COUNTERING THE PHOTON NUMBER SPLITTING ATTACK

Andrew Wang and Rachel Kim
Sir John A. Macdonald (Waterloo)

Motivation

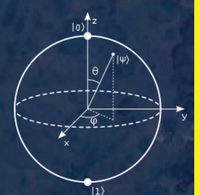
The concept of quantum mechanics is fascinating. Even better, it's extremely useful to the future of computing and communications technology. Quantum mechanics is growing at an unbelievable pace through research with optics, nanotechnology, nuclear energy and much much more.

Background

The problem of encryption is an important enigma studied for decades. QKD short for Quantum Key Distribution., revolutionizes a solution by using the fundamental laws of quantum physics and taking advantage of them.

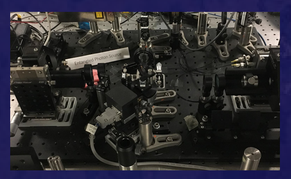
Quantum Superpositions

A quantum system in a superposition can be in multiple states at the same time.



Quantum Entanglement

Particles so interconnected that actions performed on one affect the other.

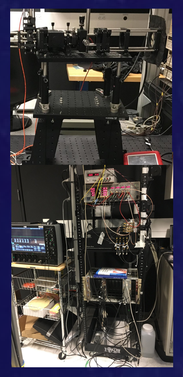


Quantum Uncertainty Principle

it states that the more precisely the position of some particle is determined, the less precisely its momentum This also states why particles can't be cloned.

Criteria required for success

-Only one photon is to be transmitted on command.
- Detector records the exact number of photons received.
- The photon moves through a medium losing any information.

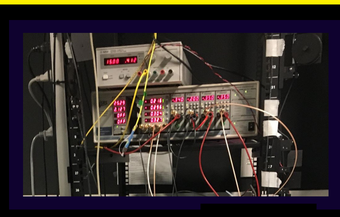


QKD

PNS

The Purpose

The purpose of this study is to explore the current state of practical QKD and analyze possible methods that may be used to counter the Photon-Number Splitting Attack.



QKD utilizes the laws of physics secret key only known "Alice" and "Bob", respectively the sender and receiver. Theoretically, QKD could bypass an eavesdropper of unlimited computational power and technological advancement, whom we will call "Eve".

Eve

The Problem

Unfortunately, existing real-life implementations of QKD cannot follow the Criteria due to technological limitations. For example, if there's more than one photons at a time - Eve can land a Photon-Number Spliting Attack.

If a signal contain more than one photon, then Eve can obtain the information by storing a single photon from the signal and allow the rest to go to Bob.. Otherwise, the signal is blocked off so that Bob doesn't recieve a signal.

Procedure and Research

Photon Sources

Weak Coherent Pulse

Weak Coherent Pulse (WPS) is a common implementation that uses laser pulses filtered to very low power. Due to the low power, pulses contain a very small number of photons.

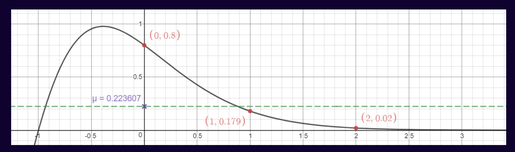
Decoy State QKD

Poission Distribution

They are distributed according to a Poisson distribution. This means most pulses contain no photons, some pulses contain the desired 1 photon and a smaller but possible chance of containing 2 or more.

$$\frac{\mu^x e^{-\mu}}{x!}$$

$$0.025e^{-\mu} = \frac{\mu^2 e^{-\mu}}{2}$$



Breaching Security

Eavesdropper Attack

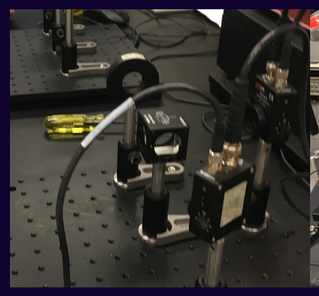
If a signal contain more than one photon, then Eve can obtain the information by storing a single photon from the signal and allow the rest to go to Bob.. Otherwise, the signal is blocked off so that Bob doesn't recieve a signal. The activity of blocking an entire signal may seem suspicious to Alice and Bob.

Countermeasures

Using Decoy States, Alice can change the filters to alter the event parameter altering the frequency photons per pulse. The change in the average number of photons per signal can be chosen as decoy states. A theoretical yield can be estimated and compared with the actual yields of how often Bob receives signals for each decoy state.

Simulation Process

General Setup



Photon Polarization

Transmission Medium

Post Processing

Results

Three different QKD protocols based on the original BB84 with special decoy states were analysed thoroughly.

Single Decoy State
This alone allows Alice and Bob the ability to identify an attack in almost all circumstances.

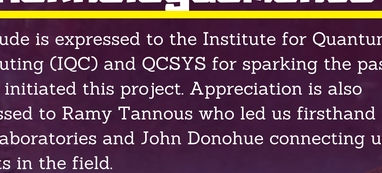
μ = 0.1 or μ = 0.5

Weak and Vacuum States
Provide a bonus increase in the distance of QKD.

μ = 0
or
μ = 0.1
or
μ >= 0.5

Infinite Decoy States
Small security improvements over Weak and Vacuum States.

0 < μ < ∞



Conclusion

Decoy State QKD is easy to implement provides multi-photon statistics that make it robust against the Photon-Number Splitting Attack. We analyzed three methods of Decoy States alongside regular QKD. A general trend in Decoy State protocols, is that as security against the eavesdropper increases, so does the distance and efficiency of the QKD implementation. Analyzing in a simulated environment, we were able to find an optimal ratio of how often to send decoy states and the average number of photons in each decoy state. This will happen to be useful when practical Decoy State QKD are being setup and will save the time of manual variable testing.

References & Acknolegdements

Gratitude is expressed to the Institute for Quantum Computing (IQC) and QCSYS for sparking the passion which initiated this project. Appreciation is also expressed to Ramy Tannous who led us firsthand in their QKD laboratories and John Donohue connecting us with experts in the field.

Diamanti, E., Lo, H., Qi, B., & Yuan, Z. (2016, November 08). Practical challenges in quantum key distribution. Retrieved February 6, 2019, from https://www.nature.com/articles/npjqi201625 Sabottke, C. F., Richardson, C. D., Anisimov, P., Yurtsever, U., Lamas-Linares, A., & Dowling, J. P. (2012, March 19). Thwarting the Photon Number Splitting Attack with Entanglement Enhanced BB84 Quantum Key Distribution. Retrieved March 16, 2019, from https://www.osapublishing.org/abstract.cfm?URI=QIM-2012-QW1A.3 Quantum computing 101. (2018, November 16). Retrieved May 17, 2019, from https://uwaterloo.ca/institute-for-quantum-computing/quantum-computing-101#What-is-quantum-computing Ma Xiongfeng, Qi Bing, Zhao Yi, & Lo, H.-K. Practical decoy state for quantum key distribution. United States. doi:10.1103/PhysRevA.72.012326