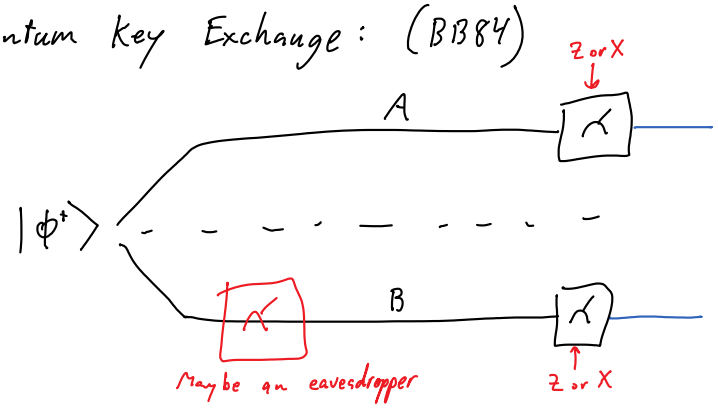
Lecture 6

Thursday, September 25, 2014
12:24 PM

Quantum Key Exchange: (BB84)



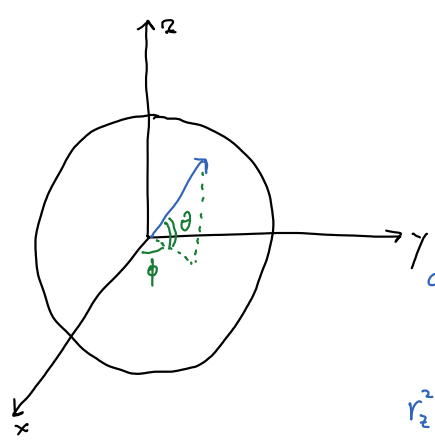
Steps: 1.) Both A and B independently choose random binary sequences $a_1 \cdots a_n$ and $b_1 \cdots b_n$ to decide the measurement orientation.
(i.e. $a_3 = 1$ means A measures X on 3rd qubit)

2.) Reveal a^n and b^n. Trash measurements when $a \neq b$.

3.) Check for eavesdropper: Select a subset of measurements to reveal (and trash)

Density Operator: Generalization of probability mass function (pmf)

Bloch Sphere:



$$|\psi\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\varphi}|1\rangle$$

coordinates
$$\begin{cases} r_z = \cos(\theta) \\ r_x = \sin(\theta)\cos(\varphi) \\ r_y = \sin(\theta)\sin(\varphi) \end{cases}$$

$$r_z^2 + r_x^2 + r_y^2 = 1$$

pure state

$$\rho = |\psi\rangle\langle\psi| = \frac{1}{2}\begin{bmatrix} 1+\cos\theta & \sin\theta(\cos\varphi - i\sin\varphi) \\ \sin\theta(\cos\varphi + i\sin\varphi) & 1-\cos\theta \end{bmatrix}$$

$$= \frac{1}{2}\left(I + r_x X + r_y Y + r_z Z\right)$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

For general ρ: $\rho =$ where $r_x^2 + r_y^2 + r_z^2 \leq 1$ ← inside the sphere.

$\{(\alpha, \rho_1), (1-\alpha, \rho_2)\}$ has density $\rho = \alpha\rho_1 + (1-\alpha)\rho_2$

$$\Rightarrow \quad r_x = \alpha r_{x_1} + (1-\alpha) r_{x_2}$$
$$r_y = \dots$$
$$r_z = \dots$$

$\Rightarrow$ mixtures of densities are averages of vectors in Bloch Sphere

Entropy is radially symmetry — binary entropy function stretched over any diameter.

Notice: $\langle X \rangle = \mathrm{Tr}(X\rho) = \frac{1}{2}\left(\cancel{\mathrm{Tr}(X)}^{0} + r_x \underbrace{\mathrm{Tr}(XX)}_{I} + r_y \cancel{\mathrm{Tr}(XY)}^{0}_{iZ} + r_z \cancel{\mathrm{Tr}(XZ)}^{0}_{iY}\right)$

$= r_x$

$\langle Y \rangle = r_y$

$\langle Z \rangle = r_z$

Unitary operations (noiseless) on mixed state.

$\{(p_x(x), U|\psi_x\rangle)\}_x \quad \Rightarrow$ density operator:

$$\sum_x p_x(x)\, U|\psi_x\rangle\langle\psi_x|U^\dagger = \boxed{U\rho U^\dagger}$$

Measurement (von Neumann)

Complete Orth. projections Π_j s.t. $\sum_j \Pi_j = I$

$$p(j|x) = \langle\psi_x|\Pi_j|\psi_x\rangle \Rightarrow \boxed{p(j)} = \sum_x p(x)\langle\psi_x|\Pi_j|\psi_x\rangle = \mathrm{Tr}(\Pi_j\rho)$$

ensemble

$\boxed{\text{Resulting state}}$: If x preparation and j measured

$$\frac{\Pi_j|\psi_x\rangle}{\sqrt{p(j|x)}}$$

$$\Rightarrow \frac{\Pi_j|\psi_x\rangle\langle\psi_x|\Pi_j}{p(j|x)}$$

Average over x: $\sum_x p(x|j) \nearrow = \sum_x p(x) \frac{\Pi_j|\psi_x\rangle\langle\psi_x|\Pi_j}{p(j)}$

$$= \boxed{\frac{\Pi_j \rho \Pi_j}{p(j)}}$$

General Measurement:

$$\{M_j\} \text{ s.t. } \sum_j M_j^\dagger M_j = I$$ (von Neumann is special case)

Pure state:

$$p(j) = \langle\psi| M_j^\dagger M_j |\psi\rangle$$

$$\text{Result} = \frac{M_j|\psi\rangle}{\sqrt{p(j)}}$$

$\Longrightarrow$

Mixed states:

$$p(j) = \mathrm{Tr}\left(M_j^\dagger M_j \rho\right)$$

$$\text{Result} = \frac{M_j \rho M_j^\dagger}{p(j)}$$

same derivation as above.

POVM: Positive operator valued measurement:

If resulting quantum system is not of concern?

Let $\Lambda_j = M_j^\dagger M_j$: $p(j) = \mathrm{Tr}(\Lambda_j \rho)$

Measurement specified by $\{\Lambda_j\}$ where 1.) $\Lambda_j \geq 0$ (pos. semi-def, Hermitian)

2.) $\sum_j \Lambda_j = I$

What does it mean to have non-orthogonal measurements? Stochastic measurements.

Extreme example: $\Pi_0 = |0\rangle\langle 0|$, $\Pi_1 = |1\rangle\langle 1|$ (von Neumann)

Let $M_0 = \Pi_0$, $M_1 = \sqrt{\alpha}\,\Pi_1$, $M_2 = \sqrt{1-\alpha}\,\Pi_1$ where $\alpha \in [0,1]$

Check $M_0^\dagger M_0 + M_1^\dagger M_1 + M_2^\dagger M_2$

$$= \Pi_0 + \alpha \Pi_1 + (1-\alpha)\Pi_1 = I$$

$$p(0) = \mathrm{Tr}(\Pi_0 \rho)$$
$$p(1) = \alpha\,\mathrm{Tr}(\Pi_1 \rho)$$
$$p(2) = (1-\alpha)\,\mathrm{Tr}(\Pi_1 \rho)$$

If measured as $|1\rangle$, measurement stochastically outputs 1 or 2 with prob. α, $(1-\alpha)$

Exercise 4.2.2: Prove that only $\log_2(d)$ bits can be reliably encoded into a qudit.

Composite densities:

Independent states: $\{ (p_X(x)p_Y(y),\ |\psi_x\rangle^X \otimes |\varphi_Y\rangle^Y) \}$

Independent Not entangled

Density $\rho \otimes \sigma$ where $\rho = \sum_x p_X(x) |\psi_x\rangle\langle\psi_x|$

"product state" $\sigma = \sum_y p_Y(y) |\varphi_Y\rangle\langle\varphi_Y|$

Seperable states: (classically correlated) $\{ (p_{XY}(x,y),\ |\psi_x\rangle \otimes |\varphi_Y\rangle) \}$

Not entangled

Density $\sum_{xy} p_{XY}(x,y)\ \rho_x \otimes \sigma_y$

General seperable state can be expressed as $\sum_z p_Z(z)\ \rho_z \otimes \sigma_z$

Local Density Operator: Consider an arbitrary density over two objects: ρ^{AB}

Measure only A with $\{M_j^A\}$. $\Rightarrow$ the measurements are $\{M_j^A \otimes I^B\}$

$$p(j) = \mathrm{Tr}\left((M_j^\dagger M_j \otimes I^B)\rho \right) = \mathrm{Tr}\left(M_j^\dagger M_j\, \rho^A \right)$$

for same ρ^A

How does ρ^A relate to ρ^{AB}?

Example: $|\phi^+\rangle^{AB}$. What is ρ^A? $\rho^A = \pi = \frac{1}{2}I$

Partial Trace: $\rho^A = \mathrm{Tr}_B(\rho^{AB}) \triangleq \sum_i (I \otimes \langle\varphi_i|)\rho^{AB}(I \otimes |\varphi_i\rangle)$

for any complete orth-norm basis $\{|\varphi_i\rangle\}$

$$\mathrm{Tr}_B(\rho^A \otimes \sigma^B) = \rho^A\, \mathrm{Tr}(\sigma^B) = \rho^A$$

An arbitrary density matrix can be expressed as a sum of tensor products, though not a sum of product states.

Classical - Quantum Ensemble: $\{|x\rangle^A\}$ an orth-norm basis for A.

usually the computational basis

$$\{ (p_X(x),\ |x\rangle\langle x|^X \otimes \rho_x^A) \} \Rightarrow \rho^{XA} = \sum p(x)\ |x\rangle\langle x|^X \otimes \rho_x^A$$

Classical (diagonal)

No entanglement

The X component keeps track of how the state was prepared.

If we measure the X component in $\{|x\rangle^A\}$ basis, the outcome follows p_x resulting state $|x\rangle\langle x|^X \otimes \rho_x$

That is, the states are orthogonal $\Rightarrow$ distinguishable.

Density of quantum part: $\mathrm{Tr}_X(\rho^{XA}) = \sum_x p_x(x)\, \mathrm{Tr}_X\left(|x\rangle\langle x|^X \otimes \rho_x^A\right)$

$$= \sum_x p_x(x)\, \rho_x^A$$

Noisy Channel:

$N(\rho)$: Completely positive trace preserving (CPTP) map.

(Classical channel is cond. prob. distributions: non-negitive, sum to one)

1.) Linear (law of total prob.)

2.) Positive: If $\rho \geq 0$ then $N(\rho) \geq 0$

Example: Transpose pos. but not completely positive

Completely positive: $I \otimes N$ is positive

3.) Trace-preserving: $\mathrm{Tr}(N(\rho)) = \mathrm{Tr}(\rho)$