Appendix B

Quantum Cryptography

Cryptography is the art of exchanging secret messages over insecure channels. Known since ancient times, cryptography is now a major branch of the telecommunications industry, aimed at protecting privacy and information security of individuals, commercial entities and governments.

Cryptography is readily accomplished if the communication parties, which we call Alice and Bob, share a prearranged, secret data set known as *secret key* or *one-time pad*. With this resource available, a cryptographic protocol can proceed as follows.

Alice chooses a piece of the secret key data which has the same length (i.e. the number of bits) as the message she wishes to send to Bob. She then applies an XOR (exclusive OR, or bitwise sum modulo 2) operation to every bit of her message and the corresponding bit of her secret key:

original message	`01110011...`
	XOR
secret key	`10011010...`
encrypted message	`11101001...`

In this way she obtains an *encrypted message* which can be safely transmitted over an insecure channel, as it cannot be decrypted by anyone who is not in possession of the secret key. Bob, on the other hand, can easily decrypt the message. To this end, he applies XOR to every bit of the encrypted message he receives and the corresponding bit of the secret key, thus recovering the original message.

encrypted message	`11101001...`
	XOR
secret key	`10011010...`
recovered original message	`01110011...`

This protocol, known as *private-key cryptography*, is secure but expensive, as it requires the distribution of the one-time pad between the partners, which, as a rule, implies a trip of a courier carrying a briefcase loaded with random data. For less sensitive applications, a family of protocols known as *public-key cryptography* is used. Without going into details, public-key cryptography relies on the existence of mathematical functions with the following property. While the function itself is easy to compute, computation of its inverse, while possible in principle, is extremely complicated, and requires an unreasonably long time even with most powerful computers. Such functions are known as *one-way functions*.

Bob initiates the public key protocol by randomly choosing a number called the *private key*. He then applies a one-way function to the private key to calculate the *public key*, which he sends to Alice via an insecure channel. Alice then encrypts her message using the public key. The encryption protocol is again a one-way function, constructed so that the encryption of the message using the public key, as well as its decryption using the private key are computationally easy, whereas its decryption without the private key is difficult. In this way, Bob becomes the only party capable of decrypting Alice's message.

Public-key protocols are ingenious in that they allow secure messaging between parties that never previously had an opportunity to exchange information privately. Nowadays, a great majority of secure communications is performed using public keys. Perhaps the most common example is online shopping. The sensitive data entered by customers, including their credit card numbers, are transferred to the server via a public-key protocol. Other applications of public-key cryptography include secure emailing, transmission of medical records, and digital signatures.

While public-key protocols are convenient and inexpensive, they are not perfectly secure. The computational power available to us doubles every year or two, so a calculation that takes years at present may take only hours a few years down the road. Furthermore, there exists a possibility of developing so-called *quantum computers* (which are based on quantum physics, but are beyond the scope of this course), capable of cracking the security of public-key protocols almost instantly.

We are thus compelled to choose between private-key cryptography, which is secure but expensive, and public-key cryptography, which is cheap, but not perfectly secure. Fortunately, quantum mechanics offers us a solution that takes the best from both these options. On the one hand, its security is guaranteed by fundamental laws of nature. On the other hand, it does not require prearranged random information shared to be between the parties.

Quantum cryptography, or *quantum-key distribution*, relies on the property of measurements to alter the quantum state they are used on. The idea is that Alice sends secret data to Bob by means of single photons, encoding the data in their quantum states. Anyone who tries to eavesdrop on this transmission will either destroy or alter these photons, thus revealing themselves.

The most well-known quantum cryptography protocol is named "BB84" after their inventors C.H. Bennett and G. Brassard. In order to implement a protocol, Alice requires a photon generator (in practice, a weak laser is typically used) and a waveplate to rotate the polarization. Bob, at his end of the line, requires an apparatus for measuring the photon polarization, akin to those described in Sec. 1.8. To implement quantum communication, Aice and Bob perform the following operations.

a) Alice chooses a random number, either 0 or 1.

b) Alice randomly chooses either the canonical or the diagonal basis.

c) Alice generates a photon and encodes the number chosen in (a) in the photon's polarization:



$0 \to |H\rangle$
$1 \to |V\rangle$

OR

$0 \to |+45^\circ\rangle$
$1 \to |-45^\circ\rangle$



d) Alice sends the photon to Bob.

e) Bob chooses randomly in which basis he will measure, either canonical or diagonal.

f) Bob measures the arriving photon in the chosen basis:
→ If he chose the same basis as Alice, he will detect the same bit value as what Alice sent him.
→ If he chose the other basis, he will detect a random bit value.

This procedure is repeated many times. Of course, both Alice and Bob must keep track of the bases they used, data encoded or measured, and the exact time when the photons were sent or received. After many thousands of such records have been collected, Alice and Bob inform each other of (via a classical, insecure channel) their choice of bases for each photon, but *not* the bit values they sent or measured. Bob also informs Alice of those instances when he did not detect a photon, e.g. if it has been absorbed in the transmission line (this requires, of course, that the timing of Alice's transmissions be known to Bob, but this information need not be secret). Subsequently, Alice and Bob discard the data for those events in which different bases were used or the photon has been lost.

Alice and Bob now share a string of identical bits, which they can use as the one-time pad in a private-key protocol. To see why this string is guaranteed to be secret, let us suppose an eavesdropper (Eve) cuts the transmission line, and intercepts Alice's photons (Fig. B.1). Will she get a copy of Alice's message? No, because she does not know in which basis she should measure.

No matter how Eve performs her measurement, it will sometimes happen that Alice and Bob choose a basis that is the same one for the two of them but different from that chosen by Eve. But in this case, according to the Second Postulate, Eve will alter the photon's state and Bob may not receive the same bit value as what Alice sent him. Thus the only thing that Alice and Bob need to do in order to detect the eavesdropper is to exchange, via an insecure channel, a part of the secret bit string they recovered. If they find non-identical bits, this may indicate eavesdropping. But if there are no (or very few) errors, they can use the remainder of the secret string as the secret key.

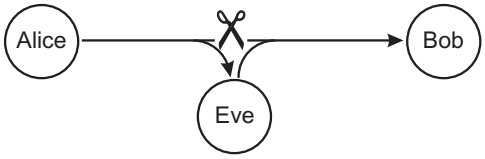


Figure B.1: Eavesdropping in quantum cryptography.

Exercise B.1 Suppose Eve intercepts Alice's photons and measures them in either the canonical or diagonal basis (she chooses at random). She then encodes the bit she measured in the same basis and re-sends it to Bob. What error rate will Alice and Bob register, i.e. what fraction of their data bits will come out different on average?

Note B.1 By using a more sophisticated strategy, Eve can reduce this error rate down to about 11%.

Quantum cryptography is no science fiction. The protocol described above is fully within reach of present day technology. In fact, there exist commercial quantum cryptography servers that can be connected to commercial fiber optical communication lines and implement the BB84 protocol. Several cities, such as Boston, Geneva, Vienna, Calgary, have constructed metropolitan quantum communication networks. Quantum cryptography has been used for communications during the 2007 Swiss federal elections and the 2010 FIFA world cup in South Africa. Further examples emerge as this text is being written.

Still, we do not see quantum key distribution universally replacing classical cryptographic protocols. Is there still a technical obstacle or is this simply inertia of thought?

Unfortunately, there do exist obstacles that are not imaginary. The primary problem with quantum cryptography is the loss in communication lines. The best fibers used in telecommunications today feature an absorption loss of about 5% per kilometer. That is, when transmitted through a 300-km communication line, only about one millionth of all photons will reach Bob; the rest will be lost.

In principle, even this enormous loss would be tolerable, as there exist lasers that generate billions of pulses per second. However, there is an additional problem. Photon detectors are so sensitive that they sometimes will generate a "dark count" event even if no photons are incident thereupon. Thus is it possible that a photon sent by Alice has been lost, but one of Bob's detector's still "clicks". If this dark event happens when Alice and Bob used the same basis, Bob will not discard this event. Furthermore, if the detector that had fired is not the one that would be expected to fire according to Alice's bit value, Alice's and Bob's distilled bit strings will not be identical. As discussed, this may be interpreted as eavesdropping.

As long as the transmission line is short enough, there are enough "good" photons reaching Bob so the fraction of errors due to dark counts is small. But this fraction increases with the length of the line. At some point, Alice and Bob can no longer be sure if the errors occur due to dark counts or due to eavesdropping, so secure transmission is no longer possible.

The secure key transfer rate is plotted in Fig. B.2 as a function of distance. Until the dark counts form a significant fraction of Bob's detection events, the rate reduces exponentially due to the losses in the transmission line. But as soon as the dark counts come into play, the secret key drops to zero almost instantly.

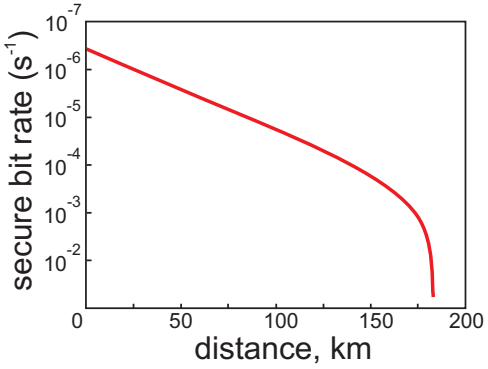


Figure B.2: Typical secure key transfer rate as a function of distance.

Exercise B.2 As discussed, a large fraction of the photons sent by Alice do not reach Bob. But Alice and Bob do not know whether these photons were in fact lost or "stolen" by an eavesdropper. Does this consideration affect the security of quantum key distribution?

Exercise B.3 Assuming that Alice has a perfect single photon source, estimate the maximum possible secure communication distance and the bit transfer rate at this distance given the following parameters:

- photon loss in the fiber communication line: 5%/km;
- emission rate of Alice's source: 10^6 photons per second;
- quantum efficiency of the photon detectors (i.e. the probability that the detector will "click" when hit by a single photon): 10%;
- probability for each detector to produce a dark count simultaneously with the photon pulse: 10^{-5} per pulse.