

MIT OpenCourseWare
<http://ocw.mit.edu>

6.453 Quantum Optical Communication
Spring 2009

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.



November 4, 2008

6.453 Quantum Optical Communication Lecture 16

Jeffrey H. Shapiro

Optical and Quantum Communications Group

RESEARCH LABORATORY OF ELECTRONICS
Massachusetts Institute of Technology

www.rle.mit.edu/qoptics

6.453 Quantum Optical Communication - Lecture 16



- Announcements
 - Turn in problem set 8
 - Pick up problem set 8 solutions, lecture notes, slides, old mid-term and solution

- 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
...1101000... \oplus ...0100101... = ...1001101...
- 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
...1001101... \oplus ...0100101... = ...1101000...
- 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
horizontal/vertical  or  +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

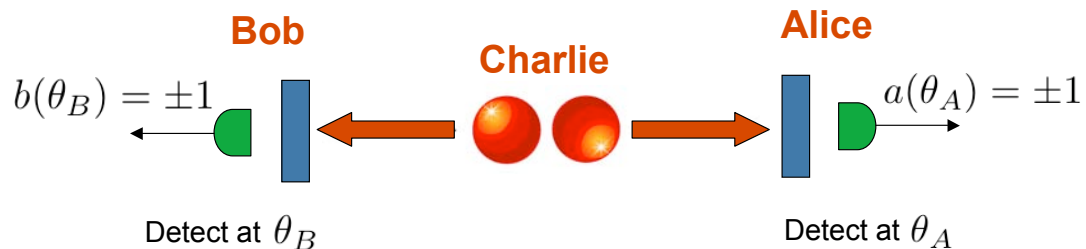
- BB84 Obviously Secure for:
 - Single-photon sources
 - Lossless propagation
 - Ideal photon counters
- BB84 Systems to Date Use:
 - Weak coherent state sources
 - Lossy and noisy propagation media
 - Geiger-mode avalanche photodiode detectors
- BB84 Systems Must Therefore Perform:
 - Sifting
 - Error detection and correction
 - Privacy amplification

Clouser-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:



+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:

$$C(\theta_A, \theta_B) = \langle a(\theta_A)b(\theta_B) \rangle$$

$$\text{for } \theta_A = 0, -\pi/4 \quad \text{and} \quad \theta_B = 3\pi/8, \pi/8$$

- If Polarizations Determined by Local Hidden Variable μ :

$$\begin{aligned} S &\equiv |C(0, 3\pi/8) + C(-\pi/4, 3\pi/8) + C(-\pi/4, \pi/8) - C(0, \pi/8)| \\ &= \left| \int d\mu \left\{ \underbrace{[a(0, \mu) + a(-\pi/4, \mu)]}_{\text{must} = \pm 2 \text{ or } 0} b(3\pi/8, \mu) \right. \right. \\ &\quad \left. \left. + \underbrace{[a(-\pi/4, \mu) - a(0, \mu)]}_{\text{must} = 0 \text{ or } \pm 2} b(\pi/8, \mu) \right\} p(\mu) \right| \leq 2 \end{aligned}$$

CHSH Inequality: Quantum Mechanics

- Polarization Bases for $k = A, B$:

$$|\mathbf{i}_k\rangle_k \equiv \cos(\theta_k)|H\rangle_k + \sin(\theta_k)|V\rangle_k$$

$$|\mathbf{i}'_k\rangle_k \equiv \sin(\theta_k)|H\rangle_k - \cos(\theta_k)|V\rangle_k$$

- Quantum Measurement Theory for $C(\theta_A, \theta_B)$:

$$\begin{aligned} C(\theta_A, \theta_B) &= |\langle \psi^- | (|\mathbf{i}_A\rangle_A \otimes |\mathbf{i}_B\rangle_B) \rangle|^2 + |\langle \psi^- | (|\mathbf{i}'_A\rangle_A \otimes |\mathbf{i}'_B\rangle_B) \rangle|^2 \\ &\quad - |\langle \psi^- | (|\mathbf{i}'_A\rangle_A \otimes |\mathbf{i}_B\rangle_B) \rangle|^2 - |\langle \psi^- | (|\mathbf{i}_A\rangle_A \otimes |\mathbf{i}'_B\rangle_B) \rangle|^2 \\ &= -\cos[2(\theta_A - \theta_B)] \end{aligned}$$

CHSH Inequality: Quantum Mechanics

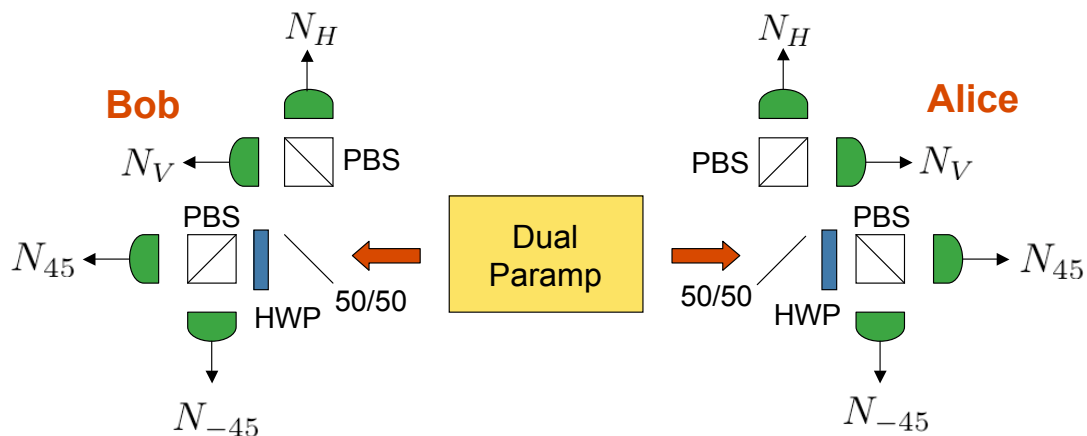
- Quantum Mechanics Can Violate Local Hidden Variables

$$\begin{aligned}
 S &\equiv |C(0, 3\pi/8) + C(-\pi/4, 3\pi/8) + C(-\pi/4, \pi/8) - C(0, \pi/8)| \\
 &= |\cos(3\pi/4) + \cos(5\pi/4) + \cos(3\pi/4) - \cos(\pi/4)| \\
 &= \left| -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} \right| = 2\sqrt{2} > 2
 \end{aligned}$$

- 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:
Thursday, November 6
 - Closed book
 - One 8 1/2 x 11 handwritten formula sheet is permitted
 -
- Schedule note:
No class on Tuesday, November 11 (Veterans' Day holiday)
- Lecture 17:
Quantization of the Electromagnetic Field
 - Maxwell's equations
 - Plane-wave mode expansions
 - Multi-mode number states and coherent states