QLab
Thomas Jefferson
Research

A Photonic Implementation of Quantum Key Distribution

Katherine Jiminez, Alec Riso, Karthik Thyagarajan, Connor Whiting
Quantum Physics and Optics Research Laboratory
Thomas Jefferson High School for Science and Technology (TJHSST)

Abstract

Quantum Key Distribution (QKD) stands as a revolutionary approach to secure communication, using the principles of quantum mechanics to establish unbreakable channels. Unlike traditional cryptography, which relies on the computational difficulty of mathematical problems, QKD utilizes the inherent properties of quantum states to achieve information-theoretic security. This means that the security of the key exchange is guaranteed by the laws of physics, making it theoretically unbreakable even by an adversary with unlimited computational power.

Currently, the most viable way to implement QKD for communication is via photonics — namely, using phase-preserving long-distance optical fibers. The objective for our project is to implement QKD in photonics in a laboratory setting which will help advance the protocol's robustness and feasibility for practical use. Furthermore, we aim to investigate the difficulty of noise in implementing the algorithm over long distances.

Introduction

QKD primarily hinges on two core concepts:

1. **Quantum States:** These states can exist in a superposition of multiple possibilities simultaneously, unlike classical bits which are either 0 or 1. This unique property allows for the creation of keys that are inherently random and unpredictable.
2. **No-Cloning Theorem:** This fundamental principle states that it is impossible to perfectly copy an unknown quantum state. Any attempt to measure or copy the state inevitably disturbs it, making it unusable for further communication. This acts as a safeguard against eavesdropping attempts, as any attempt to intercept or tamper with the key material would be readily detectable.

QKD can be applied to many sectors where information security is essential:

- **Government and Military:** Securely transmitting classified information and protecting critical infrastructure.
- **Financial Services:** Protecting sensitive financial data and transactions.
- **Healthcare:** Ensuring the privacy and confidentiality of patient information.

While traditional cryptography offers strong security, it is vulnerable to potential attacks on RSA encryption that could arise with the advancement of quantum computing.
However, implementing QKD currently faces several challenges:

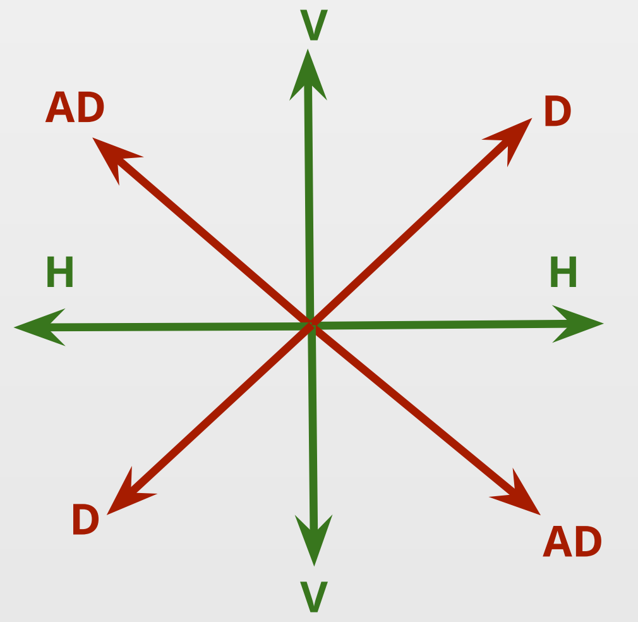
- **Cost and Complexity:** QKD systems are currently expensive and require specialized hardware and expertise.
- **Limited Range:** Quantum signals degrade over long distances, making it impractical for widespread deployment.
- **Integration:** Integrating QKD with existing communication infrastructure can be complex.
-

Despite these challenges, QKD research and development are rapidly advancing, and the technology is expected to become more accessible and practical in the future. As the threat of RSA decryption looms, QKD stands as a crucial area of research and development, offering a powerful and future-proof solution for securing communication in the digital age.

Algorithm

QKD may seem like a complex algorithm, but it can be broken down into several relatively simple steps. Let Alice be attempting to transmit a key to Bob.

Light Bases



Measuring D in the H/V basis gives a 50% chance of measuring either H or V.

Measuring D in the D/AD basis gives a 100% chance of measuring D.

Alice and Bob agree to an encoding table. When bits and bases are selected, they are converted into quantum states based on this table.

Coding Scheme	H/V-Basis	D/AD-Basis
0 bit	H	D
1 bit	V	AD

Alice first chooses a random sequence of bits.

Alice then chooses a random sequence of bases.

Finally, Alice encodes these bits based on the encoding table shown previously.

Alice	1	2	3	4	5
Bits	0	1	1	0	0
Bases	H/V	H/V	D/AD	H/V	D/AD
States	H	V	AD	H	D

These qubits are then sent to Bob.

Bob then chooses a random sequence of bases

Next, Bob measures Alice's qubits with the chosen bases

Finally, Bob decodes the qubits according to the table

Bob	1	2	3	4	5
Alice's State	H	V	AD	H	D
Bases	D/AD	H/V	H/V	H/V	D/AD
Possible State	D or AD	V	H or V	H	D
Measured State	D	V	H	H	D
Decoded State	0	1	0	0	0

Alice and Bob compare bases, and eliminate the bits that don't match

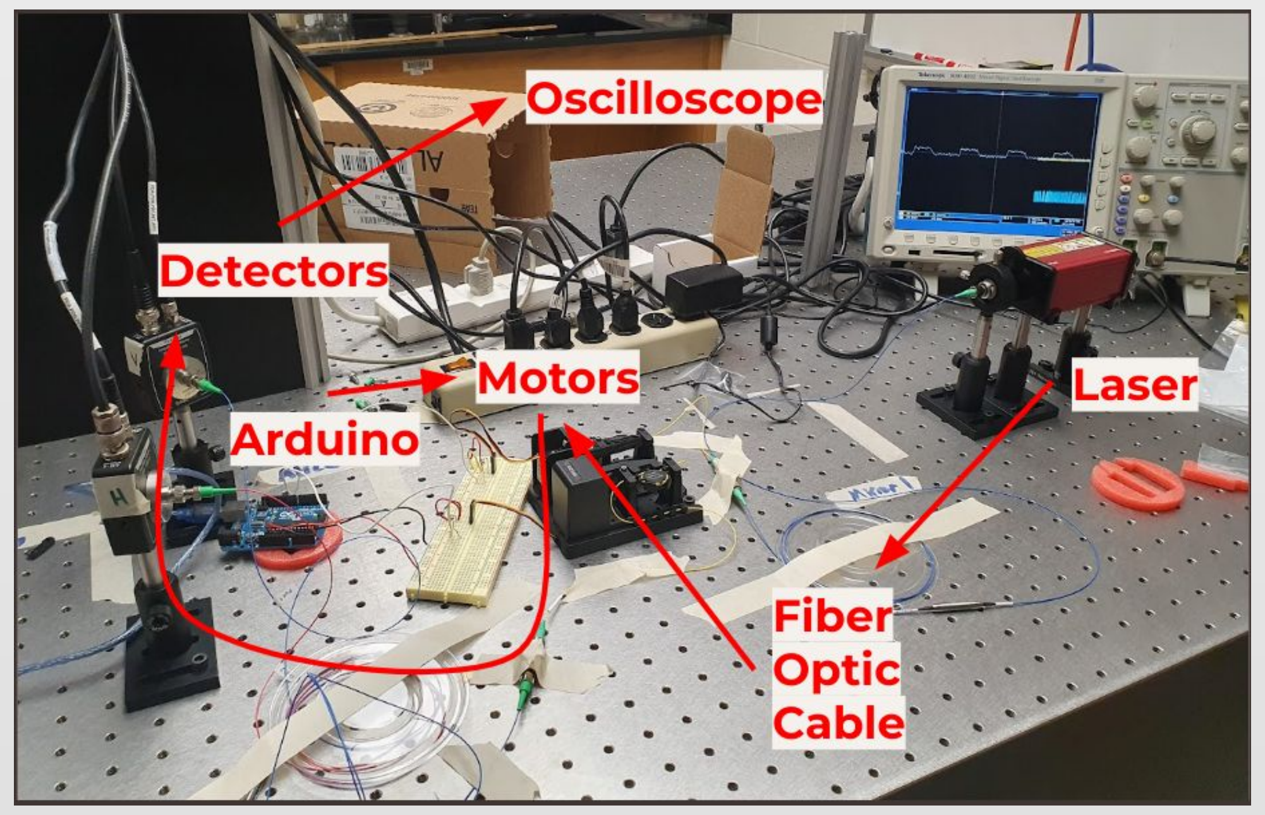
Check if Alice and Bob's bits match. If they do, then it's safe

Now, we have the final key: **100**

Compare	~~1~~	2	~~3~~	4	5
Alice's Bases	~~H/V~~	H/V	~~D/AD~~	H/V	D/AD
Bob's Bases	~~D/AD~~	H/V	~~H/V~~	H/V	D/AD
Alice's Bits	~~0~~	1	~~1~~	0	0
Bob's Bits	~~0~~	1	~~0~~	0	0
Final Key	🟩	1	🟩	0	0

Materials

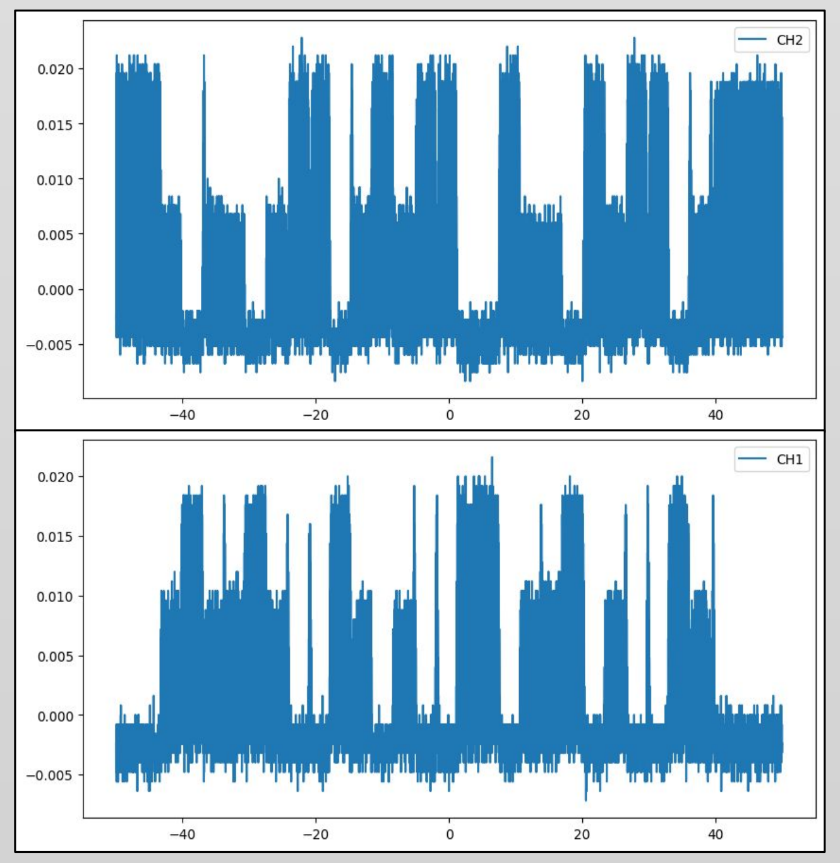
To generate the photons, we fed the output of a 650-nm laser directly into a phase-preserving optical fiber. This fiber then passed through an inline-polarizer to regularize the polarization of all photons. The fiber is then connected to a single-mode optical fiber, which passes through two servo motors, which represent Alice and Bob. Each of these servo motors are rotated by a degree amount that was experimentally determined to induce the desired phase change. Finally, the output is passed into an inline polarizing beamsplitter, which splits the light into two channels, that are then fed to two detectors and outputted on the oscilloscope. This entire process represents the measurement performed by Bob.



Results

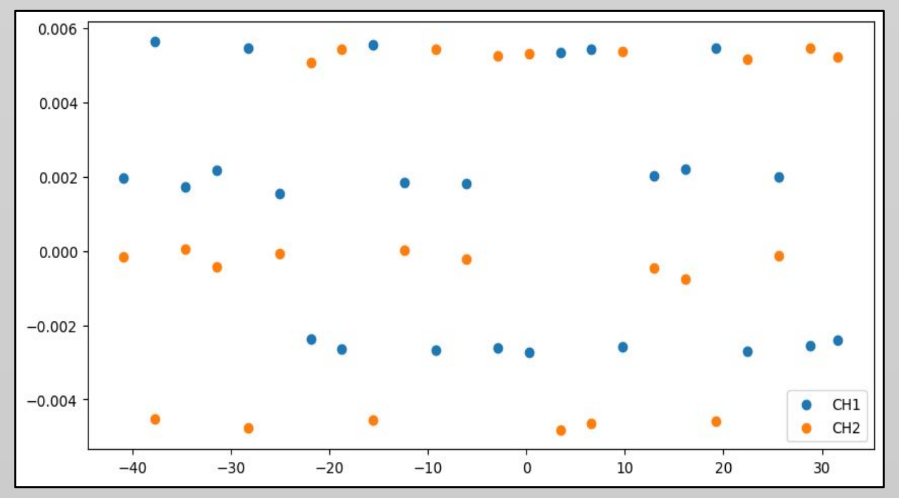
To test our implementation, we transmitted the key **110010001101000.**

The output on the oscilloscope for the two different channels can be seen to the right, with the power level of the 0 detector above and the power level of the 1 detector below.



These power levels were then sliced and processed to produce a sequence of discrete outputs, seen below on the left.

If the power level was above 0.004 mW, we declared a positive reading for that output. Otherwise, it was a random output.



The output shown to the right would have produced **0101110010010011010101100** as a possible key.

Following this, the mismatched bases were eliminated, producing the key **110010001101000.**

This is an exact match to the transmitted key.

Conclusion

Our Quantum Key Distribution (QKD) system successfully transmitted an encryption key that matched the theoretical encryption key, demonstrating the effectiveness and accuracy of our project. This achievement indicates that our implementation is capable of securely distributing encryption keys, aligning with the fundamental principles of quantum cryptography.

However, it is important to note that our specific method currently finds its most practical applications in educational settings. This limitation stems from several technical challenges we encountered during the project.

One significant difficulty was the precise alignment of the laser, which is crucial for maintaining the integrity of the quantum signal. Additionally, ensuring that the fiber optic cable preserved polarization posed another substantial hurdle, as any deviation can affect the transmission and detection of the quantum states.

Evidently, the distance traveled by the signal is extremely small (the distance between each of the motors). Theoretically, our system can easily be extended to an arbitrarily large distance, assuming that the intermediary fiber maintained consistent positioning, orientation, and temperature. However, noise and loss in the process are difficult to account for, and can only be experimentally verified with a signal that traverses the desired distance. Implementing QKD across a large distance in a more controlled environment would be a promising future direction of research.

Looking at our system specifically, there are several directions for further development of our QKD system. One key improvement would be to refine the system to send a single photon at a time, rather than a pulse of light. This enhancement would increase the security and efficiency of the key distribution process by reducing the potential for interception and error. Another critical advancement would be the introduction of an eavesdropper into the system. By simulating an adversarial presence, we can test the robustness and security of our QKD protocol against potential attacks.

These improvements will help enable our QKD system to be used in more advanced and secure communication networks beyond just educational demonstrations.

Acknowledgements

We would like to acknowledge **Mr. Hannum** for his immense support throughout this project, serving as both a lab director and mentor through the entire process. He made sure we had all the necessary materials, expertise, and guidance needed.
We would also like to acknowledge **ThorLabs** for supplying us with extremely precise optical equipment and technical expertise when needed.