Quantum Information

Chapter 21: Secure communication

Author: Giulio Chiribella

Note: *LaTeX template courtesy of UC Berkeley EECS dept.*

Learning objectives: O1) Basic working knowledge, O2) Problem modelling, O4) Creativity and self-learning

The security of our email and credit cards is based on assumptions on the complexity of solving certain problems, like finding the prime factors of large numbers. But some of these assumptions will actually fail the day somebody builds a quantum computer. At that moment, many of our "secure" protocols will not be secure anymore.

Luckily, quantum theory offers a way out. Using quantum systems, we can generate secret keys over an insecure communication channel. By using such keys, we can then communicate secretly, with a level of security that guaranteed by the fundamental laws of nature.

21.1 Secure communication [O2]

Security is important. When you send an email or call a friend over the phone, you probably want the content of your conversation to remain private. When you book an airplane ticket on the web, you probably don't want to share your credit card number with other users. Likewise, security is important for many civil and military applications. Not surprisingly, humans have been interested in cryptography since the very early days of history: apparently, the first documented use of secret codes dates back the the Egyptians at around 1900 BC.

The basic scenario is the following: Alice wants to communicate a message to Bob. To this purpose, she can use a communication channel—for example, she can send a letter, make a phone call, send an email, and so on. However, the communication channel is not *secure*: every message that Alice sends to Bob can be intercepted by an eavesdropper, Eve. In order to communicate secretly, Alice and Bob need to use a cryptographic protocol, that is, a protocol that makes it hard (ideally, impossible) for Eve to read the message.

Nowadays, most of the cryptographic protocols we use are based on complexity theory. Roughly, the idea is that encoding and decoding the message is easy for Alice and Bob, but hard for Eve. For example, the most used protocol for our emails and credit cards is the RSA protocol. As long as we believe that Eve does not have a computer that factors numbers quickly, we can trust in the security of the RSA protocol. But who knows? Maybe Eve *has* such computer! Can we communicate securely without making assumptions on Eve's computational power? The answer is *yes* and a simple protocol that achieves this goal is the *one-time pad*.

21.2 The one-time pad [O1]

Suppose that Alice wants to communicate to Bob a message of N bits, say $\mathbf{x} = (x_1, x_1, \ldots, x_N)$. Before the communication starts, Alice and Bob choose at random a *secret key*, unknown to Eve. The key is a string of N bits, say $\mathbf{k} = (k_1, k_2, \ldots, k_N)$. Later, when Alice wants to communicate to Bob, she encodes the message by adding each bit of the message to the corresponding bit of the secret key: in this way, she obtains the *encrypted message*

$$\mathbf{x}' = (x_1 \oplus k_1,\ x_2 \oplus k_2, \ldots,\ x_N \oplus k_N)\,,$$

where $\oplus$ denotes the addition modulo 2. For example, if the message is

$$\mathbf{x} = (0, 0, 1, 0, 1, 1)$$

and the key is

$$\mathbf{k} = (1, 0, 1, 0, 0, 0)\,,$$

then the encrypted message is

$$\mathbf{x}' = (1, 0, 0, 0, 1, 1)\,.$$

In order to decode the message, Bob will only need to add to each bit of the encrypted message the corresponding bit of the key: in this way, he obtains the *decrypted message*

$$\mathbf{x}'' = (x'_1 \oplus k_1,\ x'_2 \oplus k_2, \ldots,\ x'_N \oplus k_N)\,.$$

Clearly, the decrypted message is equal to the original message, because we have $k_i \oplus k_i = 0$ for every bit of the key.

On the other hand, Eve has no clue of what is the message: since the key $\mathbf{k}$ has been chosen at random, also the encrypted message $\mathbf{x}'$ will be a random string of N bits. As a result, reading the message $\mathbf{x}'$ is useless to Eve: to guess Alice's message, Eve may just as well try to guess at random each bit of her message. In other words, the probability that Eve discovers Alice's message is

$$p^{(\text{Eve})}_{\text{succ},N} = \left(\frac{1}{2}\right)^N$$

and goes exponentially to zero when N is large. In short: when Alice communicates a long message to Bob using the one-time pad, the probability that Eve discovers the message is negligible.

21.3 Information-theoretic security [O1]

The kind of security offered by the one-time-pad is known as *information-theoretic security*:

Definition 1 *A cryptographic protocol has information-theoretic security if the probability that Eve discovers the correct message is (approximately) equal to the probability of guessing the correct message with a random guess.*

Information-theoretic security the highest level of security we can imagine. After all, you can encrypt a message, but cannot prevent me from guessing what the message is. The whole point of information-theoretic security is that reading your encrypted message does not give me any chance to improve my guess.

Now, there is a problem with information-theoretic security. The problem was spotted by Claude Shannon as early as in 1949—only one year after the groundbreaking paper where he invented information theory.

The problem is simple: in order to achieve information-theoretic security, the key must be *as long as the message*. This is clear in the case of the one-time pad, where Alice uses one bit of the key to encrypt one bit of the message. Shannon's result is completely general and applies to *every* cryptographic protocol, not only to the one-time-pad. Whatever protocol you use, in order to communicate N bits with information-theoretic security, you need a secret key of (approximately[1]) N bits.

This is a big problem. How can Alice and Bob establish such a long key? One way, of course, is that Alice writes down the key on a DVD, meets Bob in a secure place, and handles him the DVD. Or she can send the key to Bob through a trusted courier. However, one way or another, in the classical world Alice and Bob need to have a *secure communication channel*—that is, one way to send bits to one another in a form that is inaccessible to Eve.

The situation is dramatically different in the quantum world: by encoding information into quantum states, Alice and Bob can generate a secure key over an *insecure communication channel*. Then, the key can be used to encrypt the message with the one-time pad, thus achieving perfect information-theoretic security.

The first quantum protocol for generating a secret key was invented by Charles H. Bennett and Gilles Brassard, two giants of quantum information science. Their paper was published in 1984—after many difficulties with the referees—and their protocol is now called the BB84 protocol.

21.4 The BB84 protocol [O1,O2]

I will first describe the protocol to you and then give you an argument to explain why the protocol is secure.

The protocol works as follows:

The BB84 protocol.

1. Alice picks at random a sequence of $4N$ bits. The factor 4 is just a convenient choice, which guarantees that in the end we end up with a secret key of approximately N bits.
2. Alice encodes each bit of her sequence into the state of a qubit. For each bit of the sequence, she chooses the encoding at random:
   (a) with probability 1/2, she encodes the bit in the computational basis, encoding the bit value $b = 0$ into the state $|0\rangle$ and the bit value 1 into the state $|1\rangle$
   (b) with probability 1/2, she encodes the bit in the Fourier basis, encoding the bit value $b = 0$ into the state $|+\rangle$ and the bit value 1 into the state $|-\rangle$.
3. One by one, Alice sends her qubits to Bob. For the transmission of the qubits, she uses an *insecure communication channel*. This means that, before reaching Bob, the qubits can end up in Eve's hands.
4. When Bob receives Alice's qubits, he measures them. For each qubit, he chooses the measurement at random:

[1] In some protocols, you may not need *exactly* N bits of key—for example, $N - O(\sqrt{N})$ bits could still be OK. But the point is that the number of bits of the key should grow like N at the leading order.

   (a) with probability 1/2, he measures in the computational basis $\{|0\rangle, |1\rangle\}$. If he finds the outcome 0, he decodes the bit value $b' = 0$, if he finds the outcome 1, he decodes the bit value $b' = 1$.

   (b) with probability 1/2, he measures in the Fourier basis $\{|+\rangle, |-\rangle\}$. If he finds the outcome $+$, he decodes the bit value $b' = 0$, if he finds the outcome $-$, he decodes the bit value $b' = 1$.

5. Alice and Bob announce publicly which bases they used.

6. Alice and Bob discard the bits where they used different bases. In this way, they remain with approximately $2N$ bits. At this point, we know that, *if Eve did not alter the state of the qubits*, the outcome of Bob's measurement should be exactly equal to the corresponding bit in Alice's string. For example, if Alice encoded the bit value $b = 0$ into the state $|0\rangle$ and Bob measured in the computational basis, the outcome of his measurement must be $b' = 0$.

7. For each of the remaining $2N$ bits, Bob chooses at random what to do with it and announces his decision to Alice.

   (a) with probability 1/2, Bob chooses to use the bit as a bit of the secret key

   (b) with probability 1/2, Bob chooses to use the bit to test Eve's behaviour. To perform the test, Alice and Bob announce publicly the values of the bit and check whether they coincide ($b' = b$). If they find a difference in one of the selected bits, they conclude that Eve has altered the state. In this case, they abort the protocol and start afresh.

This is the BB84 protocol. If Eve does not change the states sent from Alice to Bob, in the end Alice and Bob will have a sequence of approximately N bits each, with the property that:

1. the sequence of bits is completely random
2. The value of the bits in Alice's sequence is exactly equal to the values of the bits in Bob's sequence.

Such a sequence can then be used to communicate securely using the one-time-pad. Indeed, quantum theory gives us a guarantee that the sequence is unknown to Eve. To understand why this is the case, we have to analyze the test performed by Alice and Bob.

21.5 The test [O2]

In the BB84 protocol, approximately N bits are used for the test. On these qubits, Bob checks whether the outcome of his measurement coincides with the value of the bit encoded by Alice. Now, the only way to pass the test with probability 1 is that the states received by Bob are *exactly* the states prepared by Alice. This means that Eve should not change the states *at all*. Indeed, if Eve alters the states, even just a little bit, there is a high probability that this test will detect her action. The argument is the same we saw for quantum money: suppose that each state sent by Eve to Bob passes the test with probability $1 - \epsilon$, for some $\epsilon > 0$. Then, the probability to pass N tests in a row will be

$$p_{\text{pass},N} = (1 - \epsilon)^N .$$

Clearly, the probability to pass will go to zero for large N. Hence, there is only one way Eve can pass the test: she must transmit to Bob *exactly* the same state she received from Alice.

Let us make a mathematical model of this condition. To describe the action of Eve, we can use a quantum channel $\mathcal{C}$, with one input and two outputs: the input is the qubit A prepared by Alice, the first output is

the qubit B received by Bob, and the second output is a quantum system E that Eve keeps for herself. Now, Alice's qubit can be in one of the four states

$$|\psi_0\rangle = |0\rangle\,, \qquad |\psi_1\rangle = |1\rangle\,, \qquad |\psi_2\rangle = |+\rangle\,, \qquad |\psi_3\rangle = |-\rangle\,. \tag{21.1}$$

Hence, the state of systems B and E will be in one of the four states

$$\rho_{BE,\,i} = \mathcal{C}\Big(|\psi_i\rangle\langle\psi_i|\Big)\,, \qquad i = 0, 1, 2, 3\,. \tag{21.2}$$

In order to pass the test, Eve should ensure that Bob's qubit is *exactly* in the state prepared by Alice. This means that the channel $\mathcal{C}$ must satisfy the *no-disturbance condition*

$$\mathcal{C}(|\psi_i\rangle\langle\psi_i|) = |\psi_i\rangle\langle\psi_i| \otimes \sigma_i \qquad\qquad \forall i = 0, 1, 2, 3\,, \tag{21.3}$$

where σ_i are some states of system E.

21.6 No Information Without Disturbance [O1,O4]

It is not hard to show that the no-disturbance condition implies that Eve cannot extract any information from Alice's qubit:

Theorem 21.1 (No Information Without Dsiturbance) *It is impossible to construct a machine that extracts information from two non-orthogonal states without disturbing them. Mathematically: if a quantum channel with input A and output AE satisfies the* no-disturbance condition

$$\mathcal{C}(|\varphi_i\rangle\langle\varphi_i|) = |\varphi_i\rangle\langle\varphi_i| \otimes \sigma_i \qquad\qquad \forall i \in \{0, 1\}\,, \tag{21.4}$$

for two non-orthogonal states $|\varphi_0\rangle$ and $|\varphi_1\rangle$, then one has the no-information condition

$$\sigma_0 = \sigma_1\,. \tag{21.5}$$

The no-disturbance condition tells us that the state of system A after the action of the channel is the same as the state of system A before. The no-information condition tells us that the state of system E does not provide any information about the state of system A. In the case of the BB84 protocol, this tells us that, if Eve does not want to get caught (i. e. if she wants to satisfy the no-disturbance condition), then she cannot hope to get any information at all about the state transmitted by Alice to Bob.

The proof of the No Information Without Disturbance Theorem is quite simple. In fact, it is almost identical to the proof of the No Cloning Theorem. I will not give it to you here: if you are curious, you can work it out by yourself or you can ask it directly to me.

21.7 Chapter summary

The highest level of security is the information-theoretic security. When a cryptographic protocol has information-theoretic security, the probability that an eavesdropper guesses the message correctly from its encrypted version is (approximately) equal to the probability of guessing the message correctly with a random guess.

In the classical world, Shannon proved that information-theoretic security can be achieved only if Alice and Bob have a secret key that is (approximately) as long as the message they want to communicate. There is

no way that such a key can be established without having already a secure communication channel. In the quantum world, instead, we can generate a secrete key even on an insecure communication channel. This spectacular feat is achieved by the BB84 protocol, which generates a random key using the communication of qubits. The security of the BB84 protocol is based on the No Information Without Disturbance Theorem, which guarantees that the eavesdropper cannot extract any information about the key without being discovered.