University of Vienna
Faculty of Physics

Lab-Course Theoretical Physics 2021S
Dispersion relations

Milutin Popovic & Tim Vogel

Supervisor: Beatrix Hiesmyr

11. Juli, 2021

Abstract

In this report we explore the ideas of teleportation and cryptography. First we discuss what teleportation means in a classical sense, we differ between transporting matter and transporting information. Then we prospect teleportation in the quantum world with a quantum computer. Finally we introduce the OTP encryption technique and explore the possibility of reducing the risk of an eves dropper by choosing the ansatz to generate a key with help of quantum theory, in cases of two and then three mutually unbiased bases.

Contents

1 Teleportation

1.1 Classical Teleportation

In science fiction books, movies and video games the idea of teleportation, that is almost instantaneous transportation, has been endorsed to full extent. Real life realization of this concept would bring enormous advantages and solve a lot of problems for humanity. This is partly allready put been into practice via 3D printers, but imagine we have constructed a technology that would allow us to send matter over large distances almost instantaneously. We can discuss a scenario where we would like to send an object or even a human body through this apparatus, questions instantly arise. At which level would we decompose the object so , how would we decompose and/or recompose it, how long would it take to send the pieces from one location to another etc. ? Let's say we want to send a human, decomposing it on the organ level doesn't really come into question since the transportation time would be the same as for the whole human. Going lower than the atom level decomposition would just take up too much energy, since we would have to split up the atom in electrons, protons and neutrons. The atom level decomposition sounds most promising since the molecules are just too massive and would also require a lot of energy to accelerate and wouldn't make the assembly process easier.

Now, how fast can we send the human body on the atom level, how long would it take. An average human body is about 70 kg and contains approximately $7 \cdot 10^{27}$ [1]. Let's say we can accelerate these atoms to 99% the speed of light ($v = 0.99c$). But to accelerate atoms we need to ionize them, so we would need to send an extra electron with the atom. To transport one such atom of the human body from one location to the other we quickly notice that distance is not a priority factor, e.g from earth to sun (distance $150 \cdot 10^9$ m), it would take around $t = 8.5$ min for one such atom. But we need to send $7 \cdot 10^{27}$ atoms, so sending them one by one is not an option. If we can send one mole of particles ($N_A = 6.022 \cdot 10^{23}$) per second this would reduce the time required to transport them significantly to about three hours and 15 minutes plus the transportation time of one such atom to the destination. However if we sent all the atoms of a human body, we would still need to deploy the information needed to reconstruct it. In that case we could think about only sending the blueprint, since atoms are not unique and can be a prerequisite for teleportation on the other side of the teleport.

The idea of the blueprint type approach would be to map the human body ($2x1x1m$) to a discrete space with a resolution of one lattice position (10^{-10}) which is either filled with an atom (hydrogen, oxygen, calcium, kalium) or doesn't contain an atom at all. This would allow us only to send information, that is the blueprint, to the destination where we would ultimately reconstruct the human body. This can be done by sending bits of information, for instance one lattice position only requires three bits since we need to encode 5 pieces of information, $\log_2(5) \simeq 3$.We can't round down since we need to store at least 5 pieces of information . Alternatively we could encode the information in two bits, or no bits at all. Meaning if the encoder finds two bits then there is an atom of a specific kind and if it finds no bits there is no atom. On the other hand a number with the resolution of 10^{-10} has 10^{10} possibilities and can be encoded in $\log_2(10^{10}) \simeq 34$ bits. We have $2 \cdot 10^{30}$ positions to cover, ultimately needing around $\log_2((2 \cdot 10^{30})^5) \simeq 504$ bits. A light pulse frequency of $5 \cdot 10^{14}$ this would take us about 12 ps to send all those bits.

1.2 Quantum Teleportation

Consider a scenario where Alice is given a unknown quantum system, e.g. a qubit. Even though she is not interested in what state the system is, she knows that Bob wants the same quantum system. By examining different scenarios she concludes that sending the qubit through a quantum channel, there will be a non vanishing possibility that the state is changed. Thus she wants to send Bob the information needed to construct an accurate copy of the quantum system.

Let's say that both Alice and Bob own an qubit, where the overall quantum state is an entangled state, e.g. one of the Bell states.

$$|e_1\rangle_{AB} := |\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}\Big(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\Big), \tag{1}$$

$$|e_2\rangle_{AB} := |\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\Big(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B\Big), \tag{2}$$

$$|e_3\rangle_{AB} := |\phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}\Big(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B\Big), \tag{3}$$

$$|e_4\rangle_{AB} := |\phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}\Big(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B\Big), \tag{4}$$

$$\tag{5}$$

Without loss of generality we choose the state $|\phi^+\rangle_{AB}$ that Alice and Bob have and the unknown quantum state

$$|\phi\rangle_G = \alpha|0\rangle + \beta|1\rangle \tag{6}$$

with the normalization condition $|\alpha|^2 + |\beta|^2 = 1$.

We can describe these three particles with the following state

$$|\Phi\rangle_G \otimes |\phi^+\beta_{AB} = (\alpha|0\rangle_G + \beta|1\beta_G) \otimes \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = \tag{7}$$

$$= \frac{1}{\sqrt{2}}(\alpha|00\rangle_{GA} \otimes |0\rangle_B \alpha|01\rangle_{GA} \otimes |1\rangle_B \tag{8}$$

$$+\beta|10\rangle_{GA} \otimes |0\rangle_B + \beta|11\rangle_{GA} \otimes |1\rangle_B). \tag{9}$$

To formally write α and β at Bobs states we need to express the equation as the tensor product of the kets with the subscript *GA* with the subscript *B*, which can be done by rewriting the *GA* kets as a superposition of the Bell states

$$|00\rangle_{GA} = \frac{1}{\sqrt{2}}(|\phi^+\rangle_{GA} + |\phi^-\rangle_{GA}), \tag{10}$$

$$|11\rangle_{GA} = \frac{1}{\sqrt{2}}(|\phi^+\rangle_{GA} - |\phi^-\rangle_{GA}), \tag{11}$$

$$|01\rangle_{GA} = \frac{1}{\sqrt{2}}(|\psi^+\rangle_{GA} + |\psi^-\rangle_{GA}), \tag{12}$$

$$|10\rangle_{GA} = \frac{1}{\sqrt{2}}(|\psi^+\rangle_{GA} - |\psi^-\rangle_{GA}). \tag{13}$$

Substituting these into equation 9 we get

$$|\Phi\rangle_G \otimes |\phi^+\rangle_{AB} = \frac{1}{2}\big(|\psi^-\rangle \otimes (-\beta|0\rangle + \alpha|1\rangle) \tag{14}$$

$$+|\psi^+\rangle \otimes (\beta|0\rangle + \alpha|1\rangle) \tag{15}$$

$$+|\phi^-\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) \tag{16}$$

$$+|\phi^+\rangle \otimes (\alpha|0\rangle + \beta|1\rangle)\big). \tag{17}$$

Thus the unitäry transformation operators are

$$U_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad U_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{18}$$

$$U_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad U_4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{19}$$

With this Alice can send the unknown state $|\phi\rangle_G$ to Bob. For this Alice needs to make a measurement in one of the Bell basis components $\{|e_\lambda\rangle\}_{\lambda=1,2,3,4}$. Depending on this she operates on the ket via $U_\lambda|\phi\rangle_B$ and bob needs to preform the opposite measurement of $U_\lambda^\dagger$.

What if we would like to find out what state Bob possesses before or after Alice performing the measurement on the system, without Bob knowing the outcome of the measurement.

Before the measurement Bob's state is

$$\rho_{GAB} = (|\Phi\rangle_G \otimes |\phi^+\beta_{AB})(\langle\Phi|_G^\dagger \otimes \langle\phi^+|_{AB}^\dagger) = \tag{20}$$

$$= \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{|\beta|^2}{2} & -\frac{|\beta|^2}{2} & 0 & 0 & \frac{\alpha\beta^*}{2} & -\frac{\alpha\beta^*}{2} & 0 \\ 0 & -\frac{|\beta|^2}{2} & \frac{|\beta|^2}{2} & 0 & 0 & -\frac{\alpha\beta^*}{2} & \frac{\alpha\beta^*}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{\alpha^*\beta}{2} & -\frac{\alpha^*\beta}{2} & 0 & 0 & \frac{|\alpha|^2}{2} & -\frac{|\alpha|^2}{2} & 0 \\ 0 & -\frac{\alpha^*\beta}{2} & \frac{\alpha^*\beta}{2} & 0 & 0 & -\frac{|\alpha|^2}{2} & \frac{|\alpha|^2}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{21}$$

taking the trace over the *GA* components gets us

$$\mathrm{Tr}_{GA}(\rho_{GAB}) = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{22}$$

where we used $|\alpha|^2 + |\beta|^2 = 1$.

On the other hand after the measurement, Bob still doesn't know the outcome and cannot apply the measurement $U_\lambda^\dagger$ for a λ provided by Alice. With this Bob has a chance of $\frac{1}{4}$th to get the state $|\phi\rangle_G$.

1.3 Teleportation on a Quantum computer

We want to consider an algorithm, consisting of Hadamard gates, CNOT gates, and a measurement in the computational basis $(|0\rangle, |1\rangle)$ at the end. The Hadamard gates are given as $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and the CNOT gates as $|0\rangle\langle 0| \bigotimes \mathbb{I} + |1\rangle\langle 1| \bigotimes \sigma_1$. The algorithm contains the following steps: We input a set of three qubits, all in the state $|0\rangle$. We shall name them q_1, q_2 and q_3. At first we apply a Hadamard gate to q_3, followed by a CNOT gate to q_2 and q_3 in the second step. Then we apply a CNOT gate to the first two qubits, whereas a Hadamard gate is applied to the third one. For the last three steps, we start by applying a Hadamard gate onto the first two qubits in step three. For the fourth step we use a CNOT gate onto q_2 and q_3 and finally, we apply a Hadamard gate to the same two qubits and end with a measurement. So, if we input the state $I = |000\rangle$, going through all the above mentioned steps, we obtain as a result:

$$O = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle) \tag{23}$$

This means, Bob obtains the original $|0\rangle$ in any way he measures, and thus a teleportation is successful. What if we now consider an arbitrary state, given by:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = q_1 \tag{24}$$

This means, our input now looks like

$$(\alpha|0\rangle + \beta|1\rangle)|00\rangle \tag{25}$$

As to expect, this input yields a different result:

$$O = \frac{\alpha}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle) + \frac{\beta}{2}(|001\rangle + |011\rangle - |101\rangle - |111\rangle) \tag{26}$$

$$= \frac{1}{\sqrt{2}}((|\phi^+\rangle + |\psi^+\rangle)\alpha|0\rangle + (|\phi^-\rangle + |\psi^-\rangle)\beta|1\rangle) \tag{27}$$

This again completes a successful teleportation, since Bob will measure the Eigenvalue of $|0\rangle$ with a probability of $|\alpha|^2$ and the one of $|1\rangle$ with a probability of $|\beta|^2$, which is the same as measuring the initial state in the first place.

2 Quantum Cryptography

2.1 One-Time-Pad

Nowadays computers use sequences of bits, of 0's and 1's to encode information. To represent the English alphabet, which consists of 26 letters, in a sequence of bits, we need a series of 0's and 1's that have 26 possible outcomes. With N bits we can represent 2^N possible outcomes, which means the English alphabet can be encoded in $\log_2(26) \to 5$ bits. Even thought $2^5 = 32$, we need to keep in mind that we need to encode at least 26 different outcomes which would then leave 6 outcomes empty. Introducing capital letters and special characters like "!?%$#...", we ultimately need 8 bits defining 1 byte. This type of character encoding (8-bit) is the standard for electronic communication and is referred as "American Standard Code for Information Interchange", ASCII for short.

The One-Time-Pad (OTP) is a encryption technique, that uses a one time single use pre-shared key. Let's say we want to encrypt the massage "BYE" in ASII encoding this would be

$$010000100101100101000101. \tag{28}$$

With this bit sequence we add another randomly generated one which is called the key. The operations used are the basic boolean algebra operations.

Massage:	010000100101100101000101
Key:	110101100110010101110011
Code:	100101000011110000110110

The same key decrypts the code into the massage.

Code :	100101000011110000110110
Key:	110101100110010101110011
Massage :	010000110100111101000011

It is mathematically proved, that if the key is really randomly generated, at least the same length as the massage, only used once and only the sender and the receiver are in possession of the key this encryption method is not crackable.

2.2 BB-84 Protocol

To make OTP encryption more secure, a protocol based on quantum mechanics, the BB-84 protocol is introduced. The BB-84 protocol allows us to generate a random key such that it is much harder for an eavesdropper "Eve" to acquire it. The protocol calls for two mutually unbiased bases and thus four possible outcomes. This can be for example a polarized photon that is either horizontally ($|H\rangle$), vertically ($|V\rangle$), $+45^\circ$ or -45° polarized. We can translate $|H\rangle, |+45^\circ\rangle \equiv 0$ and $|V\rangle, |-45^\circ\rangle \equiv 1$. In the Bra-Ket notation we can write

$$|+45^\circ\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \tag{29}$$

$$|-45^\circ\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \tag{30}$$

which can be achieved by rotating the polarization filter by $\pm 45^\circ$ in the x-z axis.

All in all Alice has four states in her repertoire to choose from which she then sends to Bob. Bob on the other hand can analyze the incoming photons based on their polarization with a dual channel analyzer, where the $|H/V\rangle$ analyzer distracts photons left/right and the $|\pm 45^\circ\rangle$ analyzer distracts photons left/right.

To construct a randomly generated key Alice writes down a random sequence of bits, for a each 0 she chooses from the states $|H\rangle$ or $|+45^\circ\rangle$ and for each 1 she chooses from the states $|V\rangle$ and $|-45^\circ\rangle$. These polarized photons are sent to Bob's analyzer, which leads to two possibilities, he either chose the correct basis on his analyzer or he doesn't. Meaning that in the mean Bob chooses the right basis $\frac{1}{2}$ of the time. After all photons are sent, Alice and Bob need to compare the basis they chose (which they can do completely publicly) and cross of the results where they choose the wrong basis. With this we have a randomly generated key that can be used for OTP encryption.

The only way a third person, we called her Eve, can interfere is if she places herself between Alice and Bob. For this Eve needs to measure the polarization of the photon Alice sent, and then with this information send a photon to Bob. If she doesn't send anything to Bob, Bob will notice somebody is interfering and Eve would get caught. When the basis is then compared Eve will have the same key Alice has.

Let us explore what would Bob get. Eve has a $\frac{1}{2}$ chance to choose the same basis that Alice choose. This ultimately leads to a $\frac{1}{4}$ chance that Bob and Alice have the wrong key, since Bob also needs to choose a basis.

To reduce the possibility that a third person is eavesdropping, Alice and Bob need to compare a small part of their measurement results. This results in the protocol needing to being carried out much longer for the sake of security.

2.3 Six-State-Protocol

The "Six-state-protocol" SSP is a generalization of the BB-84 protocol, where instead of two, three mutually unbiased basis are used resulting in 6 states. Thus, Alice and Bob have the chance of $\frac{1}{3}$ to choose the same basis, meaning they would have to cross out $\frac{2}{3}$ of the results before getting the key.

For Eve to not get detected there are two scenarios. In the first scenario she would need to choose the same basis as Alice and Bob, that is a probability of $\frac{1}{3}$ for each measurement. In the second scenario Eve

chooses the wrong basis but Bob measures in the right basis. Eve picking the wrong basis happens with the probability of $\frac{2}{3}$, **after** that Bob measuring in the correct basis would happen with the probability of $\frac{1}{2}$, since we are dealing with MUBs. Meaning Eve remains undetected with a probability of $\frac{1}{3}$.

For Eve to get detected she would need to measure the wrong results ($\frac{2}{3}$) and **after** Bob needs to measure the wrong results ($\frac{1}{2}$). Ultimately Eve gets detected with the probability of $\frac{1}{3}$.

The probability to detect Eve trivially scales with the number of measurements, meaning $P(\text{detected}) = 1-(\frac{2}{3})^n$ where n are the number of measurements. On the other hand the chance of not being detected after n measurements is $P(\text{not detected}) = 1-P(\text{detected}$, of course this doesn't mean Eve managed to get the right key. For Eve to pick the get the right key she would also additionally need to choose the right basis.

To even further minimize the risk of an eavesdropper Alice and Bob could compare small parts of their qubit string like in the BB-84 protocol.

References

[1] Wikipedia contributors. *Composition of the human body — Wikipedia, The Free Encyclopedia*. [Online; accessed 8-July-2021]. 2021. URL: https://en.wikipedia.org/w/index.php?title=Composition_of_the_human_body&oldid=1032434369.

[2] H. Bechmann-Pasquinucci and N. Gisin. "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography". In: *Physical Review A* 59.6 (1999), pp. 4238–4248. ISSN: 1094-1622. DOI: 10.1103/physreva.59.4238. URL: http://dx.doi.org/10.1103/PhysRevA.59.4238.

[3] Charles H. Bennett et al. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". In: *Phys. Rev. Lett.* 70 (13 Mar. 1993), pp. 1895–1899. DOI: 10.1103/PhysRevLett.70.1895. URL: https://link.aps.org/doi/10.1103/PhysRevLett.70.1895.