CS 258: Quantum Cryptography

Mark Zhandry

So far in CS 258: security of classical protocols against quantum attacks

Good guy = classical Bad guy = quantum

Rest of course: quantum protocols

Everyone = quantum

Why quantum protocols?

Possibly better security / security under milder or no assumptions

(e.g. QKD)

This week

Accomplish classically-impossible tasks

(e.g. Quantum Money)

Final week

Dream inspired by QKD: maybe everything can be made information-theoretic!

Today: unfortunately, as with classical crypto, basically everything requires computational security

Example: quantum commitments

A protocol inspired by QKD

Commit phase:

$$\{|\psi_i\rangle = \mathbf{H}^b |c_i\rangle\}_i$$

For random bits c_i $\longrightarrow$

$b \in \{0,1\}$

$b_i \leftarrow \{0,1\}$

measure $\mathbf{H}^{b_i}|\psi\rangle = \mathbf{H}^{b_i \oplus b}|c_i\rangle$

$\Rightarrow c_i'$

Roughly half the b_i will be correct $\Rightarrow c_i' = c_i$

Roughly half the b_i will be incorrect $\Rightarrow c_i'$ uniform

Theorem: Protocol is (statistically) hiding

Density matrix

Consider a distribution over quantum states, where $|\phi_i\rangle$ is sampled with probability p_i. This is called a “mixed state”

Define $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$

ρ captures all statistical information about the mixed state

Examples:

$$|\phi_0\rangle = |0\rangle$$
$$|\phi_1\rangle = |1\rangle$$

$$p_0 = p_1 = \frac{1}{2}$$

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \begin{pmatrix} 1/2 & \\ & 1/2 \end{pmatrix}$$

Called the maximally mixed state

Examples:

$$|\phi_0\rangle = |+\rangle \qquad p_0 = p_1 = \frac{1}{2}$$
$$|\phi_1\rangle = |-\rangle$$

$$\rho = \frac{1}{2}\left[\frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|)\right] + \frac{1}{2}\left[\frac{1}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)\right]$$
$$= \begin{pmatrix} 1/2 & \\ & 1/2 \end{pmatrix}$$

Examples:

$$|\phi_0\rangle = |+\rangle$$
$$|\phi_1\rangle = |-\rangle$$

$$p_0 = p_1 = \frac{1}{2}$$

$$\rho = \frac{1}{2}\left[\frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|)\right] + \frac{1}{2}\left[\frac{1}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)\right]$$
$$= \begin{pmatrix} 1/2 & \\ & 1/2 \end{pmatrix}$$

Examples:

$$|\phi_0\rangle = |0\rangle \qquad p_0 = 1/4$$

$$|\phi_1\rangle = |+\rangle \qquad p_1 = 1/4$$

$$|\phi_2\rangle = |-\rangle \qquad p_2 = 1/2$$

$$\rho = \frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$$

$$= \begin{pmatrix} 5 & -1 \\ -1 & 3 \end{pmatrix} /8$$

Observations

Hermitian $$\rho^\dagger = (\sum_i p_i|\phi_i\rangle\langle\phi_i|)^\dagger = \sum_i p_i|\phi_i\rangle\langle\phi_i| = \rho$$

Positive semi-definite

$$\mathsf{Tr}(\rho) = \mathsf{Tr}\left(\sum_i p_i|\phi_i\rangle\langle\phi_i|\right) = \sum_i p_i \mathsf{Tr}(|\phi_i\rangle\langle\phi_i|) = \sum_i p_i \mathsf{Tr}(\langle\phi_i|\phi_i\rangle) = \sum_i p_i = 1$$

Classical probabilities distributions correspond to diagonal

$$\rho = \sum_i p_i|i\rangle\langle i|$$

Density matrix also captures individual systems of entangled states

$$|\psi\rangle_{\mathcal{A},\mathcal{B}} = \sum_{x,y} \alpha_{x,y} |x, y\rangle$$

System $\mathcal{A}$ has density matrix, which can be captured by imagining measuring $\mathcal{B}$, and taking the probability measurement over outcomes

(Density matrix well-defined even if $\mathcal{B}$ not measured)

$$|\psi\rangle_{\mathcal{A},\mathcal{B}} = \sum_{x,y} \alpha_{x,y} |x, y\rangle$$

Probability measurement gives y: $p_y = \sum_x |\alpha_{x,y}|^2$

Post-measurement state: $|\psi_y\rangle = \frac{1}{\sqrt{p_y}} \sum_x \alpha_{x,y} |x\rangle$

Density matrix:

$$\rho = \sum_y p_y |\psi_y\rangle\langle\psi_y| = \sum_{x,x',y} \alpha_{x,y} \alpha^\dagger_{x',y} |x\rangle\langle x'|$$

Examples:

$$|\psi\rangle_{\mathcal{A},\mathcal{B}} = \frac{1}{\sqrt{2}}|0,0\rangle + \frac{1}{\sqrt{2}}|1,1\rangle$$

Probability measuring $\mathcal{B}$ gives b : $p_0 = p_1 = 1/2$

Post-measurement state for $\mathcal{A}$: $|\psi_b\rangle = |b\rangle$

$$\rho = \begin{pmatrix} 1/2 & \\ & 1/2 \end{pmatrix}$$

Examples:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0,0\rangle + \frac{1}{2}|0,1\rangle + \frac{1}{2}|1,1\rangle$$

Probability measuring $\mathcal{B}$ gives b : $p_0 = p_1 = 1/2$

Post-measurement state for $\mathcal{A}$: $|\phi_0\rangle = |0\rangle$

$$|\phi_1\rangle = |+\rangle$$

$$\rho = \begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix} /4$$

Lemma: If $\rho = \rho'$, then no test can distinguish distributions

Proof: Suppose we apply a unitary U and measure.
Probability of observing x is:

$$\sum_i p_i |\langle x|U|\phi_i\rangle|^2 = \sum_i p_i \langle x|U|\phi_i\rangle\langle\phi_i|U^\dagger|x\rangle$$

$$= \langle x|U \left(\sum_i p_i |\phi_i\rangle\langle\phi_i|\right) U^\dagger|x\rangle$$

$$= \langle x|U\rho U^\dagger|x\rangle$$

Theorem: Protocol is (statistically) hiding

Proof: Let's look at density matrix for each $|\psi_i\rangle$

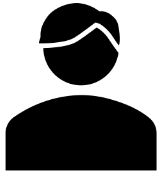
$$\rho_b = \frac{1}{2}\sum_{c_i=0}^{1} \mathbf{H}^b|c_i\rangle\langle c_i|\mathbf{H}^b = \frac{1}{2}\mathbf{H}^b\left(\sum_{c_i}|c_i\rangle\langle c_i|\right)\mathbf{H}^b$$

$$= \frac{1}{2}\mathbf{H}^b\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}\mathbf{H}^b = \frac{1}{2}\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$$

Independent of b, so no test can distinguish $b=0$ from $b=1$

Reveal phase:

Reveal $b, \{c_i\}_i$ $\longrightarrow$



$b \in \{0, 1\}$

b_i, c_i'

Check that when $b_i = b$, then $c_i' = c_i$

Theorem: Protocol is (statistically) binding????

Proof: Let's suppose Alice commits to $b = 0$ and wants to open to $b = 1$

Wherever $b_i = 1$, she has to send c_i matching Bob's c_i'

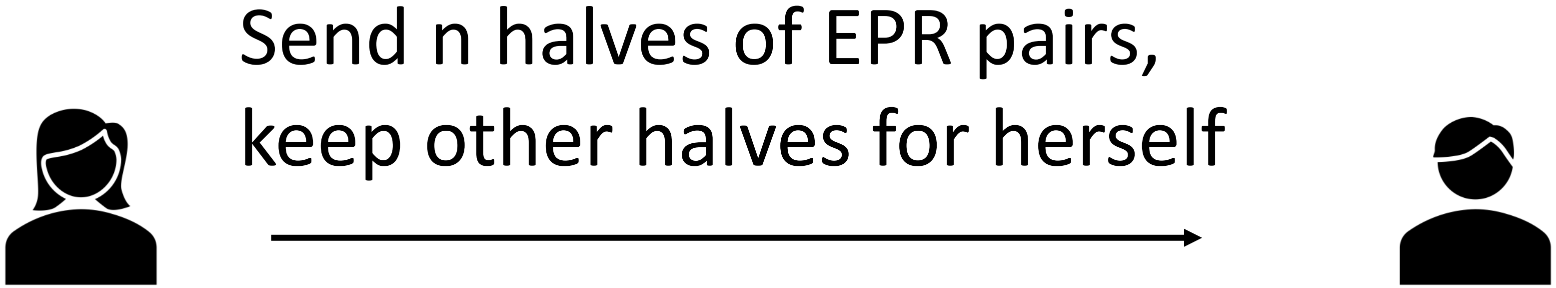
But Bob's c_i' is a random bit entirely independent of Alice's view (because it is the result of measuring $\mathbf{H}|c_i\rangle$)

Prob. of this happening for all such i is exponentially small

Problem: a malicious Alice doesn't have to commit honestly

EPR Attack

Commit phase:



Recall: $$|\mathsf{EPR}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$\mathbf{H}^{\otimes 2}|\mathsf{EPR}\rangle = \mathbf{H}^{\otimes 2}\frac{1}{\sqrt{2}}\sum_b |b,b\rangle$$

$$= \frac{1}{\sqrt{8}}\sum_{b,c,c'} |c,c'\rangle(-1)^{bc+bc'}$$

$$= \frac{1}{\sqrt{2}}\sum_c |c,c\rangle = |\mathsf{EPR}\rangle$$

Equivalently, Alice applying $\mathbf{H}$ is equivalent to Bob applying $\mathbf{H}$

Bob's verification: $|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$$\Downarrow \quad \text{Bob applies } \mathbf{H}^{b_i}$$

$$\mathbf{I} \otimes \mathbf{H}^{b_i}|\mathrm{EPR}\rangle = \mathbf{H}^{b_i} \otimes \mathbf{I}|\mathrm{EPR}\rangle$$

$$\Downarrow \quad \text{Bob measures to get } c_i'$$

Alice's state collapses to $\mathbf{H}^{b_i}|c_i'\rangle$

Note that Alice still doesn't know b_i or c_i'

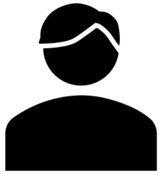
Reveal phase:

To open to b, measure

$$\mathbf{H}^b\mathbf{H}^{b_i}|c_i'\rangle = \mathbf{H}^{b_i\oplus b}|c_i'\rangle$$

to get c_i

$\{\mathbf{H}^{b_i}|c_i'\rangle\}_i$



b_i, c_i'

Roughly half the b_i will be correct ➡ $c_i' = c_i$

Roughly half the b_i will be incorrect ➡ c_i' uniform

Thus, a malicious Alice can perfectly simulate the correct view of Bob for any choice of b

But it gets worse…

Theorem: No commitment can be both statistically binding and hiding

To make proof simpler, we will assume:

- Commitment is a single message from Alice to Bob

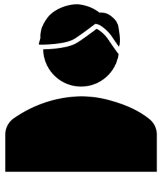
- Hiding is **perfect**

Both of these conditions can be relaxed, with more work

Canonical commitment

Commit phase:

Register $\mathcal{B}$



Alice prepares $|\psi_b\rangle_{\mathcal{A},\mathcal{B}}$

Reveal phase:

b , Register $\mathcal{A}$

Checks if joint system is $|\psi_b\rangle$

Lemma: Any single-message perfectly hiding commitment can be transformed into a canonical perfectly hiding commitment

Step 1: delay all of Alice's measurements until end

$$|\phi_b\rangle = \sum_{x,y,m_1,m_2} \alpha_{x,y,m_1,m_2} |x, m_1, y, m_2\rangle$$

Step 2: "copy" m_2

$$\sum_{x,y,m_1,m_2} \alpha_{x,y,m_1,m_2} |x, m_1, m_2\rangle_{\mathcal{A}} |y, m_2\rangle_{\mathcal{B}}$$

Don't actually perform measurement

In general, "copying" value is indistinguishable from measuring it

$$\sum_{x,y} \alpha_{x,y} |x, y\rangle$$

Measure y

$$\rho = \sum_{x,x',y} \alpha_{x,y} \alpha^{\dagger}_{x',y} |x, y\rangle\langle x', y|$$

"copy" y, then view subsystem

$$\sum_{x,y} \alpha_{x,y} |x, y\rangle |y\rangle$$

$$\Downarrow$$

$$\rho = \sum_{x,x',y} \alpha_{x,y} \alpha^{\dagger}_{x',y} |x, y\rangle\langle x', y|$$

Lemma: For any perfectly hiding canonical commitment, Alice has a perfect attack on binding

Let ρ_b be density matrix for system $\mathcal{B}$ of $|\psi_b\rangle_{\mathcal{A},\mathcal{B}}$

By perfect hiding, $\rho_0 = \rho_1$

$$|\psi_0\rangle = \sum_{x,y} \alpha_{x,y} |x, y\rangle$$

Assemble $\alpha_{x,y}$ into matrix

$$M_0 = \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} & \cdots \\ \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} & \cdots \\ \alpha_{3,1} & \alpha_{3,2} & \alpha_{3,3} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Singular Value Decomposition

$$M_0 = U_0 D_0 V_0^T$$

Where: U_0, V_0 unitary

D_0 diagonal, real, and non-negative

Moreover, $\mathsf{Tr}[D_0^2] = 1$

$$1 = \mathsf{Tr}[M_0^\dagger M_0] = \mathsf{Tr}[V_0^* D_0 U_0^\dagger U_0 D_0 V_0^T] = \mathsf{Tr}[V_0^* D_0^2 V_0^T] = \mathsf{Tr}[V_0^T V_0^* D_0^2] = \mathsf{Tr}[D_0^2]$$

$$M_0 = U_0 D_0 V_0^T$$

Equivalently: $M_0 = \sum_i \sqrt{d_i^0} |\tau_i^0\rangle\langle(\gamma_i^0)^*|$

Where $\sum_i d_i^0 = 1$ $\{|\tau_i^0\rangle\}_i$ orthonormal

$\{|\gamma_i^0\rangle\}_i$ orthonormal

Equivalently: $|\psi_0\rangle = \sum_i \sqrt{d_i^0} |\tau_i^0\rangle|\gamma_i^0\rangle$

(called Shmidt decomposition)

What is Bob's density matrix?

Applying $U_0^\dagger$ to Alice's state doesn't affect Bob's state

$$\Rightarrow \sum_i \sqrt{d_i^0}|i\rangle|\gamma_i^0\rangle$$

Density matrix for Bob is therefore

$$\rho_0 = \sum_i d_i^0 |\gamma_i^0\rangle\langle\gamma_i^0|$$

Now perform same calculation for $b = 1$

$$\rho_1 = \sum_i d_i^1 |\gamma_i^1\rangle\langle\gamma_i^1|$$

Perfect hiding: $$\sum_i d_i^1 |\gamma_i^1\rangle\langle\gamma_i^1| = \sum_i d_i^0 |\gamma_i^0\rangle\langle\gamma_i^0|$$

Insight: Left and right sides are eigen-decompositions of same matrix

$$\Rightarrow \quad d_i^0 = d_i^1 \qquad |\gamma_i^0\rangle = |\gamma_i^1\rangle$$

$$|\psi_0\rangle = \sum_i \sqrt{d_i}|\tau_i^0\rangle|\gamma_i\rangle \qquad |\psi_1\rangle = \sum_i \sqrt{d_i}|\tau_i^1\rangle|\gamma_i\rangle$$

Since $\{|\tau_i^0\rangle\}_i$ and $\{|\tau_i^1\rangle\}_i$ are each orthonormal sets, there exists a unitary W mapping between them

We actually already almost worked it out: $W = U_1 U_0^\dagger$

Alice’s Binding Attack

- Commit to 0
- Later open to 1 by applying W

It turns out that, just like in the classical world, for almost anything we would like to do in cryptography, computational security remains necessary

Intuition: with enough “information” observed, secrets revealed even if information is quantum

Next time: While quantum doesn't usually eliminate assumptions, it can make them milder

In particular, while classical cryptography cannot exist if P=NP, quantum cryptography *might* still exist if $\mathrm{NP} \subseteq \mathrm{BQP}$