November 2021

INTERFACE MULTIPLEXING TO SUPPORT QUANTUM CRYPTOGRAPHY

Rich Bradford

INTERFACE MULTIPLEXING TO SUPPORT QUANTUM CRYPTOGRAPHY

AUTHOR:
Rich Bradford

ABSTRACT

Quantum cryptography is now out of the lab. Simple networks connecting quantum encryption nodes have been created or proposed. However, there are a number of problems with scalability and basic capabilities that need to be addressed for quantum encryption nodes. Techniques presented herein provide mechanisms through which more efficient use can be made of both the port and the fiber for a quantum encryption node by optically multiplexing quantumly encrypted streams of photons with other such streams or streams of regular data.

DETAILED DESCRIPTION

Currently, quantum encryption requires dedication of an entire interface for a relatively low bandwidth delivery. It also requires the dedication of the intervening fiber. Techniques herein provide mechanisms that facilitate interface multiplexing for quantum encryption through which quantumly encrypted streams of photons can be multiplexed with 1) other quantumly encrypted streams of photons and/or 2) non-quantumly encrypted photon streams (i.e. regular optical data). In some instances, the order for multiplexing could be optimized to reduce components.

To illustrate the techniques of this proposal, consider an example involving a simplified Quantum Key Distribution (QKD) setup, as follows:

photon-src src-filter---->dest-filter dest-detector

For this example setup, the filter may be a randomly changing filter on both sides. A simple multiplexer could provide the following:

```
photon-src1 src-filter1\        /dest-filter1 dest-detector1
photon-src2 src-filter2 \ --> /dest-filter2 dest-detector2
photon-src3 src-filter3 /      \dest-filter3 dest-detector3
photon-src4 src-filter4/        \dest-filter4 dest-detector4
```

However, since the filters are randomly changing and since they only need to be secret until a destination can report the state chosen for the corresponding filter, there is no reason for the filters to be independent. Therefore, the number of filters can be reduced with the following configuration:

```
photon-src1\                                  /dest-detector1
photon-src2  \  src-filter1 --->dest-filter1 / dest-detector2
photon-src3  /                               \  dest-detector3
photon-src4/                                  \dest-detector4
```

Furthermore, even if Dense Wavelength Division Multiplexing (DWDM) is not used, the filter reduction technique could be used with multiple, independent interfaces, as follows:

```
photon-src1 src-filter1 ---->dest-filter1 dest-detector1
photon-src2 src-filter1 ---->dest-filter1 dest-detector2
photon-src3 src-filter1 ---->dest-filter1 dest-detector3
photon-src4 src-filter1 ---->dest-filter1 dest-detector4
```

Thus, a large filter could be used on multiple, closely placed photon streams by applying the same, random polarization to each stream.

In summary, provided herein are mechanisms through which more efficient use can be made of both the port and the fiber for a quantum encryption node by optically multiplexing quantumly encrypted streams of photons with other such streams or streams of regular data. As quantum cryptography may become a required feature for networked nodes for various security reasons, routers and switches may require such interfaces for secure control. Further, as optical switches may be required to transport streams of quantumly encrypted photons, the ability to multiplex streams utilizing mechanisms as discussed herein would provide a clear advantage to such devices.