Why Secure Communication?

- Sensitive data: finance, defense, healthcare
- Classical cryptography relies on computational hardness
- Quantum computers threaten RSA/ECC (Shor's Algorithm)
- Need for physics-based security → Quantum Cryptography

Quantum Concepts Relevant to QKD

- **Qubits:** Superposition of $|0\rangle$ and $|1\rangle$
- **Measurement:** Collapses state, introduces disturbance
- **No-cloning theorem:** Cannot copy unknown quantum states
- **Entanglement:** Correlated particles across distance

Core Ideas

- Alice and Bob want to establish a secret key
- Eavesdropper (Eve) cannot measure without introducing errors
- Security comes from laws of physics, not math assumptions
- Steps: Transmission $\rightarrow$ Sifting $\rightarrow$ Error Detection

BB84 Protocol: Step-by-Step

1. Alice sends photons polarized randomly in two bases
2. Bob measures with random bases
3. Publicly compare bases, keep only matching ones (sifted key)
4. Estimate error rate to detect Eve
5. Error correction + privacy amplification → final key

BB84 Visualization (Polarizations)

Rectilinear Basis	Diagonal Basis
$\leftrightarrow = 0$	$\nearrow = 0$
$\updownarrow = 1$	$\nwarrow = 1$

Conclusion

- QKD provides provably secure key exchange
- Practical implementations already exist
- Still facing engineering challenges
- Future: Quantum internet and global secure communication