Quantum Cryptanalysis

Developing simulation models to test the effectiveness of existing cryptanalysis techniques against different QKD protocols under controlled conditions.

Analyze the success rates and limitations of these attacks.

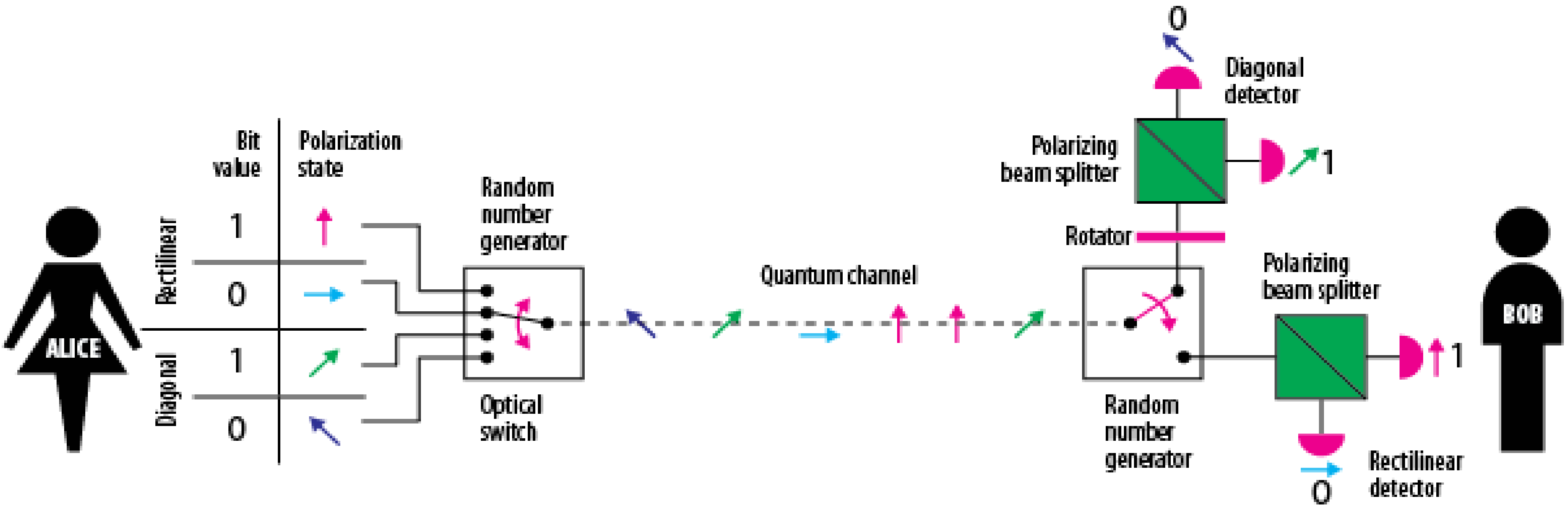
Quantum Cryptography

- **Quantum cryptography** is a method of encryption that uses the naturally occurring **properties of quantum mechanics** to secure and transmit data in a way that cannot be hacked.
- Quantum cryptography **uses individual particles of light, or photons**, to transmit data over fiber optic wire. The photons represent binary bits.
- Photons are used for quantum cryptography because they offer all the necessary qualities needed: **Their behaviour is well understood, and they are information carriers in optical fibre cables**. One of the best-known examples of quantum cryptography currently is **quantum key distribution** (QKD), which provides a secure method for key exchange

How Quantum Cryptography Works?

- Regular encryption, the kind you use every day for online banking or sending emails, scrambles information with a key. This key is like a complex password that unlocks the scrambled data. The problem is, these keys can be broken by powerful computers.
- Quantum cryptography steps in to solve this problem. It uses the weird world of quantum mechanics to create unbreakable keys.
- **The Player: Photons:** Quantum cryptography uses light particles called photons to transmit the key. These photons are special because they can be in multiple states at once (superposition) and linked together (entanglement).

- **Unbreakable Key Delivery (QKD):** This is where the magic happens. QKD protocols define how these photons are sent and measured. The sender transmits photons in random quantum states, like their polarization (vertical, horizontal, etc.).
- **Security Through Uncertainty:** Here's the cool part. If someone (an eavesdropper) tries to peek at the photons, they disturb their quantum state, alerting the sender and receiver. This is based on the Heisenberg uncertainty principle, a law of quantum mechanics.
- **Key Verification:** Both sender and receiver compare their measurements of a small portion of the photons. If they match and no eavesdropping is detected, they can use the remaining photons to build a shared secret key.



Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	✛ Rect	✕ Diag	✕ Diag	✛ Rect	✕ Diag	✕ Diag	✕ Diag	✕ Diag
	ALICE tells BOB which bits to keep		✓		✓		✓	✓	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

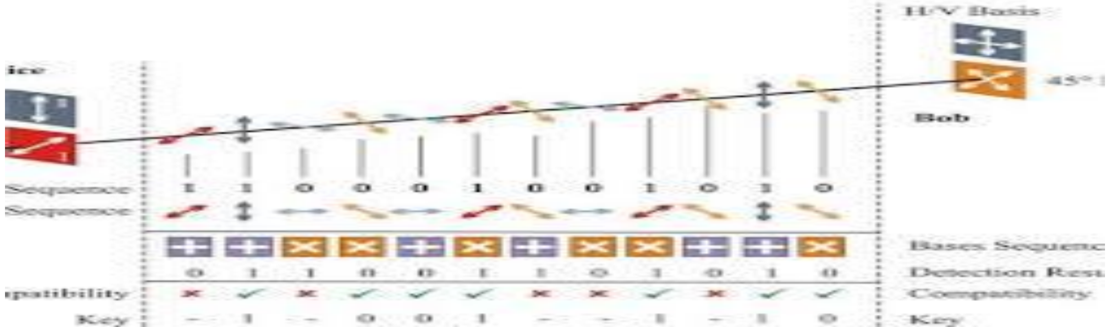
QKD in action

Imagine Alice and Bob want to exchange messages securely.

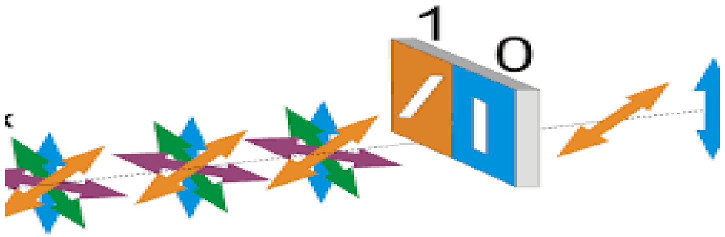
1. Alice sends Bob photons in random quantum states using QKD protocols.
2. Bob measures the photons and compares his results with Alice over a regular communication channel (like a phone call).
3. If their measurements match and no eavesdropping is detected, they use the remaining photons to create a shared secret key.
4. Now, Alice encrypts her message with the key and sends it to Bob. Only Bob, with the matching key, can decrypt the message.
5. While QKD creates a super secure key, it doesn't directly encrypt the message itself. For that, Alice uses traditional encryption algorithms like AES, which rely on the key to scramble the data. This encrypted message is then sent over a regular channel.

QKD Protocols and their working

- **BB84 (Bennet-Brassard 1984)**
  1. **Quantum Encoding:** Alice transmits photons, each representing a bit (0 or 1) encoded in its polarization state. She randomly chooses between two bases: rectilinear (horizontal/vertical) or diagonal (plus/minus diagonal).
  2. **Basis Agreement:** Alice sends Bob a separate classical message (through a regular, insecure channel) revealing which basis she used for each photon. But she keeps the specific polarization state (0 or 1 within a basis) secret.
  3. **Error Detection:** After receiving the photons, Bob randomly chooses his own basis (either rectilinear or diagonal) for measuring each one. He then compares his basis choices with Alice's via the classical channel.
  4. **Key Distillation:** Any discrepancies in the basis choices indicate Eve's tampering. Alice and Bob discard those bits and keep only the ones where their bases matched. This shared key is now secure because Eve couldn't have copied the photons without introducing errors detectable by Bob.



- **B92 (Bennett 1992)**
  1. **Non-Orthogonal States:** Unlike BB84 using completely different polarization states, B92 uses two non-orthogonal states. For example, Alice might use horizontal (H) for 0 and diagonal (+45°) for 1.
  2. **Random Basis Selection:** Similar to BB84, Alice randomly chooses between a basis (e.g., rectilinear or diagonal) to send each photon.
  3. **Bob's Measurement:** Bob also randomly chooses a basis to measure each received photon.
  4. **Decoding and Discards:** Here's the key difference:
     - If Bob's basis matches Alice's and the measurement outcome aligns perfectly (e.g., H for both), it's a clear 0.
     - If the basis matches but the outcome is inconclusive (e.g., Bob gets H in the rectilinear basis for Alice's diagonal +45°), that bit is discarded.
     - The same happens if the basis mismatch occurs (discarded bit).
  5. **Secure Key:** Only the bits where both basis and outcome agree are kept as the shared secret key.



Ideation : To gather a Dataset

- To develop a simulation framework to test existing cryptanalysis techniques (e.g., intercept-resend attacks, photon-number splitting) against different QKD protocols (BB84, B92) under controlled conditions.
- This framework will simulate the communication channel with noise, Alice (sender)'s actions, Eve's (eavesdropper) attacks, and Bob's (receiver) actions, including error correction (if applicable).
- Will run multiple simulations with varying parameters (e.g., noise level, Eve's attack strategy) to gather a comprehensive dataset.

Ideation : To create a ML model

- Once we have simulation results, we will leverage ML for deeper analysis
  - **Identifying Attack Patterns:** Will train a classification model (e.g., decision tree, Support Vector Machine) to classify successful Eve attacks based on simulation parameters. This can help identify patterns in successful attack strategies and noise conditions.
  - **Predicting Eve's Success:** Train a regression model (e.g., linear regression, Random Forest) to predict Eve's success rate (percentage of key bits she can guess) based on various factors like noise level, chosen attack strategy, and protocol parameters. This can provide insights into the impact of different factors on Eve's effectiveness.

Eve’s attacks on bb84 protocol

- **Intercept-Resend Attack (IRA)**
    - This is a fundamental attack where Eve intercepts qubits sent by Alice.
    - She then tries to measure the qubits in her own basis (rectilinear or diagonal), potentially introducing errors.
    - Eve resends the (potentially altered) qubits to Bob (receiver).
    - **Working :**
        - Simulate Eve receiving the qubit from the communication channel.
        - Implement a random choice for Eve's basis selection (rectilinear or diagonal).
        - Based on the chosen basis, simulate Eve measuring the qubit (potentially introducing a bit-flip error to represent an imperfect measurement).
        - Send the potentially altered qubit back to Bob through the simulated channel.
        - Track how many bits Eve manages to guess correctly based on her chosen basis and the actual basis used by Alice. Consider factors like the bit-flip error rate in the channel when calculating Eve's success rate.

Eve’s attacks on b92 protocol

- **Intercept-Resend Attack (IRA)**
  - Simulate Eve intercepting qubits sent by Alice.
  - Implement random choice for Eve's basis selection (plus or cross).
  - Based on the chosen basis, simulate Eve measuring the qubit (potentially introducing a bit-flip error). Unlike BB84, Eve might get more information in some scenarios due to B92 encoding.
  - Track how many bits Eve manages to guess correctly based on her chosen basis and the actual basis used by Alice. Consider factors like the bit-flip error rate in the channel when calculating Eve's success rate.
- **Phishing Attack:**
  - This attack exploits the fact that B92 requires prior agreement on basis selection between Alice and Bob.
  - Simulate Eve sending a fake basis selection message to Bob before the actual transmission.
  - If Bob accepts the fake message, subsequent communication might be vulnerable.

Fields that my dataset will have

- **Protocol Parameters:**
  - **Protocol Type:** Categorical variable indicating the QKD protocol used (e.g., BB84, B92).
  - **Basis Selection:** If applicable, the number of basis choices available (e.g., 2 for BB84, 2 for B92).
- **Channel Characteristics:**
  - **Bit Error Rate (BER):** Continuous variable representing the probability of a bit flip during transmission.
  - **Noise Level:** Continuous variable representing the overall noise affecting the channel.
- **Eve's Attack Strategy:**
  - **Attack Type:** Categorical variable indicating the specific attack employed by Eve (e.g., Intercept-Resend Attack (IRA), Phishing attack)
- **Eve's Success Rate:**
  - **Key Bits Guessed:** Continuous variable representing the percentage of key bits Eve can correctly guess or the information she gains about the key.
- **Bob's Detection/Correction Outcomes:**
  - **Error Rate After Channel:** Continuous variable representing the error rate observed by Bob after the communication channel (before error correction).

How can I distinguish between these attacks?

- **Success Rate:** Analyze the percentage of key bits Eve can correctly guess or the information she gains about the key. This can vary depending on the attack and the success of Eve's actions.
- **Noise Level:** Noise can introduce bit flips, potentially masking Eve's actions or making it harder for Bob to detect errors. However, excessive noise can also hinder Eve's ability to measure qubits accurately.
  - **High noise might render IRA and phishing attacks in B92 less effective due to unreliable Eve measurements.**
- **Bit Error Rate (BER):** A higher BER generally benefits Eve. Increased errors make it harder to distinguish legitimate qubits from those tampered with by Eve.
  - BB84 vs. B92: **Both are affected, but B92 might be slightly more sensitive due to two-qubit encoding (errors in either qubit can affect Eve's information gain).**
- **The effectiveness of these factors depends on the specific implementation of the QKD protocol**