

Introduction to quantum information and quantum cryptography: Lecture 2

WANTED



DEAD & ALIVE
Schrödinger's cat

$$\frac{1}{\sqrt{2}}(|\text{DEAD}\rangle + |\text{ALIVE}\rangle)$$

Density matrix, mixed state

Density matrix, mixed state

Density matrix has already been partly explained in the introductory chapter of the textbook of our subject. Now we detail some of its important features which will be useful later. First of all we have to define a very considerable idea, namely: *ensemble* which is a set of similar quantum systems prepared in different states. Suppose we select one of these systems. The probability of selecting a system whose state is Ψ_i equals p_i and $\sum_{i=1}^n p_i = 1$, where n denotes the number of the systems. Measuring a physical quantity A , we would like to know its expectation value on this ensemble. In other words, we want to know $\langle \hat{A} \rangle$. In a state $|\Psi_i\rangle$ – as we know – the expectation value of A can be calculated in the following way: $\langle \Psi_i | \hat{A} | \Psi_i \rangle$.

Density matrix, mixed state

However we need to average twice: besides the former expression, we have to average over weights too. Hence

$$\langle \hat{A} \rangle = \sum_{i=1}^n p_i \langle \psi_i | \hat{A} | \psi_i \rangle = \text{Tr}(\hat{\rho} \hat{A}),$$

where $\hat{\rho}$ is the well known density operator which features the ensemble and as we can surmise

$$\hat{\rho} = \sum_{i=1}^n p_i |\psi_i\rangle \langle \psi_i|.$$

How did we get this expression of $\hat{\rho}$?

Density matrix, mixed state

Let us consider the followings: As we know:

$$|\Psi_i\rangle = \begin{pmatrix} \alpha_i \\ \beta_i \end{pmatrix} = \begin{pmatrix} \alpha_i \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ \beta_i \end{pmatrix} = \alpha_i \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta_i \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha_i |0\rangle + \beta_i |1\rangle.$$

Let us take the inner product between $|\Psi_i\rangle$ and $|\Psi_j\rangle$:

$$\langle \Psi_i | \Psi_j \rangle = (\alpha_i^* \quad \beta_i^*) \begin{pmatrix} \alpha_j \\ \beta_j \end{pmatrix} = \alpha_i^* \alpha_j + \beta_i^* \beta_j$$

Let us mark this result and consider the outer product of these kets:

$$|\Psi_i\rangle \langle \Psi_j| = \begin{pmatrix} \alpha_i \\ \beta_i \end{pmatrix} (\alpha_j^* \quad \beta_j^*) = \begin{pmatrix} \alpha_i \alpha_j^* & \alpha_i \beta_j^* \\ \beta_i \alpha_j^* & \beta_i \beta_j^* \end{pmatrix}$$

Density matrix, mixed state

As we can see, having the trace of the outer product (summing the diagonal element of the matrix above), we obtain exactly the result of the inner product.^a So

$$\begin{aligned} \text{Tr}(|\Psi_i\rangle\langle\Psi_j|) &= \sum_n \langle n|\Psi_i\rangle\langle\Psi_j|n\rangle = \sum_n \langle\Psi_j|n\rangle\langle n|\Psi_i\rangle = \\ & \langle\Psi_j|\hat{I}|\Psi_i\rangle = \langle\Psi_j|\Psi_i\rangle. \end{aligned}$$

That is the operation of the trace makes the outer product an inner product. Returning to the initial statement:

$$\text{Tr}\left[\hat{A}\sum_i p_i|\Psi_i\rangle\langle\Psi_i|\right] = \sum_i p_i \text{Tr}\left[\hat{A}|\Psi_i\rangle\langle\Psi_i|\right] = \sum_i p_i \langle\Psi_i|\hat{A}|\Psi_i\rangle$$

^aThe only difference is that i is replaced with j .

Density matrix, mixed state

So the density operator describes an ensemble. Nevertheless, there is another interpretation of the density operator, namely: when a subsystem of a larger system is considered. As an example, let us suppose we have two systems, A and B . In this case the common state vector is $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, which can be expressed on the following base: $\{|n\rangle_A\}; \{|m\rangle_B\}$. Hence $|\Psi\rangle = \sum_{nm} c_{nm} |n\rangle |m\rangle$ and $\sum_{nm} |c_{nm}|^2 = 1$. Let us consider a system X_A , which is one of the physical quantities of system A . In this situation, $\hat{X}_A \otimes \hat{I}_B$ is a two-system operator measuring X_A in system A , but leaving B untouched.

Density matrix, mixed state

Its expectation value is

$$\begin{aligned}\langle \hat{X}_A \rangle &= \langle \Psi | \hat{X}_A \otimes \hat{I}_B | \Psi \rangle = \\ &= \sum_n \sum_m \langle \Psi | \hat{X}_A \otimes \hat{I}_B (|n\rangle_A |m\rangle_B) \langle n|_B \langle m| \rangle | \Psi \rangle = \\ &= \sum_n \langle n|_A \left[\sum_m \langle m| \Psi \rangle \langle \Psi | m \rangle_B \hat{X}_A |n\rangle_A \right],\end{aligned}$$

where

$$\sum_m \langle m| \Psi \rangle \langle \Psi | m \rangle_B$$

is the reduced density operator of subsystem A denoted by $\hat{\rho}_A$.

Density matrix, mixed state

In the derivation $\sum_n A \langle n | \sum_m B \langle m | \Psi \rangle$ is just an expression factor and $\langle \Psi | m \rangle_B$ was also replaceable, because \hat{X}_A does not have an effect on $|m\rangle_B$, because it is in system B .)

Knowing that

$$\hat{\rho}_A = \text{Tr}_B |\Psi\rangle\langle\Psi| = \left(\sum_m B \langle m | \Psi \rangle \langle \Psi | m \rangle_B \right),$$

we have that

$$\langle \hat{X}_A \rangle = \text{Tr}_A (\hat{\rho}_A \hat{X}_A).$$

In this case, though the larger system is in a pure state, its subsystem is in a mixed state.

Density matrix, mixed state

Let us consider examples for both interpretations:

Example for the ensemble interpretation (in case of qubits):

Let us suppose we have many qubits and half of the qubits are in state $|0\rangle$, while the other half of them are in state $|1\rangle$. In this case the density operator is

$$\hat{\rho} = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\hat{I}.$$

Let us try to find out the expectation value of σ_z . As we know it is one of the three Pauli operator represented by the following matrix:

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Density matrix, mixed state

By the way $|0\rangle$ and $|1\rangle$ are the eigenstates of σ_z with eigenvalues 1 and -1 :

$$\sigma_z|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$\sigma_z|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ -1 \end{pmatrix} = -|1\rangle$$

From this it follows that

$$\langle\sigma_z\rangle = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot (-1), \text{ which is obviously equals } \text{Tr}(\hat{\rho}\sigma_z) = 0.$$

Density matrix, mixed state

Example for a system consisting of two qubits in a state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B).$$

We do not know it yet^a but this is one of the four famous *Bell* states:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

^aBut it will be shortly discussed.

Density matrix, mixed state

Now let us see the spin of A . We know that $\text{Tr}_B(|\Psi\rangle\langle\Psi|) = \hat{\rho}_A$, thus

$$\begin{aligned}\hat{\rho}_A &= \sum_{m=0}^1 {}_B\langle m| \left\{ \frac{1}{\sqrt{2}} (|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B) + \right. \\ &\quad \left. \frac{1}{\sqrt{2}} ({}_A\langle 0| {}_B\langle 1| + {}_A\langle 1| {}_B\langle 0|) \right\} |m\rangle_B = \\ &= \frac{1}{2} \sum_{m=0}^1 {}_B\langle m| \left\{ |0\rangle_A |1\rangle_B {}_A\langle 0| {}_B\langle 1| + |0\rangle_A |1\rangle_B {}_A\langle 1| {}_B\langle 0| + \right. \\ &\quad \left. |1\rangle_A |0\rangle_B {}_A\langle 0| {}_B\langle 1| + |1\rangle_A |0\rangle_B {}_A\langle 1| {}_B\langle 0| \right\} |m\rangle_B = \\ &= \frac{1}{2} (|0\rangle_A {}_A\langle 0| + |1\rangle_A {}_A\langle 1|).\end{aligned}$$

Density matrix, mixed state

Since $\sigma_{zA} = \sigma_z \otimes \hat{I}_B$,

$$\langle \sigma_{zA} \rangle = \text{Tr}(\sigma_z \rho_A) = 0.$$

In this formalism, if we want, also a pure state can be described by a density operator, where

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i| = |\psi\rangle \langle \psi|$$

because each element of the ensemble is in the same state, whose weight is 1. Weight belonging to all the other states is 0. The expectation value of a physical quantity A is

$$\langle \hat{A} \rangle = \text{Tr}(\hat{\rho} \hat{A}) = \text{Tr}(|\psi\rangle \langle \psi| \hat{A}) = \langle \psi | \hat{A} | \psi \rangle.$$

Density matrix, mixed state

Both pure and mixed states can be featured by density operators. If a density operator has a shape like this $\rho = |\Psi\rangle\langle\Psi|$, the state is said to be a pure state, but in case of weighted sum of pure states – $\rho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|$ – the related state is a mixed state. It is natural to ask that in case we have a density operator, how can we find out if it is a pure or a mixed state? This question can be answered with the properties of density operators:

Density matrix, mixed state

- $Tr(\hat{\rho}) = 1$

Proving:

$$\begin{aligned} Tr(\hat{\rho}) &= Tr\left(\sum_i p_i |\Psi_i\rangle\langle\Psi_i|\right) = \sum_i p_i Tr\left(|\Psi_i\rangle\langle\Psi_i|\right) = \\ &= \sum_i p_i \langle\Psi_i|\Psi_i\rangle = \sum_i p_i = 1 \end{aligned}$$

- $\hat{\rho} = \hat{\rho}^\dagger$

This feature comes from the construction of the density operator, because $|\Psi_i\rangle$ and $\langle\Psi_i|$ are the adjoints of each other. From this feature, it follows that eigenvalues of $\hat{\rho}$ are real.

Density matrix, mixed state

- $\hat{\rho}$ is a positive operator, that is $\langle \Psi | \hat{\rho} | \Psi \rangle \geq 0$. Proving:

$$\begin{aligned} \langle \Psi | \hat{\rho} | \Psi \rangle &= \langle \Psi | \left(\sum_i \rho_i |\Psi_i\rangle \langle \Psi_i| \right) | \Psi \rangle = \sum_i \rho_i \langle \Psi | \Psi_i \rangle \langle \Psi_i | \Psi \rangle = \\ &= \sum_i \rho_i |\langle \Psi_i | \Psi \rangle|^2 \geq 0 \end{aligned}$$

Density matrix, mixed state

- $\hat{\rho}$ is positive if and only if all of its eigenvalues are $\lambda_i \geq 0$. Being a Hermitian operator, it has a diagonal production: $\hat{\rho} = \sum_i \lambda_i |u_i\rangle\langle u_i|$, where it is true that $\langle u_i | u_j \rangle = \delta_{ij}$ and $\sum_i |u_i\rangle\langle u_i| = \hat{1}$, ($\lambda_i \geq 0$). Though different $|\Psi_i\rangle$ -s are not necessarily perpendicular to each other diagonalization can be made (spectral theorem).
 $\hat{\rho}$ is a pure state if and only if

$$\text{tr}(\hat{\rho}^2) = 1.$$

Obviously, in case $\hat{\rho}$ is a pure state:

$$\hat{\rho} = |\Psi\rangle\langle\Psi| \Rightarrow \hat{\rho}^2 = (|\Psi\rangle\langle\Psi|)(|\Psi\rangle\langle\Psi|) = |\Psi\rangle\langle\Psi| = \hat{\rho}$$

(let us remember: $\langle\Psi|\Psi\rangle = 1$), and the trace of $\hat{\rho}$ is 1.

Density matrix, mixed state

Without additional provings, we declare that in case of a mixed state

$$\text{Tr}(\hat{\rho}^2) < 1 = \text{Tr}(\hat{\rho})$$

and for a pure state

$$\text{Tr}(\hat{\rho}^2) = 1 = \text{Tr}(\hat{\rho}).$$

A quantum cryptographical protocol

A quantum cryptographical protocol



A quantum cryptographical protocol

So far, we have learned the simplest tools which are necessary for us to understand the most elementary algorithms and methods in quantum information. Hence, by this time, we have become clever enough :-) to begin to deal with some of the simplest applications of the easiest parts of quantum mechanical toolkit in the area of quantum communication. Nevertheless, some algorithms and methods belonging to the same area have to be treated separately, because even now, we do not have knowledge enough in quantum mechanics. What is it all about? For understanding this dilemma, let us consider - for example - the quantum cryptographical protocols. These methods should be explained in the same chapter, accordingly their goals.

A quantum cryptographical protocol

But we can not do this, for several reasons. Just as an example of these reasons: there is a cryptographical protocol called E91 which is based on the phenomenon of quantum entanglement, and if we would like to understand how it works, we have to know the fundamental theoretical background of the entanglement. Being an important topic which is unknown for us, entanglement requires an own chapter, thus it should be treated before learning about certain cryptographical – and some other – protocols.

A quantum cryptographic protocol

Nevertheless we would like to maintain the attendance of students, hence we start to learn about *practical applications* which can be already understood using the discussed / known theoretical tools, and those applications which still can not be understood will be discussed in a future chapter after explaining their theoretical background. This tutorial method results a structure which is based on not the goal of algorithms, but on the theoretical basics which we need to know for understanding them. So, let us start it.

The BB84 protocol


The BB84 protocol

- Question: what does *cryptology* mean?
- Answer: it is the art of secret communication.

Let us consider the following situation where Alice wants to send a secret message to Bob. In a case like this Alice's message has to be encoded using some kind of cryptographic key. Probably the oldest and simplest method to make a message secret is the *Caesar code/cipher*, which is a substitutive encryption procedure, where each letter of the alphabet is replaced by another letter.

The BB84 protocol

The distance between the position of the original letter and its substitutive is given as a key for the encryption method and its value can have (1, 2, 3,etc). In this procedure – in Caesar's time in the history – the primary alphabet was the Latin alphabet and the secondary alphabet was obtained by using this ciphering method. Nowadays, using English alphabet, if "*I love this semester!*" is the message to be encrypted and the value of the letter-transpose (the key) is 2, each letter of the English alphabet will be transposed by 2 places and the encrypted message will be "*k nqyg vjku ugoguvgt!*"¹.

¹Provided we do not handle upper and lower cases. 

The BB84 protocol

Evidently this is an easy breakable kind of ciphering. However, if we use a random value of transpose for each letter and we use the obtained key only once, we get an unbreakable² encryption method called *Vernam cipher* or in other words *One Time Pad* (OTP). (The only disadvantage of this method is that the used key is as long as the text itself.)

So, Alice needs to have two important things:

- One of them is the *algorithm* of the encryption. (For example transposing the letters.)
- The other one is the *key*. For example, using a Caesar code, it is the value of the distance of the transpose.

²Proved by Shannon.

The BB84 protocol

Nevertheless, we must keep in mind the following – proved – theorem:

the safety of a crypto-system does not depend on the secrecy of the applied algorithm, but depends on the secrecy of the key only. Hence, to find a secret/safe way to share/distribute the encryption key to the parties of the communication is the most important task to solve. This problem can not be solved by using any of the classical methods.

However, we have *a new hope*, because applying one of the several *quantum key distribution* protocols the problem is solvable, with a complete safety.

The BB84 protocol

Let us consider a present-day example to understand how encryption works. So, Alice's message consists of a set of bits, like this one below:

0 1 . . . 1 1 . . . 0 1

In addition to this, she has a randomly generated encryption key consisting a set of bits, too:

1 1 . . . 1 0 . . . 0 1

She can encrypt her message by adding the responsive elements of her message and the key, according to *modulo-2*, where

$$0 \oplus 0 = 0,$$

$$0 \oplus 1 = 1,$$

$$1 \oplus 0 = 1,$$

$$1 \oplus 1 = 0.$$

The BB84 protocol

The resulted encrypted message can be seen below:

Original message	0	1	1	1	0	1
Encryption key	1	1	1	0	0	1
Encrypted message	1	0	0	1	0	0

Now then, this encrypted message will be sent to Bob, who needs to have the encryption key used by Alice, provided he wants to find out what Alice wanted to communicate.

Supposing Bob has the key, it is natural to ask how he will decode the message he got?

The BB84 protocol

The answer is very simple: the received (encrypted) message and the key has to be added to obtain the original message:

Encrypted message	1	0	0	1	0	0
Encryption key	1	1	1	0	0	1
Original message	0	1	1	1	0	1

As we can see, it is an unbreakable – or at least a hard breakable – encryption algorithm. However, it has a weakness, namely it can not be guaranteed that Alice and Bob are the only persons who have the secret key. In addition to this the presence of an eavesdropper (let us call her Eve) can not be debunked. Let us see, how quantum cryptography help us to eliminate this problem.

The BB84 protocol

So, the goal of Alice and Bob is to share a common secret key known by themselves only to ensure the secrecy of their communication. Before all, they need to share a quantum and a classical channel (the latter can be anything, even smoke signals). Their common quantum channel is a one way channel from Alice to Bob and the classical channel is a two-way channel. First of all, Alice randomly generate a set of classical bits³:

0 1 1 0 1 0 1 1 1 0 1 0

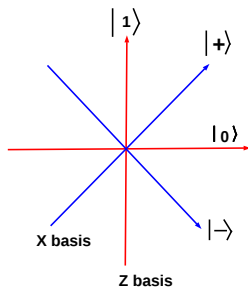
³Naturally, in a real life situation the length of a set like this is much more longer than the presented one.

The BB84 protocol

After finishing it, Alice encodes each bit of the set into a quantum bit, in the following way: for every qubit, she randomly chooses a preparation basis which can be either the basis spanned by the eigenvectors of σ_z Pauli matrix or another one spanned by the eigenvectors of σ_x Pauli matrix. Let us label the former basis as Z basis and the latter one as X basis. As we already know, elements of the Z basis are $\{|0\rangle; |1\rangle\}$ and the two basis vectors of the X basis are $\{|+\rangle; |-\rangle\}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Bearers of the quantum bits used in this protocol can be photons, and their observable polarization (eigen)states play the role of the basis vectors. In this picture, if Z basis is considered as a horizontal polarization basis, then X basis corresponds to the rectilinear polarization basis, where these two bases are the $\pi/2$ rotated of each other.

The BB84 protocol

Now then, depending on the chosen preparation basis, bit 0 can be encoded into either $|0\rangle$ or $|+\rangle$, and similarly, bit 1 can be associated with either $|1\rangle$ or $|-\rangle$. As a visualization, these bases can be imagined in the following graphic way:



The BB84 protocol

In this situation – as in general in any of real life cases – the orientations of the basis elements matter only, or rather we can say the orientations of the axes matter only. It is important to realize and to keep in mind that

if a qubit is in either of the eigenstates of one of these two bases, its state is a superposition on the other basis, and vice versa.

If we keep in mind this fact, we will understand how BB84 quantum key distribution protocol works.

The BB84 protocol

Let us consider the figure below, where in the first row, we can see the randomly generated set of classical bits, in the second row – for each bit – the randomly chosen preparation bases can be seen, and in the third row the prepared quantum bit states are enumerated, where 0-s or 1-s are encoded into each qubit.

	0	1	1	0	1	0	1	1	1	0	1	0
	X	X	+	X	+	+	+	X	X	+	+	X
Quantum bits sent by Alice to Bob:	↗	↖	↑	↗	↑	→	↑	↖	↖	→	↑	↗
	X	+	+	X	X	+	X	+	X	X	+	X
	↗	↑	↑	↗	↖	→	↗	→	↖	↖	↑	↗
	0	1	1	0	1	0	0	0	1	1	1	0
	↗	-	↑	↗	-	→	-	-	↖	-	↑	↗
This is the raw key:	0		1	0		0			1		1	0

The BB84 protocol

From the 4th row, Bob's side is presented. This row contains the measurement bases chosen randomly for each qubit by Bob. What is it all about? After obtaining the qubits sent by Alice, Bob chooses randomly a measurement basis (Z or X) for each qubit he got, and he makes a measurement on every single qubit in the corresponding basis. After completing his work on measurement, he documents the set of the resulted values. After this, Alice and Bob check the set of their randomly chosen bases (not the results) via a public classical channel, and they keep those elements of their sets of bits where they chose the same basis. The bits which remained form the *raw key*⁴, which – in the presented situation – is the following set:

0 1 0 0 1 1 0

⁴The reason for calling this set *raw key* will be shortly discussed.

The BB84 protocol

One more thing remains to be understood for us to see why this method is better and safer (or rather: absolutely safe) than any of the classical key distributions. First of all let us try to find out what an eavesdropper can do to get the secret key. She (supposing her name is Eve) can catch the quantum bits sent by Alice and before retransmitting them to Bob, she can make a measurement on each quantum bit she caught. And *this is a critical moment*, because she does not know which bases were chosen by Alice and which bases will be chosen by Bob (because Alice and Bob will check their bases publicly only *after* Bob obtains the qubits). Hence Eve must select one of the two used bases (Z or X) and make her measurements "blindly" without any knowledge about Alice's or Bob's bases.

The BB84 protocol

And here comes the essence of this protocol:

Alice and Bob know their results are necessarily the same for every qubit where they chose the same basis⁵. As we already know these results form the raw key. Now, we say the reason why we call this kind of key a *raw* key. To obtain the "final" key which will be used in the secret communication between Alice and Bob, they need to compare a part of the raw key publicly (immolating the selected part), because they know the following important thing:

⁵according to the fundamental laws of quantum mechanics, as we already know

The BB84 protocol

If in these cases – where Alice and Bob chose the same basis – the measurement basis chosen by Eve were not the basis which were selected by Alice and Bob, Eve's measurement results a state which is a *superposition* in the basis chosen by Alice and Bob. Hence Alice and Bob can find different results with a probability of $1/2$ where their results should be the same because of the superposition caused by Eve's measurement (in her wrong chosen basis).

Hence, the presence of an eavesdropper – in our case: Eve – can be detected

because of the non-reversible disturbance introduced into the quantum state by her measurement. The reason for the $1/2$ value of the probability is that even a superposition state can fall into the "good" eigenstate of Bob's basis with a porabability of $1/2$. In this case, the presence of Eve remains undetected.

The BB84 protocol

Moreover, it is imaginable for Eve to choose the "good" basis with a probability of $1/2$. In a situation like this her presence can not be detected by comparing Alice's and Bob's results. Fortunately, Alice and Bob work with a raw key whose length is much more longer than the presented set, hence they can apply a statistical method which makes possible for them to detect the presence of Eve with a complete security. In case of detecting an eavesdropper, they drop the key and create a new one. Summarized: in case of the quantum key distribution, the presence of an eavesdropper can not be kept dark.

This is the reason why quantum cryptography is unbreakable.

The BB84 protocol

However..... what if Eve decide to copy / clone each quantum bit she caught before retransmitting it to Bob and in this way she can make two clones of every quantum bit sent by Alice. In this situation, having two clones of each quantum bit, she can make a measurement on one of the clones, in basis Z , and can make another measurement on the other clone, in basis X . In a case like this, it is possible for her to circumvent BB84 protocol.

Let us realize there is a crucial point in Eve's process, namely: we have not known if cloning of an unknown quantum state is a possible quantum map or not. This topic will be discussed next week.