

common measurement bases, their photons will have a high likelihood to be detected in identical time slots. To not be mistaken with the quantum states, this time slot information does not contain any information of the mode bases; therefore, it can be publicly revealed (see FIG. 7).

5 The entangled photon generation process, as used in connection with the present invention, does not require or limit to any specific method of generating entangled photons. In practicing the present invention, any entanglement property can be utilized, such as given time, frequency, polarization, etc.

According to an aspect of the present invention, there is provided a method for secure communications between multiple parties, comprising the steps of:

10 transforming private information into measurement bases;
generating a plurality of sets of entangled photons, wherein each photon of said plurality of sets of entangled photons represents a corresponding optical pulse or a quantum mechanical superposition of optical pulses;
transmitting said plurality of sets of entangled photons, one set of entangled photons at a time, to
15 a plurality of communication parties, wherein each communication party of said plurality of communication parties receives a photon from each set of said plurality of sets of entangled photons in the order in which said plurality sets of entangled photons are transmitted;
assigning each set of entangled photons an index number based on the order in which said plurality of sets of entangled photons are transmitted to said plurality of communication parties,
20 whereby optical pulses corresponding to photons from the same corresponding set of entangled photons are associated with identical index numbers;

applying said measurement bases to said optical pulses and detecting said photons on said measurement bases to obtain respective data for each party of said plurality of communication parties in the order in which said optical pulses are received by each party;

generating from said respective data corresponding lists of relevant indices for each party of said plurality of communication parties; and

computing a secure communication by comparing said corresponding lists of relevant indices.

5 Moving now to summarize the present invention, it exploits quantum entanglement of photons to thereby share common information without any exchange of information regarding the photons' states. Via the superposition of the photon state, it becomes possible to exploit the true randomness and uniqueness of the chosen property to be measured (e.g., photon arrival time, photon temporal mode, photon spatial mode, etc.). Through quantum frequency conversion, for
10 instance, the methods practiced in accordance with the present invention can use the private information as the measurement basis, and therefore, determine the outcome of the quantum state. Entangled photons collapse into the same states on each communication end. However, when they are measured, only the choice of identical measurement bases will return the same results. If the private information does not match (i.e., the measurement bases are different), detected
15 photons return different results.

This disclosure is independent of the measurement bases encryption method. Regardless of how the information is encrypted given temporal modes, spatial modes, etc., the concept that is central to the present invention involves using secret information as the measurement bases of entangled photons.

20 A novel, privacy-preserving computational method that leaks zero individual data is presented in an embodiment of the present invention, which is based on quantum entanglement, quantum measurement, and in some embodiments, quantum frequency conversion. By deploying unique properties of quantum mechanics, the methods of the present invention constitute a

With the methods practiced in accordance with the present invention, it becomes possible to perform computations based on the information of multiple parties in a pool of data without revealing the actual information of each party, and without any trusted third party. The present invention therefore constitutes a solution to the zero-knowledge proof problem, which is used in authentication and verification, while also enabling secure multiparty computation, which is used in data mining and blockchain. The present invention also obviates the need for any homomorphic encryption step, which is usually the process employed to protect data-in-use, while still maintaining the absolute security of the data-in-use.

The present invention seeks to provide a privacy-preserving verification method for comparing one or more data values, numerical or otherwise, for equality (e.g., $A=B$).

The present invention seeks to provide a privacy-preserving verification method for comparing one or more numerical values to confirm or establish one or more inequalities (e.g., $A>B$).

The present invention seeks to allow for computation via communication of indices, thereby averting the revelation of secret and/or private information.

The present invention seeks to provide true private-preserving communications without the need for multiple majority honest communication parties, any kind of honest communication party, or any extra party.

The present invention seeks to provide a system and method that guarantees the probability of fooling from any party is zero. As a result, establishing participants as honest parties is not a pre-requisite for collaboration in computing and/or verifying information. In this protocol, even if some party is cheating, they cannot convince other parties that they are being honest with the outcomes that they send to the public channel.

The present invention seeks to provide true privacy-preserving computations to compare data of more than two parties by, for example, expanding the linearity of the emitted signals, thereby enabling unconditionally secured, private

What is claimed is:

1. A method for secure communications between multiple parties, comprising the steps of:

transforming private information into measurement bases;

generating a plurality of sets of entangled photons, wherein each photon of said plurality

5 of sets of entangled photons represents a corresponding optical pulse or a quantum mechanical superposition of optical pulses;

transmitting said plurality of sets of entangled photons, one set of entangled photons at a time, to a plurality of communication parties, wherein each communication party of said

plurality of communication parties receives a photon from each set of said plurality of sets of

10 entangled photons in the order in which said plurality sets of entangled photons are transmitted;

assigning each set of entangled photons an index number based on the order in which said plurality of sets of entangled photons are transmitted to said plurality of communication parties, whereby optical pulses corresponding to photons from the same corresponding set of entangled photons are associated with identical index numbers;

15 applying said measurement bases to said optical pulses and detecting said photons on said measurement bases to obtain respective data for each party of said plurality of communication parties in the order in which said optical pulses are received by each party;

generating from said respective data corresponding lists of relevant indices for each party of said plurality of communication parties; and

20 computing a secure communication by comparing said corresponding lists of relevant indices.

2. The method of Claim 1, wherein said applying step is performed independently by each party of said plurality of communication parties, and/or

wherein the method further comprises the step of establishing rules for effecting said

25 transforming step.

3. The method of Claim 1, further comprising the step of continuously sending a reference signal to each party of said plurality of communication parties, said reference signal having a predetermined period,
wherein, preferably, one optical pulse is transmitted to each party of said plurality of communication parties for each said period of said reference signal.
4. The method of Claim 1, wherein said computing step is performed publicly, and/or wherein the method further comprises the step of announcing said corresponding lists of relevant indices.
5. The method of Claim 1, wherein said private information never leaves said plurality of communication parties, and/or wherein said computing step includes determining whether respective private information is the same for each party of said plurality of communication parties.
6. The method of Claim 1, wherein said computing step includes assessing an inequality between respective private information of each party of said plurality of communication parties, and/or wherein said measurement bases comprise photon arrival times, wherein said photon arrival times preferably comprise discrete time bins.
7. The method of Claim 1, wherein said applying step includes subjecting said photons to a quantum measurement module, wherein said quantum measurement module preferably comprises sum frequency generation.
8. The method of Claim 1, wherein said private information is a password, authentication codes, data strings, values, or a set of private data needed in a multiparty computation function, wherein the method preferably comprises a step of verifying shared knowledge of said private information without communicating said private information.
9. The method of Claim 1, wherein said computing step constitutes data processing at zero knowledge, and/or

wherein said computing step involves data mining.

10. The method of Claim 1, wherein said measurement bases comprise spectral modes, temporal modes, or spectral-temporal modes of said photons, and/or wherein said photons of each set of said plurality of sets of entangled photons are received by their respective parties of said plurality of communication parties at the same time.

11. The method of Claim 1, wherein said photons of each set of said plurality of sets of entangled photons are received by their respective parties of said plurality of communication parties at different times.

12. The method of Claim 1, wherein said step of transforming private information into measurement bases includes the step of performing computation of information such that the context of said secure communication is not restricted to numbers, and wherein the step of performing computation of information includes the step of performing at least one of addition, subtraction, multiplication, and division.

13. The method of Claim 12, wherein parties of said plurality of communication parties process public data using private computation algorithms and transform the results into measurement bases, by which the computation algorithms amongst communication parties are compared.

14. The method of Claim 1, where said corresponding lists of relevant indices by communication parties are analyzed to identify the statistical relation between the lists of relevant indices, by which the relation between the private information is estimated.

15. The method of Claim 14, where said private information corresponds to a private number held by each communication party, and said statistical relation includes the conditional probabilities of the list of relevant indices reported by one communication party on that from another party

wherein, preferably, the statistical relation is used to determine the ranking of the number held by each communication party, but the values of said private numbers are, preferably, not revealed during the process.