Quantum Cryptography Notes (summary of Code Book Chapter 8)

Note: This book was published in 1999, so it's very likely that the ideas in this summary are outdated and that many achievements have occurred in quantum cryptography that are well beyond what is described here. Here we simply describe a way to exchange a secret key (random bitstring) that can be used for a symmetric cryptosystem such as AES.

Quantum physics ideas are often at odds with what makes intuitive sense. Quantum cryptography makes use of the idea of superposition and to help explain how this would help cryptography, these notes abstract away the rigorous details of the physics and provide a very simple model of how these particles act.

Abstract idea of a qubit

We can think of a qubit as a single bit that is transmitted over a fiber-optic line. The bit can be set to either 0 or 1. In order for the receiver to "read" the bit, she needs to have a reader. For our purposes, we'll have two possible readers:

(1) + (we can think of this as something closed with two slits, one vertical and one horizontal. If something passes through, then we can detect whether it passed through horizontally or vertically. We can assign vertical = 1, horizontal = 0, for example.

(2) x (we can think of this as something closed with two slits, one on a forward diagonal and one on a backward diagonal. If something passes through, the we can detect whether it passed through on a forward diagonal or a backward diagonal and we can assign 1 = forward diagonal, 0 = backward diagonal.

So, one simple way for Alice to communicate bits to Bob would be to tell him in advance to use the + reader, and then she can send each particle (qubit) as either 1 (vertical) or 0 (horizontal). Since Bob knows what reader to use, he'll correctly read each qubit.

What happens if someone uses the wrong reader?

Let's say Alice sends a 1 using the vertical orientation, but Bob accidentally uses the x reader.

In this situation, the vertical orientation is 45 degrees off going through the forward diagonal split and 45 degrees off going through the backward diagonal split. What happens, according to quantum theory, is that the particle will squeeze through in one of the two orientations with equal probability of either of them. Thus, if this situation were to occur, two things happen:

(1) Bob reads the correct result, 1, 50% of the time **AND** the particle's orientation **changes** to be on a forward diagonal now.

(2) Bob reads the incorrect result, 0, 50% of the time **AND** the particle's orientation **changes** to be on a backward diagonal now.

Either way, Bob's attempt at reading the particle has **changed** the orientation of the particle.

The key idea here from quantum theory is that the attempt to observe a particle actually affects the particle itself. Namely, there's no way to observe the particle without affecting it to know what it "would have done" if you didn't try to observe it. In real life, this sort of things happens with human behavior. For example, when I would try to observe my daughter at pre-school many years ago, she would always invariably see me hiding and she would alter her behavior, because she knew I was there.

Detecting a illicit listener

One of the problems with our traditional use of cryptography is that messages are sent in the open via the internet in signals that anyone can observe and it's fairly difficult to detect whether or not someone has attempted to read the signal. If we knew someone listened to something, we could just act accordingly and throw that data out.

With qubits, this problem becomes easier; we have a way of detecting if anyone is listening, because if they don't know what reader to use and they use the wrong reader, they are liable to change the qubit's orientation, and that could be proof that a third person who shouldn't be, is listening on a fiber-optic line.

Detection Idea Described Further

Now, let's assume that we have Alice is sending a qubit on a line with Eve listening first and then Bob. There are 8 possibilities of what could happen, each with probability 1/8 delineated below:

Alice Orientation	Eve Orientation	Bob Orientation	Result Received
+	+	+	Correct
+	+	X	Incorrect 50%
+	X	+	Incorrect 50%
+	X	X	Incorrect 50%
X	+	+	Incorrect 50%
X	+	X	Incorrect 50%
X	X	+	Incorrect 50%
X	X	X	Correct

The red rows represent where Alice and Bob's readers don't match. In these cases, Bob will receive a random bit that's only correct 50% of the time. If we know that Alice and Bob used different readers than the answer Bob receives is meaningless.

The green AND orange rows represent situations where Alice and Bob used the same reader. In these cases, Bob would definitely get the bit that Alice sent, **unless Eve is listening**.

Thus, the idea is as follows:

Alice sends Bob many bits, say n = 1300 or so, randomly choosing an orientation for the reader and a bit to send.

After sending the bits, Alice chooses k = 100 bit positions to sample. These bit positions should be distinct randomly distributed integers in the range [0..n-1]. So there should be a list like: 1, 6, 12, 13, 18, etc. For each of these bit positions, Alice and Bob, on an insecure line, state which reader they used, which bit Alice sent and which bit Bob received. It's expected that 50% of these will be the red cases (so about 50 bits) and will be thrown out. For the other 50 cases, Alice and Bob's answers (what Alice sent and what Bob received) should match. If Eve is listening however, we see that there's a 50% chance that she picked the wrong reader when Alice and Bob's readers match, and that when she picks the wrong reader, there's a 50% chance that Bob receives the wrong bit.

Thus, we can simplify this table into fewer important categories as follows:

Event	Probability
Alice, Bob readers don't match	50% (4/8 = 1/2)
Alice, Bob and Eve have matching readers	25% (2/8 = 1/4)
Alice, Bob match, Eve has the wrong reader but Bob reads the right bit.	12.5% (1/8)
Alice, bob match, Eve has the wrong reader and Bob gets the wrong bit.	12.5% (1/8)

If we limit our sample space to the bits where Alice and Bob used the right reader, then the probabilities for those interactions are:

Event (given that Alice and Bob use same reader	Probability
Eve's reader matches Bob's	50%
Eve's reader does NOT match Bob's but bit is read correctly.	25%
Eve's reader does NOT match Bob's and bit is read incorrectly.	25%

The probability, that with 100 sampled bits, that Eve is on the line but goes undetected (meaning that Alice and Bob's bits match all the times they used the same reader), is roughly round $(\frac{7}{8})^{100} \sim 1.6 \times 10^{-6}$. More accurately, if we know that Alice and Bob used the same reader for m bits, the probability Eve would go undetected would be $(\frac{3}{4})^{m}$. If m = 50, this is roughly 5.7×10^{-7}.

If we wanted a greater assurance that no one was on the line listening, then we could sample more bits.

Finishing Up: Exchanging a Secret Key

To finalize the idea of how Alice and Bob can exchange a secret key with each other securely, have Alice send Bob n bits in the fashion previously described. Sample k bits randomly. If all of these bits where Alice and Bob used the same reader are read correctly, then that's reasonable proof no one was listening on the line. Then, go back and just share the reader orientations for ALL of the rest of the bits (NOT the sampled ones). For the first X number of these bits, where X is the length of the secret key to be shared, where Alice and Bob used the same reader, Bob can be assured that he has correctly read the bits Alice had intended to send, and that no one else has read those X bits.