Kyle Romero

Professor Eggert

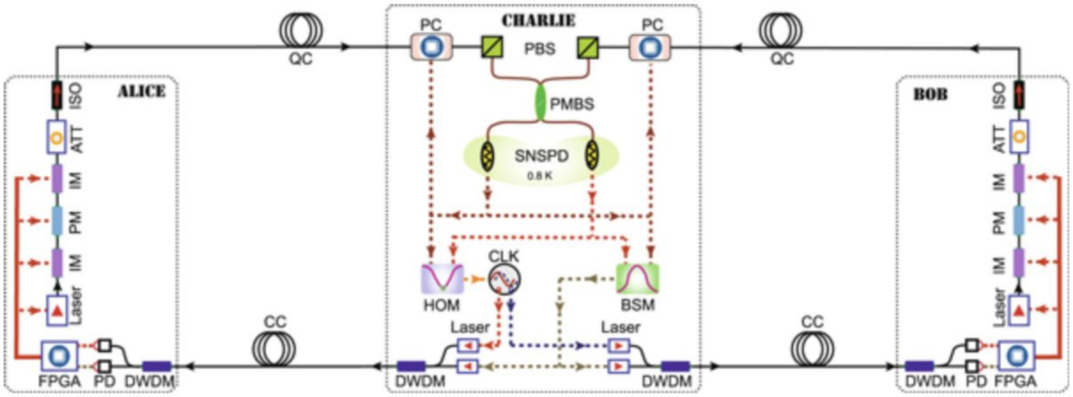
Computer Science 35L

December 8th, 2017

Promising Bounds in Quantum Key Distribution Systems

Quantum computing is a branch of computer science that utilizes quantum mechanical phenomena to complete data operations. Although similar to classical computing in many respects, quantum computing relies on qubits to store data, as opposed to bits, and quantum gates to perform operations on quantum bits, instead of CMOS gates and transistors. Quantum computing is a heavily researched topic in computer science because of the potential speedup advantages to using quantum computing over classical computing. Since the advent of quantum computing the late 1900s, researchers have found a multitude of applications to the field of cryptography. For example, quantum key distribution(QKD) is a method of performing a quantum cryptographic task that involves producing a shared, random key that can be used the encrypt and decrypt messages. Although this form of key generation is theoretically secure, there are often vulnerabilities in the technical specification of the devices and components that are used to realize the system. Measurement devices used to generate a secure key from quantum phenomena represent a significant security fault in an otherwise secure system. Therefore, the development of a measurement-device-independent QKD system, is advantageous to improving the security of such QKD systems.

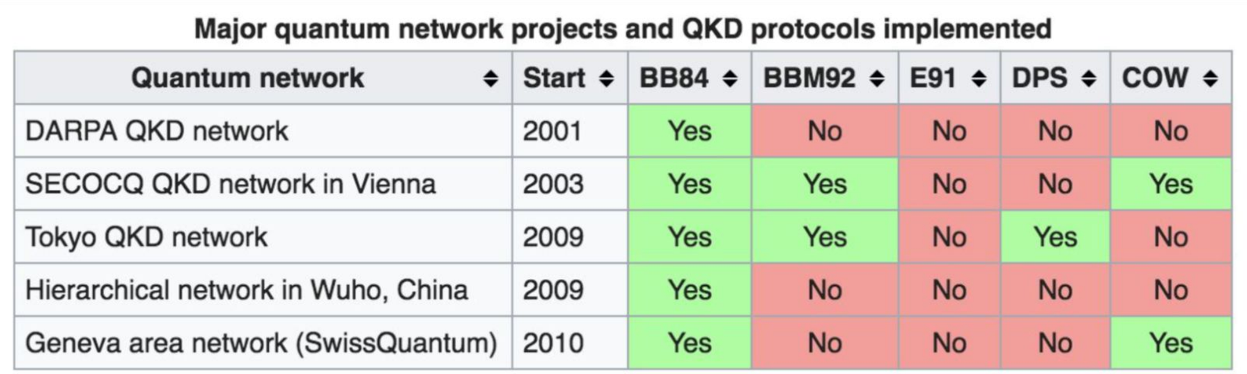
In the article *Cost Effective Quantum Moves a Step Closer* published in the ACM TechNews feed from September 22nd, 2017, the author summarizes the main points of a recent scientific paper in *Quantum Science and Technology* that presents a new means of realizing a QKD system. The team that published these findings consisted of researchers from the University of Calgary, the California Institute of Technology, and the National Institute of Standard and Technology, Colorado. The experiments outlined in the paper demonstrate the security and reliability of one such measurement-device-independent QKD system that is realized with commercially available hardware such as distributed feedback lasers and field-programmable gate arrays.



The measurement-device-independent QKD system implemented in the research paper referenced in my article. Source: http://iopscience.iop.org/article/10.1088/2058-9565/aa8790/meta

Furthermore, the above system protects against most quantum hacking techniques that take advantage of the vulnerabilities in technical specification of each component. For example, a Trojan Horse Attack, in the context of quantum hacking, involves transmitting bits via shining an outside laser at a small sensor in order to alter the bits being transmitted between components of the QKD system. This system protects against this specific attack by providing a more precise cover to a variety of laser sensors to ensure that only authorized lasers can transmit bits within the system. Another safeguard against potential quantum hacking is the system's independence from measurement devices. Since the system does not rely on a device to generate and output the key, there is no possible way that a quantum hacker could take advantage of a vulnerability in this third-party device.

Early on in the development of quantum computing, QKD systems were recognized as a means of solving many security vulnerabilities with our current methods of encrypting and decrypting information transmitted over a secure network. Thus, a significant amount of previous work has been done to implement these systems. As far back as the 1980s, researchers developed varying protocols for generating and transmitting quantum keys within a secure system. For example, in an article published in 2000 titled “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”, authors Peter Shor and John Preskill present a proof that the BB84 QKD Protocol, developed in 1984, is secure.

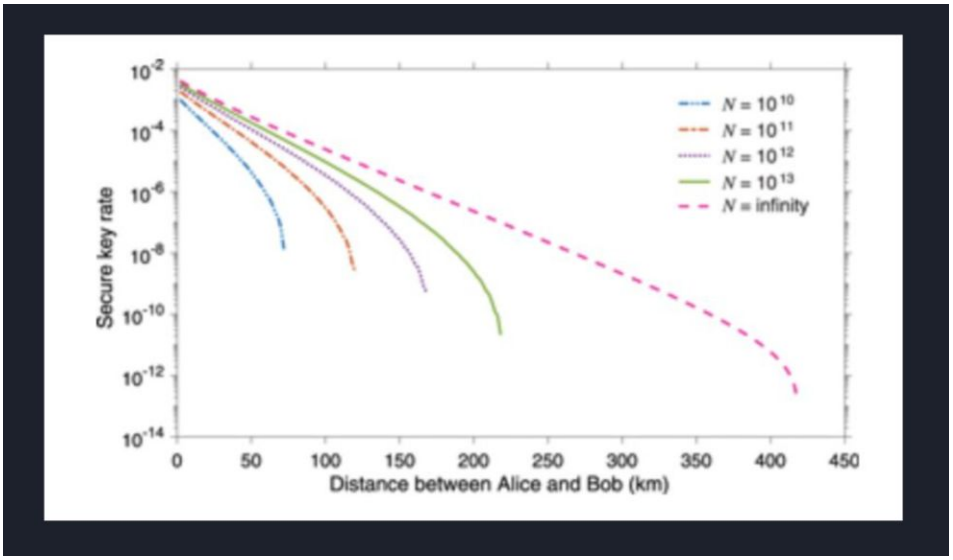


Major quantum network projects and QKD protocols implemented

Quantum network	Start	BB84	BBM92	E91	DPS	COW
DARPA QKD network	2001	Yes	No	No	No	No
SECOCQ QKD network in Vienna	2003	Yes	Yes	No	No	Yes
Tokyo QKD network	2009	Yes	Yes	No	Yes	No
Hierarchical network in Wuho, China	2009	Yes	No	No	No	No
Geneva area network (SwissQuantum)	2010	Yes	No	No	No	Yes

Since the 1980s, many new QKD protocols have been developed and implemented in lab environments across the globe. Source: https://en.wikipedia.org/wiki/Quantum_network

In addition to developments in the protocols being used the generate and distribute keys and information inside of a QKD system, there have been significant developments in the device-independence of QKD systems. Several categories of QKD systems have been developed in practice and in theory: device-independent QKD systems, semi-device independent QKD systems, and one-sided device independent QKD systems. Since its introduction in the research paper , “Measurement-Device-Independent Quantum Key Distribution Systems” written by Hoi-Kwong Lo, Marcos Curty, and Bing Qi, measurement-device-independent QKD systems have been recognized as the implementation with the best balance of security and feasibility for the improvement of modern encrypted networks.



The measurement-device-independent QKD system that is implemented in my research paper demonstrates the effectiveness of secure quantum keys over long distances. Successful results are shown above. Source: http://iopscience.iop.org/article/10.1088/2058-9565/aa8790/meta

Since my article promises a cost-effective, readily available, and secure implementation of a QKD system, the security of common encrypted systems could be vastly improved in the coming years. Applications for such a system are widespread since security is an important aspect of any computer system that is implemented around the world. Some possible applications include, transaction information for a bank, health records for an insurance company, and social security numbers for the government. I am personally excited for the possibility of widespread security improvements around the world in the data that I am transmitting and receiving each and every day.

Works Cited

Lo, Hoi-Kwong, et al. “Measurement-Device-Independent Quantum Key Distribution.”Physical Review Letters, American Physical Society, 30 Mar. 2012, journals.aps.org/prl/abstract/10.1103/PhysRevLett.108.130503.

IOPPublishing. “Cost effective quantum moves a step closer.” *EurekAlert!*, www.eurekalert.org/pub_releases/2017-09/ip-ceq091817.php.

“Quantum key distribution.” *Wikipedia*, Wikimedia Foundation, 26 Oct. 2017, en.wikipedia.org/wiki/Quantum_key_distribution.

“Quantum network.” *Wikipedia*, Wikimedia Foundation, 29 Oct. 2017, en.wikipedia.org/wiki/Quantum_network.

Raju Valivarthi *et al* 2017 *Quantum Sci. Technol.* 2 04LT01 http://iopscience.iop.org/article/10.1088/2058-9565/aa8790/meta

Shor, Peter W., and John Preskill. “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol.” Physical Review Letters, American Physical Society, 10 July 2000, journals.aps.org/prl/abstract/10.1103/PhysRevLett.85.441.