Announcements

- Turn in problem set 8
- Pick up problem set 8 solutions, lecture notes, slides, old mid-terms and their solutions

Quantum Cryptography

- One-time pad cryptography
- Bennett-Brassard protocol quantum key distribution
- Clauser-Horne-Shimony-Holt form of Bell’s inequality
- Ekert protocol quantum key distribution
**Perfectly Secure Digital Communication: The One-Time Pad**

- Alice has a plaintext message to send to Bob securely
- She sends ciphertext = plaintext $\oplus$ random binary key
  
  $\ldots1101000\ldots\oplus\ldots0100101\ldots = \ldots1001101\ldots$
- Ciphertext is a completely random binary string
  impossible to recover plaintext from ciphertext without the key
- Bob decodes ciphertext $\oplus$ *same* binary key = Alice’s plaintext
  $\ldots1001101\ldots\oplus\ldots0100101\ldots = \ldots1101000\ldots$
- Security relies on single use of the secret key
- Decoding relies on Alice and Bob having the *same* key

**Quantum Key Distribution (QKD): Bennett-Brassard (BB84) Protocol**

- Underlying Principle: the state of an unknown qubit cannot be determined… so eavesdropping on an unknown qubit is detectable
- Alice and Bob randomly choose photon-polarization bases

  
  \[ \text{horizontal/vertical} \quad \text{or} \quad \text{+45/-45 diagonal} \]

  
  for transmission (Alice) and reception (Bob)
- Alice codes a random bit into her polarization choice
- When Alice and Bob use the same basis…
  - their measurements provide a shared random key
  - eavesdropping (by Eve) can be detected through errors she creates
Quantum Key Distribution (QKD): Bennett-Brassard (BB84) Protocol

- **BB84 Obviously Secure for:**
  - Single-photon sources
  - Lossless propagation
  - Ideal photon counters

- **BB84 Systems to Date Use:**
  - Weak coherent state sources
  - Lossy and noisy propagation media
  - Geiger-mode avalanche photodiode detectors

- **BB84 Systems Must Therefore Perform:**
  - Sifting
  - Error detection and correction
  - Privacy amplification

Clauser-Horne-Shimony-Holt Inequality: Setup

- Charlie Produces Polarization-Entangled Photon Pair:
  \[ |\psi^-\rangle = (|H\rangle|V\rangle - |V\rangle|H\rangle)/\sqrt{2} \]

- Alice and Bob Do Polarization Analysis:
  \[ b(\theta_B) = \pm 1 \]
  \[ a(\theta_A) = \pm 1 \]

  +1 if photon is detected; -1 if no photon is detected

- Measurements Repeated and Averaged
**CHSH Inequality: Local Hidden Variable Theory**

- Perform Repeated Measurements to Determine:
  \[ C(\theta_A, \theta_B) = \langle a(\theta_A) b(\theta_B) \rangle \]
  for \( \theta_A = 0, -\pi/4 \) and \( \theta_B = 3\pi/8, \pi/8 \)

- If Polarizations Determined by Local Hidden Variable \( \mu \) :
  \[
  S = |C(0, 3\pi/8) + C(-\pi/4, 3\pi/8) + C(-\pi/4, \pi/8) - C(0, \pi/8)|
  \]
  \[
  = |\int d\mu \{ [a(0, \mu) + a(-\pi/4, \mu)] b(3\pi/8, \mu) \\
  \quad + [a(-\pi/4, \mu) - a(0, \mu)] b(\pi/8, \mu) \} p(\mu) | \leq 2
  \]
  \[
  \text{must } = \pm 2 \text{ or } 0
  \]
  \[
  \text{must } = 0 \text{ or } \pm 2
  \]

**CHSH Inequality: Quantum Mechanics**

- Polarization Bases for \( k = A, B \):
  \[
  |i_k\rangle_k \equiv \cos(\theta_k)|H\rangle_k + \sin(\theta_k)|V\rangle_k
  \]
  \[
  |i'_k\rangle_k \equiv \sin(\theta_k)|H\rangle_k - \cos(\theta_k)|V\rangle_k
  \]

- Quantum Measurement Theory for \( C(\theta_A, \theta_B) \):
  \[
  C(\theta_A, \theta_B)
  \]
  \[
  = |\langle \psi^- | (i_A)_{A} \otimes (i_B)_{B} |\rangle^2 + |\langle \psi^- | (i'_A)_{A} \otimes (i'_B)_{B} |\rangle^2
  \]
  \[
  - |\langle \psi^- | (i'_A)_{A} \otimes (i_B)_{B} |\rangle^2 - |\langle \psi^- | (i_A)_{A} \otimes (i'_B)_{B} |\rangle^2
  \]
  \[
  = -\cos[2(\theta_A - \theta_B)]
  \]
**CHSH Inequality: Quantum Mechanics**

- Quantum Mechanics Can Violate Local Hidden Variables

\[
S = |C(0, 3\pi/8) + C(-\pi/4, 3\pi/8) + C(-\pi/4, \pi/8) - C(0, \pi/8)| \\
= |\cos(3\pi/4) + \cos(5\pi/4) + \cos(3\pi/4) - \cos(\pi/4)| \\
= \left| -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} \right| = 2\sqrt{2} > 2
\]

- Experiments with Bi-Photon Sources Show \( S > 2 \)

---

**Ekert Protocol Quantum Key Distribution**

- Passive Random Selection of Polarization Basis

- Alice + Bob Check \( S \approx 2\sqrt{2} \) to Detect Eavesdropping

- Alice + Bob Generate Shared Random Key as in BB84
Coming Attractions: Mid-Term Exam + Lecture 17

- Mid-Term Exam:
  Tuesday, November 8
  - Closed book
  - One 8 1/2 x 11 handwritten formula sheet is permitted

- Lecture 17:
  Quantization of the Electromagnetic Field
  - Maxwell’s equations
  - Plane-wave mode expansions
  - Multi-mode number states and coherent states