u1 + u1 \wedge u2 + \gamma$

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

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

30

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

[0111] Identical terms cancel each other out since they are binary additions on a single bit (without a carry), thus equivalent to an exclusive "or". Therefore, this expression can be simplified, effectively, into $a+b+c = x_i \wedge x_j$

5

[0112] One can thus obtain, by this simple binary sum of independent terms, the value of the logical "and" between the bits x_i and x_j chosen respectively by the first participant C_i , and the second participant C_j without their value being known by another entity than the one that chose it. Thus, the desired property of secure multi-party computation is ensured.

10

[0113] Moreover, in the case where the first phase (quantum) is carried out in advance, the phase of effective computation of this "logical and" (second phase) is very effective since it only involves a double exchange between the two participants (step S6), bit additions and the provision of the values a , b , c which can simply be summed to obtain the result.

15

[0114] According to one embodiment of the invention, the security of the method can be enhanced in various ways.

20

[0115] The conventional communication channel L_c can be secured by conventional or quantum means.

[0116] As previously described, a bit r can be shared secretly between the participants and the server. This bit can be shared using a quantum key distribution, for example.

25

[0117] Quantum key security mechanisms are known per se, and there are various commercial devices to perform this step. Among others, mention may be made of the devices "Cerberis3 QKD System" marketed by ID Quantique, "QKD System" marketed by Toshiba, or "Quantum Key Distribution (QKD)" from Quintessence Labs.

30

[0118] Another example is the patent application FR1909839 entitled "Method for secure transmission of quantum state sequences between multiple online participants over a quantum communication channel".

5

[0119] Also, a different bit, r_1 , r_2 , r_3 can be shared between each pair of the set constituted by the participants and the server. Thus, the first participant C_i and the server C_1 exchange a first bit r_1 ; the second participant C_j and the server C_1 exchange a second bit r_2 , and the first and second participants exchange a third bit r_3 .

10

[0120] During the initialization phase S_1 , it is then possible to have:

- The first participant C_i send to the server C_1 the value $t_1' = p + r_1 + r_3$
- The second participant C_j send to the server C_1 the value $t_2' = q + r_2 + r_3$
- The server C_1 can then form the values $t_1 = t_1' + r_1$ and $t_2 = t_2' + r_2$

15

[0121] The computation of a binary logical "and" can be applied to solve any computational problem distributed between the two participants C_i , C_j .

20 [0122] In the case of an application to an auction mechanism, it is assumed that each of the participants C_i , C_j holds two numbers, respectively x_i , x_j , of n bits each and representing a bid value: $x_{j,j} \in \{0, 1\}^n$

[0123] For two binary inputs a , b , we define the function $f(a,b) = 1 + a \wedge (1 + b)$. This function takes the value 1 if $b \geq a$, and 0 otherwise.

25

[0124] This function can be calculated, for one bit, according to the method previously described. Indeed, noting that $1 + b$ is a logical NOT, this function is calculated as $f(a,b) = \text{NOT}(a \text{ and } (\text{NOT } b))$

30

[0125] It is then possible to determine the winner between two bids in the auction by performing a bit-by-bit comparison of the two values x_i , x_j starting from the most significant bit, and using this comparison function f for each bit.

- 5 [0126] If f returns 0 for one bit, then $x_i > x_j$ and C_i carries the bid over C_j ; otherwise $x_j \geq x_i$ and the bid is either carried by C_j or both participants have made the same bid.

- 10 [0127] By doing this computation in both directions, that is also by swapping x_i and x_j for the second computation, it can be determined in all situations which of the participants won the auction.

Claims

1. A method for calculating a logical AND between two chosen bits, x_i , x_j held by a first and a second participants, C_i , C_j respectively, connected to each other and to a server (C_1), by at least one quantum communication channel (Lq) and one conventional communication channel (Lc), comprising
- 5 a first phase using said quantum communication channel and comprising
- a first step (S1) wherein said first and second participants randomly determine, respectively, a first α and second β correlation variable; they
- 10 each determine a random bit, respectively p and q , and transmit to said server (C_1), a value dependent on said respective random bit p , q ;
- a second step (S2) wherein said server (C_1) prepares a photon in a first state in an orthonormal basis, and transmits it to said first participant (C_i);
- 15 a third step (S3) wherein said first participant (C_i) applies a first transformation $V^\alpha U^p$ to said photon, and transmits it to said second participant (C_j), the logic gate V transforming a state into an orthogonal state and the logic gate U being a square root of the logic gate V ;
- a fourth step (S4) wherein said second participant (C_j) applies a second
- 20 transformation $V^\beta U^q$ to said photon, and transmits it to said server;
- a fifth step (S5) wherein the server C_1 performs a third transformation $(U^*)^{p+q}$, measures the state of said photon and determines a third correlation variable γ based on said state, so as to form a correlation between said correlation variables; and,
- 25 a second phase comprising
- a sixth step (S6) wherein said first and second participants exchange a value u_1 , u_2 depending on the sum between the random bit, p , q , and the chosen bit, x_i , x_j , they hold, respectively;
- a seventh step (S7) wherein said first participant calculates and
- 30 provides a first value $a = \alpha + x_i \wedge u_2$, said second participant calculates and provides a second value $b = \beta + x_j \wedge u_1 + u_1 \wedge u_2$ and said server provides the third correlation variable γ ,

so that the result of the computation of the logical "and" between said chosen bits can be obtained by summing said first and second values and said third correlation variable.

- 5 2. The method according to the preceding claim, wherein said first phase is carried out before said chosen bits are known to said participants
3. The method according to any of the preceding claims, wherein in said first step (S1) said first and second participants transmit respective values
- 10 $t_1=p+r$ and $t_2=q+r$, where r is a bit secretly shared by said first and second participants;
4. The method according to any one of the preceding claims, wherein said first state is the $|+\rangle$ state
- 15
5. The method according to any one of the preceding claims, wherein said conventional communication channel (L_c) is a secure channel.
6. A device for calculating a logical AND between two chosen bits, x_i, x_j
- 20 held by a first and a second participants (C_i, C_j respectively), connected to each other and to a server (C_1), by at least one quantum communication channel (L_q) and one conventional communication channel (L_c), comprising means for implementing the method according to one of the preceding claims.
- 25 7. The device according to the preceding claim, wherein said first and second participants belong to a chain of participants, wherein the two participants at the ends (C_1, C_N respectively) implement said server, an upstream participant being able to emit a photon, and a downstream participant (C_N) being able to receive a photon and measure its state.
- 30
8. The device according to claim 6, wherein said first and second participants belong to a ring of participants, such that a given participant (C_1)

implements said server and is able to emit a photon, receive a photon, and measure its state.

9. The device according to any one of claims 6 to 8, wherein said server
5 comprises a laser adapted to generate photons and an initial modulator adapted to modulate a degree of freedom of a photon generated by said laser.

10. The device according to any one of claims 6 to 8, wherein said first and
second participants comprise modulators capable of modulating an
10 electromagnetic field through which the photons pass in order to change a degree of freedom thereof.