An Overview of Quantum Key Distribution (QKD)

Author: Dr. Alistair Finch **Publication Date:** September 15, 2025

Abstract

Quantum Key Distribution (QKD) represents a paradigm shift in secure communications, leveraging the principles of quantum mechanics to establish a provably secure shared secret key between two parties. Unlike traditional cryptographic methods that rely on mathematical complexity, QKD's security is based on the fundamental laws of physics. This paper provides a high-level overview of the BB84 protocol, the most well-known QKD protocol.

The Eavesdropping Problem

In classical cryptography, an eavesdropper (traditionally named Eve) can intercept and copy a key without being detected. The security relies on the encryption algorithm being too computationally intensive to break in a reasonable timeframe. However, the advent of quantum computing threatens the foundations of many current public-key cryptography systems.

The BB84 Protocol

The BB84 protocol, developed by Charles Bennett and Gilles Brassard in 1984, solves this problem. The process is as follows:

1. **Photon Transmission (Alice):** The sender, Alice, transmits a stream of photons to the receiver, Bob. Each photon is randomly polarized in one of four states: horizontal (0°), vertical (90°), 45°, or 135°. These states correspond to two different bases: the rectilinear basis (+), and the diagonal basis (x).
2. **Photon Measurement (Bob):** For each incoming photon, Bob randomly chooses one of the two bases (rectilinear or diagonal) to measure it.
3. **Basis Reconciliation (Sifting):** After the transmission, Bob communicates with Alice over a classical, public channel. They announce which basis they used for each photon, but not the measurement result. They discard all measurements where they used a different basis. On average, they will have used the same basis for 50% of the photons. The remaining sequence of bits is the "sifted key."
4. **Error Estimation:** The core principle of QKD is that if an eavesdropper, Eve, tries to measure a photon, she will inevitably disturb its quantum state. To detect this, Alice and Bob publicly compare a small, random subset of their sifted keys. If the error rate is above a certain threshold, they assume an eavesdropper is present and discard the key.

Conclusion

The act of measurement in quantum mechanics is also an act of disturbance. It is this principle that guarantees the security of QKD. If no significant errors are found, the remaining bits of the sifted key are guaranteed to be secret, providing a foundation for secure, one-time pad encryption.