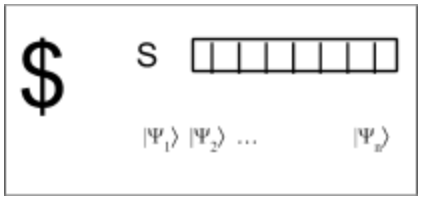
Thurs Feb 9

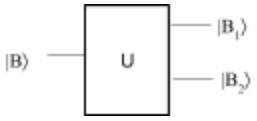
Guest Lecture by Supartha Podder



Continuation of Quantum Money

Last time we covered how classical money is copyable and showed a scheme for making money uncounterfietable through an application of the No Cloning Theorem.

Let's consider a counterfeiter.

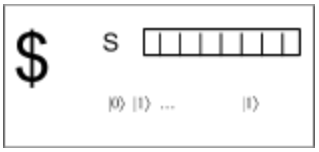
Wants to take a legitimate bill B and do 

such that both new bills pass the verification scheme.

Say the counterfeiter decides to measure all qubits in the $|0\rangle,|1\rangle$ basis.

Their new bill becomes:

- S gets copied
    - (classical information)
- Puts $|0\rangle$ or $|1\rangle$ as each qubit.



So the bank will check each quantum state, the ones that should be in the $|0\rangle|1\rangle$ basis are correct ½ the time. The ones that should be in $|+\rangle|-\rangle$ are correct ¼ of the time.

The odds of success of the counterfeiter (bank reading all states correctly is $(⅝)^n$.

This sort of attack has an upper success bound of $(¾)^n$.

Interactive Attack

There's an attack on this scheme based around the fact that verification involves giving the bank the bill, then the bank returns the bill and whether or not it's valid.

We can repeatedly go to the bank, ask them to verify the bill.

For some qubit that we set to $|0\rangle$

if the bank measured it correctly, we know it's not $|1\rangle$

if the bank measured it incorrectly, we know it's not $|0\rangle$

We can similarly distinguish out $|+\rangle$ and $|-\rangle$

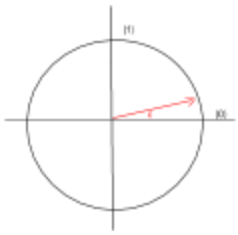
So running the verification scheme over each possibility for that quantum state allows us to get a strong picture of what state the bank is verifying it against.

Running this procedure O(log(n)) times and you can copy the note with probability $O(1=1/n^2)$.

Can we come up with another attack?

Recall the **Elitzur Vaidman Bomb**. The general idea is that through repeated applications of a unitary transformation to a state that starts at either $|0\rangle$ or $|1\rangle$, we can with a high probability of success get it to measure as $|1\rangle$. Applying this sort of procedure to quantum money gives us an…

Attack Based on the Elitzur Vaidman Bomb



Set $|c\rangle$ to $|0\rangle$

Repeat $\pi/2\varepsilon$ times:

Apply R_ε to $|c\rangle$

Apply cNOT to $|c\rangle|\Psi_1\rangle$

Then send the bill back to the bank.

Each time we apply cNOT given $|\Psi_1\rangle = |0\rangle$, we get $(\cos\varepsilon|0\rangle + \sin\varepsilon|1\rangle)|0\rangle = \cos\varepsilon|00\rangle + \sin\varepsilon|11\rangle$

Most of the time $|c\rangle$ will stay at $|0\rangle$.

Which means at each step the probability of getting caught is $\sin^2\varepsilon$.

Thus Prob[getting caught at all] is bounded at $\leq \pi/(2\varepsilon)\ \sin^2\varepsilon = O(\varepsilon)$

The same holds for $|1\rangle$ and $|-\rangle$.

But if $|\Psi_1\rangle = |+\rangle$, cNOT doesn't have the same effect

$(\cos\varepsilon|0\rangle + \sin\varepsilon|1\rangle)\otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ will eventually rotate the qubit to $|1\rangle$.

So when we measure at the end, we can distinguish $|+\rangle$ from the other states, because it's the only one that will be measured at $|1\rangle$.

We can similarly distinguish the other three states by starting $|c\rangle$ to the other three values.

What solution exists for this vulnerability?

The bank can just return a new copy of the money instead of the one that was verified.

This scheme still has a fundamental problem, which is that to make a transaction, you need to go to the bank. If you have to go to the bank, you might as well do an account transfer instead. The point of currency is that anyone should be able to verify it. Which brings us to...

Public Key Quantum Money

The bank produces money that can be verified by anyone.

Proposed by (Aaronson 2009), (Aaronson, Christiano 2012).

With this sort of scheme you'll always need computational assumptions on the counterfeiter, because technically they could always just try *every* possible quantum state with infinite computational power.

Quantum Key Distribution

Proposed by (Bennett, Brassard 1984) and thus called BB84

Key distribution is a fundamental task in cryptography. There's a technique in classical cryptography we can use for this called the **One-Time Pad**.

Given shared $k \in \{0,1\}^n$

Alice has secret message $m \in \{0,1\}^n$

Alice produces, sends c, for which $c_i = m_i \oplus k_i$

Bob decodes the message m as $m_i = c_i \oplus k_i$

As the name implies, this technique can only be used once securely, and it requires Alice and Bob to share some initial knowledge. In fact, it's been proven that Alice and Bob either need initial secret information in common or you must make computational assumptions on an eavesdropper Eve.

So we want a scheme with no assumptions on Eve in which to share a secret (presuming we have a classical authenticated channel: cannot be tampered by Eve, can be read)

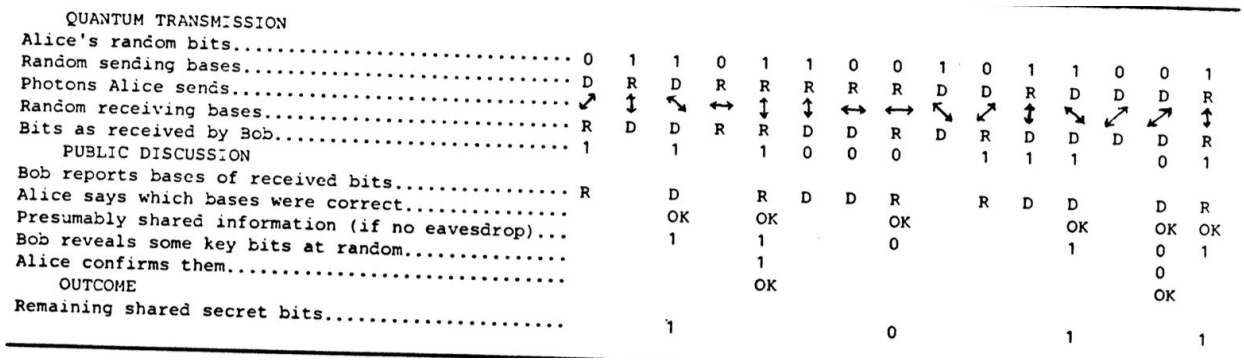
In cryptography we want secrecy and authentication.
This protocol is only going to deal with secrecy.

BB84

This quantum encryption scheme was already there in Wiesner's paper and was later formalized by B&B. It circumvents the issues we've seen in maintaining a qubit, because it only requires coherence for the time it takes for communication between Alice and Bob.

There are companies that are currently already doing quantum key distribution through fiber optic cables over up to 10 miles. There are people trying it working from ground to satellite which would get around the limitations of fiber optics, basically letting you do quantum key distribution over arbitrary distances. China actually has a satellite up for this express purpose.

Here's a diagram from the original paper that shows how BB84 works.



The basic idea is that you're trying to establish some shared secret knowledge and you want to know for certain that no eavesdroppers on the channel can uncover it. You've got a channel in which to transmit quantum information, and a channel in which to transmit classical information. In both, no one can impersonate Alice or Bob (authenticity) by eavesdroppers may be able to listen in (no secrecy).

- So Alice chooses a string x of random bits $\epsilon \{0,1\}^n$
- And another string y of random bits $y \epsilon \{0,1\}^n$ which she uses to decide which basis to encode each bit from x in.
- She then encodes the qubits in the $|0\rangle|1\rangle$ basis (in the diagram it's R) or the $|+\rangle|-\rangle$ basis (D)
- Then she sends over the qubits to Bob.
    - Bob picks his own random string $y' \epsilon \{0,1\}^n$ and uses y'_i to decide which basis
        - To decode the i^{th} qubit send over (picking again between D and R)

Now Alice and Bob share which bases they picked to encode and measure in (the Y's) and discard any instances where they didn't pick the same one (about half the time).

At this point we consider an eavesdropper Eve who was listening in to the qubits that were sent over. The whole magic of using qubits is that if Eve listened in on the transmission she inherently changed the qubit's that Bob received. Sure, if she measured a $|0\rangle|1\rangle$ qubit in that axis, the qubit didn't change, but what if she measured a $|+\rangle|-\rangle$ qubit in the $|0\rangle|1\rangle$ basis?

If Alice sent $|+\rangle$, then Eve measured $|0\rangle$ and passed that along to Bob. Then Bob has a 50% chance of measuring $|+\rangle$ *or* $|-\rangle$.

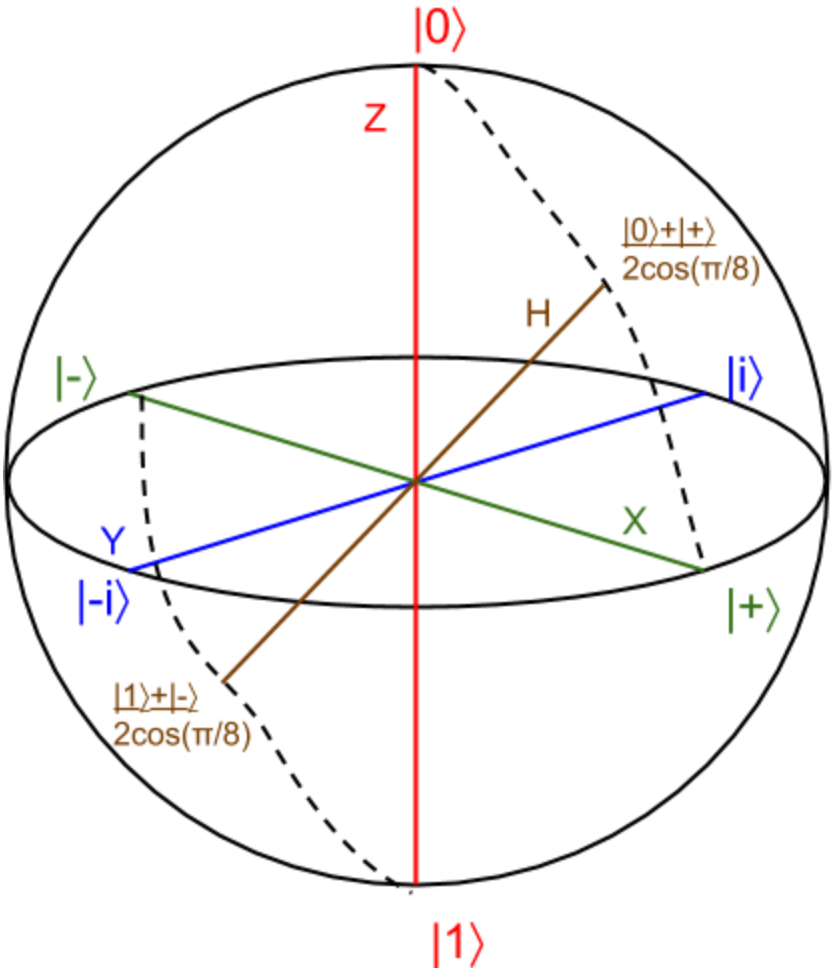
So Alice and Bob can verify that no one listened in to their qubit transmission by making sure that some portion of their qubits that they believe match do match. Of course these qubits aren't going to be secret anymore, but they've still got all the others.

If any of the qubits didn't match, then Eve eavesdropped and they can just try again and again until they can get an instance where no one listened in.

The idea is that now Alice and Bob share some initial information and can thus use some classical encryption scheme, like a 1 Time Pad.

Recitation Session

(Patrick)



Applying gates X,Y,Z or H is the same as doing a half turn on their respective axis.

S corresponds to a quarter turn around Z. [in the $|+\rangle$ to $|1\rangle$ direction]

$T^2 = S$, so T corresponds to an eighth turn around Z.

$R_{\pi/4}$ corresponds to a quarter turn (i.e. $\pi/4$) on Y.