Manuel Rosenthaler

BB84 Protocol

Overview

In this work we take a closer look at the BB84 protocol. The BB84 protocol is a cryptographic method basesd on quantum mechanical processes to establish a secure line on which communication can be performed.

The protocol was invented in 1984 by Charles Bennett and Gilles Brassard. As a small sidenote: Thats where the Name comes from. BB84 stands for "Bennett and Brassard (protocol, from 19)84". It is the first quantum cryptographic protocol in history.[1] The special thing about cryptographic methods basesd on quantum mechanical processes is that the two main parties of the communication - the receiver and the sender - are able to determine whether a (supposedly malicious) unknown third party is listening in on the line. This is done by using the property that the state of the qubits can change during a measurement, that a measurement *influences* the state of a quantum object. Furthermore, a quantum state cannot be reproduced with certainty. This statement is based on the *no-cloning theorem*[2]

Of Alice, Bob and Eve

Let's assume we have Alice and Bob. They would like to exchange encrypted messages with each other. However, they know that somewhere out there lurks the evil Eve to uncover their most secret secrets[3]. To achieve this, Alice and Bob want to agree on a secret key with which they can encrypt their messages. The only problem is that they did not agree on this key beforehand and now they have to agree on a key via the potentially corrupted public channel(s). So how can they agree on a key without Eve getting the key as well, if she is listening to the line? The BB84 protocol poses a solution to this problem.

As a prerequisite for the BB84 protocol you need two things. First, a classic communication line, with which Alice and Bob can exchange classical bits, and second, a quantum channel, with which qubits can be exchanged. Also they agree that the sent qubits are either in the X base or the Z base.

Mathematically speaking, the different states can be expressed as follows. We get

[1] As seen in [WIKIPEDIA, 2020]
[2] See e.g. [wik, 2020]
[3] Yes, puns intended.

four states described by[4]:

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

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

$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

So in this case we use exactly the X and Z base states.

The protocol starts with Alice creating a series of qubit. Alice makes sure to randomly use either the X-base or the Z-base for every qubit she generates. Alice notes down exactly which qubits in which bases were generated by her and sends them to Bob. She can achieve this by taking the following approach:

If Alice wants to create qubits, she first creates a string of normal randomized bits, consisting of zeros and ones. Then, Alice transforms these classic bits into qubits by matching the bits with a corresponding base. This could look like this[5]:

Initial classical bit string: 1000101011010100

use of the following bases: ZZXZXXXZXZXXXXXX

yields the following results: $|-\rangle\,|0\rangle\,|+\rangle\,|0\rangle\,|1\rangle\,|0\rangle\,|1\rangle\,|+\rangle\,|1\rangle\,|-\rangle\,|+\rangle\,|-\rangle\,|0\rangle\,|-\rangle\,|0\rangle\,|+\rangle$

After sending the qubits over the quantum channel there is no way for Bob (nor for Eve for that matter) to find out in which bases the qubits were generated.

Bob receives the qubits sent by Alice. Since Bob does not know in which bases the qubits were generated, Bob randomly selects a base - either X or Z base - for each measurement of a single qubit to measure the qubits received.

Suppose Alice generated and sent a qubit in the X base and Bob randomly measures in the X base as well. In this case, Bob will get the exact result - the true value of the qubit that was originally generated by Alice. However, if Bob measures in the other, Z base, there is a 50% chance that Bob will get the wrong result.

[4]from [WIKIPEDIA, 2020]
[5]Example taken from [enc, 2020]

So first of all, we have a 50% chance that Bob will choose the wrong bases, but if we choose the wrong bases, there is still a 50% chance that Bob will get the right qubit. This means that - without the intervention of Eve - Bob's qubit strings should be $50\% + 25\% = 75\%$ equal to Alice's qubit strings.

However this number changes, as soon as Eve tries to interfere with the quantum channel. Suppose Eve has managed to hack into the quantum channel and intercepts the qubits sent by Alice. Eve also has no way of knowing the bases on which the qubits were created. Therefore, just like Bob, she measures each qubit on a randomly selected X or Z base. She will achieve a hit accuracy of 75%, just like Bob before without Eves interference. Eve continues to try to copy/generate the intercepted qubits after her measurement and send them back to Bob in the Quantum channel so that he doesn't notice Eve's interference. But she encounters a big problem.

Now, as we have already seen at the beginning, there is a fundamental law that states that it is not possible to make an exact copy of a qubit. The no-cloning theorem. It states that it is impossible to determine the full quantum state of a single quantum object. Every measurement of a quantum state projects the state onto the bases in which the measurement was made. So all you can get is a value of the projection of the quantum state on the bases you have chosen.

Eve does not know in which bases the qubits she stole were created. Therefore Eve cannot generate the exact qubit sequence in the correct bases with 100% certainty. This is the central circumstance that Bob and Alice can exploit to find out if theyr Quantum Channel was intercepted.

Furthermore, all the qubit get destroyed when they are measured. Eve cant measure the qubits and also forward them to Bob at the same time. It is after all also a fundamental property of quantum mechanics that measuring a quantum object changes or destroys its state. Therefore Eve decides after each measurement of hers to generate a *new* qubit in the same base that she has determined by her measurement and send this qubit to Bob, in hopes that he wont notice her interference. However, Eve also has a 50% chance that she measures the qubit in the wrong base. Therefore, in that case, she will send Bob a qubit in the wrong bases. In total, only 75% of the qubits that arrive at Bob's are equal to the original qubits sent by Alice. So Bob has to make his measurements on a qubit set that already contains wrong qubits!

We can even determine how much of a percentage of Bobs measurements will still be the same to Alices qubits, after Eves interference. We know that only 75% of the

qubits Bob receives are correct, i.e. are *the same as Alice originally generated and sent to Bob*.

Based on the same considerations we made above, only 75% of Bob's measurements on the 75% correctly by Eve sent qubits will be correctly measured by Bob again and thus are the same as Alice have. (50% of the time he chooses the correct base, the other 50% Bob has a 50% chance to randomly get the correct result, resulting in 75%).

But, Bob applies his measurements also to the 25% qubits where Eve used the wrong base! And even in this 25%, Bob still has the possibility to measure the qubits originally sent by Alice. Of the 25% wrong qubits, bob has a 50% chance to chose the opposite base in that Eve sent him the qubit. Furthermore he has in this case again 50% chance to get the correct, originally by Alice intended result, just by chance. This means that the amount of matching qubits between Alice and Bob *with* the intervening Eve amounts to:

$$75\% \text{ of } 75\% + 50\% \text{ of } 50\% \text{ of } 25\% = \underline{\underline{62.5\%}}$$

Thus, when Eve interferes with the quantum channel, Bob's qubits will not be 75% identical to Alice's, but only 62.5%. This difference in the percentage values can be used to determine if Eve was listening.

Now, independent of whether Eve has corrupted the channel or not, Bob next communicates the bases (not his measurement results!) he used to measure each qubit via the classical channel. Alice compares the bases with the ones she used to generate the qubits and discards those qubits from her list where Bob used the wrong bases. In addition, Alice also communicates to Bob which qubits he has to discard. As a result, both Alice and Bob end up with the same qubits sequences - given that Eve has not compromised theyr channel.

In order for Alice and Bob to find out if Eve was listening to the channel, they go through the so-called *reconciliation* process. Alice and Bob, after throwing away the qubits in which Bob used the wrong bases for measurement, should have the same quantum objects. However, if Eve interfered and sent 25% wrong qubits to Bob, this means that for 25% of the sent qubits, Bob could receive a wrong result, despite measuring in the correct bases. Thus he will then have qubits that differ from Alice's - even though Alice and Bob can be sure that all qubits in Bob's possession were measured in the correct bases.

To find out if there were an interference, Bob chooses a subset of his qubits and sends them to Alice. If Alice sees that all the bits sent by Bob match hers, she can be sure that Eve did not intercept her channel and can use the remaining qubits to create a secret key with Bob. However, if there are differences in the subset's qubits sent by Bob, they know that Eve has been listening in on the line. So the line is not safe to agree on a key yet.

Calculation of the probability that Eve will remain undiscovered

In order to calculate the chance that Eve's interventions will remain undetected, we have to consider three cases.

If Eve happens to use the same measurement bases that Alice used to create the qubit, her intervention remains undetected because she can send the correct quantum state to Bob.

However, if Eve chooses the wrong bases for her measurement, there is still a 50% chance that Bob will measure the correct qubit. This is shown in the following figure.

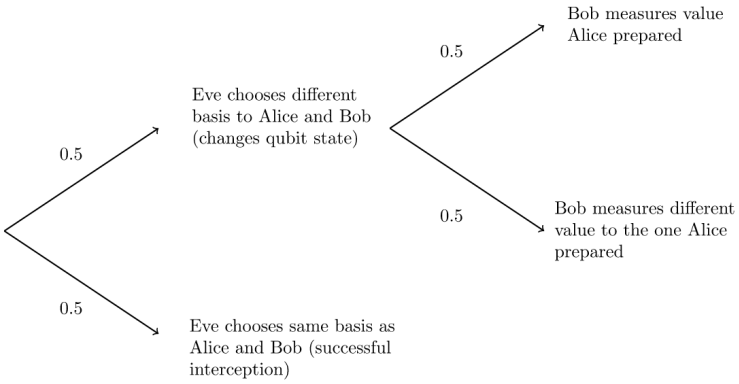

Figure 1: Graph that shows the probability tree of the different possibilities that could happen when Eve is interfering the channel. Source: [enc, 2020]

So the chance that Eve's interference will remain undetected is 75% for every qubit Bob receives. This results in the probability that Eve will remain undetected for a number of n transmitted qubits of[6]

$$P(undetected) = 0.75^n$$

So if Alice sends only 1 qubit to Bob, the chance that Eve's interference is not detected is 75%. However, if e.g. 50 qubits are sent, the probability that Eves

[6]Formula also from [enc, 2020]

interference is *not* detected amounts only to 0.00006%.

How it's done in reality

Now that we have a general idea about how the BB84 protocol works, let's delve a bit deeper into how you can in reality produce and send qubits.

First of all i want to note, that, despite using the X and the Z bases in our example, of course all bases would work as long as the two different bases are mutually unbiased as well as the bases them selves have two orthogonal states.

In reality, however, the different quantum mechanical bases are often produced as follows: A single photon source is used to produce a photon. After its creation, the photon is polarized using a polarization filter. Two different polarization gates are used, which stand for e.g. the X base and the Z base. Such a structure can be observed in Figure 2.

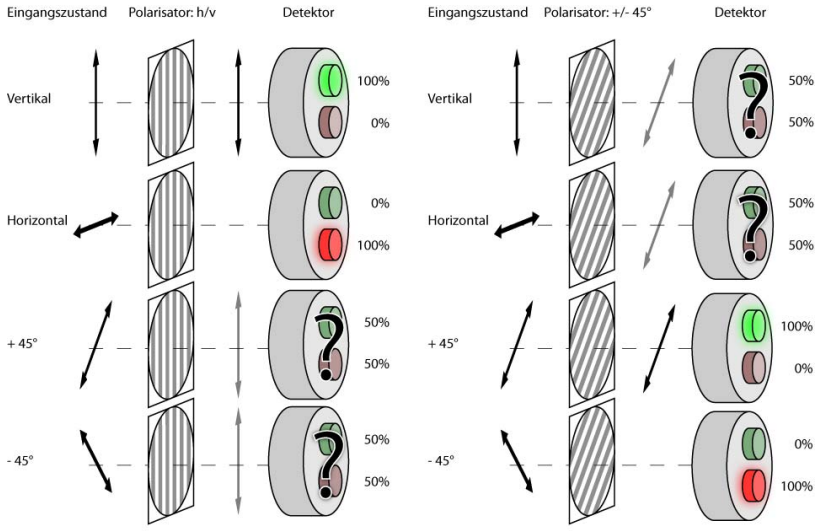

Figure 2: Image of a setup of polarization filters to measure the polarization of a photon. Source: [pol, 2020]

We can see in the figure that with the help of the polarization filters in the presented orientations, exactly our four quantum states can be represented. The horizontal and vertical polarization represent one base, the polarization filters rotated by 45 degrees represent the other base.

Once we've generated our photons, we can send them e.g. via a glass fibre cable to our recipient. Once the photons have arrived there, a setup very similar to that used to generate the polarized photons can also be used to measure the polarization

of the photon again.

As we have already seen, it is not possible for the receiver to know which polarization filter to use. Therefore, he has to randomly select a polarization filter with which he will perform the measurement. As we have seen in figure2, if we also use the horizontal polarization filter for a vertically polarized photon, we will get correctly a 0 (we wont detect a photon since it gets blocked by our polarization filter). However, if we use a polarization filter that is tilted by 45° degrees from the horizontal one, we only have a 50% chance to get the correct result.

Thus, with the help of photons and polarization filters, one can create exactly the four states required for the BB84 protocol. The photons can be transmitted via fiber optic cables and at the other end the polarization can be measured with a light sensor and the same set of polarization filters. This would provide the real physical requirements for a functioning BB84 protocol.

References

[pol, 2020] (2020). *Image of a setup of polarization filters to give a photon a polarization.*. https://qig.itp.uni-hannover.de/quanth/index.php/A3/Das_BB84_Kryptographie_Protokoll.

[enc, 2020] (2020). *Qiskit textbook about the BB84 algorithm*. https://qiskit.org/textbook/ch-algorithms/quantum-key-distribution.html.

[wik, 2020] (2020). *Wikipedia article about the no-cloning theorem*. https://en.wikipedia.org/wiki/No-cloning_theorem.

[WIKIPEDIA, 2020] WIKIPEDIA (2020). *Wikipedia article about the BB84 protocol*. https://en.wikipedia.org/wiki/Quantum_key_distribution.