Abstract

Protocol Parameter Optimization and Characterization of Superconducting Nanowire Single Photon Detector

He Xu
Master of Applied Science
Graduate Department of Electrical and Computer Engineering
University of Toronto
2014

The Internet has offered us a great deal of convenience, and as the Internet grows in size, the security becomes an issue. The current technology protects information in the Internet by means of computational complexity, but it is vulnerable to a supercomputer or a quantum computer that might be developed in the future. It is provable that the current and the most widely used algorithms will collapse once a quantum computer can factor large numbers.

Quantum Cryptography (QC) promises an unbreakable encryption algorithm, and Quantum Key Distribution (QKD) is one of the most technological feasible parts of QC. The unconditional security of QKD is based on quantum physics. However, unconditional security, which relies on reasonable assumptions, is not the same as absolute security, which make no assumptions, and QC protocols can be breached by means of side channels. Recently, Measurement Device Independent QKD (MDI-QKD) has been proposed to remove the side channels.

MDI-QKD can defeat many attacks on detectors, but its performance in terms of the key rate heavily hinges on a few parameters of the protocol, e.g. the number of decoy state and the intensity of each state. As a result, to extract the most performance out of the MDI-QKD protocol, these parameters need to be set appropriately and methodically. Prior to our work, there is no unified procedure on how to optimize these parameters, and most of the parameters are either partially optimized or are chosen in ad-hoc manners. In this thesis, we present a local search algorithm that is faster and more reliable. Using this algorithm, we obtained a 200 % increase in key rate along with results on the optimal number of decoy states and the optimal parameters values.

In parallel to improving performance by optimization, we also worked on the technological side by implementing a better detector than previous Single Photon Avalanche
Diode (SPAD). Superconducting Nanowire Single Photon Detector (SNSPD) has emerged among others as a promising technology. In this thesis, we present a characterization procedure of SNSPD, and we report the important finding of the phenomenon of “after-pulse”, which is a clustered detection event at 180ns after a first event in a chain. Then, we postulate that the origin of this afterpulse is from the limited bandwidth of the amplifier. By replacing the amplifiers with those with a larger bandwidth, the phenomenon of afterpulse disappears.