BB84

Introduction to Practical Quantum Cryptography

- Today, we'll explore a concept related to quantum money but more practical for current use.
- Focus: Quantum Key Distribution (QKD) - A method that doesn't require long-term storage of quantum states.
- Why it matters: QKD has real-world potential for secure communication, even though its market remains small.
- Goal of Key Distribution: Enable two agents, Alice and Bob, to share a secret key.
- Purpose: Once they share a key, they can securely exchange messages.
- Key Concept: The shared key is a random string known only to Alice and Bob.

The One-Time Pad (OTP)

- How it works:
  - Step 1: Alice uses the shared key and her secret message.
  - Step 2: She sends the message encrypted with a technique called XOR.
  - Step 3: Bob uses the key to decrypt and retrieve the original message.
- Limitation: OTP requires a new key each time it’s used for secure encryption.

Classical Limitations

- Challenge: Secure communication requires either:
  - Initial shared secret information, or
  - Computational assumptions about the eavesdropper (Eve).

Quantum Key Distribution (QKD)

- Advantage: QKD uses quantum mechanics to provide encryption without computational assumptions.
- Requirement: Quantum channels for sending quantum states.
- Primary Goal: Secrecy in communication.
- Exclusion: We will focus on secrecy only, without addressing authentication.

BB84

- BB84 Scheme: First complete quantum key distribution protocol
- Proposed by: Bennett and Brassard in 1984
- Key Insight: Requires qubit coherence only during communication time, making it feasible in practice
- Real-World Impact: Companies now perform QKD over fiber optics (up to 10 miles); recently, a team in China achieved QKD over thousands of miles via satellite.

BB84 Scheme - Key Concepts

- Goal: Establish a shared secret key while preventing eavesdropping
- Two Channels:
  - Quantum Channel (transmits qubits)
  - Classical Channel (transmits classical information)
- Assumption: Classical channel ensures authenticity (messages are verifiable as coming from Alice or Bob)

BB84 Protocol Steps

- Alice:
  - Chooses a random bit string x
  - Chooses another random string y to decide the basis for each bit
  - Encodes each bit in one of two bases, depending on corresponding bit in y
  - Sends qubits to Bob
- Bob:
  - Chooses a random string y' to decide his basis for decoding each qubit
  - Measures each qubit using the chosen basis

Basis Comparison and Bit Discarding

- After transmission:
  - Alice and Bob share the bases they used
  - Discard any bits where they didn’t pick the same basis (about 50% of bits)
- Result: Remaining bits are a potential shared key if no eavesdropping occurred

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↕	↘	↔	↕	↕	↔	↔	↘	↗	↕	↘	↗	↗	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Eavesdropping Detection

- Introducing Eve:
  - If Eve tries to measure qubits in transit, she inevitably changes some qubit states
  - Example: If Eve measures a $|+\rangle$ qubit in the standard basis, she risks altering the qubit
- Outcome: This change can be detected by Alice and Bob during their basis check

Security Check

- Verification Process:
  - Alice and Bob check if their qubits match in the same basis
  - If mismatches occur, they infer that Eve eavesdropped
  - If all matches hold, they assume the channel was secure
- Final Step:
  - Once verified, Alice and Bob use the remaining matched qubits as a secure shared key
  - Next Use: Apply the shared key in classical encryption, like the One-Time Pad, for secure message transmission

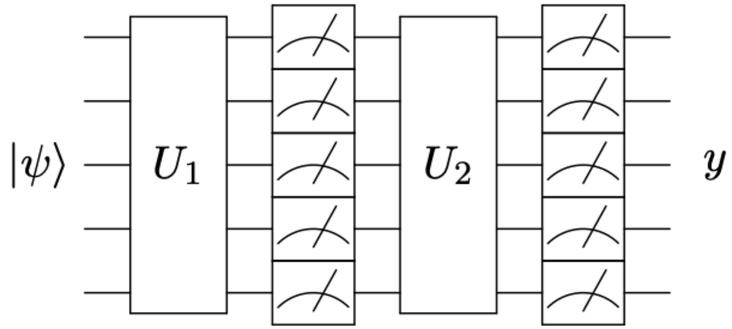
Conclusion - Benefits of BB84

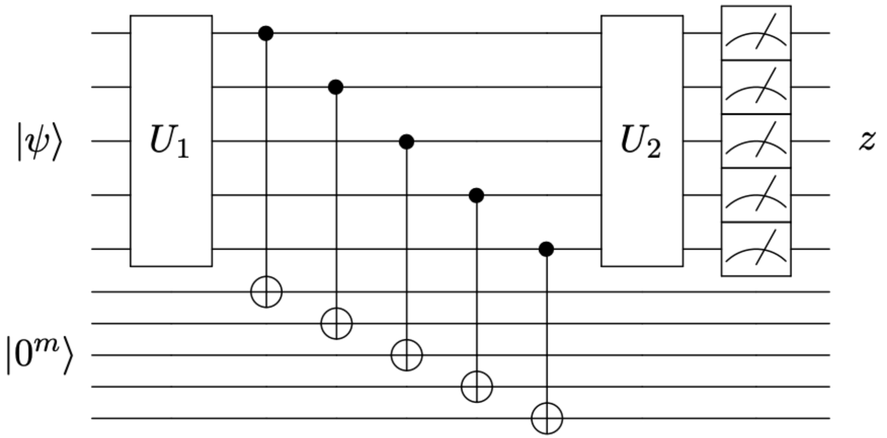
- BB84 Highlights:
  - Quantum mechanics enables secure key exchange without computational assumptions
  - Effective detection of eavesdropping
- Limitation: Eve can block communication but cannot eavesdrop undetected
- Future: Quantum key distribution holds potential for highly secure communications

Deferred Measurement Principle

Deferring Measurements in Quantum Computation

- Concept: Measurements in quantum circuits can be deferred to the end by using ancilla qubits.
- Why: Allows computations to proceed without collapsing states mid-process, providing flexibility in algorithm design.
- Example: Two different approaches with measurement placement:
  - Measurement in the middle of two gates
  - Using CNOT gates and ancilla qubits to defer measurement


$|\psi\rangle$
U_1
U_2
y


$|\psi\rangle$
U_1
U_2
z
$|0^m\rangle$

Measurement in the Middle of Two Gates

- Process:
  - Start with initial state $|\psi\rangle$.
  - Apply U_1 to reach intermediate state $U_1|\psi\rangle$.
  - Measure, yielding a probability distribution over states.
  - Pass through U_2, and measure output.
- Probability Calculation:
  - Final probability depends on intermediate measurements and states.

Deferring Measurement with Ancilla Qubits

- Setup:
  - Use CNOT gates to transfer state information to ancilla qubits.
  - System now includes both original qubits and ancilla qubits.
- Process:
  - U_1 applied to initial state creates entangled intermediate state.
  - CNOT gates copy information to ancillas.
  - After U_2, measure final output state z with equivalent results to mid-computation measurement.
- Benefit: Measurement is deferred, but results remain consistent.

More Adversary Methods

Introduction to the Weighted Adversary Method

- The basic adversary method often fails to provide optimal lower bounds for algorithms.
- To improve, we use the Weighted Adversary Method.
- It's based on a similar idea: define sets Y and Z use a relation R
- Unlike the basic method, pairs (y, z) in R now carry different weights.
- We assign weights based on the difficulty of distinguishing pairs.
- Harder-to-distinguish pairs receive higher weights.
- This approach can yield more accurate lower bounds.
- Leads to better understanding of algorithmic complexity.

Weight Matrix Definition

- Define a weight matrix Γ where $\Gamma[y, z]$ is the weight of (y, z).
- Each $\Gamma[y, z]$ is a non-negative real number, and $\Gamma[y, z] = 0$ if and only if $F(y) = F(z)$.
- Symmetry requirement: $\Gamma[y, z] = \Gamma[z, y]$
- Maximum eigenvalue absolute value of Γ is denoted as $\|\Gamma\|$, which serves as an analogue to $\sqrt{mm'}$ in the basic adversary method.
- Adds flexibility over equal weighting in basic adversary approaches.
- Lays foundation for more refined lower bounds.

Query Distinguishability Analogue

- Query distinguishability in the weighted method mirrors $\sqrt{\ell \ell'}$ from the basic adversary method.
- Define Γ_i by zeroing out Γ entries unless $y_i \neq z_i$.
- For $i \in \{0,1,\ldots,n\}$, Γ_i is updated for each position.
- Then compute $\max\{\|\Gamma_i\| : i \in \{0,\ldots,n\}\}$.
- This maximum is crucial for calculating quantum query complexity.
- Allows for adjusting distinguishability weights in different positions.
- Helps achieve optimal quantum query lower bounds.
- Extends the method's utility beyond basic cases.

Quantum Query Lower Bound Theorem

- Theorem: Quantum Query lower bound for F is given by

$$\|\Gamma\|/\max\{\|\Gamma_i\| \mid i \in \{0,\ldots,n\}\}$$

- Proof is challenging and requires deeper understanding.
- The theorem provides a precise lower bound for queries in quantum computing.
- First proven by Høyer, Lee, and Špalek in 2007 [HLS07].
- Builds on classical lower-bound techniques in quantum contexts.
- Extends the robustness of the adversary method framework.
- Important for complexity analysis of quantum algorithms.

Negative Weights Adversary Method

- Extends the Weighted Adversary Method by allowing negative weights $\Gamma[y, z]$.
- Maintains the same basic framework as the Weighted Adversary.
- $\text{ADV}^{\pm}(F)$: Represents the best lower bound using negative weights.
- Fun Fact: $\text{ADV}^{\pm}(F)$ is computable in polynomial time.
- Semi-definite programming (SDP) allows efficient calculation using F's truth table.

Reichardt's Theorem

- Theorem 5.1: Reichardt's Theorem links $\text{ADV}^{\pm}(F)$ to Quantum Query Complexity.
- States that Quantum Query Complexity of F is exactly $\text{ADV}^{\pm}(F)$.
- Therefore, the Negative Weights Adversary Method provides both upper and lower bounds.
- Significance: Offers a precise measurement of complexity for quantum queries.