CLAIMS

1. A method for delegating a quantum computation by at least one client to a server, the method comprising

- a first step (S1) comprising the transmission, by a client to the server, of a description of entanglements to be performed in a quantum memory in the server ;

- a second step (S2) comprising the emission of a sequence of quantum states by a source, distinct from said server, to at least one of said at least one client;

- a third step (S3) comprising a modification, by said at least one client, of a quantum state of said sequence,

- a fourth step (S4) comprising the transmission, by at least one of said at least one client, of said sequence to said server after the modification has been applied;

- a fifth step (S5) comprising the application, by the server, of a sequence of measurements according to a given base to qubits of the received sequence once stored within said quantum memory whose content has been entangled according to said description, and the transmission, from the server to the client, of the result of each measurement.

2. The method according to the preceding claim, wherein the quantum states supplied by said source are a superposition of orthogonal states, and the modification performed by said at least one client is in the form $Z^{\theta+c.\pi}$ wherein Z is Pauli gate according to the axis Z, θ is randomly selected from a list {0; $\pi/4$; $\pi/2$; $3\pi/4$} and c is randomly selected amongst the 0 and 1 values.

3. The method according to claim 1, wherein the quantum states supplied by said source are a superposition of orthogonal states, the method including a step of determining a subset of trapped qubits and wherein said third step comprises a modification of qubits neighboring said trapped qubits according to said description of entanglements, in the form X^dH, wherein H is the Hadamard transformation, X is a Pauli gate according to the X axis and d is selected amongst the 0 and 1 values, the method including a step of comparing, by said at least one client, a result of a measurement of one of said trap qubits with an expected result for said trap qubit, and determining a honesty of said server.

4. The method according to one of the preceding claims, wherein said at least one client comprises a plurality of clients connected to said server by one single communication line (30) by forming a chain, wherein each of said at least one client is configured to modify only a part of

the quantum states allocated thereto, wherein the transmission of said subsequence comprises a transmission, by each client that is not the last client in the chain, of said sequence to a subsequent client in the chain.

5. The method according to the preceding claim, wherein said part is determined by an allocation of a time window.

6. The method according to one of the preceding claims, wherein several clients can successively modify the same quantum state of said sequence.

7. A system for delegating a quantum computation from at least one client (10) to a server (20), the system including a source, the server and said at least one client, wherein the source is distinct from the server, wherein

- said source (40) is configured to emit a sequence of quantum states to at least one of said at least one client;

- said at least one client includes an input interface (11) for receiving said sequence, a transformation device (12) adapted to modify a quantum state of said sequence and an output interface (13) for transmitting said sequence once the quantum state has been modified; and

- said server includes a quantum memory and a measurement device (21) configured to (i) apply a sequence of measurements according to a given base to qubits of the sequence once received by the server from at least one of said at least one client and stored within said quantum memory whose content has been entangled according to a description of entanglements received from a client and (ii) transmit the result of each measurement to the client.

8. The system according to the preceding claim, wherein said transformation device (12) includes a first device for applying a first transformation aiming to prepare quantum states for performing a blind quantum computation, and a second device for applying a second transformation aiming to prepare quantum states to verify a honesty of said server.

9. The system according to the preceding claim, wherein a plurality of clients are connected to said server by one single communication line (30) by forming a chain, so that said quantum states are progressively transmitted from said source to said measurement device via the chain.

10. The system according to the preceding claim, wherein each of said clients is configured to modify only the part of the quantum states allocated thereto.

11. The system according to one of claims 7 to 10, wherein said quantum states are photons and said transformation device is an optical modulator.

12. The system according to one of claims 7 to 11, wherein said source is adapted to supply quantum states in the form of a superposition of orthogonal states, and said transformation device is adapted to perform a modification in the form $Z^{\theta+c.\pi}$, wherein Z is a Pauli gate according to the axis, θ is randomly selected from a list {0; $\pi/4$; $\pi/2$; $3\pi/4$} and c is randomly selected amongst the 0 and 1 values.