Quantum Communication

Emad Rezaei Fard Boosari[1]

[1]University of Warsaw

January 9, 2024

1 Quantum Communication[1]

1.1 No-cloning theorem[2]

We copy classical data almost every day. In fact, this is amongst the most common functions with digital media. (Of course we should not copy media that are copyright protected.) This cannot be done in quantum information theory! We cannot clone an unknown quantum state with unitary operations.

THEOREM:
An **unknown quantum system** cannot be cloned by unitary transformations.

proof: Suppose there would exist a unitary transformation U that makes a clone of a quantum system. Namely, suppose U acts, for any state $|\phi\rangle$, as

$$U : |\phi\rangle |0\rangle \longrightarrow |\phi\rangle |\phi\rangle \tag{1.1}$$

Let $|\phi\rangle$ and $|\varphi\rangle$ be two states that are linearly independent. Then we should have $U |\phi\rangle |0\rangle = |\phi\rangle |\phi\rangle$ and $U : |\varphi\rangle |0\rangle = |\varphi\rangle |\varphi\rangle$ by definition. Then the action of U on $|\psi\rangle = \frac{(|\phi\rangle + |\varphi\rangle)}{\sqrt{2}}$ yields

$$\begin{aligned} U |\psi\rangle |0\rangle &= \frac{1}{\sqrt{2}}(U |\phi\rangle + U |\varphi\rangle) |0\rangle \\ &= \frac{1}{\sqrt{2}}(|\phi\rangle |\phi\rangle + |\varphi\rangle |\varphi\rangle) \end{aligned} \tag{1.2}$$

If U were a cloning transformation, we must also have

$$\begin{aligned} U |\psi\rangle |0\rangle &= |\psi\rangle |\psi\rangle \\ &= \frac{1}{2}(|\phi\rangle + |\varphi\rangle)(|\phi\rangle + |\varphi\rangle) \\ &= \frac{1}{2}\Big(|\phi\rangle |\phi\rangle + |\varphi\rangle |\phi\rangle + |\varphi\rangle |\phi\rangle + |\varphi\rangle |\varphi\rangle \Big) \end{aligned} \tag{1.3}$$

which contradicts the previous result. Therefore, there does not exist a unitary cloning transformation. Clearly, there is no way to clone a state by measurements. A measurement is probabilistic and non-unitary, and it gets rid of the component of the state which is in the orthogonal complement of the observed subspace.

It should be kept in mind that the no-cloning theorem states that we cannot copy an arbitrary state $|\Psi\rangle = a|0\rangle + b|1\rangle$. The loophole is that the theorem does not apply if the states to be cloned are limited to $|0\rangle$ and $|1\rangle$. For these cases, the copying operator U should work as

$$U : |0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle \qquad U : |1\rangle|0\rangle \longrightarrow |1\rangle|1\rangle \tag{1.4}$$

which CNOT gate can do this for us.

2 Quantum Key Distribution [1, 2, 3, 4]

Quantum key distribution (QKD) is a secure way of distributing an encryption and decryption key by making use of qubits. The sender and the receiver can detect a possible third party eavesdropping their communication by comparing the sequence sent with that of the received one.

One-time pad is an absolutely secure cryptosystem if and only if the key for encoding and decoding is shared only between the sender and the receiver and used once for all. Suppose we want to send a message 1100101001 in a binary form using a key 1001010011, for example. The message is encrypted by adding the message to the key bitwise modulo 2, which we denote by $i \oplus j$. We have explicitly $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0$. For the above case, we have the encrypted message 0101111010. For decryption, the receiver is required only to add the same key bitwise again since $(i \oplus j) \oplus j = i$. Decryption of an encrypted message is impossible without the key since there are 2^n possible keys for an n-bit string and many of them yield sensible messages. This cryptosystem is not secure any more if the same key is used many times. A key must be sent from the sender to the receiver, or in the opposite direction, each time this cryptosystem is used. If the key is sent through a classical communication channel, there always exists a possibility of eavesdropping. However, this problem is completely solved if a quantum channel is employed as we show now.

Suppose Alice wants to send Bob a one-time pad key to encode and decode her secret message. They can communicate with each other using a bidirectional classical channel. There also exists a quantum channel that is unidirectional from Alice to Bob. See Fig. 2.1. There is a possibility that their communication is being eavesdropped by a third party, which we call Eve. Alice sends Bob many qubits, one by one, and Bob measures the states of each of the qubits he receives. To make our discussion concrete, we assume qubits are made of polarized photons.

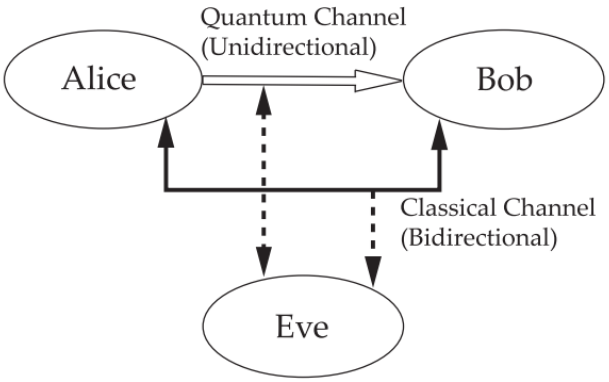

Figure 2.1: Quantum key distribution protocol BB84.

2.1 BB84 Protocol

The *protocol BB84*, discovered by *Bennett and Brassard in 1984*. In this protocol Alice starts by choosing two random classical bit strings $a = (a_1, a_2, \cdots, a_{4N})$ and $b = (b_1, b_2, \cdots, b_{4N})$, both of length $4n$. The first string determines the bit value she wants to send (0 or 1), and the second string determines the basis she uses to encode the bit: 0 represents computational basis (also called the z-basis) and 1 represents the Hadamard basis (or x-basis). The letters of the z- and x-alphabets are associated with the eigenstates of the Pauli matrices σ_z and σ_x, respectively. According to the strings a and b, Alice prepares a block of $4N$ qubits

$$|\psi\rangle = \bigotimes_{i=1}^{4N} |\psi_{a_i b_i}\rangle \tag{2.1}$$

$$= |\psi_{a_1 b_1}\rangle \otimes |\psi_{a_2 b_2}\rangle \otimes \cdots \otimes |\psi_{a_{4N} b_{4N}}\rangle \tag{2.2}$$

where a_i is the i-th bit of string a and b_i is the i-th bit of string b: Hence, each of the individual qubits is in one of the four states

$$|\psi_{00}\rangle = |0\rangle \tag{2.3}$$

$$|\psi_{10}\rangle = |1\rangle \tag{2.4}$$

$$|\psi_{01}\rangle = |+\rangle \tag{2.5}$$

$$|\psi_{11}\rangle = |-\rangle \tag{2.6}$$

Note that the four states are not all mutually orthogonal: For instance,

$$\langle\psi_{00}|\psi_{01}\rangle = \frac{1}{\sqrt{2}} \tag{2.7}$$

This property ensures that there is no measurement that can perfectly distinguish between all of the states with certainty.

The BB84 protocol cab be describe in two phases, *Quantum transmission* phase and post processing phase. In the next two sections BB84 protocol has been explained in more details.

2.1.1 Quantum transmission:

1. Alice generates a random sequence of 0's and 1's. As an Example from Table 1 it can be

$$\text{Alice's data bits} = 1000110101 \tag{2.8}$$

2. Alice encodes each data bit in a qubit, $|0\rangle$ or $|+\rangle$ if the corresponding bit is 0, $|1\rangle$ or $|-\rangle$ if the corresponding bit is 1. For each bit, Alice chooses randomly between the x- and the z-alphabet, by means of a fair coin (e.g., if the coin lands heads (H) Alice chooses the x-alphabet, while the z-alphabet is chosen when the coin lands tails (T)). For our example we have 10 bits and we will toss the coin 10 times and the result can be like $HTHTHHHTTH$ which is correspond to

$$\text{Alice's alphabet} \quad = \quad xzxxzxzxzz \tag{2.9}$$

3. The resulting string of qubits is sent by Alice and received by Bob. In our example this output states will be like

$$\text{Transmitted qubits} \quad = \quad |-\rangle\,|0\rangle\,|+\rangle\,|0\rangle\,|-\rangle\,|-\rangle\,|+\rangle\,|1\rangle\,|0\rangle\,|-\rangle \tag{2.10}$$

Quantum Transmition										
Alice's data bits	1	0	0	0	1	1	0	1	0	1
Alice's alphabet	x	z	x	z	x	x	x	z	z	x
Transmitted qubits	$\|-\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$
Bob's alphabet	x	z	x	x	z	x	z	x	z	z
Measurement outcomes	1	0	0	0	0	1	0	0	0	1
Bob's data bits	1	0	0	0	0	1	0	0	0	1
Raw key	1	0	0	-	-	1	-	-	0	-

Table 1: An example of the BB84 protocol.

4. For each qubit, Bob decides at random what axis (alphabet) to use for the measurement, x or z. Similar to the Alice, he randomly choose the alphabet like

$$\text{Bob's alphabet} \quad = \quad xzxxzxzxzz \tag{2.11}$$

In the first case, he measures the spin polarization along the x axis, in the latter along the z axis. Note that half of the time Bob chooses the same axis as Alice. In this case, assuming that there are no eavesdroppers or noise effects, Alice and Bob share the same bit (here we summarize under the word noise effects such as imperfect state preparation or detection, interactions of the transmitted qubit with the environment, etc.). In contrast, if Bob chooses an axis different from Alice, the bit resulting from his measurement agrees with the bit sent by Alice only half of the time. For instance, if Bob receives the qubit $|-\rangle$ and measures σ_z, the outcomes 0 and 1 have equal probability. After this step, Alice and Bob both hold a classical bit string, denoted $X = (X_1, \cdots, X_N)$ for Alice and $Y = (Y_1, \cdots, Y_N)$ for Bob. This is called the *raw key* pair. In our example X and Y are

$$X = 1000110101 \tag{2.12}$$

$$Y = 1000010001 \tag{2.13}$$

2.1.2 Classical Post-processing:

From now on Alice and Bob exchange only classical information over a public channel

5. Bob publicly announces the alphabets he has chosen to measure the states Alice has sent. Of course, he does not communicate the results of these measurements. Alice compares Bob's alphabets to the ones she used and says which of them has chosen correctly, i.e., in which cases their choices coincide. Alice and Bob discard all bits for which the encoding and measurement bases are not the same. This is called the *sifting step*.

Classical Post-Processing										
Bob report his alphabets	x	z	x	x	z	x	z	x	z	z
Alice's confirm them	OK	OK	OK	-	-	OK	-	-	OK	-
Presumabley shared information	1	0	0			1			0	
Bob's reveals some key bits	1					1				
Alice confirm them	OK					OK				
Outcome										
Remaining shared secret bits		0				1			0	

Table 2: Post processing.

6. The next step is the *parameter estimation* step, where Alice and Bob want to compute a guess for the error rate in the quantum channel, i.e., the fraction of positions i where X_i and Y_i disagree. To achieve this, Bob reveals some bits of his key at random. **In case of no**

eavesdropping, these bits should be the same as Alice's bits and she confirms them. If the error rate is too high, this indicates that there has been some eavesdropping and Alice and Bob abort the protocol. The bits that have been revealed during this step are discarded afterwards as their information is now public to an eavesdropper.

7. To compute the final key, Alice and Bob perform certain steps to correct errors in their keys and increase the secrecy of their key. These steps are called error correction (sometimes also referred to as information reconciliation), where they erase all errors in their bit strings, i.e., after this step Alice and Bob hold identical strings. The second step is **privacy amplification**, which is a procedure that minimizes Eve's knowledge of the key. These steps have not been discussed in the original proposal of the protocol and first appeared a few years later.

Remarks:
Here maybe a simple Question was why did we sent $4N$ qubit from Alice to Bob? The answer is related to statistics behind this protocol. Just Consider Alice sent $4N$ qubits for Bob and since the Bob's measurment in the random basis can be agreed with Alice bits only with probability $\frac{1}{2}$ in the cases. Thus, Bob after stifing step has only $2N$ qubits on average. To make sure that no one eavesdrps their quantum channel, they choose N cases randomly out of $2N$ cases with the same coding systems employed and exchange N bits (0 or 1) associated with these N cases over the classical channel. If there are no eavesdroppers operating, they should have the same bits for all the N cases. After verifying that they are free from eavesdroppers, they discard these N cases (since the classical channel may be eavesdropped) and use the remaining N bits to generate a one-time pad key.

2.1.3 Security of the BB84 Protocol

The security of the BB84 protocol relies on the fact that in quantum mechanics it is not possible to gain information about a quantum system without disturbing it. Hence, every interaction the eavesdropper has with a quantum state that is sent alters the state in some way. How can Alice and Bob recognize that an adversary is listening to their communication while performing the steps of the BB84 protocol? Let us have a look at what happens if Eve tries to gain information about the quantum state that Alice sends to Bob. Consider the first bit in the example of Table 1, but now

Eve interacts with the quantum state:

$$\text{Alice's bit: } \longrightarrow \quad 1 \tag{2.14}$$

$$\text{Alice's alphabet: } \longrightarrow \quad z \tag{2.15}$$

$$\text{Transmitted qubit: } \longrightarrow \quad |0\rangle \tag{2.16}$$

$$\text{Eve's measurement basis: } \longrightarrow \quad x \tag{2.17}$$

$$\text{State after the measurement: } \longrightarrow \quad |1\rangle_x \tag{2.18}$$

$$\text{Bob's measurement basis: } \longrightarrow \quad z \tag{2.19}$$

$$\text{Bob's bit: } \longrightarrow \quad 0 \tag{2.20}$$

In this case, Bob and Alice have used the same bases, hence after the sifting step they believe that they are holding the same bit value. Eve's interaction, however, has changed the quantum state in a way that Bob's measurement has yielded a different bit than the one Alice encoded. In the parameter estimation step, where Bob and Alice compare parts of the actual bit strings they hold, they will find that these bits do not match and reveal that an eavesdropper has tried to get some information.

Remarks:

We stress that the validity of the BB84 protocol is based on the Heisenberg principle. The two alphabets are associated with two non-commuting observables, σ_x and σ_z. Eve cannot measure both the polarization along x and along z for the same qubit. For instance, if she measures σ_z for the qubit $|0\rangle_x$, she obtains the outcomes 0 or 1 with equal probability. Thus, she has irreversibly randomized the polarization originally sent by Alice. We also stress the importance of the no-cloning theorem: it guarantees that Eve cannot distinguish with certainty between non-orthogonal quantum states. If a quantum cloning machine existed, Eve could make a large number of copies of each qubit sent by Alice and distinguish with arbitrary accuracy between eigenstates of σ_x and σ_z. For instance, assume that Eve measures σ_z for the qubit and all its copies. If she received $|1\rangle$, she always obtains outcome 1. On the other, if she received $|1\rangle_x$, she obtains outcomes 0 and 1 with equal probabilities. Finally, Eve could resend a copy of the intercepted qubit to Bob. Therefore, if it were possible to violate the no-cloning theorem, Eve could intercept the qubits sent by Alice and resend them to Bob, leaving no trace of her intrusion.

Finally, we note that one of the main drawbacks of quantum cryptography is that no mechanism is known for authentication. Thus, a classical secret key is required for this purpose. Indeed, in order to be sure that they are not communicating with someone else, Alice and Bob need to send an authentication key over a classical secure channel. After this they can implement a quantum protocol like BB84 and "expand" the existing authentication key.

2.1.4 Eves Strategies:

Eve can choose different eavesdropping strategies:

1. intercept and resend: Eve intercepts and measures the qubits sent by Alice and resends them to Bob;

2. translucent attack: Eve has probes (ancillary qubits) interacting with the qubits sent by Alice and she measures the state of these probes;

3. collective attack: Eve manipulates not a single qubit at a time but a block of qubits.

Intercept and Resend Strategy :
Let us have a closer look at how eavesdropping interferes with the states and how Alice and Bob can detect it. We will sketch a very simple strategy that Eve can pursue, which is the *intercept-and-resend* strategy. Here, Eve intercepts all $4N$ qubits that Alice sends to Bob. Since cloning the states is forbidden by the no-cloning theorem, the simplest way to get information about the states is to measure them. At this point of the protocol, Alice has not yet announced her choice of basis, so Eve has to guess in which basis she has to measure the states, thereby randomly choosing the basis she measures in z or x basis. In about half of the cases, i.e., for the $2n$ qubits, her basis will be the same as the one that Alice chose for encoding the bit and Eve gets completely correlated bit values. In the other $2n$ cases, however, her guess will be wrong and she gets a random result[1]. Of course, as long as Alice has not revealed her choice of basis, Eve does not know which states she has measured in the correct basis. Since Bob is expecting to receive the qubits from Alice, Eve has to send states to Bob. Because she does not know which are the correct bases, she simply prepares each qubit in the same basis that she has used for the measurement. Hence, $2n$ of the qubits will be prepared in the wrong basis. Bob then receives the qubits and measures them, again by randomly choosing the measurement basis. In n cases Bob and Alice have chosen the same basis, but Eve's basis is different. Since in these cases Bob gets a random result, there will be $\frac{n}{2}$ errors in the sifted key. Since the length of the sifted key is $2n$, this corresponds to an error rate of 25%. Hence, if Alice and Bob observe such a high error rate during parameter estimation they abort the protocol. We have depicted an example of this eavesdropping attack using ten qubits in Table 3. After the sifting step, Alice and Bob are left with six of the initially ten qubits. Next, Alice and Bob use half of the remaining bits to estimate the knowledge that Eve has. They find that one of those three bits is wrong; hence, they have an estimated error of $\frac{1}{3}$ in their key bit string. Since this error is above 25%, they know that Eve has intercepted the communication and abort the protocol. What about Eve's knowledge? How much information on the raw key (i.e., the key string after the parameter

[1]For instance, suppose Alice has prepared the state $|0\rangle$, which is in the computational basis. If Eve measures this state in the Hadamard basis, she gets the result 0 50% of the time and the result 1 also 50% of the time.

key bit	0	1	1	1	0	0	1	1	1	0
Alice's basis	z	z	x	z	z	x	x	z	x	x
Alice's states	$\|0\rangle$	$\|1\rangle$	$\|1\rangle_x$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle_x$	$\|1\rangle_x$	$\|1\rangle$	$\|1\rangle_x$	$\|0\rangle_x$
Eve's basis	x	z	z	x	z	x	z	x	z	x
Eve's states	$\|0\rangle_x$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle_x$	$\|0\rangle$	$\|1\rangle_x$	$\|1\rangle$	$\|1\rangle_x$	$\|1\rangle$	$\|0\rangle_x$
Bob's basis	x	z	x	x	x	z	x	z	x	z
Bob's result	0	1	0	0	0	0	1	1	0	0
sifting	-	✓	✓	-	✓	-	✓	✓	✓	-
key bit		1	0		0		1	1	0	
P.E.			-				✓	✓		

Table 3: Simple eavesdropping strategy for the BB84 protocol. Eve intercepts, measures, and resends every qubit that Alice sends. This introduces errors (highlighted in grey) to Alice and Bob's key bits that they can exploit to detect the eavesdropping during the parameter estimation (P.E.) step

estimation step) did she get? Since she guesses the correct basis in $\frac{1}{2}$ of the cases, she knows 50% of the key bits. Let us check how much knowledge of the key bits she has in the example discussed in Table 3. After she has measured the qubits, her bit string is

$$0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \tag{2.21}$$

After Alice announces her choice of basis, Eve discards those bits where she has measured in a different basis than Alice, so she is left with

$$- \quad 1 \quad - \quad - \quad 0 \quad 1 \quad - \quad - \quad - \quad 0 \tag{2.22}$$

She also has to discard those bits that Alice and Bob discard during their sifting procedure:

$$- \quad 1 \quad - \quad - \quad 0 \quad - \quad - \quad - \quad - \quad - \tag{2.23}$$

At last, she has to discard the bits that were used for parameter estimation, which leaves her with

$$- \quad - \quad - \quad - \quad 0 \quad - \quad - \quad - \quad - \quad - \tag{2.24}$$

Therefore, in the end she knows one of the three bits of the raw key. Of course, since we have only used 10 qubits in this example, the numbers we get for the error fraction and the amount of Eve's knowledge are not very meaningful, but still you get the idea.

2.2 B92 Protocol [3]

The BB84 protocol can be generalized to use other states and bases, and similar conclusions hold. In fact, a particularly simple protocol exists in which only two states are used. For simplicity, it

is sufficient to consider what happens to a single bit at a time; the description easily generalizes to block tests just as is done in BB84. Suppose Alice prepares one random classical bit a, and, depending on the result, sends Bob

$$\begin{cases} |0\rangle \quad if \quad a = 0 \\ \\ \dfrac{|0\rangle + |1\rangle}{\sqrt{2}} \quad if \quad a = 1 \end{cases} \tag{2.1}$$

2.3 Ekert 91 (E91) Protocol

In 1991, Arthur Ekert developed a scheme that exploits entanglement to generate a secret key. The protocol works as follows: Alice and Bob have access to a source that distributes maximally entangled pairs of qubits among them, for instance, states of the form

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}) \tag{2.1}$$

For each of these bipartite states $|\Psi^-\rangle_{AB}$ Alice and Bob measure an observable that is randomly chosen from the sets $\{A_i\}$ and $\{B_i\}$, respectively. These observables are spin components lying in the $x-z$-plane of the Bloch sphere and are depicted in Fig. 2.2. In general, these operators are defined as

$$A_i = \cos\varphi_i^A + \sin\varphi_i^A \tag{2.2}$$

$$B_i = \cos\varphi_i^B + \sin\varphi_i^B \tag{2.3}$$

$$\tag{2.4}$$

with $\varphi_1^A = 0$, $\varphi_2^A = \frac{\pi}{2}$, and $\varphi_3^A = \frac{\pi}{4}$ for Alice and $\varphi_1^B = 0$, $\varphi_2^B = -\frac{\pi}{4}$, and $\varphi_3^B = \frac{\pi}{4}$ for Bob. In terms of the measurement operators σ_z and σ_x, the measurements can also be written as

$$A_1 = \sigma_z \qquad B_1 = \sigma_z \tag{2.5}$$

$$A_2 = \sigma_x \qquad B_2 = \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x) \tag{2.6}$$

$$A_3 = \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x) \qquad B_3 = \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x) \tag{2.7}$$

Note that the measurements A_1 and B_1 as well as A_3 and B_3, respectively, are those where Alice and Bob measure in the same direction.

In the next step, Alice and Bob announce the directions they chose for each measurement. For those pairs where the directions match, i.e., the pairs (A_1, B_1) and (A_3, B_3), they get completely anti-correlated results. Therefore, by inverting all bits for one party, the outcomes of these measurements form the sifted key. The results from the measurement pairs (A_1, B_3), (A_1, B_2), (A_2, B_3), and

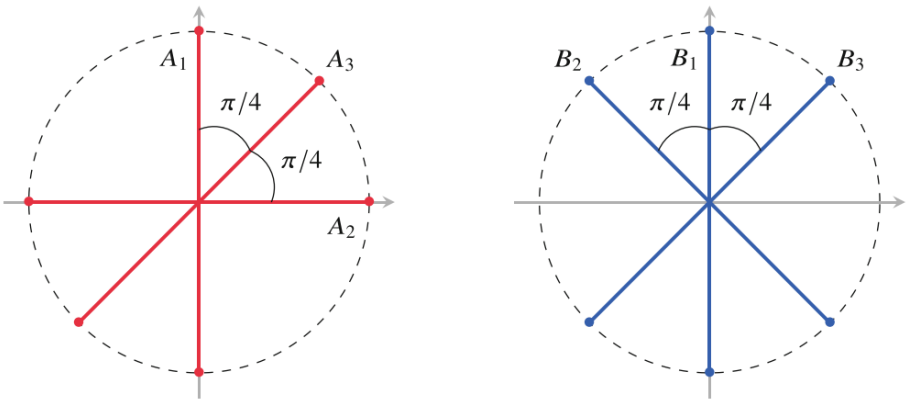

Figure 2.2: Measurement directions for the Ekert protocol. The measurements are depicted in the $x-z$-plane of the Bloch sphere. On the left side are the three different measurements that Alice can choose between, and on the right side Bob's possible measurement directions are shown

(A_2, B_2) are used to estimate how much information an eavesdropper has about the key. This is done by checking a so-called CHSH inequality. The CHSH inequality, named after the initials of its four discoverers [13], is a bound on the expectation values of certain classical correlations. It is part of a larger set of inequalities known as Bell inequalities (because the first one was found by John Bell [3]). Suppose you have four classical random variables, A_1, A_2, B_2, B_3. Suppose each of them can take one of two values, +1 or -1. One can easily verify that $A_1(B_3+B_2)+A_2(B_3-B_2) = \pm 2$, simply by checking all possibilities. By taking the expectation value of these quantities over N assignments of the random variables, we get

$$|\langle A_1(B_3 + B_2) + A_2(B_3 - B_2)\rangle| \leq 2. \tag{2.8}$$

Since taking the expectation of a random variable is a linear operation, we can rewrite this and obtain the CHSH inequality:

$$|\langle A_1B_3\rangle + \langle A_1B_2\rangle + \langle A_2B_3\rangle - \langle A_2B_2\rangle| \leq 2. \tag{2.9}$$

where $\langle A_iB_j\rangle = \frac{1}{N}\sum A_i^\nu B_i^\nu$, and A_i^ν and B_j^ν represent the assigned values ν to the random variables A_i and B_i. We can now consider A_1, A_2, B_2, B_3 to be quantum observables as described in the Ekert protocol. The expectation value for their products is then given by

$$\langle AiBj\rangle = \mathrm{Tr}(A_i \otimes B_j\rho) \tag{2.10}$$

Using the measurement directions defined in the Ekert protocol, we can evaluate their expectation values with respect to the state $\rho = |\Psi^-\rangle\langle\Psi^-|$. For instance, the expectation value of A_1 and B_3 is

$$\langle A_1B_3\rangle = \langle\Psi^-|\sigma_z \otimes \frac{(\sigma_z + \sigma_x)}{\sqrt{2}}|\Psi^-\rangle = -\frac{1}{\sqrt{2}}. \tag{2.11}$$

In this way we can evaluate all terms in the sum of expectation values S and find that

$$S = 2\sqrt{2} \tag{2.12}$$

This is a violation of the CHSH inequality that we have derived above and tells Alice and Bob that they share a maximally entangled state. In this case, Eve has no information about the key, since a maximally entangled bipartite state cannot be entangled with a third party. This is actually the highest value for S that can be achieved. In general, it is possible to obtain lower values for S that still violate the CHSH inequality. In this case, Eve can have some knowledge about the key. However, it is still possible to extract a secret key from this data as long as there is some violation of the CHSH inequality. If $S \leq 2$, this indicates that Alice and Bob share a pair of separable states, i.e., it is impossible to generate a secret key. If their measurement results pass the test, Alice and Bob can proceed to the next step of the protocol and obtain the final secret key by doing error correction and privacy amplification. The steps of the protocol are summarized below:

Ekert91:

1. Alice and Bob distribute a number of $|\Psi^-\rangle_A B$ states between them, where the first subsystem belongs to Alice and the second one to Bob.
2. For each state, Alice and Bob randomly choose a measurement from the sets $\{A_i\}$ and $\{B_i\}$, respectively.
3. Alice and Bob announce the bases they chose for each measurement. In the cases where the directions match, (A_1, B_1) and (A_3, B_3), the results form the sifted key.
4. The results where Alice and Bob chose the directions (A_1, B_3), (A_1, B_2), (A_2, B_3), and (A_2, B_2) are used to check a CHSH inequality.
5. Alice and Bob perform error correction and privacy amplification to turn the sifted key into a shared secret key.

References

[1] Giuliano Benenti, Giulio Casati, Davide Rossini, and Giuliano Strini. *Principles of quantum computation and information: a comprehensive textbook*. World Scientific, 2019.

[2] Mikio Nakahara and Tetsuo Ohmi. *Quantum computing: from linear algebra to physical realizations*. CRC press, 2008.

[3] Michael A Nielsen and Isaac L Chuang. Quantum computation and quantum information. *Phys. Today*, 54(2):60, 2001.

[4] Ramona Wolf. *Quantum key distribution*. Springer, 2021.