SYSTEMS AND METHODS FOR QUANTUM-SECURED, PRIVATE-PRESERVING COMPUTATIONS

Cross-Reference to Related Application

This application claims the benefit of and priority to U.S. Provisional Patent Application Serial No. 62/923,322 filed October 18, 2019, the entire disclosure of which is incorporated herein by reference.

Field of the Invention

The present invention relates to secure data sharing and processing among untrusted parties that minimizes the risk of privacy breach and sensitive information compromise. More particularly, the present invention pertains to privacy-preserving computation and quantum implementations thereof, zero knowledge data processing and quantum implementations thereof, and data mining, authentication and verification.

Statement Regarding Federally Sponsored Research

None.

Background of the Invention

Maintaining the security of data, especially during exchange of information, is an increasingly urgent issue. Current secure multi-party computation methodologies protect individual information by modifying the original data with techniques such as noise adding, information blocking, data encryption, etc. However, these techniques only guarantee the privacy to a certain level, through distortion of information, because in some applications, such as data mining, extracting distorted knowledge may make them inoperable or perform inefficiently. Mitigating these issues, however, often comes at the cost of information security (e.g., by making it susceptible to leaks of personal information data).

Even with such techniques involving data modification, privacy is not provably (i.e., unconditionally) secured against known privacy intrusion methods. In other words, while those methods may prevent or challenge these privacy intrusion methods, they do not guarantee

information security, or are only conditionally secure. In many existing cyber technologies, data-at-rest and data-in-transit are encrypted, but data-in-use might not be. To protect data-in-use, homomorphic encryption techniques may be applied. However, this is a complex process that is limited in applicability and capability.

Furthermore, current technology typically requires either a trusted set up (i.e., a method involving a trusted third party serving as an intermediary for the information) or the proof size becomes excessive. For instance, blockchain privacy technology has been one attempt to provide zero-knowledge proof, conducted via Boolean circuits. While it does not require a trusted setup or any interaction between prover and verifier, the proof size is too large to be used in blockchain or limited computing devices. It is also not provably secure.

Summary

Before summarizing the present invention, the following terms are being defined to facilitate the discussion and consideration of the present invention.

Measurement basis is what is used to measure the state of each photon. The type of measurement basis can be chosen as photon arrival times, spectral modes of photons, etc. The present invention is applicable to any choice of measurement bases, so long as quantum entanglement can be established on those bases. The type of measurement basis should be announced publicly to parties in the computation pool. FIG. 3 describes an example of measurement basis choice based on photon arrival time.

Mutually unbiased bases are sets of state bases for a quantum system, each set forming a complete description of the system, with the inner product of any state basis in one set with any basis in another having about the same amplitude.

Pulse index represents the time slot number of a detected photon. All parties in the communication pool are synchronized to a common reference signal to keep track with their detected photon time slot. The system should be set up such that at most one entangled photon pair can be created during each period of the reference pulse. Therefore, if Alice and Bob have

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).

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:

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 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, 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.

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 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 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.

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

fundamentally new method to secure privacy, distinct from traditional approaches. In other words, the present invention involves a fundamentally new approach to address the challenge of private data sharing and data mining, which are becoming increasingly critical as the data industry expands.

In practice, the present invention provides a methodology immune against attacks on encryption protocol because the private information never leaves the local host to the network, either directly, or under encryption cover. Moreover, this methodology provides high efficiency because there is no complex encryption and decryption computation.

The present invention presents a system and method to perform unconditionally secured private communication, without the need to establish the integrity of any participant, or use an honest third party. Three main essences make the protocol established by the present invention unconditionally secure: First, private data stays with local hosts (i.e., they are never transmitted through communication channels, either public or private, during the computation process). Second, entangled photons continuously provide entangled states with truly random measurement outcomes at each local host for correlation verification. Third, the computation process occurs in a public channel (i.e., no private channel or keys are needed).

Specifically, the private information to be computed or processed jointly between the parties is translated to measurement bases chosen locally by each party according to publicly announced and agreed upon rules. The measurement bases are mutually unbiased, so that at each party, the quantum states are projected onto a particular set of mutually unbiased states. Only when the parties choose the same set can the measurement outcomes be correlated. Entangled photons are sent to each party in a sequence of optical pulses during the computation. Each party then measures the state of each photon using his or her measurement bases. Publicly, each party announces indices of the pulses where photons are detected. By comparing the correlation of each party's indices, computation is completed, without revealing the secret private information.

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

multi-party communication wherein zero knowledge is revealed to any party in the computation pool, or outside the computational pool.

Brief Description of Figures

For a more complete understanding of the present disclosure, reference is made to the following drawings, in which:

FIG. 1 is a flow chart of an exemplary system in accordance with an embodiment of the present invention;

FIG. 2 is a flow chart of an exemplary method in accordance with an embodiment of the present invention;

FIG. 3 is a chart and table illustrative of base conversion for an exemplary photon arrival time basis;

FIG. 4 is a pair of tables demonstrating encryption using the arrival time basis of FIG. 3;

FIG. 5 is a schematic chart illustrating a case in which common time bins are chosen as the bases by two parties;

FIG. 6 is a schematic chart illustrating a case in which different time bins are chosen as the bases by two parties;

FIG. 7 is a schematic chart illustrating a process of index selection in accordance with an embodiment of the present invention;

FIG. 8 is an alternate schematic chart and table illustrative of base conversion for an exemplary photon arrival time basis;

FIG. 9 is a system diagram illustrating an exemplary case in which the private information of two parties is different; and

FIG. 10 is a schematic chart illustrating a case in which private information is compared and one party's information has a larger value than the second party's information.

Detailed Description of Exemplary Embodiments

The methods of the present invention exploit properties of quantum mechanics to provide unconditional security to private information. As an operating principle, the information itself is converted into the measurement bases for the entangled photons by which the encryption takes place. Referring now to FIG. 1, an exemplary process is outlined. The data of interest remains with each of the parties in the pool and are never transmitted through communication channels, whether they be private or public, during the computation process. Instead, entangled photons received by each of the parties in the pool provide continuous, truly random entangled states that allow for verification through correlation of the entangled states. Meanwhile, the computational implementation can occur in a completely public channel, without requiring access to the unencrypted, secret data. Therefore, no private channels or encryption keys are necessary.

For the purpose of simplicity, the following discussion will assume that the computation pool for the absolute secure computations consists of only two parties; however, it should be understood that the methods of the present invention may be applied to mutual computations of more than two parties as well. This can be achieved by using higher orders of nonlinearity, for example, by creating three entangled photons for three parties, creating four entangled photons for four parties, and so on.

FIG. 2 is a flow-chart overview of a generalized method in accordance with the present invention. Each set of private information 110, 112 undergoes a corresponding encryption (i.e., conversion) step 114, 116, respectively. Entangled photon generation 118 then occurs. The present invention does not require or limit any particular method of generating entangled photons. Any entanglement property can be utilized, such as given time, frequency, polarization, etc. The generated photons then undergo quantum measurement modules 120, 122, respectively (e.g., quantum frequency conversion) and are measured in accordance with the encrypted bases 114, 116, respectively. Announcement of indices 124, 126 then occurs, based on the application of modules 120, 122, and finally, public computation 128 of the indices 124, 126 occurs.

In one embodiment of the present invention, it is desirable to compare data values for the purpose of determining if such values are equal (i.e., A=B). As a concrete example, suppose two people (i.e., Alice and Bob) wish to determine if they have the same birthday. However, privacy is desired to the extent that neither party wishes to disclose his or her birthday to the other, or anybody else, while performing the comparison, unless they have the same birthday. A further condition is that if their birthdays match, no one else but Alice and Bob should be able to glean their birthdays from what is communicated between the two parties by conventional communication means and/or shared computing resources.

As an initial step of an exemplary process of the present invention, the private information can be converted into measurement bases. This can be achieved by considering each bit of information as a basis in the set. In an embodiment, the type of basis used is photon arrival time; although, it should be noted that any measurement bases can be chosen, so long as quantum entanglement can be established on those bases. For instance, the spectral modes of the entangled photons can constitute an alternative measurement basis.

In order to prevent either party from cheating or trying to guess the measurement basis the other party uses, the measurement bases will be mutually unbiased. In other words, the measurement shall be performed under certain sets of mutually unbiased bases, as chosen by each party according to publicly announced and agreed upon rules.

FIG. 3 is an example of a photon arrival time basis set. In this example, Alice's birthday is February 25, 1995, while Bob's birthday is April 27, 1966. FIG. 4 shows how their information is encrypted into measurement bases. This process is done locally by each party.

The measurement bases are applied to a first pulse train of entangled photons (i.e., signal ("A")) and a second pulse train of entangled photons (i.e., idler ("B")) prepared by Alice, Bob, or any third party. Signal "A" is sent to Alice, while idler "B" is sent to Bob. The entangled state can be described as:

$$|\boldsymbol{\Psi}\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d}|t_j^s\rangle\,|t_j^i\rangle$$

where $|t_j^s\rangle$, $|t_j^i\rangle$ are the superpositions of states that signal and idler photons can collapse into, and d is the number of dimensions in Hilbert space of the photons. In practice, the actual quantum states will deviate from the above ideal form, but will nonetheless allow for computing and operation. For example, in time bin entanglement, d is the number of time bins (i.e., the number of possible timespans in which the photon may arrive). In this specific example, photon arrival time basis set has d = 36. In other words, the Hilbert space of the quantum superposition of the states is represented by thirty-six (36) bases, corresponding to the thirty-six (36) respective distinct time bins (i.e., t_1, t_2, t_3... t_{36}). As shown in FIGS. 3 and 4, each bit of data is converted to a corresponding time bin dependent on its value. Accordingly, each birthday is translated from eight digits (two for the day, two for the month and four for the year) into eight corresponding quantum states (i.e., time bins).

When Alice and Bob receive the entangled photons, each of them then measures with the measurement bases that they have prepared locally. For Alice and Bob to detect photons from the same pair, they should use common measurement bases to project onto the entangled state. It should be emphasized that the secret information itself is transformed into the measurement bases that are projected onto the entangled state.

$$\langle t_j^s\, t_k^i \mid \Psi\rangle = \delta_{j,k} \text{ where } \begin{cases} \delta_{j,k} = 1, if\ j = k \\ \delta_{j,k} = 0, otherwise \end{cases}$$

In one embodiment, the quantum measurement module is a sum frequency generation (SFG) process. Signal photon "A" has frequency $\omega 1$ while idler photon "B" has frequency $\omega 1'$. Each interacts with its respective measurement bases photons of $\omega 2$ and $\omega 2'$ to produce ω and ω' where

$$\omega = \omega 1 + \omega 2$$

$$\omega' = \omega 1' + \omega 2'$$

If Alice and Bob have the same private information (i.e., A=B), they should have the same choice of measurement bases, which means they choose to convert the same time bins during the SFG. FIG. 5 demonstrates this case where j = k. In this scenario in which they convert the same time bin, it is expected that the measurements made will observe the same detection or non-detection of a photon following the collapse of the arrival time superposition. Otherwise, as FIG. 6 illustrates, if detection occurs for Alice but not Bob or vice versa, it means they have different measurement bases choice ($j \neq k$).

FIG. 9 provides a system-level diagram of the computation process in which some of the chosen measurement bases differ between the parties (i.e., the secret information is not the same). In one embodiment, the measurement bases photon or the pump photon has very narrow temporal width compared to the entangled photon pulse width.

Following the application of measurement bases, Alice and Bob continuously and simultaneously announce to the public channel the index of pulse in the pulse train when a photon is detected on their ends. For example, in FIG. 7, Alice announces REF #1, #2, #4, …, #(n + 1), while Bob announces REF #1, #2, …, #n, #(n + 1).

The pulse index represents the time slot number of a detected photon. All parties in the communication pool are synchronized to a common reference signal to keep track of their detected photon time slot. The system should be set up such that at most one entangled photon pair can be created during each period of the reference pulse. Therefore, if Alice and Bob have common measurement bases, their photons will have a high likelihood to be detected in identical time slots. Contrary to the quantum states, this time slot information does not contain any information of the mode bases; therefore, it can be publicly revealed with little consequence.

Once the reference indices are publicly announced, the computational step can be initiated. An exemplary process compares if the amount of common reference indices is larger than a certain threshold. The threshold is determined by the level of confidence and system noise level. In one embodiment, the probability of common reference, $P(A \cap B)$ is defined as the number of common reference indices over the total number of the pulses under test. A sample criterion can be set as P_threshold=100 *P(A)*P(B), with P(A) and P(B) being probability of photon detection rate for Alice and Bob, respectively, calculated as their respective number of total pulses with detection over the total pulses under test. In this example, the threshold is set at one hundred times the predicted theoretical probability of both Alice and Bob detecting a photon at a particular index as calculated from the experimental probabilities P(A) and P(B). If the experimental probability of both Alice and Bob detecting a photon at a particular index, $P(A \cap B) >$ P_threshold, then the two measurements are said to be correlated, which indicates that the same measurement bases have been used by Alice and Bob, and therefore, they have the same birthday. Alice and Bob accomplish the comparison without birthday information ever leaving either individual. Otherwise, the two measurement bases are not the same, or there is no conclusive judgement whether they are the same or not.

For the scenario of determining inequalities (e.g., $A > B$ or $A < B$), as opposed to a comparison for equality ($A=B$), the protocol is based on the following postulate: there is either no loss, or equal loss when transferring entangled photons from the source to each party. The procedure is analogous to the scenario of verifying if $A = B$ prior to the performance of the computational step described in the preceding paragraph. Nonetheless, a suitable measurement bases encryption process still needs to be provided. FIG. 8 is an example of how the secret information may be encrypted to be used as measurement bases for the case of inequalities. In this example, if Alice and Bob want to compare their ages, where Alice is 21 years old and Bob is 15 years old. Alice's age is higher, and therefore, it is encrypted as larger pulse width compared to Bob's. The translation of the measurement bases to pulse widths is illustrated in FIG. 10.

Upon reaching the aforementioned computational step, the reference indices are collected to perform conditional probability as follows:

$$P(A|B) = (P(A \cap B))/(P(B)) \quad \text{and} \quad P(B|A) = (P(A \cap B))/(P(A))$$

where P(A|B) is the probability of detecting a photon on Alice's detection setup, given that a photon had already been detected on Bob's side, and P(B|A) is the probability of detecting a photon on Bob's detection setup, given that a photon had already been detected on Alice's side, with P(B) being the probability of detecting a photon on Bob's detection setup and P(A) being the probability of detecting a photon on Alice's detection setup, and where $P(A \cap B)$ is the probability of detecting a photon on Alice's side and Bob's side, these latter three probabilities calculated as previously described hereinabove.

Because Alice's measurement bases correspond to larger pulse widths for the purpose of this example, $P(A|B) > P(B|A)$. Therefore, on the public channel, from the reference indices announced by Alice and Bob, it can be determined that $A > B$.

The method and system described herein can perform unconditionally secured private computation between parties, as the private information to be computed is translated to measurement bases locally by each party. With entangled photons being sent to each party in a sequence of optical pulses during the computation, each party can independently measure the state of each photon using his or her measurement bases. Each party can then announce indices of the pulse where a target state is detected. By comparing the correlation of each party's indices, the computational process is completed, without ever revealing the secret/private information. This makes the methods of the present invention immune against attacks on encryption protocol because the private information never leaves the local host to the network, either directly, or under encryption cover.

Additionally, the system and method of the present invention accomplish true private-preserving computations without ever requiring multiple honest communication parties, any kind of honest communication party, or any extra party at all. The present invention also minimizes the probability of fooling from any party to near zero. The system and method can be further extended to provide private-preserving computations for multiple communication parties where absolute zero knowledge is either revealed to any party in the computation pool or anyone else outside the computation pool.

In this protocol, no private information is revealed under any kind of encrypted data in the public channel. Therefore, meaningful attacks to the protocol can only come from dishonest parties within the communication pool. We describe attack models below and specify design requirements to secure the system unconditionally.

Attack 1: At Bob's local host, instead of preparing the quantum MUBs corresponding to his private information, he uses a beamsplitter (BS) to split the light into k branches, and then uses k numbers of single photon detector to measure all given k MUBs simultaneously. Hence, if there is N number of photons expected to be detected in the correct MUBs, this attack model allows Bob to detect N/k number of photons per branch. This attack could allow Bob to acquire information on Alice's measurement bases, thus her private information, by computing the correlation of the REF IDs Bob obtains in each channel with those by Alice. To secure the system against this type of attack, the size of MUBs should be large enough such that N/k is less than or comparable to 1, or such that the correlation of the REF IDs by Alice and Bob cannot be reliably derived.

Attack 2: Given k is the size of MUBs, at Bob's local host, instead of preparing the quantum MUBs corresponding to his private information, he uses a beamsplitter to split the coming light into m branches ($m<k$), and then uses m number of single photon detector(s) to measure m MUBs

simultaneously. This gives Bob a chance to beat the noise level of matched REF IDs if the MUBs containing private information happen to be in the set of m MUBs he chose. By constantly swiping through all different sets of m MUBs among the k MUBs during measurement, Bob has a chance to collect part of the private information. To secure against this attack, private information can be encrypted to quantum measurement bases using the secret sharing encryption methods. This scheme distributes private information into n pieces such that if Bob collects fewer than n pieces, he has no more information about the private information than as if he collects zero pieces. Only a collection of all n pieces can recover the private information. Examples of the secret sharing encryption methods can be found here: https://en.wikipedia.org/wiki/Secret_sharing.

Attack 3: Bob pretends to share the same information with Alice, or holds the information Alice is looking for, by creating a fake list of REF IDs to pass the correlation test. To secure against this attack, Alice and Bob will distribute their respective private information into n pieces, either directly or by using secret sharing encryption, the latter adopted to ensure zero information exposure. Then, they will perform private computing on each of the n information pieces sequentially, with Alice and Bob taking turns to first announce the REF IDs for each. For example, for the 1st piece, Alice will announce the REF IDs first, followed by Bob. For the 2nd piece, Bob will announce the REF ID first, followed by Alice. Each party will choose to terminate the communications with each other at any point when the correlation test fails. In this way, neither party can pretend to have the information by making fake REF ID lists.

For the reasons above, the present invention may assist in a variety of contexts. In data mining, it can enable multiple databases to perform collaborative communication while preserving privacy. In the context of electronic auctions, bidders may be able to keep their bid prices a secret while still allowing auctioneers to recognize the highest bid. Yet another envisioned use is enabling zero-knowledge authentication, wherein one party can prove its

identity by showing knowledge of a password, while not revealing it for any other party to see. A fourth, not necessarily final, application can involve blockchain multiple party communication, wherein multiple participants collaborate on a computation over an existing blockchain, without the need for a trusted outside party.

It will be appreciated by those skilled in the art that while the invention has been described above in connection with particular embodiments and examples, the invention is not necessarily so limited, and that numerous other embodiments, examples, uses, modifications and departures from the embodiments, examples and uses are intended to be encompassed by the present invention described herein.

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 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 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;

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.

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 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.