

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.
3. The method of Claim 1, further comprising the step of establishing rules for effecting said
- 25 transforming step.

4. 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.
5. The method of Claim 4, wherein one optical pulse is transmitted to each party of said plurality of communication parties for each said period of said reference signal.
6. The method of Claim 1, wherein said computing step is performed publicly.
7. The method of Claim 1, further comprising the step of announcing said corresponding lists of relevant indices.
8. The method of Claim 1, wherein said private information never leaves said plurality of communication parties.
9. The method of Claim 1, wherein said computing step includes determining whether respective private information is the same for each party of said plurality of communication parties.
10. 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.
11. The method of Claim 1, wherein said measurement bases comprise photon arrival times.
12. The method of Claim 11, wherein said photon arrival times comprise discrete time bins.
13. The method of Claim 1, wherein said applying step includes subjecting said photons to a quantum measurement module.
14. The method of Claim 13, wherein said quantum measurement module comprises sum frequency generation.
15. 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.
16. The method of Claim 15, further comprising the step of verifying shared knowledge of said private information without communicating said private information.

17. The method of Claim 1, wherein said computing step constitutes data processing at zero knowledge.
18. The method of Claim 1, wherein said computing step involves data mining.
19. The method of Claim 1, wherein said measurement bases comprise spectral modes, 5 temporal modes, or spectral-temporal modes of said photons.
20. 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 the same time.
21. The method of Claim 1, wherein said photons of each set of said plurality of sets of 10 entangled photons are received by their respective parties of said plurality of communication parties at different times.
22. 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 15 performing computation of information includes the step of performing at least one of addition, subtraction, multiplication, and division.
23. The method of Claim 22, 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.
- 20 24. 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.
25. The method of Claim 24, where said private information corresponds to a private number held by each communication party, and said statistical relation includes the conditional 25 probabilities of the list of relevant indices reported by one communication party on that from another party.

26. The method of Claim 25, where 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 not revealed during the process.