qitd162

Quantum Cryptography

Robert B. Griffiths
Version of 26 March 2003 with some later updates

References:

Scarani = Valerio Scarani et al. Rev. Mod. Phys. 81 (2009) 1301-1350. Lengthy review with much valuable material.

QCQI = *Quantum Computation and Quantum Information* by Nielsen and Chuang (Cambridge, 2000), Sec. 12.6 through 12.6.3. The material becomes more and more difficult as Sec. 12.6 advances

Stinson = D. R. Stinson, *Cryptography: Theory and Practice* (CRC Press, 1995). Contains considerable material on classical cryptography

H. K. Lo and N. Lutkenhaus, "Quantum cryptography: from theory to practice," (2007). arXiv:quant-ph/0702202. A short and very readable introduction.

H. K. Lo, Y. Zhao, "Quantum cryptography," (2009). arXiv:0803.2507v4. A longer review article

Contents

1 Introduction

◦ Stinson, Chs. 1 and 2, provides a good introduction to the subject of (classical) cryptography. Scarani is a recent review with lots of references. Along with theoretical issues, it discusses various practical schemes for carrying out quantum cryptography. QCQI gives a compact introduction to quantum cryptography followed by a rather detailed (and not very easy to read) discussion of the issue of security.

★ Cryptography is the science of sending a message between two parties in such a way that its contents cannot be understood by someone other than the intended recipient.

• Military applications go back to antiquity. Spies need to get messages back to headquarters. In the modern world, credit card numbers need to be transmitted securely over the Internet. Etc.

• A few technical terms, from Stinson. The original message or *plaintext* is *encrypted* using an *encryption rule* utilizing a *key* in order to produce an unintelligible (one hopes!) *cyphertext*. The intended recipient applies a *decryption rule*, utilizing the same key, to this cyphertext in order to recover the original plaintext message.

• Example: The encrypted Valentine's Day message JMPWFZPV is obtained by applying to the original plaintext the encryption rule that each letter is shifted forwards or backwards in the alphabet by a number of letters specified by the key k. For example, if $k = 3$, A is replaced by D, D by G, Z by C, and so forth, so that plaintext ANDREW becomes the unintelligible cyphertext DQGUHZ. Decryption is carried out by shifting k letters in the reverse direction. This particular encryption scheme is very insecure, as demonstrated in the following exercise.

□ Exercise. Decrypt JMPWFZPV by guessing the key k.

★ The quantum cryptographic schemes discussed below are based on the notion of a *private key* as exemplified by Vernam's one-time pad (Stinson, p. 50). Alice and Bob share identical strings of N random bits, 0 or 1, thought of as written down on pads of paper. (Old fashioned: Vernam described the idea back in 1917.) These strings constitute the key k. To encrypt a message m, thought of as plain text written out in a string of 0's and 1's, Alice adds each bit of m to the corresponding bit of k modulo 2. To recover the original message, Bob applies exactly the same procedure to the cyphertext.

◦ Here is an example

Plaintext	0	0	0	1	1	1	0
Key	1	0	1	1	1	0	0
Cyphertext	1	0	1	0	0	1	0

(1)

• Vernam's one-time pad is *ideal* in that it provides perfect secrecy as long as the only people who know the key are Alice and Bob. The reason is that the cyphertext is as random as the key, and an eavesdropper Eve who doesn't know the key has no way of extracting the original plaintext other than by guessing what it was, something she can do equally well without knowing the cyphertext!

• The practical difficulty that limits the utility of this scheme arises from the fact that a *one-time* pad can be used only once. If it is used repeatedly, the result will be correlations among successive parts of the message (or successive messages), and these correlations can be used to extract information about the key, compromising its security. Hence the key must be as long as the message. But how can Alice and Bob arrange to share long strings of random bits? Sending them by trusted courier is expensive, and not altogether free of risks. Transmitting them over the Internet is clearly not a good idea, unless one first encrypts them — but that is the problem we are trying to solve! These difficulties constitute the *key distribution problem*.

◦ If Alice and Bob know that some unauthorized person has information about the shared string, they will at least be aware that using it to encrypt sensitive messages is risky. The really dangerous situation, from their point of view, is one in which Eve has gained information about the key without their knowing it, so she is able to decrypt messages they believe to be secure.

★ Quantum cryptography provides a solution to the key distribution problem if Alice and Bob can communicate (at least in one direction) through a *quantum channel*. It will work even if the channel is somewhat noisy (more about that later), and even if Eve can gain some information about what passes through the channel. What makes the scheme secure is the fact that Eve cannot gain information without at the same time creating noise, and by measuring the noise Alice and Bob can obtain a quantitative bound on how much information Eve is extracting. By using this bound they can refine the information sent over the quantum channel to produce a shared key (Vernam pad) about which Eve knows essentially nothing.

2 The BB84 Scheme

★ In 1984 Bennett and Brassard proposed a scheme for quantum cryptography based on the idea that Alice can send qubits to Bob through a quantum channel, and that in addition Alice and Bob can communicate through a public "classical" channel (ordinary telephone, email). It is assumed that the eavesdropper Eve has access to both the quantum and public channel. She is allowed to listen in on and possibly modify what goes through the quantum channel, and listen to, but not modify, what Alice and Bob tell each other over the public channel.

◦ One can imagine Eve trying to tamper with the public channel, e.g., by impersonating Alice. This belongs to a separate set of "classical" security issues, including things like breaking into Bob's laboratory or bribing his assistant. We ignore them in order to focus on the essentially new possibility arising from the existence of a quantum channel.

• The BB84 protocol is described in QCQI Sec. 12.6.3. Here is a brief summary. Alice generates a random string a of bits $a_1, a_2, \ldots$, each 0 or 1, some fraction of which will form (or, more precisely, be used to produce) the final string which constitutes the Vernam pad. In addition, she generates an auxiliary random string b of equal length. When a_j and b_j have been generated, Alice transmits a one-qubit state $|\psi\rangle$ over the quantum channel according to the following protocol:

$$\begin{array}{ccc} a_j & b_j & |\psi_j\rangle \\ 0 & 0 & |0\rangle \\ 1 & 0 & |1\rangle \\ 0 & 1 & |+\rangle \\ 1 & 1 & |-\rangle. \end{array} \tag{2}$$

That is to say, if $b_j = 0$, the bit a_j is transmitted as a qubit $|a_j\rangle$ in the standard, or computational, or (in Bloch sphere language) Z basis, whereas if $b_j = 1$, the X basis is used:

$a_j = 0$ is sent as $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and $a_j = 1$ as $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. (These are the same as $|x^+\rangle$ and $|x^-\rangle$, up to a phase.)

• Bob generates an auxiliary string b' of random bits, completely independent of Alice's a and b, which he uses as follows. When the j'th qubit arrives from Alice, he measures it in the Z basis if $b'_j = 0$, and in the X basis if $b'_j = 1$. He records a measurement outcome corresponding to $|0\rangle$ or $|+\rangle$ as $a'_j = 0$, and one corresponding to $|1\rangle$ or $|-\rangle$ as $a'_j = 1$.

• If the quantum channel is perfect, this protocol leads to $a'_j = a_j$ in all cases in which $b'_j = b_j$, while a'_j and a_j are statistically independent if $b'_j \neq b_j$. Suppose, for example, that $a_j = 1 = b_j$, so Alice transmits $|-\rangle$. If $b'_j = 1$, then Bob measures in the X basis, and with probability 1 he will find $|-\rangle$, so he records $a'_j = 1$. If, on the other hand, $b'_j = 0$, Bob measures in the Z basis, and finds $|0\rangle$ or $|1\rangle$ with equal probability.

• When the quantum transmission is complete, Bob and Alice use the public channel to compare the bit strings b and b'. For those j (roughly half) for which $b'_j \neq b_j$, they simply discard a_j and a'_j. The bit strings $\bar{a}$ and $\bar{a}'$ that remain correspond to the cases where $b'_j = b_j$, i.e., Alice sends and Bob measures in the same basis. If the quantum channel is perfect, $\bar{a}$ and $\bar{a}'$ are identical random strings of bits, which form a Vernam pad.

◦ By listening in on the public channel, Eve learns only worthless information about the positions of the "good" bits in the original a string; the actual values are not revealed.

3 Eavesdropping

★ Eve also has access to the quantum channel. What prevents her from using this to determine the values of the bits in the a and b strings? It is here that quantum mechanics plays an essential role.

• To begin with, each $|\psi_j\rangle$ sent by Alice contains at most one bit of information (see notes on "Dense Coding, Teleportation, No Cloning"), so even if Eve captures this qubit and subjects it to arbitrary measurements, she cannot determine the two bits of information required to specify both a_j and b_j.

• What can Eve learn about a_j, which is what interests her, if she does not know b_j? According to (2), $a_j = 1$ could be represented as $|1\rangle$ (if $b_j = 0$), and $a_j = 0$ as $|+\rangle$ (if $b_j = 1$). But $|1\rangle$ and $|+\rangle$ are nonorthogonal states, and no measurement will distinguish them with certainty, so Eve cannot reliably tell the difference between a_j values if she does not know b_j.

★ Eve can, however, obtain partial information, or perfect information part of the time. One of the simplest attacks involves a nondestructive measurement carried out using the circuit in Fig. 1. (A more practical strategy, given that controlled-not gates are hard to construct using present technology, is for Eve to measure the qubit from Alice in the Z basis and send Bob another qubit in the state corresponding to the measured value. The quantum circuit provides a simple schematic representation of this "measure and resend" approach to eavesdropping.)

• Every time Alice sends a $|0\rangle$ or a $|1\rangle$ to Bob, Eve's apparatus will determine its value

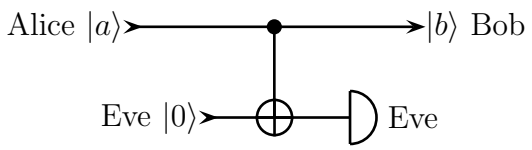

Figure 1: Simple eavesdropping strategy.

and leave it unchanged. On the other hand, when Alice uses the X basis and sends a $|+\rangle$ or $|-\rangle$, Eve will gain no information about it, as her detector outcome will be completely random. Even worse, her apparatus will disturb the X basis signal sent on to Bob in such a way that when he measures in the X basis, his outcome will be statistically independent of what Alice sent.

□ Exercise. Work out the probability that Bob will measure $|+\rangle$ or $|-\rangle$ when Alice sends a $|+\rangle$ or a $|-\rangle$, using the circuit in Fig. 1. Does it make a difference whether or not Eve measures the ancillary qubit? What if Eve uses an initial state other than $|0\rangle$ for the ancillary qubit?

• After using the quantum channel for some time, Alice and Bob will be able to detect the presence of Eve's probe by selecting at random some values of j for which $b'_j = 1 = b_j$, and comparing the values of a'_j and a_j, using the public channel. Since the values of these bits become known to Eve, they must be "sacrificed", and cannot be employed as part of the final secret key. But only a relatively small fraction of bits must be sacrificed in this way in order to estimate the channel noise in the X-basis, so the device in Fig. 1 is easily detected if present.

• Security comes not from the eavesdropper's inability to read information going through the quantum channel, but rather from the fact that attempting to do so generates noise which can be detected by the legitimate users of the channel.

4 Information Reconciliation and Privacy Amplification

★ If there is noise in the quantum channel (whether or not due to an eavesdropper), the strings $\bar{a}$ and $\bar{a}'$ shared by Alice and Bob after the steps of the BB84 protocol described above will not be completely identical; there will be some differences. Getting rid of these requires a process of *information reconciliation* carried out using the public channel in a manner which limits the information leak to Eve.

• A relatively crude way of doing this if the number of errors is not too large is to break up $\bar{a}$ and $\bar{a}'$ into corresponding blocks which are short enough so that the possibility of two discrepancies occurring in the same block is quite small. Alice and Bob compute the parity (even or odd number of 1's) of each block and compare them over the public channel. If corresponding blocks have the same parity, they are retained; if the parities differ, the blocks are discarded. Should the probability of differences in the remaining strings be considered

too high, the process can be repeated. The end result will be a pair of identical strings of bits which we denote by $\hat{a} = \hat{a}'$. Of course, Eve has also gained some additional information: she knows the parities of the blocks which make up $\hat{a}$.

★ Suppose that by measuring the amount of noise in the quantum channel and (conservatively) ascribing all of it to eavesdropping, and by calculating the amount of information leakage during the process of reconciliation, Alice and Bob can place an upper bound of m bits on the amount of (Shannon) information that Eve possesses about the final M bit shared string $\hat{a}$. If the quantum channel is not too noisy (see Sec. 5 below), one can expect that $m \approx \epsilon M$ when M is large, with ϵ a constant significantly less than 1, and in this case Alice and Bob can carry out a process of *privacy amplification* in order to map $\hat{a}$ onto a shorter K-bit random string about which Eve knows essentially nothing.

• Privacy amplification is carried out as follows. Alice chooses at random a particular function f that maps M-bit strings into K-bit strings, from a suitable collection of such functions, and communicates her choice to Bob over the public channel. Both Alice and Bob apply f to $\hat{a} = \hat{a}'$ in order to obtain $a^* = a'^*$, the final Vernam pad. Eve also knows f, but it can be shown that this does her no good as long as $K < M - m$: the information she possesses about the final string a^* is less than one bit!

• Neither information reconciliation nor privacy amplification requires the use of quantum concepts; they are both "classical" processes, and the security of the resulting key can be demonstrated using ordinary ("classical") information theory. For more details: QCQI Sec. 12.6.2, which is rather compact; or Bennett et al., SIAM J. Comput. **47**, 210 (1988).

5 Bounding Eve's Information

★ From the foregoing discussion it follows that demonstrating the security of *quantum* cryptography depends on the ability to bound the amount of information Eve obtains about the random string a (or $\bar{a}$), during the process of transmitting signals through the quantum channel, as a function of channel noise. The latter can be measured empirically by comparing some of the shared bits over the public channel. Finding a bound requires the use of quantum mechanics.

• The key point, as noted in Sec. 3, is that an eavesdropping strategy which provides information about what is being transmitted in the Z basis produces noise in the X basis, and vice versa. Given a specific scheme, such as that in Fig. 1, one can calculate how much noise is produced and the average amount of information obtained by Eve.

• Obtaining a general bound applicable to *any* eavesdropping strategy is more difficult. See Scarani

★ Fuchs et al., Phys. Rev. A **56**, 1163 (1997), obtained a bound assuming that Eve is limited to the following sort of attack. For each transmission from Alice to Bob, she can attach any type of probe she wishes, prepared in whatever state she wants, to the quantum channel, and then wait until she learns the strings b and b' (by listening to the public channel) before carrying out whatever measurement she wishes on the probe, which is

retained in her possession. Waiting could be advantageous, since if Eve knows that for $j = 12$ Alice transmitted and Bob received in the Z basis, she might analyze probe 12 differently than if they had used the X basis.

• This bound states that if the noise rate (errors per bit) for X basis transmission is ϵ_X, referring only to those cases in which $b'_j = 1 = b_j$, then the information I_Z per bit available to Eve *about those bits in $\bar{a}$ which were transmitted and received in the Z basis*, is bounded by

$$I_Z \leq \tfrac{1}{2}\,\phi[2\sqrt{\epsilon_X(1-\epsilon_X)}], \tag{3}$$

where

$$\phi(w) = (1+w)\log(1+w) + (1-w)\log(1-w). \tag{4}$$

◦ When ϵ_X is small, the right side of (3) is approximately $(2/\ln 2)\epsilon_X$, so the information is bounded by a term linear in the noise, and goes to zero as the noise goes to zero.

◦ In a similar way, Eve's information I_X (per bit) about the the bits in $\bar{a}$ transmitted and received in the X basis is bounded by (3) with ϵ_X replaced by ϵ_Z, the error rate for Z basis transmissions through the channel.

• It may at first seem surprising that the Z information is bounded by the X error rate, and vice versa. However, as noted in connection with the circuit in Fig. 1, it is quite possible for Eve to gain perfect information ($I_Z = 1$) about Z transmissions in a manner which creates no noise at all *for this kind of transmission*. The essential idea behind quantum cryptography is that a device which provides information about Z transmissions *necessarily* introduces noise in an incompatible basis of states which are nonorthogonal to $|0\rangle$ and $|1\rangle$. This feature is a purely quantum effect, with no analog in classical physics.

• In the symmetrical case in which X and Y transmissions occur equally often, and the noise rates are equal, $\epsilon_X = \epsilon_Y = \epsilon$, Eve's information I, per bit, about the string $\bar{a}$ is bounded by (3) with the subscripts omitted.

★ The proof of (3) depends on the assumption that Eve measures the probe associated with each transmission separately. One can imagine that at some future date technology will improve to the point where Eve could store the probes until *after* listening in on the entire discussion carried out by Alice and Bob over the public channel, including information reconciliation and the choice of the privacy amplification function f (Sec. 4), and only then apply to the entire collection of probes the most general sort of measurement imaginable (i.e., allowed by the principles of quantum theory). In this way she might gain some additional information. Would it be enough to render the final key a^*, constructed under the assumption that (3) is valid, insecure?

• The issue of the security of quantum codes has been extensively discussed in a series of lengthy papers that are not at all easy to read. See Scarani, and Lo and Zhao for some discussion of these matters.

6 The EPR Scheme

★ What QCQI, p. 591, call the "EPR protocol" is closely related to BB84, but provides an alternative point of view which is sometimes helpful, especially in proofs of security against an eavesdropper. The idea is that Alice and Bob initially share a large number of qubit pairs in one of the Bell states, for example $|B_0\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

◦ The name "EPR" refers to the famous Einstein-Podolsky-Rosen paper of 1935 in which the authors claimed that the existence of entangled states demonstrates that quantum mechanics must be an incomplete theory. Because Bohm in 1952 illustrated the essential idea behind the EPR argument using two spin-half particles in a spin singlet state ($|B_3\rangle$ in our notation), Bell states are often referred to as "EPR pairs".

★ Suppose Alice and Bob take one of their $|B_0\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ pairs and measure it in the standard (Z) basis. The outcome will be random: with probability 1/2 they will both find 0, with probability 1/2 they will both find 1. They have generated the first bit for a Vernam pad. Repeat the process for a second $|B_0\rangle$ pair and they share a second random bit, and so forth. Nothing could be simpler. And since the measurements take place entirely inside Alice's and Bob's laboratories, Eve (as long as she cannot get inside) is left totally informationless!

• The weak point in this ideal scenario lies in creating the $|B_0\rangle$ pairs in the first place, which is the quantum counterpart of the practical difficulty in producing a classical Vernam pad shared by only two parties. Creating entangled pairs in Alice's laboratory and then conveying half of each pair to Bob is subject to the usual security risks if it is done by courier. Sending half of each pair through a quantum channel could subject it to measurement or other meddling by someone with access to the channel.

★ However, things are actually somewhat better than in the classical case. If Alice and Bob share a large number of qubit pairs which are nominally in the state $|B_0\rangle$, they can check them in the following way. Choose a few pairs at random, and for some of them measure both qubits of the pair in the Z basis, for others measure both in the X basis. If all pairs are initially in the state $|B_0\rangle$, these measurement outcomes will be completely correlated: Both Alice and Bob will find $|0\rangle$, or both will find $|1\rangle$, if they measure in the Z basis; similarly, measurements in the X basis will either both yield $|+\rangle$ or both $|-\rangle$. Furthermore, outcomes correlated in this way are a unique signature of the $|B_0\rangle$ state. Anything else will at least occasionally yield different values in either the Z or the X basis; see the following exercises.

□ Exercise. Rewrite each of the Bell states (see "Correlations and Entanglement") in the X ($|+\rangle$, $|-\rangle$) basis, and then determine the probability for each $|B_j\rangle$ that measurements carried out by Alice and Bob in the X or in the Z basis will yield the same or opposite results.

□ Exercise. Show that a density operator for two qubits which assigns probability 1 to equal values (i.e., $|00\rangle$ or $|11\rangle$) in the Z basis, and also probability 1 to equal values in the X basis, must be the projector $[B_0]$ on $|B_0\rangle$.

• A comparison of the outcomes of X and Z measurements requires communication between Alice and Bob, and if this is done over an insecure public channel these particular

results must be sacrificed, and cannot be part of a secure key. However, if the measured pairs have been selected at random, a large number of results consistent with $|B_0\rangle$ provides strong evidence that the remaining pairs are, with high probability, in the same state, and therefore the outcomes of correlated measurements on the remaining pairs, the results of which are not publicly announced, can be used as a secure shared key.

★ Suppose that comparison of the results of measurements on randomly chosen pairs reveals that not all of them are in the $|B_0\rangle$ state. What can be done?

• If the fraction of impurities in the collection is not too large, there are two strategies Alice and Bob can employ to obtain a secure shared key.

1. They can go ahead and carry out correlated measurements on the pairs in their possession, and then use information reconciliation and privacy amplification, just as in the case of the BB84 protocol, to obtain a secure key.

2. By sacrificing a certain number of pairs in a process employing local operations and classical communication over the public channel, Alice and Bob can "distill" out a smaller collection of pairs all of which are, with very high probability, in the state $|B_0\rangle$. This purified collection can then be used to construct a shared key by carrying out correlated measurements in the manner indicated earlier.

7 The B92 Scheme

★ An interesting alternative to BB84 known as B92 was published by Bennett in 1992. It is described in QCQI Sec. 12.6.3, starting on p. 589.

• Alice prepares a single string a of random bits. If $a_j = 0$ she sends a qubit in the state $|0\rangle$ to Bob over a quantum channel, whereas if $a_j = 1$ she sends $|+\rangle$.

• Bob generates an independent random string a'. If $a'_j = 0$ he measures the j'th qubit arriving from Alice in the Z basis, and records the outcome $|0\rangle$ as $b'_j = 0$, and $|1\rangle$ as $b'_j = 1$. If $a'_j = 1$ he measures in the X basis and records $|+\rangle$ and $|-\rangle$ as $b'_j = 0$ and 1, respectively.

• After the quantum transmission is over, Bob tells Alice over the public channel the value of b'_j for every j. They then discard a_j and a'_j if $b'_j = 0$, The remaining random bits, those corresponding to $b'_j = 1$, have the property that $a'_j = 1 - a_j$ if the quantum channel is perfect, and thus constitute a Vernam pad.

□ Exercise. To see why the method works, make up a table which shows all possible outcomes (b'_j values) of Bob's measurements for each of the four possible values of (a_j, a'_j).

• In the case of a noisy quantum channel, information reconciliation and privacy amplification are necessary, and are carried out by using the public channel in precisely the same way as for BB84.

★ The protocol will also work with other choices besides $|0\rangle$ and $|+\rangle$ for the two states transmitted by Alice, as long as they are *nonorthogonal*. Using two states that are close to but not quite orthogonal makes it easy for Eve to steal information without being detected. Using nonorthogonal states that are almost identical means that a very large number of

transmissions are required to construct a shared key (see the following exercise). The choice of $|0\rangle$ and $|+\rangle$ is a reasonable, but by no means unique, compromise.

□ Exercise. Work out the B92 protocol for two nonorthogonal states of a qubit corresponding to points on the Bloch sphere separated by an angle ω. (In the protocol described above, $\omega = \pi/2$.) Arrange things so that $b'_j = 1$ implies $a'_j = 1 - a_j$. Show that when ω is small it will take a long time to construct a shared key.

★ Despite its evident simplicity, B92 is in practice not as good a scheme as BB84. The reason is that the amount of noise Eve has to generate to obtain a given amount of information can be considerably less than for BB84, making eavesdropping harder to detect.