The No-cloning Theorem and its Implications in Quantum Cryptography

Jose Manuel Torres López, Kapitza Society, Spring 2022

April 19, 2022

Abstract

For the last thirty years, the interest on quantum information science has been growing enormously within the physics community. The main reason behind this trend is that quantum systems show promise to simulate computations that are inaccessible within the classical realm, by taking advantage of properties that are fundamentally quantum in nature, such as quantum entanglement. An important example of such applications is quantum cryptography, where quantum theory is applied to devise safe protocols for the safe transmission of information. This is often feasible thanks to the fact that, generally speaking, measuring a quantum system unavoidably alters its original state. More concretely, the no-cloning theorem states that it is impossible to measure information that distinguishes between two non-orthogonal quantum states without altering them. This is useful for quantum communications because it implies that an eavesdropper cannot read a message without disturbing it, and there exist procedures to check that an original state has not been altered in this way.

In this paper, I first introduce the basic idea of quantum cryptography through the procedure of "EPR quantum key distribution", which leads to an instance of the no-cloning theorem. Then, the no-cloning theorem is presented and proven in its general form.

1 EPR quantum key distribution

Cryptography is the practice and study of techniques for secure communication in the presence of adversarial behavior [1]. A classical approach to ensure this type of communication is the use of a private key, which is a password code that can be used to encrypt and decrypt the message and must be shared by the communicating parties but kept outside the reach of adversaries. For instance, if the message is converted to binary code, the private key can be takes to be a string of random bits as long as the message, which is added mod 2 to the message once for the encryption and once more to the received message to recover the original string. This approach works because the encoded message by itself carries no information about the original message on its own; rather, the correlation between the two is encoded in the private key. Therefore, there is no problem with the transmitted message being intercepted as long as the private key is not.

In classical communication, then, the difficulty of the private-key procedure lies in performing the one-time exchange or transmission of the key in a secure way. There exist "public key" distribution protocols, but these are only safe under the assumption that the adversaries do not have the powerful computational resources needed to decode the transmitted message in a reasonable amount of time.

In contrast with the classical limits, the use of quantum information allows for distribution protocols that are completely invulnerable to any attack. To illustrate this idea, consider an agent called Alice

who is trying to send a message to her accomplice Bob, making sure that the information will not be intercepted and read by an adversary eavesdropper, called Eve. This discussion will follow the presentation of EPR quantum key distribution found in [2].

Now, suppose that Alice and Bob share a supply of qubits that are entangled in pairs, in such a way that all pairs are in the state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, which corresponds to a perfect correlation between the two qubits in any pair. We will see how this previously-created correlation between qubits can be exploited at any moment to readily create a private key that is available to both parties, in an automatic and therefore secure way. This is achieved through the following protocol.

To each possessed qubit, Alice and Bob independently decide to measure one of the spin components σ_1 or σ_3, each with a frequency of 50%. After these measurements, Alice and Bob announce publicly what observables they measured, but not the measurement results. In about half of the cases, statistically speaking, their choice of observable coincides, so that there measurements of spin are along the same axis and therefore their results will be perfectly correlated in those cases. Hence, the two possible measurement outcomes, which for the σ_i equal ± 1, can be interpreted as the two possible values of a bit; and the set of all correlated measurement can be used as a common private key that was in fact randomly generated. In contrast, the cases where Alice and Bob choose different observables lead to uncorrelated outcomes, but these can be simply discarded.

The protocol just introduced is called "EPR quantum key distribution", because the private key is obtained by using EPR entangled pairs as a resource. In principle, there is one way in which the safety of this protocol may be compromised. It was previously assumed that the Alice and Bob share a perfect ensemble of $|\phi^+\rangle$ states that are pure in the sense that they are not entangled with another qubit outside the considered pair, and the details of the creation of this ensemble were ignored through abstraction. But, how can we be sure that these states were not tampered with at some point, in such a way to entangle them with a set of pointer qubits in possesion of Eve? The concern if this is the case is that Eve might perform measurements on her own qubits that can provide some information about the pairs shared by Alice and Bob. This possibility can be ruled out by a security check on the original pairs, which we present next. To do this, consider the most general possible state of an AB pair entangled with some set of E qubits:

$$|\Gamma\rangle_{ABE} = |00\rangle_{AB}|e_{00}\rangle_{AB} + |01\rangle_{AB}|e_{01}\rangle_E + |10\rangle_{AB}|e_{10}\rangle_E + |11\rangle_{AB}|e_{11}\rangle_E \tag{1}$$

where Eve's states $|e_{ij}\rangle_E$ are arbitrary and, in particular, not necessarily normalized nor mutually orthogonal. We would like to reduce the number of states of this form that might underlay our seemingly safe $|\phi^+\rangle$ pairs. To do this, we exploit a characteristic property of $|\phi^+\rangle$; chiefly, the fact this it is an eigenstate of both $\sigma_1^{(A)}\sigma_1^{(B)}$ and $\sigma_3^{(A)}\sigma_3^{(B)}$ with eigenvalue $+1$ in both cases, as we prove now:

$$\begin{aligned}(\sigma_1^{(A)}\sigma_1^{(B)})|\phi^+\rangle &= (\sigma_1^{(A)}\sigma_1^{(B)})\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}(\sigma_1^{(A)}|0\rangle\sigma_1^{(B)}|0\rangle + \sigma_1^{(A)}|1\rangle\sigma_1^{(B)}|1\rangle) \\ &= \frac{1}{\sqrt{2}}(|1\rangle|1\rangle + |0\rangle|0\rangle) = +1|\phi^+\rangle\end{aligned}$$

(since σ_1 interchanges the first and second entries of a column two-vector), and

$$(\sigma_3^{(A)}\sigma_3^{(B)})|\phi^+\rangle = (\sigma_3^{(A)}\sigma_3^{(B)})\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$= \frac{1}{\sqrt{2}}(\sigma_3^{(A)}|0\rangle\sigma_3^{(B)}|0\rangle + \sigma_3^{(A)}|1\rangle\sigma_3^{(B)}|1\rangle)$$
$$= \frac{1}{\sqrt{2}}((-1)|0\rangle(-1)|0\rangle + (1)|1\rangle(1)|1\rangle) = +1|\phi^+\rangle$$

(since $|0\rangle, |1\rangle$ are themselves the eigenstates of σ_3 with respective eigenvalues -1, $+1$).

We can enforce these two properties as conditions on $|\Gamma\rangle_{ABE}$. In fact, Alice and Bob are always able to check that a large number or their pairs the eigenvalue $+1$ when acted upon with $\sigma_1^{(A)}\sigma_1^{(B)}$ or $\sigma_3^{(A)}\sigma_3^{(B)}$; if they ever obtain outcomes of 0 with a frequency that is not consistent with the error rate of the quantum channel, they will confirm that an adversary tampered with their ensemble of pairs and they can discard their set of entangled pairs and create new ones. Therefore, let us consider how the condition coming from $\sigma_3^{(A)}\sigma_3^{(B)}$ restricts the shape of the general state $|\Gamma\rangle_{ABE}$:

$$\begin{aligned}
&(\sigma_3^{(A)}\sigma_3^{(B)})|\Gamma\rangle_{ABE} = |\Gamma\rangle_{ABE} \\
&\rightarrow (\sigma_3^{(A)}\sigma_3^{(B)})(|00\rangle_{AB}|e_{00}\rangle_{AB} + |01\rangle_{AB}|e_{01}\rangle_E + |10\rangle_{AB}|e_{10}\rangle_E + |11\rangle_{AB}|e_{11}\rangle_E) = \\
&((-1)^2|00\rangle_{AB}|e_{00}\rangle_{AB} + (-1)(1)|01\rangle_{AB}|e_{01}\rangle_E + (1)(-1)|10\rangle_{AB}|e_{10}\rangle_E + (1)^2|11\rangle_{AB}|e_{11}\rangle_E) \\
&= |\Gamma\rangle_{ABE} = (|00\rangle_{AB}|e_{00}\rangle_{AB} + |01\rangle_{AB}|e_{01}\rangle_E + |10\rangle_{AB}|e_{10}\rangle_E + |11\rangle_{AB}|e_{11}\rangle_E) \qquad (2)
\end{aligned}$$

where we have again used the fact $|0\rangle, |1\rangle$ are eigenstates. This allows us to conclude that $|e_{01}\rangle = 0 = |e_{10}\rangle$, so we drop these terms at this point. Similarly, the other condition $\sigma_1^{(A)}\sigma_1^{(B)}|\Gamma\rangle_{ABE} = 1|\Gamma\rangle_{ABE}$ further requires:

$$\begin{aligned}
&(\sigma_1^{(A)}\sigma_1^{(B)})|\Gamma\rangle_{ABE} = |\Gamma\rangle_{ABE} \\
&\rightarrow (\sigma_1^{(A)}\sigma_1^{(B)})(|00\rangle_{AB}|e_{00}\rangle_{AB} + |11\rangle_{AB}|e_{11}\rangle_E) = \\
&(|11\rangle_{AB}|e_{00}\rangle_{AB} + |00\rangle_{AB}|e_{11}\rangle_E) \\
&= |\Gamma\rangle_{ABE} = (|00\rangle_{AB}|e_{00}\rangle_{AB} + |11\rangle_{AB}|e_{11}\rangle_E) \qquad (3)
\end{aligned}$$

where we have again used the fact that σ_1 swaps $|0\rangle$ and $|1\rangle$. Thus, we see that $|e_{00}\rangle_E = |e_{11}\rangle_E$, so that

$$|\Gamma\rangle_{ABE} = \frac{1}{\sqrt{2}}(|00\rangle_{AB}|e\rangle_E + |11\rangle_{AB}|e\rangle_E) = |\phi^+\rangle|e\rangle_E \qquad (4)$$

In other words, it is only possible for the AB pairs to be pure eigenstates of $\sigma_1^{(A)}\sigma_1^{(B)}$ and $\sigma_3^{(A)}\sigma_3^{(B)}$ only if they are separable or completely unentangled with respect to Eve's qubits (in fact, any other quantum states outside AB). Therefore, no potential measurement by Eve will provide information about Alice's and Bob's key, as long as Alice and Bob check the properties used above by measuring $\sigma_1^{(A)}\sigma_1^{(B)}$ and $\sigma_3^{(A)}\sigma_3^{(B)}$. This fact makes the private key safely private and represents an instance of the no-cloning theorem. In the more detailed words of Preskill [2]:
"*To verify the properties $\sigma_1^{(A)}\sigma_1^{(B)} = 1 = \sigma_3^{(A)}\sigma_3^{(B)}$, Alice and Bob can sacrifice a portion of their shared key, and publicly compare their measurement outcomes. They should find that their results are indeed perfectly correlated. If so they will have high statistical confidence that Eve is unable to intercept the key. If not, they have detected Eve's nefarious activity. They may then discard the key, and make a fresh attempt to establish a secure key.*"

There are different variations of the quantum key distribution procedure presented above. For instance, instead of using an ensemble of entangled pairs that was previously created and distributed, Alice can prepare the $|\phi^+\rangle$ ensemble herself, measure a single qubit from each pair, and then send the other half of each pair to Bob. This is equivalent to preparing and sending, for each pair, one of the four states

$$|\uparrow_z^+\rangle, |\downarrow_z^-\rangle, |\uparrow_x^+\rangle, |\downarrow_x^-\rangle$$

chosen at random with equal probability 1/4. This variation is called the BB84 quantum key distribution protocol, and it is fundamentally equivalent to the entanglement-based scheme.

Finally, we comment on an important fact about the robustness of quantum cryptography against errors due to channel imperfections. It can be shown that, if the channel error rate is low enough, the use of error-correcting techniques and checks of non-disturbance (such as the eigenvalue properties of $|\phi^+\rangle$ used earlier) suffices to make quantum communication completely safe, in the sense that the amount of information accessible by adversaries can be reduced below any $\epsilon > 0$ [2]. Nonetheless, the proof of this fact is outside the scope of this paper.

2 The No-cloning Theorem

As anticipated, the security of quantum key distribution depends an underlying fact of quantum information that prohibits the existence of a perfect copying machine for arbitrary quantum states. In other words, it is impossible to distinguish between nonorthogonal quantum states by performing measurement of them unless the original states are disturbed.

Proof:

The most general quantum copying machine takes any two quantum states $|\psi\rangle, |\phi\rangle$ and outputs two copies of each after a unitary transformation, possibly by using the environment F as a resource and modifying it in the process. Hence, we need to allow for a full Hilbert space larger than the product of the spaces for the original and copy states. The general form of such a transformation U is given by

$$\begin{aligned} U : |\psi\rangle_A|0\rangle_E|0\rangle_F &\rightarrow |\psi\rangle_A|\psi\rangle_E|e\rangle_F \\ |\phi\rangle_A|0\rangle_E|0\rangle_F &\rightarrow |\phi\rangle_A|\phi\rangle_E|f\rangle_F. \end{aligned} \tag{5}$$

Now, note that unitarity requires products to be conserved by the transformation U. Therefore we have:

$$\begin{aligned} {}_A\langle\psi|\phi\rangle_A &=_A \langle\psi|\phi\rangle_{AE}\langle 0|0\rangle_{EF}\langle 0|0\rangle_F \\ &=_A \langle\psi|\phi\rangle_{AE}\langle\psi|\phi\rangle_{EF}\langle 0|0\rangle_F. \end{aligned} \tag{6}$$

If we are trying to copy nonorthogonal states, then ${}_A\langle\psi|\phi\rangle_A \neq 0$ and Eq. 6 implies

$${}_E\langle\psi|\phi\rangle_{EF}\langle 0|0\rangle_F = 1. \tag{7}$$

But the states are normalized, so Eq. 7 can only be true if both factors equal 1. In particular, ${}_E\langle\psi|\phi\rangle_E = 1$, so that $|\psi\rangle$ and $|\phi\rangle$ must be the same state. Therefore, we confirm indeed that no quantum machine is able to perfectly copy two different, nonorthogonal quantum states while preserving the original states. This is the statement of the no-cloning theorem.

As a particular case, we see that the BB84 quantum key distribution protocol is safe against eavesdropping as a consequence of the no-cloning theorem, given that the four states $|\uparrow_z^+\rangle, |\downarrow_z^-\rangle, |\uparrow_x^+\rangle, |\downarrow_x^-\rangle$ being sent are not all mutually orthogonal, and their generation is random so that there is no way for the eavesdroppers to know which state is being sent.
On the other hand, if the only states being used in the protocol where $|\uparrow_x^+\rangle, |\downarrow_x^-\rangle$ or $|\uparrow_z^+\rangle, |\downarrow_z^-\rangle$ (in general, sets of mutually orthogonal states), there are of course corresponding choices of measurements that will identify one of the two states inside the pair without altering the state. This of course happens for the measurement of an operator that has the two possible outcomes (i.e. the two possible states being transmitted) as eigenstates. For instance, $|\uparrow_x^+\rangle, |\downarrow_x^-\rangle$ can be perfectly distinguished without alteration if we measure σ_x on them (and similarly for $|\uparrow_z^+\rangle, |\downarrow_z^-\rangle$ and σ_z), which of course implies that they can be copied perfectly without disturbing them. In fact, the notions of distinguishing between arbitrary states and copying them are equivalent. The direction just used is obvious. For the other direction, suppose that we are free to make copies of a quantum state, say, a qubit $|\phi\rangle$. Then, we can create an ensemble of identical $|\phi\rangle$s large enough to measure non-commuting observables such as $\sigma_x, \sigma_y, \sigma_z$ as many times as needed to determine their mean values. In the limit of infinite measurements of each σ_i, which is achievable thanks to our assumed ability to copy $|\phi\rangle$ infinitely many times, the mean values measure approach the spin components of $|\phi\rangle$ to a perfect accuracy. But this components together determine the qubit state $|\phi\rangle$ exactly. Therefore, the fact that nonorthogonal states cannot be distinguished implies also that it is not possible to arbitrarily copy quantum states, and the two concepts are thus equivalent.

Of course, it was reasonable to expect the fact that the no-cloning theorem does not prohibit the copy of orthogonal quantum states. Indeed, it is perfectly feasible to copy arbitrary bits in the context of classical information, and sets of orthogonal quantum states can be interpreted as classical bits of information. In other words, a qubit that is restricted to stay in $\{|0\rangle, |1\rangle\}$ (with no linear combinations of the two allowed) is just a classical bit with two possible values, and as such it can be copied in principle. In fact, this is illustrated by the following unitary tranformation:

$$\begin{aligned} U : |0\rangle_A|0\rangle_E &\to |0\rangle_A|0\rangle_E \\ |1\rangle_A|0\rangle_E &\to |1\rangle_A|1\rangle_E, \end{aligned} \tag{8}$$

which copies the first bit onto the second slot. But, of course, U does not act in the same way for other input qubits (that is, for states that are in a superposition of $|0\rangle$ and $|1\rangle$). This remark concludes our introduction to the no-cloning theorem and, by extension, to its central role in quantum cryptography.

References

[1] Rivest, Ronald L (1990). *Cryptography*, In J. Van Leeuwen (ed.). Handbook of Theoretical Computer Science. Vol. 1. Elsevier.

[2] Preskill, John (2001). *Lecture Notes for Ph219/CS219: Quantum Information and Computation, Chapter 4* , California Institute of Technology.