October 20, 2019

Abstract

1 Introduction

1.1 One Time Pad

The classical One Time Pad (OTP) is perhaps the oldest and most well known quantum cryptographic method. We will first discuss this protocol as a setup to the quantum version. Although originally proposed in 1884 [4], the OTP was first formalized and proven secure in 1949 [5]. Since then, the scheme has essentially remained the same due to its simplicity. A typical OTP goes as follows:

Alice and Bob start with a uniformly random key $k \in \{0,1\}^n$. Alice wants to send some message $m \in \{0,1\}^n$ to Bob. She encrypts m using the key k by means of an xor gate, generating payload $x^n = m \oplus k$.[1] After this step, she sends x to Bob who applies k again to x to receive m since $k \oplus x = m^n$. The assumption on Eve in this scheme is that she doesn't know k and can intercept x. However, if k was truly uniformly random, x is so too, leaving Eve with a random variable even after a successful interception. The main drawback of this scheme is the fact that the key has to be the same size as the message and that this key can only safely be used once.

1.2 Quantum One Time Pad

In the Quantum One Time Pad (QOTP) Alice and Bob again both share a uniformly random key $\alpha \in \{0,1,2,3\}^n$ and want to communicate some quantum state, ρ. Alice first transforms ρ with a random Pauli map, σ_α. After she has prepared this state she sends it to Bob over a quantum channel. He can then apply the Hermitian adjoint of this random Pauli resulting in the original ρ sent by Alice. This step exploits the unitary property of the Pauli maps. Eve, who doesn't know α, can measure the state sent from Alice to Bob. However, from her perspective, this is the fully mixed state. Mathematically, this can be seen as follows:

$$\rho' = \sum_{0}^{3} \frac{1}{4}\sigma_\alpha \rho \sigma_\alpha^\dagger = \frac{1}{2}\mathbb{I} \tag{1}$$

In principle, the QOTP is similar to the OTP. By means of encrypting a piece of information with a random key which is unknown to Eve but shared by Alice and Bob the latter can achieve

[1] In different realizations of the OTP, Alice has different methods of encrypting her message. With that being said, applying an xor to the key and the message is one of the most common versions.

secure communication. As a communication protocol, QOTP is not very efficient. Alice and Bob need use two bits as a key per bit of communicated information. However, as a scheme for the encryption of qubits it is actually applicable to various protocols as it allows for the eight-state encoding of qubits [2]. *See if need some more information here* *Ask question about combining dense coding with QOTP*

1.2.1 Diagrammatic Implementation

In the diagrammatic formalism we can construct a set of maps that have the same property as the Pauli maps in equation 1, the Bell maps. These are defined in terms of the Pauli matrices as follows [1]:

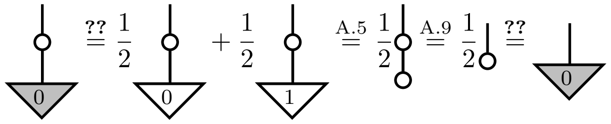
$$\sigma_0 = B_0 \quad \sigma_1 = B_1 \quad \sigma_2 = iB_3 \quad \sigma_3 = B_2 \tag{2}$$

In order to form diagrams for these Bell maps we have to understand them a little bit better. One of their properties is that they can be constructed from rotations on the Bloch sphere around the z and x axes [3], also known as bitflips around these axes. For random $u, w \in \{0,1\}^n$ and $\alpha \in \{0,1,2,3\}^n$ we can write this mathematically as follows:

$$Z^u X^w = B_\alpha \tag{3}$$

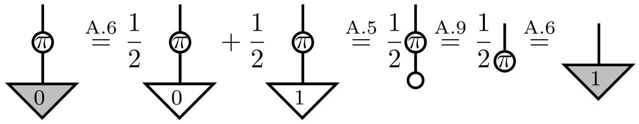
Where Z^u and X^w denote the maps that do a bitflip in the z and x bases respectively.

Let's see if we can construct these smaller constituents, Z^u and X^w, diagrammatically. Starting with X^w, remember that a bitflip in the x basis corresponds to a rotation around the z axis on the Bloch sphere. Therefore we need to find a diagrammatic map that either rotates the Bloch sphere around its z axis by π radians (X^1) or not (X^0). Since a single spider without a phase is the identity A.5 and the z basis is represented by the color white diagrammatically, we can use the white phaseless spider for the case where we don't flip the bit or rotate around the z axis. Let's send the 0 state through in the gray (x) basis to test if this map behaves as expected:



(4)

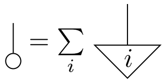
This map does seem to behave appropriately. We see that whenever we send a gray 0 through, we get a gray 0 as output. Following similar logic, we could also use the white spider with a π phase to make a rotation around the z axis, and thus a bitflip in the x basis. Let's test if this works too:



(5)

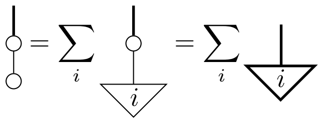
These maps do exhibit the correct properties. Indeed, whenever we send a gray 1 through we also get the expected results. It seems that we have formed the X^0 and X^1 maps. While we will not go through the full math here, the Z^0 and Z^1 maps follow very similar logic and also behave as expected. Perhaps unsurprisingly, the former is a gray phaseless spider whereas the latter is a gray spider with a phase π.

Now that we have created our four constituent maps we are in principle ready to make any Bell map of choice. However, we do not want to make a choice, we want to select a random Bell matrix. We still need to find a diagrammatic method to generate a random u and w on which our choice of Bell matrices depend. Recall that generating a random bit is the following diagram A.5:



(6)

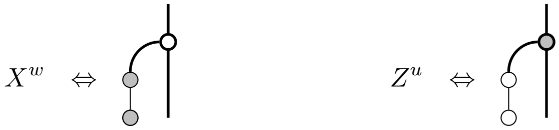
We could encode this random classical bit into a qubit as follows:



(7)

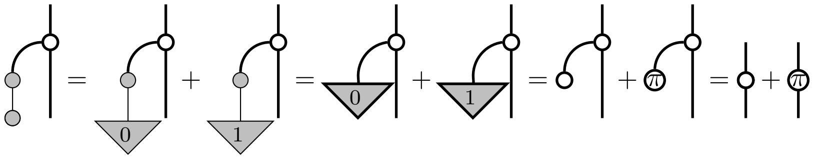
The previous two equations are entirely analogous for the gray (x) basis.[2]

We now have the necessary ingredients to make a map that applies a random bitflip or not in x and another map that makes a random bitflip or not in z. The results are as follows:



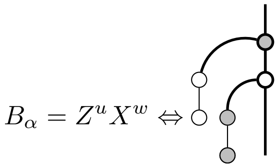
(8)

Let's confirm that the diagrammatic version of X^w does indeed behave as expected:



(9)

So depending on whether the random bit was a 0 or a 1, we get the map from equation 4 (X^0) or the map from equation 5 (X^1). Again, this derivation is analogous for the map Z^u. We have thus successfully made the constituents to our Bell matrices. The random Bell map itself is then as follows:

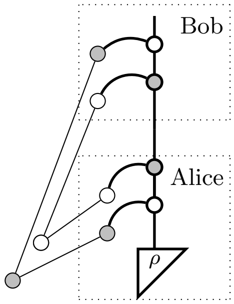


(10)

To make a diagrammatic version of QOTP without Eve we need to compose the Hermitian adjoint of this Bell map to its input. The bottom Bell map can then be seen as Alice encrypting her state and the top Bell map can be seen as Bob decrypting this state. We also need to make

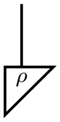
[2] In fact, we can make an even stronger statement about the diagrams in equation 7: They are actually equal to the analogous diagrams in the gray basis. Note that the rightmost diagram is the adjoint of discarding, which can be interpreted as preparing the fully mixed state, up to a number. Since this state is independent of the basis, these diagrams of white basis are equal to the analogous diagrams in the gray basis.

sure that Alice and Bob make the same choice in α and thus use the same Bell map. This can be done by connecting the outputs of the spiders that generate the random numbers to the Bell maps of both Alice and Bob. In all, this makes QOTP without Eve to be the following diagram:



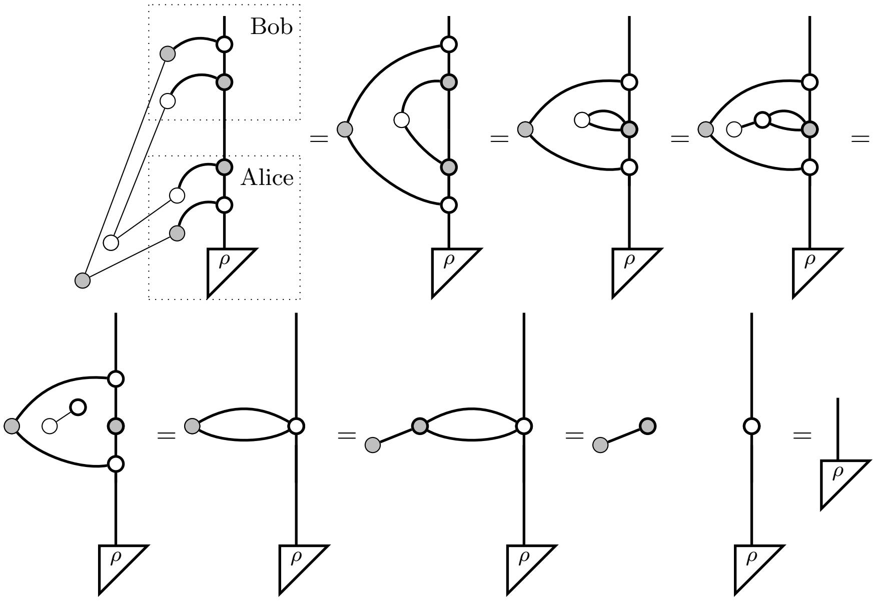
(11)

For this protocol to be a good candidate for communication we need equation 11 to reduce to the following:



(12)

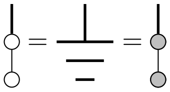
This simply states that Alice's qubit is sent to Bob through the identity map. We already know that this is true due to the unitarity of the Bell maps. Diagrammatically, the proof is as follows:



(13)

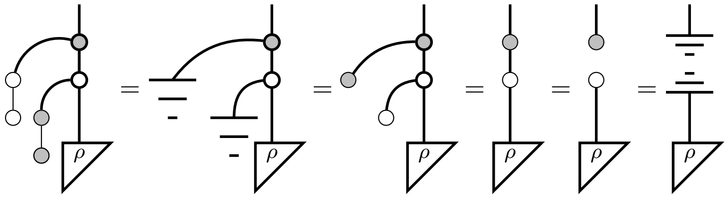
Now that we have diagrammatically shown that QOTP without Eve is indeed a communication protocol, we can start to introduce Eve. First of all, let's see what the result is of Alice encrypting her state by means of a Bell map. We will thus analyze QOTP purely as an encryption protocol.

To understand what happens in this case diagrammatically we need to first extend equation 7. Note that RHS of this equation is actually the Hermitian adjoint of discarding as it is defined in 33, which is in turn the fully mixed state. Since this state is independent of the choice of basis we can construct the following equation:



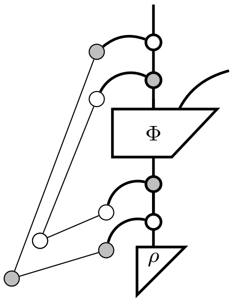
(14)

Using equation 14 we can prove that whenever Alice encrypts a state with a Bell map and discards her classical u and w she prepares the fully mixed state:



(15)

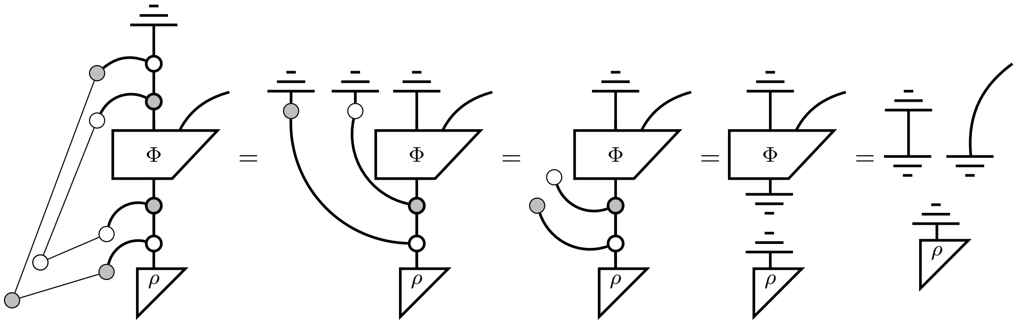
This might give some intuition for what Eve would receive after Alice has encrypted her state. However, one major difference between QOTP as an encryption protocol and QOTP as a communication protocol that in the latter case Alice can not discard her classical u and w. Somehow she has to communicate them with Bob. The diagram of QOTP as a communication protocol and Eve with the ability to intercept the quantum state but not u or w is as follows:



(16)

Where Eve controls the map Φ *and receives the rightmost output of this map.*

Let's see what happens when we look at this situation from Eve's perspective and thus trace out (discard) Bob's channel.



(17)

The third diagram in equation 17 is up until Eve's map Φ the same as equation 15. We therefore see that from Eve's perspective Alice gives her the fully mixed state due to the Bell map that she applies to her original state. So even as a communication protocol, the Bell map is responsible for encrypting the state such that Eve can extract no information from it.

Finally, we can check that whenever we trace out (discard) the state of Eve, Alice and Bob can communicate. **But this does not always have to be true!!! Eve can just completely jam the state of Alice, ask this!!!**

1.3 Quantum Teleportation

In quantum teleportation Alice and Bob want to communicate a qubit, ρ_1, using the fact that they share an EPR pair, ρ_{23}, and a classical communication channel. Note that the subscripts in this paragraph help keep track of the different particles present. Subscript 1 refers to Alice's particle, 2 to her side of the EPR pair and 3 to Bob's side of the EPR pair. Alice measures ρ_1 together with ρ_2 in a Bell measurement, entangling these two states to give the total entangled state of ρ_{123}. This projects ρ_3 to one of four possible pure states dependent on the result of the Bell measurement done by Alice. Using the classical communication channel, Alice can send this measurement outcome to Bob in two classical bits. In order for Bob to extract ρ_1 from his part of the EPR state, ρ_3, he needs to apply to it the Bell map that corresponds to the measurement outcome of Alice's Bell measurement.

The name "Quantum Teleportation" might lead one to think that it includes the teleportation of information. However, this is not the case. This protocol does not achieve faster than light communication. Although the projection of ρ_3 onto a pure state happens simultaneously with Alice making the Bell measurement, in order for Bob to receive any information one ρ_1 from ρ_3 he must know the result of Alice's Bell measurement.

References

[1] Bob Coecke and Aleks Kissinger. *Picturing Quantum Processes*. Cambridge University Press, Cambridge, 2017.

[2] Manon de Vries and Boris Skoric. Quantum Key Recycling with Eight-State Encoding. *Cryptology ePrint Archive*, 2016.

[3] Ivan Djordjevic. Chapter 7 - quantum error correction. In Ivan Djordjevic, editor, *Quantum Information Processing and Quantum Error Correction*, pages 227 – 276. Academic Press, Oxford, 2012.

[4] John Markoff. Codebook Shows an Encryption Form Dates Back to Telegraphs, 2011.

[5] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 1949.

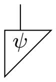
A Diagrammatic Overview

This section serves as a concise introduction to the diagrammatic method for a reader who is familiar with quantum mechanics and Dirac notation. It also functions as a section supplementary to the report which can be used to look up diagrammatic concepts.

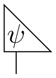
A.1 Keywords

A.2 States, Effects, and Hermitian Operations

The **ket** in Dirac notation is defined as a triangle with its sharp edge down in diagrammatic notation. It can be interpreted as the preparation of a state, in this case ψ. It is referred to as **state** throughout the thesis.

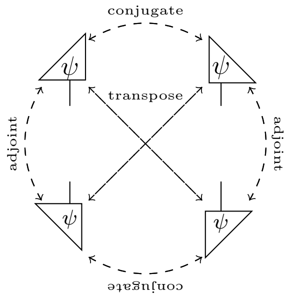
$|\psi\rangle =$  (18)

The **bra** in diagrammatic notation is the flipped state, and is referred to as **effect**.

$\langle\psi| =$  (19)

Triangles are the smallest building blocks in the diagrammatic notation. Most diagrams can be reduced to just triangles. This makes them a powerful tool for translating complicated diagrams to Dirac notation and vice versa.

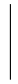
From the fact that the **Hermitian adjoint** of a bra gives a ket and reversedly it follows that the operation of flipping a diagram around its horizontal axis corresponds to taking the Hermitian adjoint. Flipping a diagram around its vertical axis is also a legal operation and this corresponds to taking the **Hermitian conjugate**. Both of these operation applied together takes the **transpose**. All of these diagram operations can be summarized as follows:

 (20)

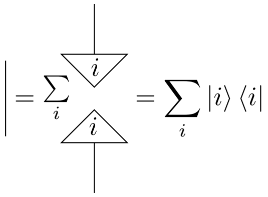
Note that there are also triangles that are not on their side. These are representations of objects that are not affected by conjugate transformations, such as integers.

A.3 Wires

The identity map in the diagrammatic notation is given by the following diagram, referred to as a **wire**.

 (21)

A wire can be reduced to triangles (and subsequently to a ket and a bra) as follows:

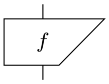


(22)

Every wire has an associated **system type**, the space of the information that it carries. In the context of this report, the system types are Hilbert spaces or the tensor product of Hilbert Spaces.

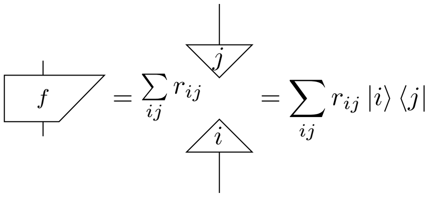
A.4 Maps

A **linear map** is given by the following diagram:



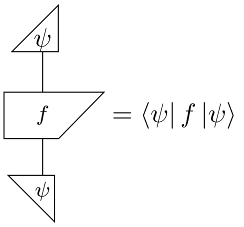
(23)

We can find the equivalent form in Dirac notation as follows:



(24)

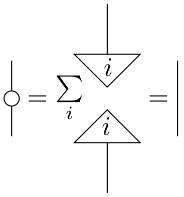
In the context of a bra and a ket, we can translate the diagrammatic linear map to Dirac notation as such:



(25)

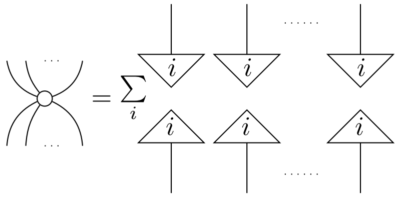
A.5 Spiders

A **spider** is a special map which functions as a Kronecker delta. It forces the inputs to be the same as the outputs. In the case where we have one input and output this gives a trivial result:



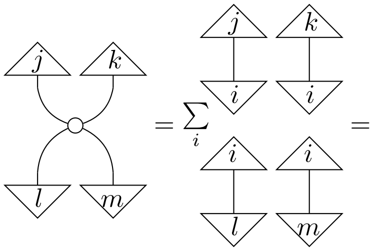
(26)

In the case where there are multiple outputs and inputs it forces all to be the same:



(27)

By applying arbitrary in- and outputs we can see how the **Kronecker delta** arises from Dirac notation. The following example is for two two inputs and two outputs but the same principle extends to an arbitrary amount of in- and outputs.



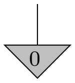
$$\sum_i \langle i|j\rangle \langle i|k\rangle \langle l|i\rangle \langle m|i\rangle = \delta_{jk}\delta_{lm}\delta_{jl}$$

(28)

Spiders with single in- or outputs also exist. A spider with a single output is the creation of a random variable and a spider with a single input is the deletion of any variable.

A.6 Colours and Bases

In the diagrammatic notation, the **colour** of an object such as a spider or a triangle determines its base. In the context of this paper it is sufficient to define two orthonormal **bases**, the Z and X bases. The Z basis has white diagrammatic elements, for the X basis they are gray. The following is an example of how to translate between bases in this notation:



$$= \frac{1}{\sqrt(2)}(\boxed{white0} + \boxed{white1}) \qquad (29)$$

This equation is of course entirely analogous to its Dirac notation counterpart, with $|-\rangle$ and $|+\rangle$ being the orthonormal basis states in the X basis and $|0\rangle$ and $|1\rangle$ the orthonormal basis states in the Z basis:

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad (30)$$

A.7 Doubling

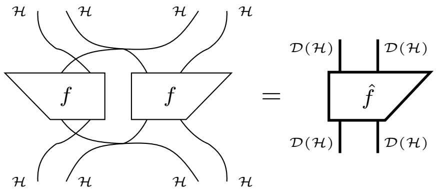
Doubling is the operation of taking the tensor product of a diagram with itself. In the usual case, where the system type of a single wire is a Hilbert space ($\mathcal{H}$), the doubled wire has the set of density matrices on that Hilbert space as system type.:

$$\mathcal{H} \oplus \mathcal{H} = \mathcal{D}(\mathcal{H}) \qquad (31)$$

Where $\mathcal{D}(\mathcal{H})$ is the set of density matrices on $\mathcal{H}$. $\oplus$ is the tensor product.

Doubled maps and and states represent **pure** maps and states. Single maps and states represent their **mixed** counterparts. The most intuitive interpretation, and how it is mostly used in this report, is that the single wires represent classical data and thick wires represent data encoded into a quantum state.

Doubling in diagrammatic notation is nothing more than placing a second conjugate diagram next to the original diagram. In doubled diagrams lines are drawn thick, for example:

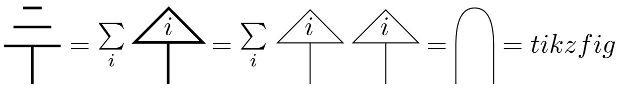


(32)

The notation of a map with a hat, such as $\hat{f}$, means that that map is pure.

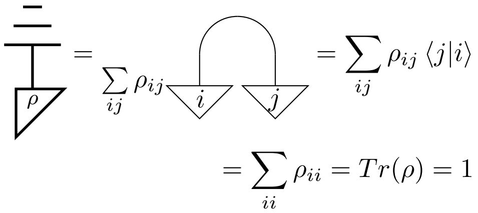
A.8 Discarding

Discarding is the process of removing part of a diagram from the whole, or removing the whole diagram altogether. For doubled diagrams it is defined as follows:



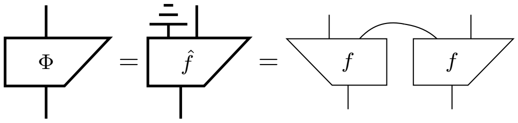
(33)

It is trivial to see that applying discarding to any arbitrary (normalized) state always results in the number 1. In fact, discarding a state or map is equivalent to taking its **trace**. As an example, we discard an arbitrary normalized **density matrix**, ρ:


ρ
$=$
$\sum_{ij} \rho_{ij}$
i
j
$= \sum_{ij} \rho_{ij} \langle j|i\rangle$
$= \sum_{ii} \rho_{ii} = Tr(\rho) = 1$

(34)

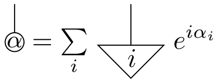
Discarding is not a pure map. It connects the two counterparts of a doubled state by a single wire. This allows discarding to be used to purify any arbitrary state or map. For the case of a map Φ **purification** is as follows:



(35)

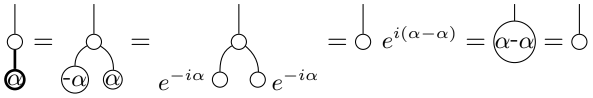
A.9 Phase Spiders

Phases spiders follow the same rules as normal spiders. However, perhaps unsurprisingly, they carry a **phase**. This phase is subject to a new set of rules which is evident from the definition of the phase spider.



(36)

An example of the principle that underlies these rules is given below, which shows how the phase gets eliminated in the process of **decoding** a quantum state to classical information.



(37)

Equation (37) exemplifies how phases behave when spiders fuse, they add. Furthermore, it shows how the phase gets eliminated when one tries to extract classical information, also known as measure, a quantum state.