COS 533: Advanced Cryptography — Princeton University
Lecture 22 (December 6, 2017)
Lecturer: Mark Zhandry — Scribe: Fermi Ma

Notes for Lecture 22

1 Qubits and Measurement

1.1 Single Qubits

Last time we started talking about qubits. A qubit has some state $|\psi\rangle$ which we can write as $\begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix} = \alpha_0|0\rangle + \alpha_1|1\rangle$. We require $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

We can apply unitary operations to the qubit, where we multiply by a unitary matrix $U^\dagger U = I$. This transforms $|\psi\rangle \to U|\psi\rangle$.

If we measure in an arbitrary basis $B = \{|b_0\rangle, |b_1\rangle\}$, the result is 0 with probability $|\langle b_0|\psi\rangle|^2$, and the state becomes $|b_0\rangle$.

For the remaining lectures, we'll use a special basis called the computational basis $B = \{|0\rangle, |1\rangle\}$.

Measurement in any arbitrary basis $\{|b_0\rangle, |b_1\rangle\}$ can be implemented using unitary matrices and measurements in the computational basis. To see this, let U be the matrix such that $U|0\rangle = |b_0\rangle$ and $U|1\rangle = |b_1\rangle$. Basically U has b_0 in the first column and b_1 in the second column. U is a unitary matrix because b_0 and b_1 are orthonormal vectors. To measure $|\psi\rangle$, we compute $|\psi'\rangle = U^\dagger|\psi\rangle$ (note the conjugate transpose of a unitary matrix is unitary). Then we can measure $|\psi'\rangle$ in the computational basis. This gives 0 with probability $|\langle 0|U^\dagger|\psi\rangle|^2 = |\langle b_0|\psi\rangle|^2$, since $\langle 0|U^\dagger$ is the conjugate transpose of $U|0\rangle = |b_0\rangle$. Then finally we apply U to whatever is left. If it is $|0\rangle$, we get $|b_0\rangle$, and if it's $|1\rangle$, we get $|b_1\rangle$.

So in general we can restrict our attention to the computational basis. All the bases are the same as long as you know the unitary matrix that goes between them.

1.2 Multi Qubit System

So far we've only talked about one qubit, but there's no reason why we can't have multiple photons. With two photons, we have four possibilities for their polarization (each can be vertical or horizontal). The right way to think of $|\psi\rangle$ is as a vector

$$\begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix} = \alpha_{00}|00\rangle + \alpha_{01}|01 + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

where $\sum_{b_0,b_1} |\alpha_{b_0,b_1}|^2 = 1$. Now the unitary matrix is a 4 by 4 matrix.

We can measure and get (b_0, b_1) with probability $|\langle b_0 b_1|\psi\rangle|^2 = |\alpha_{b_0 b_1}|^2$. Basically everything generalizes to many-qubit systems.

One thing that is different is that now I can measure just one photon. There's no particular reason I have to measure both photons.

A partial measurement is where I measure 1 qubit out of many. Given

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{00}|11\rangle,$$

if I measure the 1st qubit, I get 0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$

If I get a 0, basically the new state is just the pieces that are consistent with that measurement. We're left with $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle$, but to normalize we divide by $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$.

We can verify the computation to see that if I then measure the second qubit, the probability of any outcome (b_0, b_1) is the same as it would be if we measured both qubits at the same time.

Examples of two qubit systems:

- $|00\rangle$ is just 2 qubits each in state $|0\rangle$ (think of two qubits both in vertical polarization).

- $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$. What does this correspond to? Recall from last lecture that a polarization at a 45 degree upward-pointing angle corresponds with $|0\rangle + |1\rangle$, and a 45 degree angle downward-pointing angle corresponds with $|0\rangle - |1\rangle$. The claim is that this two qubit state is equivalent to the first photon being in the $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ state and the second being at the $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ state. If we multiply this out we get the above two qubit state.

- $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is a state that can't be decomposed into two separate qubits. We call such a state "entangled". If Alice measures and gets a 0, then the entire system collapses to $|00\rangle$. So the outcome of Alice's measurement determines what Bob gets. Even if these photons are placed on opposite ends of the galaxy, measuring one will immediately determine the other (though there's no way to use this mechanism to transmit information, so this doesn't violate the fact that information can't travel faster than the speed of light).

2 No Cloning

Last time we showed that if we had an authenticated way to send classical messages, we could do key exchange. One of the crucial things for this key exchange protocol to be secure is that it must be impossible to clone quantum states.

Theorem 1 *(No Cloning Theorem) It is impossible in general to clone quantum states.*

Proof. We'll sketch out a proof that it is impossible to clone in general. We'll restrict to just unitary procedures, but it's possible to make this proof more formal. We want to prove that there's no fixed procedure that takes in a quantum state and produces two identical copies of it. We want a U such that $U|\psi\rangle = |\psi\rangle|\psi\rangle$. Note that there's a syntactical problem here. If we just think of one qubit, then $U|\psi$ is a 2 dimensional vector while $|\psi\rangle|\psi\rangle$ is a 4 dimensional vector. To get around this we'll just pad the input ψ with 0's. We'll assume towards contradiction that we have such a U that satisfies $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$. We'll actually restrict our attention further to matrices U that can only clone two fixed states $|\psi\rangle$ and $|\phi\rangle$, so

$$\begin{aligned} U|\psi\rangle|0\rangle &= |\psi\rangle|\psi\rangle \\ U|\phi\rangle|0\rangle &= |\phi\rangle|\phi\rangle. \end{aligned}$$

We consider the term formed by taking the conjugate transpose of the left-hand side of the second equation and multiplying by the left-hand side of the first equation

$$\begin{aligned} (\langle\phi|\langle 0|U^\dagger)(U|\psi\rangle 0\rangle) &= (\langle\phi|\langle\phi|)(|\psi\rangle|\psi\rangle) \\ &= \langle\phi|\psi\rangle^2 \end{aligned}$$

But we have another way of evaluating the left-hand side by canceling out the unitary matrices

$$\begin{aligned} (\langle\phi|\langle 0|U^\dagger)(U|\psi\rangle 0\rangle) &= (\langle\phi|\langle 0|)(|\psi\rangle|0\rangle) \\ &= \langle\phi|\psi\rangle\langle 0|0\rangle \\ &= \langle\phi|\psi\rangle \end{aligned}$$

$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$ imples that $\langle\phi|\psi\rangle \in \{0, 1\}$. This means that either $|\phi\rangle = |\psi\rangle$, or they're orthogonal. But if I can already prepare two states ϕ and ψ that are the same, I know the state, and so I can "clone" by just preparing the state again. In this case, "cloning" is trivial. If the two states are orthogonal, a similar argument applies.

This analysis rules out cloning when the two states are not the same or orthogonal, so general cloning through a unitary procedure is impossible. □

3 Quantum Money

One application of the No Cloning Theorem is to build unforgeable money. Classically this is impossible because we can just copy bits. Note that bitcoin gets around this difficulty by using a public ledger (which just makes it very hard to forge if you believe certain computational assumptions), but quantum money allows us to just say that certain qubits are unforgeable.

3.1 A Basic Scheme

First, imagine a world where there is just one banknote. Clearly this is a useless system of "money", but we'll show how to add more functionality later. A one bill system has two procedures:

- $GenNote(1^\lambda)$ prepares some quantum money state $|\$\rangle$ and a serial number s.
- $Ver(s, |\$\rangle)$ accepts or rejects.

We can imagine a correctness procedure where if the mint produces one banknote, it can immediately verify that banknote. The verifier should accept valid banknotes and leave them unchanged (though it may destroy invalid bank notes).

Consider the following security experiment. The challenger runs $s, |\$\rangle \leftarrow GenNote(1^\lambda)$ and gives $|\$\rangle$ to the adversary. The serial number is kept secret. The adversary attempts to produce two valid banknotes $|\$_0\rangle, |\$_1\rangle$. The challenger runs $Ver(s, |\$_0\rangle), Ver(s, |\$_1\rangle)$ and outputs 1 if both accept.

We'll start with a scheme that doesn't work and then we'll make it work.

- $GenNote(1^\lambda)$: Let the serial number be randomly sampled $s = (b, c) \leftarrow \{0, 1\}^2$.
  If $b = 0, c = 0$, the bill is $|0\rangle$.
  If $b = 1, c = 0$, the bill is $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
  If $b = 0, c = 1$, the bill is $|1\rangle$.
  If $b = 1, c = 1$, the bill is $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
- $Ver(s, |\$\rangle)$ will measure in the basis specified by b and check if the result is c.

Think of $b = 0$ as specifying the $|0\rangle, |1\rangle$ basis, and $b = 1$ as specifying the $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ basis.

The c bit just picks one of the two basis vectors.

It turns out we can attack this scheme. Just pick between the two bases randomly. If we pick the correct basis (1/2 probability), we can make a measurement and determine

c. This tells us exactly what the bill is. If we pick the incorrect basis, our measurement tells us nothing about c. So half the time, we can only guess the correct bill with probability one half, which means we cannot succeed with probability greater than 3/4.

A 3/4 probability of counterfeiting is much higher than what we want, so we can just repeat this scheme many times to reduce the counterfeit probability to be negligible. So we produce λ qubits, where each qubit is produced in the way as before. Then we accept only if all the qubits are accepted. Doing this λ times, the success probability of an arbitrary strategy is at most $(3/4)^\lambda$. However, this scheme is still not good enough if we consider what happens in practice.

If we make the serial number public, this allows you to construct the state from scratch. But the serial number is required for verification. So now a merchant can't verify without interacting with the bank. But if we have the ability to send to the bank and check if a note is valid, the adversary should be allowed to make verification queries in the security experiment. It turns out that allowing verification queries in the experiment is deadly, and this scheme is no longer secure.

3.2 Adding Functionality

What we want is public key quantum money, where we can verify publicly. Now a merchant doesn't need to go to the bank.

Note that if we have a public verifier, we can keep running the verifier over and over and each time it "corrects" the bank note. It turns out this is very hard to build in practice, and this is an active area of research.

How do we increase the number of banknotes? In the secret key setting, we can run $GenNote(1^\lambda)$ many times and get $s_i|\$_i\rangle$. We can keep a database (i, s_i) of index, serial number pairs. Then we hand out $(i, |\$_i\rangle)$ as money state. This has the undesirable property that we need to keep a large database.

To get rid of the database, we can try to use a PRF. The bank chooses a $k \leftarrow \{0,1\}^\lambda$. Then we set $s_i = PRF(k, i)$, and we give out the index i along with the banknote. Now the bank can recompute the serial numbers on the fly instead of storing them.

For a public key quantum money scheme, this won't work. If we can construct the bank note from the serial number, clearly the adversary can make a counterfeit bank note by choosing a new serial number and building the corresponding quantum state. So the bank will sign the serial numbers with a digital signature scheme, and it includes $\sigma_i \leftarrow Sign(sk, s_i)$ in the banknote. The new public notes are then $(s_i, \sigma_i|\$_i\rangle)$. This means we can build public key quantum money scheme with many bills if we can support one bill.

What we've seen is that quantum mechanics allows us to do things that we couldn't do in classical crypto. With quantum key distribution, we can build key exchange without computational assumptions. For quantum money, we can build unforgeable bank notes. However, quantum mechanics also gives ways to break cryptographic scheme. With quantum computers, we can solve discrete log in polynomial time. Even for NP complete problems, this can speed things up by a polynomial factor. Next week, we'll see how quantum mechanics can be used to attack crypto.