6.857 Computer and Network Security	November 27, 2001

Lecture Notes 22 : Quantum Cryptography

Lecturer: Ron Rivest *Scribe: Cruz/Davtchev/Kim/Rahnev*

1 Quantum Computation

Previously all computers were based on a "deterministic" or even "randomized" models of computation. What can be done if we "change rules of the game" even further, and allow computation to depend on quantum-mechanical principles?

Peter Shor says you can factor large numbers and take discrete logarithms efficiently with quantum computers. Much current public-key cryptography would then become vulnerable.

Question: Would you also have problems with block ciphers?
Answer: A block cipher that depended on these number-theoretic problems would become vulnerable. For other ciphers, such as AES, we still don't know.

Question: Are P and NP equal with quantum computation?
Answer: Probably what you mean is: with polynomial-time quantum computation, can you solve all problems in NP? (I.e., is NP a subset of QP?) We don't know.

Bits in a classical computer are 0 or 1. A quantum computer stores *qubits* that may store a linear superpositions of these two. $|0\rangle$ or $|1\rangle$ in "ket" notation or $\alpha|0\rangle + \beta|1\rangle$ where α and β are complex numbers called *amplitudes* that represent "how much" of a zero or one is in a qubit. $|\alpha|^2 + |\beta|^2 = 1$. Quantum mechanics is all about linear operations.

What happens when you look at a qubit? Is it $|0\rangle$ or is it $|1\rangle$? We see qubit $= |0\rangle$ with probability $|\alpha|^2$ and see qubit $= |1\rangle$ with probability $|\beta|^2$. A qubit changes to the state that was measured (no longer with superposition), so reading is destructive because of a so-called collapse of the wave function.

There are many ways to build a qubit: electron spins, polarization of light, etc. We will use polarization of light for this class. For example:

$$\updownarrow \equiv |0\rangle$$

$$\leftrightarrow \equiv |1\rangle$$

We can use a calcite crystal as a beam splitter, which allows only photons of certain polarization to pass through.

So you can measure polarization with a calcite crystal and a photodetector.

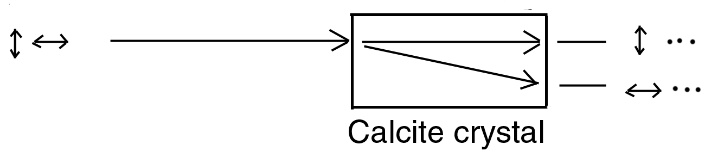

Figure 1: Beam splitter.

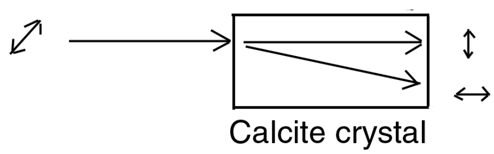

Figure 2: If we measure $(\alpha|0\rangle + \beta|1\rangle)$, we get $\updownarrow$ with probability $|\alpha|^2$ and $\leftrightarrow$ with probability $|\beta|^2$. The original polarization is lost.

2 History of Quantum Computing

In 1970, Weisner proposed "unforgeable money." His goal was to have a quantum dollar bill with an uncopyable serial number.

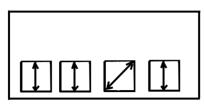

Figure 3: Quantum dollar bill.

The qubits are storing a bit in either the *vertical/horizontal* + direction, or else the *diagonal(rising/falling)* X direction. There are thus two "bases" that can be used. Using the wrong one to read the qubit gives a random result and destroys the stored qubit.

The bank knows how to align the polarizing crystal to read the first bit.

If a qubit = $\updownarrow$ measured in the X orientation, you see the following (with probabilities)1/2 $\nearrow$ 1/2 $\searrow$. If a qubit = $\leftrightarrow$ measured X you see the same as above.

Therefore, one cannot tell the difference between $\updownarrow$ and $\leftrightarrow$ if in the wrong basis. If guessing, you are done, lost information. So there is no way to copy a bill, a.k.a. the "No Cloning Theorem" $\Rightarrow$ we cannot copy a quantum state exactly.

Question: Can't you just destroy some money and try over and over on different bills to determine orientation of first bit?
Answer: No, because different bills have different serial numbers.

Question: How does this help? You cannot clone bills but you can always destroy them.
Answer: A forger can not create bills that would read and give a valid serial number at the bank. That was the design goal here.

3 Quantum key agreement

Bennet and Brassard, 1983.

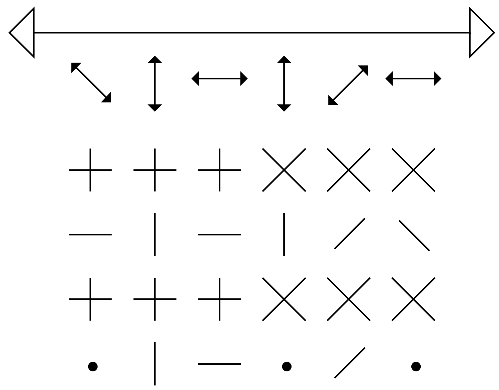

Figure 4: Alice and Bob's key agreement over a fiber optic channel.

Alice submits photons one at a time to Bob with one of 4 different polarizations, in a random pattern that Bob does not know. Bob measures each one in either + or X. Alice and Bob know good bits. Claim: An eavesdropper is unable to know anything with this key agreement. Alice and Bob can do parity checking to see if an eavesdropper destroyed bits to confirm they got same bits.

Question: Doesn't Eve know all bits if Bob tells how he measured and Alice says what is correct?
Answer: No, Bob tells + or X and Alice tells which are correct, but nobody else knows what Bob got. Bob tells Alice the bases he is using to measure, but not the results he got.

Question: Is there a way to do signatures with quantum computing? A Man-in-the-middle attack still fails here.
Answer: Man-in-the-middle does fail here. There are a lot of open questions here; this is a slippery field. It is an open problem as to whether you can do signatures with quantum computers, as far as I know.

Question: Isn't there computation involved once you have the keys?
Answer: It depends what you do with it. (For example, you can use the key now for a one-time pad.)

The problem with this scheme is that you cannot have repeaters, so there are physical limitations. In practice, however, researchers were able to run a wire all the way under Lake Geneva and share a key secretly.

Question: Might this be good for intellectual property issues?
Answer: Yes, maybe for MP3s ... QP3s. :-)

Adi Shamir proposed a scheme to break this:

Shine a light *backwards* along the fiber into Alice's polarizing crystal, and then measure the polarization of the returned photons. Thus Eve can measure the polarization used without touching the photon that Alice sends to Bob.

4 Factoring/Computation

So, we need to see how to compute with quantum computers. We can begin with computations on a single qubit, $\alpha|0\rangle + \beta|1\rangle$. These computations are always *linear*.

$$\begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}$$

Let $U = \begin{pmatrix} \cdot & \cdot \\ \cdot & \cdot \end{pmatrix}$. Here U must be *unitary*; U is a unitary transformation iff $U^*U = I$, where U^* is the conjugate transpose of U.

Here is another one-qubit operation: NOT.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$

Here is another interesting one: COIN-FLIP.

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} (\alpha+\beta)/\sqrt{2} \\ (\alpha-\beta)/\sqrt{2} \end{pmatrix}$$

$$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

While the above coin-flipped $|0\rangle$ and $|1\rangle$ are indistinguishable upon measurement (collapse of the wave function) because they have $1/2$ probability of turning up as either state, the coin-flip operation is unitary and can be inverted (!).

All unitary transformations are reversible and preserve information.

The theory of quantum computing thus can build upon the previously-studied field of "reversible computation." This has independent interest since irreversible operations are ones that consume energy; reversible operations can be done in principle using little or no energy. But in quantum computation, each operation (except the final measurement of the result) *must* be reversible.

Question: How are the computations performed experimentally?
Answer: Researchers are exploring many ways of building a quantum computer. You might use nuclear spin: a cup of coffee has many carbon atoms, each with its own nuclear spin that can represent a qubit. Use NMR (nuclear magnetic resonance) to manipulate the qubits. Quantum computers with a few qubits have been built; larger machines seem difficult to build for a number of reasons, such as the fact that there is no "restoring logic" in quantum computers (you can't clone a value, which is what you would need to do).

Let's look at 2-qubit quantum computers now.

Input two-qubit register: $|00\rangle|01\rangle|10\rangle|11\rangle$. Suppose that the two qubits are independently set up to have a superposition. Then

$$(\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

Let us simplify notation by denoting as follows: $w = \alpha\gamma$, $x = \alpha\delta$, $y = \beta\gamma$, $z = \beta\delta$.

If we read both qubits simultaneously then, we see

$$\begin{array}{c} |00\rangle \text{ with Prob } |w|^2 \\ |01\rangle \text{ with Prob } |x|^2 \\ |10\rangle \text{ with Prob } |y|^2 \\ |11\rangle \text{ with Prob } |z|^2 \end{array}$$

Suppose that instead we read only the first of the two qubits. We would see:

$$\begin{array}{c} |0\rangle \text{ with Prob } |w|^2 + |x|^2 \\ |1\rangle \text{ with Prob } |y|^2 + |z|^2 \end{array}$$

With the standard "wave function collapse", the new state of the quantum computer is (assuming that the first qubit was read as a 0):

$$\begin{array}{c} |00\rangle \text{ with amplitude } \frac{w}{\sqrt{|w|^2+|x|^2}} \\ |01\rangle \text{ with amplitude } \frac{x}{\sqrt{|w|^2+|x|^2}} \end{array}$$

In the above example, the two qubits were independent. But it is possible to have *entanglement*, where they are not. For example, we can have the computer in the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ — here is one bit is read, the wave function collapses so that both qubits have the same value.

An n-qubit system thus seems to require 2^n complex amplitudes to represent its state—one amplitude for each of its possible 2^n basis states. This can seem fundamentally surprising—the universe seems to "make up" storage somehow to represent all of these values.

We are still figuring out what really quantum computing is.