

QUANTUM KEY DISTRIBUTION NETWORK AND METHOD

FIELD OF INVENTION

The present invention relates broadly to a quantum key distribution network and method.

5

BACKGROUND

Any mention and/or discussion of prior art throughout the specification should not be considered, in any way, as an admission that this prior art is well known or forms part of common general knowledge in the field.

- 10 Quantum Key Distribution (QKD) is an optical technology that enables the generation of correlated but private keys at distant locations sharing an optical link. QKD is primarily a point-to-point technology and is often marketed as such.

- 15 QKD in its most mature form is hence a point-to-point method for delivering automated private encryption keys. This works well for two-party communication, but sometimes it is necessary to have multiple parties on a small network being able to communicate with each other using keys delivered via QKD.

- 20 QKD networks based on a single source of entangled photon pairs have been discussed in the literature previously. However, this requires engineering the source to have a specific bandwidth, and then using wavelength division multiplexing techniques to actively route photons to different parties. The installation problems are challenging with this approach.

For small networks, QKD is often marketed with a central co-ordinating centre or common node that manages keys between all parties. The common node actively manages keys between all the nodes. This common node is also known as the “trusted-node”. The use of trusted-nodes can be disadvantageous because:

- 25 a. long term storage of keys for the entire network is located at a central location. This creates a high value target with a single point of failure.
- b. when using prepare-and-send QKD, crucial elements such as the light source must be located within a trusted node. This makes it difficult to outsource the QKD service to 3rd party service providers.
- 30 An alternative approach to network QKD is to equip each node with a transmitter, and then ensure that the node has an optical connection to every other node on the network. While this avoids the challenge of “trusted- nodes” it greatly increases the requirements on the optical network.

Embodiments of the present invention seek to address at least one of the above problems.

SUMMARY

In accordance with a first aspect of the present invention, there is provided a quantum key distribution network comprising:

5 a source configured to generate photon pairs based on spontaneous parametric downconversion;

a splitter configured for splitting photons generated by the source into different optical links;

10 a plurality of nodes configured to receive the photons via respective ones of the optical links; and

a communication link between the nodes for exchanging timing information about the reception of the photons between the nodes to determine photons of one pair being received by two of the nodes.

15 In accordance with a second aspect of the present invention, there is provided a method of quantum key distribution in a network, comprising the steps of:

generating photon pairs based on spontaneous parametric downconversion using a source;

splitting photons generated by the source into different optical links using a splitter;

20 providing a plurality of nodes configured to receive the photons via respective ones of the optical links; and

providing a communication link between the nodes for exchanging timing information about the reception of the photons between the nodes to determine photons of one pair being received by two of the nodes.

25 BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:

30 Figure 1 shows a schematic drawing illustrating an asynchronous entangled photon pair source for a network according to example embodiments.

Figure 2 shows a schematic diagram illustrating photon pairs emitted by the source in a network with N nodes being subjected to a passive 1/N splitter, according to an example embodiment. Each photon experiences a 1/N probability of being directed to a single node.

The probability that both photons in the pair end up at a single node, and are not useful for QKD is $1/N/N$. Each node carries out the conventional QKD protocol with every other node according to an example embodiment. The splitter can be built completely out of passive components according to example embodiment, such as, but not limited to, partially silvered mirrors, partially transmitting beamsplitters, or even spatial demodulators. Furthermore, the routing of the photons to the nodes can also be built entirely out of passive components according to example embodiments.

Figure 3(a) shows a graph illustrating the key rate fraction for the entire network and for any two parties according to example embodiments, relative to a standard 2-node QKD network. As the number of parties increases, the overall network becomes more efficient but any two nodes will have a lower key rate.

Figure 3(b) shows a graph illustrating the increase in network overhead according to example embodiments, assuming that all parties carry out the standard QKD protocol in those embodiments.

Figure 4 shows a schematic drawing illustrating the QKD process performed in a network according to an example embodiment.

Figure 5 shows a flowchart illustrating a method of quantum key distribution in a network, according to an example embodiment.

DETAILED DESCRIPTION

Embodiments of the present invention provide a solution to end-users who require a small network to be able to perform encryption tasks using keys delivered via quantum key distribution (QKD).

Embodiments of the present invention work by having all parties on the network sharing a centralized source of entangled photon-pairs. The central source uses a passive splitter to distribute photons with $1/N$ probability to the N nodes in the network. In this way, each node will always share entangled photons with every other node, advantageously enabling, for example, the conventional two-party QKD protocol to be carried out but in a network environment.

The network architecture according to example embodiments advantageously does not require a classical key management scheme. Instead all parties on the network can derive a key with every other party. In addition, the network according to example embodiments is powered by a single centralized source of entangled photon-pairs. Each party, or node, on the network requires only a single optical link to the centralized source. By making this a direct optical link, the need for intermediate “trusted-nodes” is advantageously removed.

Such a network according to example embodiments can advantageously be built entirely out of passive optical components removing the need for active control over switches, relays or circulators. An advantage of passive components in an entangled photon distribution network is that these components (e.g. beamsplitters) do not need to be trusted, further simplifying the network requirements. Furthermore, the centralized source of entangled photon-pairs is operated asynchronously, so that the photon-pairs are generated at random times. By using the intrinsic timing between the photon-pairs, the nodes can generate a timing synchronization signal, as will be described in more detail below for example embodiments. This advantageously removes the need for an additional time service common to all nodes within the network. In some embodiments of the network, the entangled photons themselves are used to provide a time-synchronization service. Finally, the use of entanglement allows a 3rd party service provider to operate the photon source on behalf of end-users who are operating the nodes, without having to be a “trusted provider”.

Embodiments of the present invention can be implemented very simply, and do not require any active control over the bandwidth. In example embodiments the photons are in the general transmission window of the optical channel, e.g. in the C or O band for fiber based networks. The “splitter” for distributing photons to the user nodes can be built out of any passive light splitting element in various embodiments. Examples are semi-silvered mirrors, partially transmitting beamsplitters or spatial demodulators. The “splitter” is not tied to any specific switching technology such as wavelength division multiplexers (WDM).

The features of an example embodiment of the present invention can include the following:

1. The network will be serviced only by a centralized source of entangled photon-pairs.
2. Each node on the network will have only one optical link to the central source.
3. The centralized source is operated asynchronously with the photon-pairs generated at random times. This is achieved by using a pump laser operating in continuous-wave (CW) mode in an example embodiment.
4. The intrinsic timing between photon-pairs (which is on the order of a few femto-seconds) enables any two nodes to achieve timing synchronization for performing QKD. This removes the need for an additional timing service within the network.
5. In some embodiments of the network, this feature can be used as a time synchronization service.
6. The optical link between source and node is direct and can be built entirely out of passive components.

As mentioned above, no active devices are needed according to example embodiments. This is highly advantageous in a security context as the command signals sent to active components such as circulators, switches or relays must also be secured. The passive components in our networks according to example embodiments (such as beamsplitters or

connectors), do not need to be trusted. Embodiments of the present invention enables 3rd party network operators who do not have to satisfy a “trusted” arrangement to provide photons as a service to end-users.

When using an entangled photon pair source for the carrier photons according to example
 5 embodiments, the quality of the quantum correlations between the photon pair is used to quantify the security of the derived key. The quality of the correlations for entanglement is checked against a mathematical expression known as the Bell Inequality. This enables a 3rd party to make commercial provision of the photon pairs because any tampering by the 3rd party or any other eavesdropper will affect the quantum correlations, resulting in a drop in
 10 quality, and unveils the tampering efforts.

With reference to Figure 1, the asynchronous operation of the photon-pair source 100 for a network according to example embodiments follows a photon-pair generation process, known as Spontaneous Parametric Downconversion (SPDC), and can be achieved when a signal 102
 15 from a pump laser 104 passes through a nonlinear medium 106 with $\chi^{(2)}$ nonlinearity. These media 106 are typically crystals of some kind. During SPDC a single pump photon is sometimes split into two lower energy photons 107a, b obeying energy and momentum conservation. When the pump laser 104 is operating continuously, in CW-mode, the time interval between the generation of one photon-pair and the next is random. However, for each photon-pair 107a, b the timing synchronization between the photons of each pair is on the
 20 order of a few femto-seconds. For this reason, the pair-production process is said to be asynchronous. However, the detected presence of one photon indicates the presence of its twin to within a very precise time. With reference to Figure 2, if the photon-pairs generated within the central source 100 were distributed across different nodes 1, ..., N equally, this enables each node to perform timing synchronization with every other node. This
 25 advantageously removes the need for the QKD network 200 to rely on an external timing service.

To use the entangled photon pair source 100 in the network 200 with N nodes (where N is greater than 2), one only has to pass the photon pairs through a $1/N$ splitter 202. After this
 30 splitter 202, the probability that both photons end up at the same node (and being unuseable) is $1/N^2$ leading to a network yield of $1 - 1/N$. Any pair of nodes e.g. 1, 2 within the network 204 will have a key rate of $2/N^2$.

Consider a network of four nodes and let us label the photons within a pair as the signal and idler photons.

Each individual photon will be subjected to a $1/4$ splitter. So, for both signal and idler photons
 35 to end up at the same node (and be of no use to QKD), the probability is $1/16$. This is true for all four nodes, so the total unuseable fraction is $1/4$. Conversely, the total useful fraction is $1 - 1/4 (1 - 1/N)$, or $3/4$.

Now consider two different nodes 1 and 2 out of the four nodes. The probability that the signal photon ends up at node 1 is $1/4$, while the probability that the idler photon ends up at

node 2 is $1/4$. This combined probability is again $1/16$. The same combined probability holds for idler at node 1 and signal at node 2. So the total fraction of useful photon pairs between nodes 1 and 2 is $1/8$ ($2/N^2$).

Figure 3(a) shows the effect of the network size on the key rates for the overall network according to example embodiments (curve 300) and any 2-party yield within the network according to example embodiments (curve 302), relative to the conventional two-node QKD connection (key rate = 1), while Figure 3(b) shows the impact of the network size on communication overheads for the network according to example embodiments (curve 304), relative to the conventional two-node, point-to-point QKD connection (overhead = 1). As it is assumed that all parties carry out the conventional two-party protocol for QKD within the network according to example embodiments as illustrated in Figure 3(b), the overhead scales linearly with the number of links in the network according to example embodiments (link number = $N(N-1)/2$). There are a few ways to mitigate this increased overhead, e.g. by having a sequential communication sequence or improving the two-way protocol according to preferred example embodiments. What is unavoidable, however, is the drop in key rate for any two nodes in the network according to example embodiments, see curve 302. Putting the information in the two graphs in Figures 3(a) and (b) together a network size of not more than 15 is recommended for example embodiments, but can be pushed up further depending on the ability of the end-user to manage network overhead, or tolerance for a lower key rate according to various embodiments.

Figure 4 shows a schematic diagram illustrating the QKD process in a network 400 according to an example embodiment. As described above, the asynchronous operation of a photon-pair source 402 for the network 400 according to an example embodiment follows a photon-pair e.g. 404, 406 generation process, SPDC. For each photon-pair e.g. 404, 406 the timing synchronization between the photons of each pair is on the order of a few femto-seconds. The generated photon pairs e.g. 404, 406 are transmitted to an $1/N$ splitter 408 of the network 400 via an optical link 409, which can be direct and entirely built from passive components in a preferred embodiment. The photons are randomly directed via the $1/N$ splitter 408 to the nodes of the network 400, including to the node 410 labelled Alice and the node 412 labelled Bob, via respective optical links 414, 416, which can also be direct and entirely built from passive components in a preferred embodiment. Also shown in Figure 4 is one of the other nodes 418 of the N nodes of the network 400, with its corresponding optical link 420 to the $1/N$ splitter 408. As will be appreciated by a person skilled in the art, the network 400 thus provides direct optical links between the source 402 and each of the nodes e.g. 410, i.e. via link 409 and e.g. link 414.

In the scenario illustrated in Figure 4, two photons 421, 422 of one correlated pair 424 generated by the source 402 are arriving at Alice's node 410 and at Bob's node 412, respectively. As described above, the detected presence of one of the photons 421, 422 at nodes 410, 412 indicates the presence of its twin to within a very precise time. This enables Alice and Bob to perform timing synchronization with each other by exchanging timing information on the detected arrival via an alternative communication channel 424, such as,

but not limited to, a wired or wireless local area network (LAN) network. This advantageously removes the need Alice and Bob to rely on an external timing service, since only relative timing information is required. It is noted that for identification of pairs as such, there is no need to invoke Bell Inequality. Furthermore, to derive a secret key, the Bell
5 Inequality is not the only way to do so – one can, for example just use the Quantum Bit Error Rate (QBER), as will be appreciated by a person skilled in the art.

Once the photon pairs between Alice and Bob have been identified from their timing correlations, Alice and Bob carry out the conventional postprocessing steps of QKD, namely: basis sifting, error correction and privacy amplification. These steps enable Alice and Bob, or
10 any other pair of nodes on the network, to derive a secure key from the quantum signals, as will be appreciated by a person skilled in the art..

Embodiments of the present invention can have a number of advantages over active switching of photon pairs via time-division multiplexing or wavelength-division multiplexing in previous proposed QKD networks. By using completely passive elements, the instrument
15 cost is substantially reduced and the network overhead is further reduced as there is no need for active synchronisation across parties. The synchronisation is derived directly from the timing correlation (down to 0.25 ns given typical detector timing jitter) born out of the photon pair production process and folded into the existing QKD backend protocol.

In addition, embodiments of the present invention can provide a technological leap over prepare-and-send systems that are already on the market. Prepare and send systems are systems which do not employ entanglement, in contrast to embodiments of the present invention.. Such systems have the disadvantage of needing to prepare the state of the photon in well defined state before transmission, see for example
https://www.idquantique.com/quantum-safe-security/products/#quantum_key_distribution
25 Cerberis or Clavis systems from IDQ.

The QKD service achievable in embodiments of the present invention is delivered via a very fundamental quantum process. In this sense, the QKD network according to example embodiments is driven by true quantum processes that can be mathematically quantified leading to security that is absolutely secure from an information-theoretic standpoint.
30 Coupled together with existing expertise in side-channel attacks (for example as described in in “Full-field implementation of a perfect eavesdropper on a quantum cryptography system“; Ilija Gerhardt, Qin Liu, Antia Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, Vadim Makarov. Nature Communications, 2, 349 (2011)), embodiments of the present invention can deliver an attractive solution for QKD over networks., in
35 particular over small networks (compare discussion of Figures 3(a) and (b) above.

In one embodiment, a quantum key distribution network comprises a source configured to generate photon pairs based on spontaneous parametric downconversion; a splitter configured for splitting photons generated by the source into different optical links; a plurality of nodes

configured to receive the photons via respective ones of the optical links; and a communication link between the nodes for exchanging timing information about the reception of the photons between the nodes to determine photons of one pair being received by two of the nodes.

- 5 The source may be configured to generate the photon pairs at random times.

The source may comprise a pump laser for passing a laser beam through a nonlinear medium with $\chi^{(2)}$ nonlinearity.

The pump laser may be configured for operating continuously, in CW-mode.

- 10 The network may be configured to provide the timing information about the reception of the photons as a time synchronization service.

The optical links between the splitter and the nodes may be direct.

The optical links may be built entirely out of passive components.

An optical source link between the source and the splitter may be direct.

The optical source link may be built entirely out of passive components.

- 15 Figure 5 shows a flowchart 500 illustrating a method of quantum key distribution in a network, according to an example embodiment. At step 502, photon pairs are generated based on spontaneous parametric downconversion using a source. At step 504 photons generated by the source are split into different optical links using a splitter. At step 506, a plurality of nodes configured to receive the photons via respective ones of the optical links are provided.
- 20 At step 508, a communication link is provided between the nodes for exchanging timing information about the reception of the photons between the nodes to determine photons of one pair being received by two of the nodes.

The method may comprise generating the photon pairs at random times using the source.

- 25 The method may comprise passing a pump laser beam through a nonlinear medium with $\chi^{(2)}$ nonlinearity.

The pump laser beam may be operated continuously, in CW-mode.

The method may comprise provide the timing information about the reception of the photons as a time synchronization service.

The optical links between the splitter and the nodes may be direct.

- 30 The optical links may be built entirely out of passive components.

An optical source link between the source and the splitter may be direct.

The optical source link may be built entirely out of passive components.

Embodiments of the present invention can have one or more of the following features and associated benefits/advantages:

Feature	Benefit/Advantage
QKD within a network	This extends QKD beyond the traditional two party model.
Centralized source of entangled photons	Simplifies hardware requirements
Single optical connection between centralized source and each node	Simplifies network requirements
No central key management	No central keybank is necessary in our model. Each party will derive a key with every other party on the network. Thus, there is no single point of attack available for an eavesdropper.
Uses only passive components. With N parties, a simple passive splitter transmits photons to each party with 1/N probability.	No active elements needed. The passive splitter can be built out of any passive system such as beamsplitters, half-silvered mirrors or spatial demodulators.
No trusted components necessary in the optical path between source and node.	Some instances of network QKD require “trusted-nodes” or “relays”. Other instances require secure synchronization signals. Yet other instances require active switching components and the switching commands themselves must be trusted. The combination of entangled photons and passive components reduces the need for trusted elements, and simplifies hardware and network requirements.
Uses entangled photon pairs	Traceable to Bell Inequality for security
Operable by untrusted 3rd party service provider	Ability to outsource service

Embodiments of the present invention can solve the problem when end-users require a network for QKD, in particular small networks for QKD, to be provided by 3rd party service providers.

5 Aspects of the systems and methods described herein may be implemented as functionality programmed into any of a variety of circuitry, including programmable logic devices (PLDs), such as field programmable gate arrays (FPGAs), programmable array logic (PAL) devices, electrically programmable logic and memory devices and standard cell-based devices, as well as application specific integrated circuits (ASICs). Some other possibilities for implementing aspects of the system include: microcontrollers with memory (such as electronically erasable
10 programmable read only memory (EEPROM)), embedded microprocessors, firmware, software, etc. Furthermore, aspects of the system may be embodied in microprocessors having software-based circuit emulation, discrete logic (sequential and combinatorial), custom devices, fuzzy (neural) logic, quantum devices, and hybrids of any of the above device types. Of course the underlying device technologies may be provided in a variety of
15 component types, e.g., metal-oxide semiconductor field-effect transistor (MOSFET) technologies like complementary metal-oxide semiconductor (CMOS), bipolar technologies like emitter-coupled logic (ECL), polymer technologies (e.g., silicon-conjugated polymer and metal-conjugated polymer-metal structures), mixed analog and digital, etc.

The above description of illustrated embodiments of the systems and methods is not intended
20 to be exhaustive or to limit the systems and methods to the precise forms disclosed. While specific embodiments of, and examples for, the systems components and methods are described herein for illustrative purposes, various equivalent modifications are possible within the scope of the systems, components and methods, as those skilled in the relevant art will recognize. The teachings of the systems and methods provided herein can be applied to
25 other processing systems and methods, not only for the systems and methods described above.

The elements and acts of the various embodiments described above can be combined to provide further embodiments. These and other changes can be made to the systems and methods in light of the above detailed description.

30 In general, in the following claims, the terms used should not be construed to limit the systems and methods to the specific embodiments disclosed in the specification and the claims, but should be construed to include all processing systems that operate under the claims. Accordingly, the systems and methods are not limited by the disclosure, but instead the scope of the systems and methods is to be determined entirely by the claims.

35 Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise," "comprising," and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in a sense of "including, but not limited to." Words using the singular or plural number also include the plural or singular number respectively. Additionally, the words "herein," "hereunder," "above," "below," and
40 words of similar import refer to this application as a whole and not to any particular portions

of this application. When the word "or" is used in reference to a list of two or more items, that word covers all of the following interpretations of the word: any of the items in the list, all of the items in the list and any combination of the items in the list.