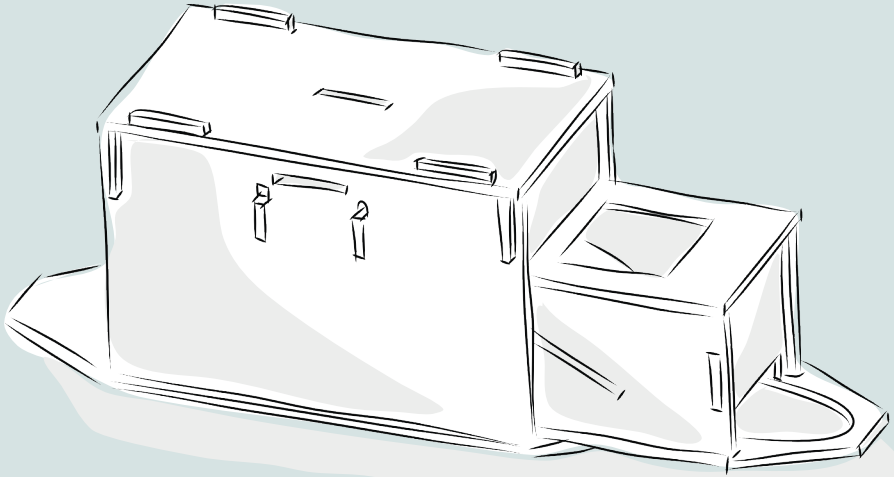
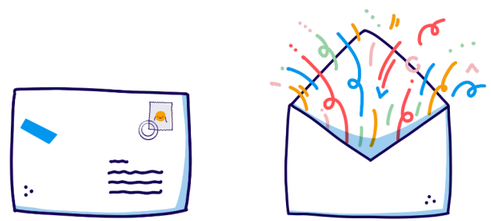
Instruction

TüftelAkademie

Quantum encryption

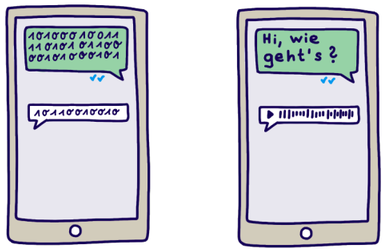
Qey-Gen - The Quantum Key Generator

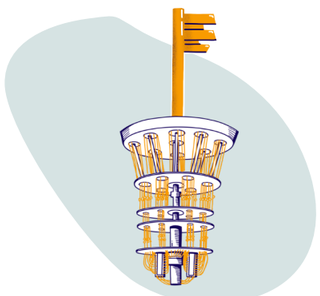




Introduction

A major concern of today's world is the transmission of confidential messages. For this purpose, one often generates a secret key with which one can make messages unreadable for strangers. But the problem is, both persons have to agree on a key beforehand. But how is this supposed to work without someone already listening in on the key exchange?



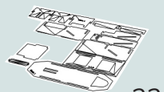


In order to make our messages tap-proof in the future, people have been looking into a subfield of physics, quantum mechanics, for some time. Because we will see that extremely secure (quantum) keys can be generated with the help of quantum mechanical phenomena.

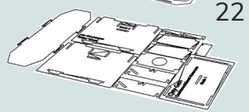
Content:

10 playing sheets

Coin



22 wooden components (Divided into 2 bags)



Instruction

Build:

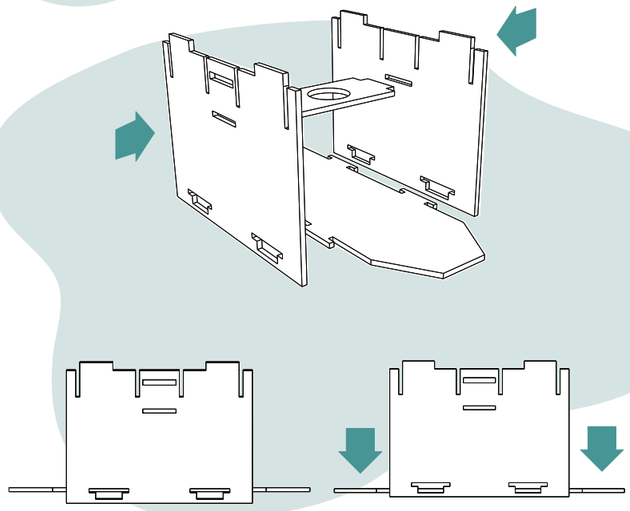
In the following section you will get step-by-step instructions to assemble the box or you can simply watch our **videos**.

Video tutorial

https://bit.ly/3hHrbhr

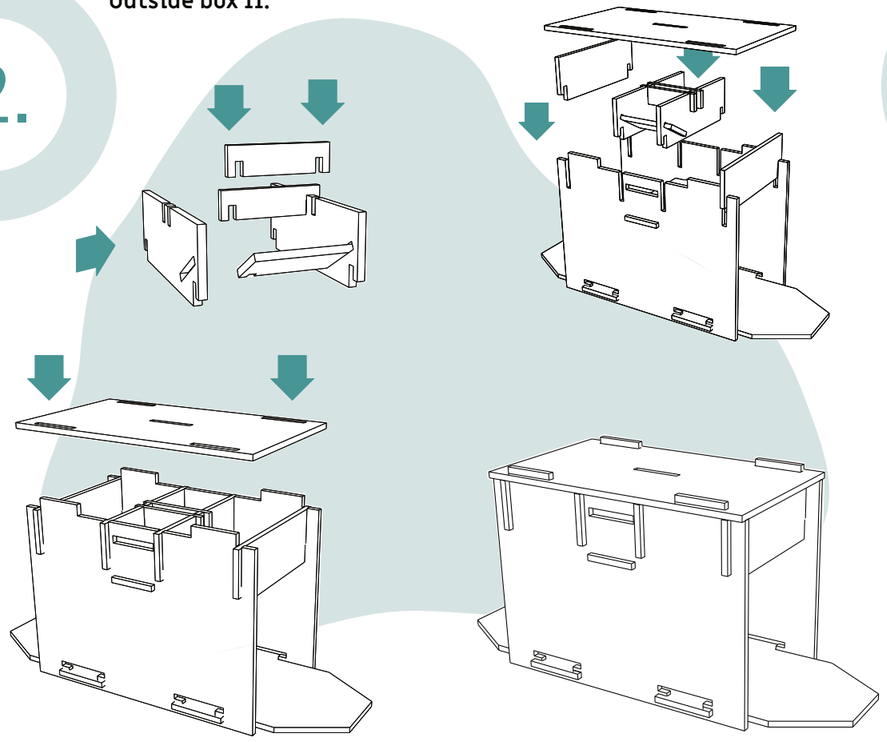
1.

Outside box I.



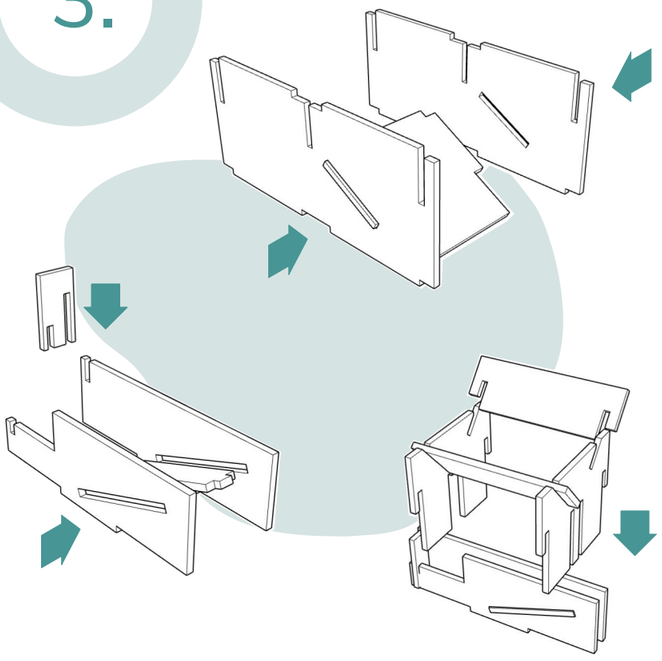
2.

Outside box II.



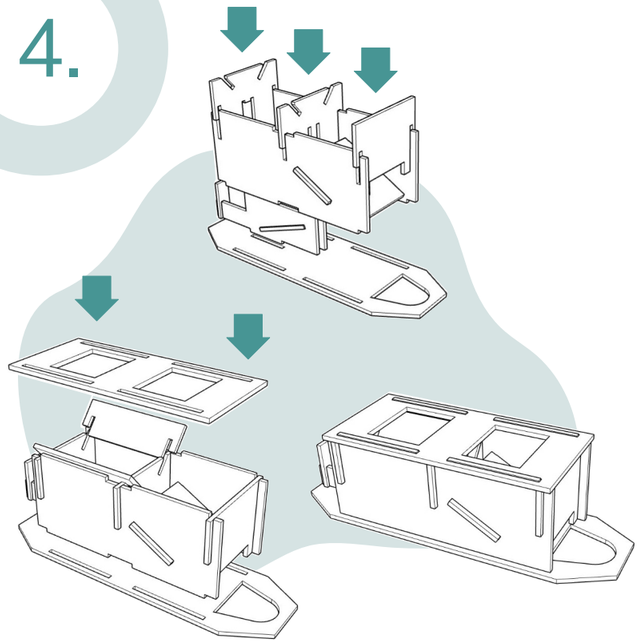
3.

Inside box I.



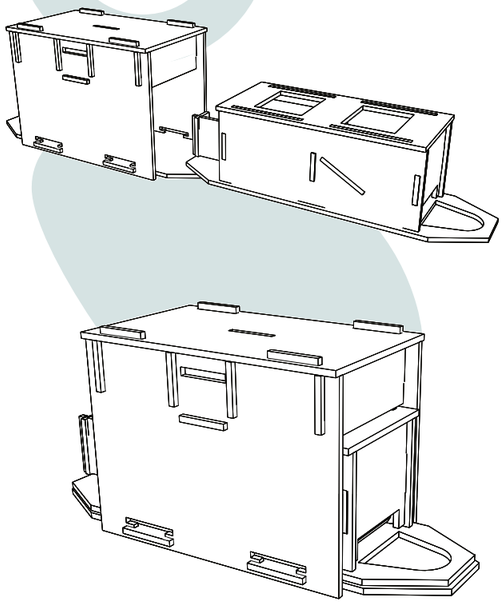
4.

Inside box II.



5.

Inside- and outside box



6.

Game coin

We have already prepared your quantum game coin for you. But why a 50ct coin? The Qey-Gen is designed exactly for the weight and size of the coin. If you lose your original coin you can easily use one of your own.

Functionality of the box - quantum mechanical measurement process

Imagine you lay a coin flat on the ground. It lies horizontally. We now call this a horizontal base (h). Whether number or head points upwards we call the value of the coin.

Base: h

Value: 0

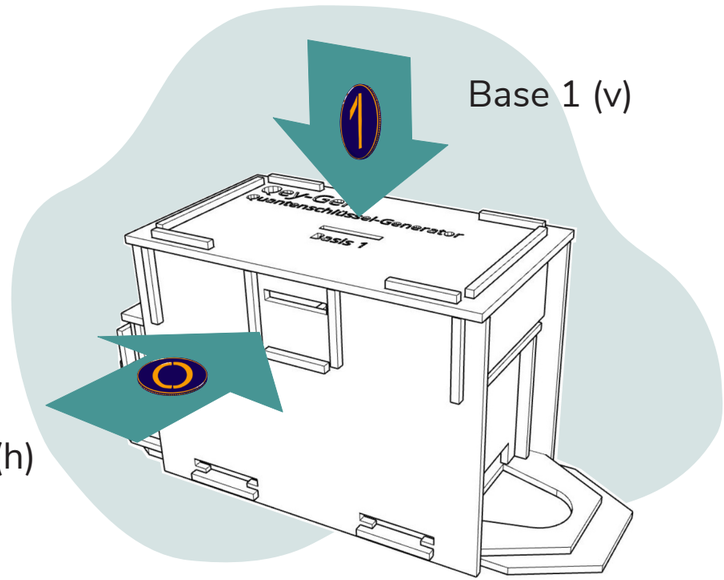
In contrast, we can also balance the coin on its side in front of us, which we then call the vertical base (v). Whether number or head points to you again indicates the value of the coin.

Base: v

Value: 1

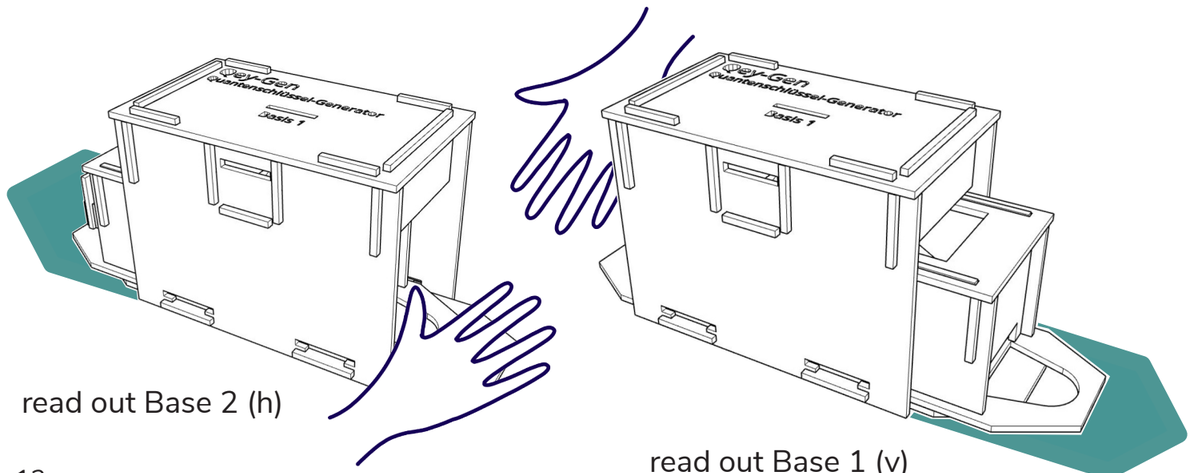
Now comes the interesting part. Does it make sense to ask on the right coin whether tails or heads are **on top**? No, just as it makes no sense to ask on the left coin whether tails or heads **is facing you**. To get meaningful answers, you have to read the coin in the same base as it was prepared. So with the left coin, you can ask what **is pointing up**. With the right one, what **points to you**.

The box has two slots into which a 50 cent coin can be inserted. If we choose one of them, we call it "a certain basis for describing the coin state".

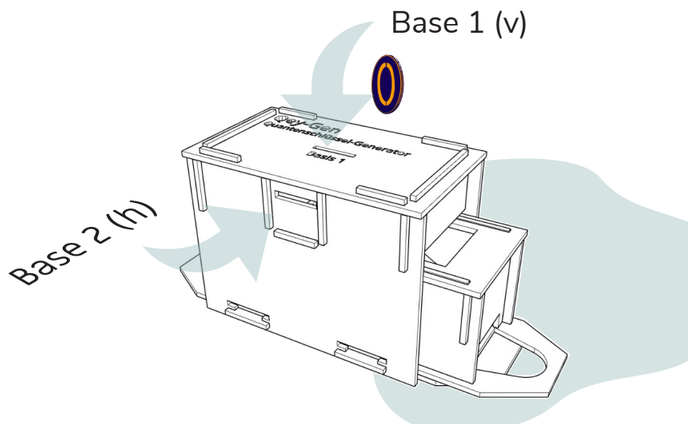


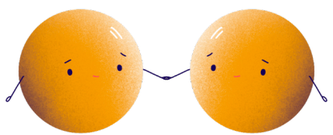
Functionality of the box - quantum mechanical measurement process

With the box we can now prepare a coin in the h or v base by inserting it into slot 1 or slot 2. From the outside, it is no longer possible to decide which base it is in. By pushing the box in from the left or right, we can then read the coin in base h or v. Just try it out!



The trick comes now. If we read the coin in the same base as the one in which the coin was prepared, we can say with 100% certainty how the coin was in the box before. If we measure it in different base, we get 50% heads and 50% tails by chance. Physicists would say about quanta "The wave function collapses and the quantum has a fixed state". So our coin is now heads or tails in the corresponding base".

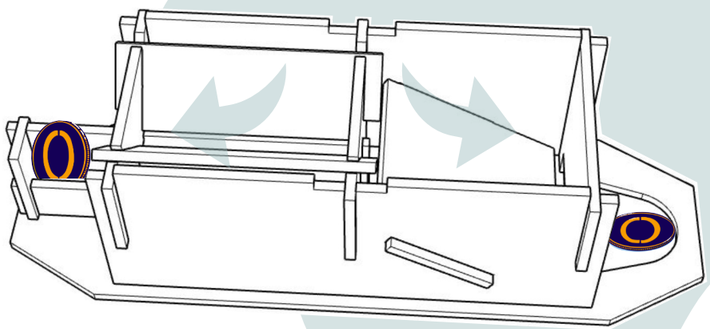


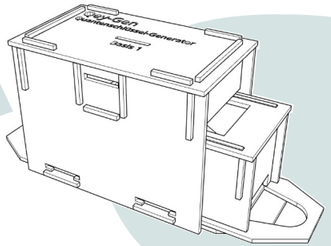


This thought experiment is considered the basis of quantum cryptography. Instead of coins, however, photons are used in reality, which are prepared in different bases.

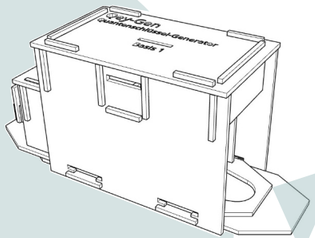
Measuring with the box

The inner box can be moved to the left or right, where the coin either slides down a ramp and stays flat on the ground, or drops down a kind of funnel and ends up on the edge. Similar to the insertion, this is called a base 1 (horizontal) or base 2 (vertical) measurement.





Measurement in base 1



Measurement in base 2

So if you put a coin in base 1 and also measure it in base 1, the state of the coin remains unchanged. If number points upwards, then number also points upwards when measured. However, if you measure in base 2, the coin flips to an edge, and 50% of the time a 0 and 50% of the time a 1 shows to you.

Don't worry if you don't immediately understand what it's all about or how the box works. Just try it a few times and eventually it will click, I promise! You can also find an instruction **video** here:

In order to send messages in our digitalized world that cannot be overheard by others, we have to encrypt them. To decrypt the encrypted message again, we need - of course - a key!

Nowadays such a key is often created with the help of large prime numbers. How this works exactly is not important at first. Simply put, it is based on calculations that are easy in one direction and difficult in the other.

Example:

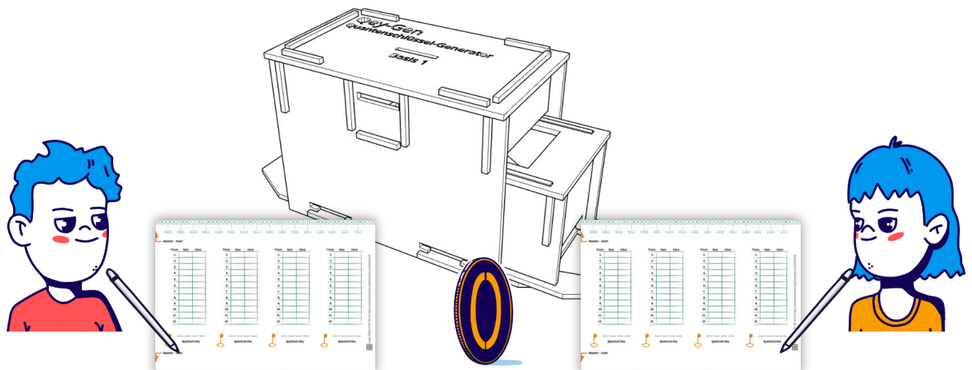
1. Can you figure out what a and b are for the case of: a x b = 323.

2. What is 17 x 19?

Is 1. or 2. more difficult?

The difficult thing is that the key must first be exchanged safely. Actually, you would have to meet in advance for that. But with the help of quantum mechanics, we can also generate keys that nobody knows, even though we generate the key together by sending quanta to each other.

The quantum key generator game can be played by two or three players. First, set up the box and put the prepared 50 cent coin ready. Each player also needs a pen and a game sheet.



Generate a quantum key

In our example, we call player 1 "Alice" and player 2 "Bob" for simplicity.

Alice secretly pushes the coin into slot 1 or 2 and notes the base and value of the coin on her spreadsheet.

Optional: An eavesdropper could now secretly read the coin in either base 1 or 2 (i.e., open the drawer to the right or left). So that his eavesdropping is not noticed, he pushes the coin again as above into a slot. (But in which slot and how around does he put the coin? He must decide that for himself).

Bob makes a measurement in either base 1 or 2 and also notes on his game sheet the value of the coin and in which base he measured.

„Alice“

Throw	Base	Value
1.	1	1
2.	1	0
3.	2	1
4.	1	1
5.	1	1
6.	1	1
7.	2	1
8.	1	0
9.	2	0
10.	2	1
11.	2	1
12.	1	0

„Bob“

Throw	Base	Value
1.	1	0
2.	1	0
3.	1	1
4.	1	1
5.	2	0
6.	2	1
7.	1	1
8.	1	0
9.	2	0
10.	2	1
11.	1	0
12.	1	0

This process is repeated 12 times

Afterwards, Alice and Bob can openly discuss in front of the eavesdropper which base they chose on which roll, without revealing the value. They cross out all the throws with different bases. They can then use the remaining lines to test whether anyone was listening and, if not, build a key.

„Alice“

Throw	Base	Value
1.	-	-
2.	1	0
3.	-	-
4.	1	1
5.	-	-
6.	-	-
7.	-	-
8.	1	0
9.	2	0
10.	2	1
11.	-	-
12.	1	0

Throw	Base	Value
1.	-	-
2.	1	0
3.	-	-
4.	1	1
5.	-	-
6.	-	-
7.	-	-
8.	1	0
9.	2	0
10.	2	1
11.	-	-
12.	1	0

With this you make your louse test and the key

„Bob“

Louse test:
Now the test is performed to see if someone has been eavesdropping. To do this, Alice & Bob openly compare in front of the eavesdropper, their results for a part of their readings. e.g. litter 2 and 4.

Question: What do you expect when someone has been eavesdropping?
Answer: Some of the results do not agree.
Question: What do you expect if there was no eavesdropping?
Answer: All results agree.

The key:
If there was no eavesdropping, i.e. Alice and Bob had the same results for their first measured values, they can build a quantum key from the remaining and still "secret" or not publicly communicated measured values. In our example, for litter 8, 9, 10 and 12, the values are therefore either "0" or "1". Alice and Bob write the quantum key hidden on their spreadsheet. If you did everything right, you should have the same quantum key as a result. Tada!

The more often you perform the measurement process and the more values you compare for the eavesdropper test, the more certain you can be that no one has tried to read the key generation. With one comparison, the eavesdropper would have a 50% chance of guessing correctly and not being noticed. With two comparisons it is already only 25%, with three comparisons 12.5% and with five comparisons even only 3.125%.

Throw	Base	Value
1.	-	-
2.	1	0
3.	-	-
4.	1	1
5.	-	-
6.	-	-
7.	-	-
8.	1	0
9.	2	0
10.	2	1
11.	-	-
12.	1	0

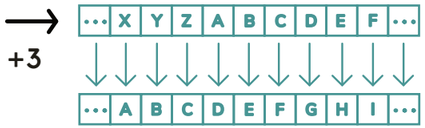
Louse test

On the 10th comparison, the chance of guessing correctly is less than 0.1%.

Attention: Since you have already used the first two measured values for the louse test and thus discussed them publicly, you must not use them for your secret key under any circumstances! The remaining four values, on the other hand, are known only to Alice and Bob and are therefore super safe!

Caesar encryption

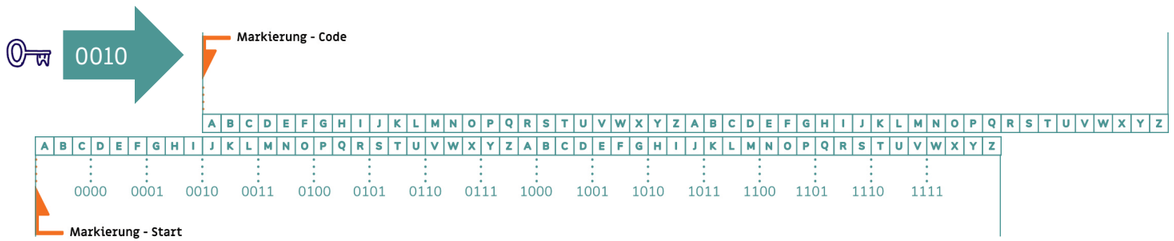
Caesar encryption is one of the oldest encryption methods.
It involves replacing letters of a word with others in the alphabet.
To encrypt and decrypt as easily as possible, you can write down the alphabet on two strips and move the upper one to the right by the length of the key. It is said Caesar mostly used the key "3". Thus every "A" of our message becomes a "D" in the cipher, and every "B" becomes an "E" and so on.



Caesar encryption with the Qey gen

To use Caesar encryption with your already generated numeric key "0010" (see p.21), you can use the two strips shown on the right. Besides letters, there are also number markings on them so that you can use your key of zeros and ones to encrypt letters.

First, place both strips under each other so that the "Code" and "Start" markings meet. Now move the upper strip to the right until the "Code" mark points to the matching key, i.e. "0010" in this case.



Hooray! Now you've created a tap-proof quantum key and have the ability to send secret messages.

What is the Quantum Coin Toss?

The quantum coin toss is a method in quantum cryptography in which two parties who do not trust each other can perform a random decision analogous to the classical Coin Toss over long distances.

The basic idea is this:

Alice and Bob are talking on the phone because they want to have dinner together later. Alice wants to eat sausage, but Bob is more in the mood for sushi. Alice suggests flipping a coin to decide. But Bob doubts the method and worries that Alice is simply lying so she can get her sausage. After all, Bob has no way to check if Alice is telling the truth because he can't see the coin.

This is exactly the point where the quantum Coin Toss comes into play. Alice sends a light particle to Bob, which can be prepared or, more precisely, polarized in two different ways. If Bob guesses the right way, he wins and gets sushi; if he guesses wrong, Alice gets her sausage.

The cool thing is that there is a trick to make sure that Alice can't lie about which of the two polarizations she used. You'll read about how exactly the trick works in the next section.

! And again for your information: We do not use polarized light particles, but coins.

1. Alice secretly chooses a base (slot 1 or slot 2).

2. Alice secretly inserts the coin with any value into the slot of the selected base and writes it in her table.

3. Bob measures the coin in any drawer and writes the base and value in his table.

4. Steps 2 and 3 are now repeated 8 times. Alice always uses the same slot. Bob may choose different drawers.

5. Bob guesses which base Alice has chosen. If he guesses correctly, he wins.

6. Alice reveals whether he guessed correctly or not.

But how can Bob now be sure that Alice is telling the truth?

Imagine Bob guesses base 1 and Alice claims she chose base 2. So Bob would have guessed wrong. How can Bob now be sure that Alice is not lying?

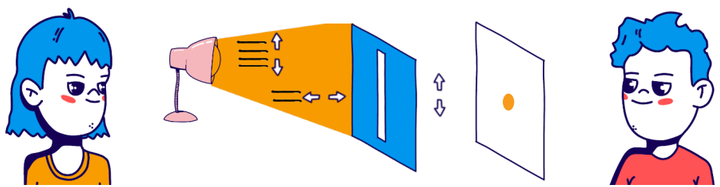
Very simple. Alice now reveals the values of the coin she sent to Bob and Bob compares them with the values he measured at base 2.

If Alice had told the truth, all values would have to match. In case she is lying, some values are different. This is because in this case Alice used base 1 and Bob measured in base 2. This is because, as we know, when bases are different, the measurement results are random. So it is very unlikely that Alice is telling exactly the values measured by Bob.

Attention: It is not impossible that Alice is lying and the values still match. But the more coins you send to each other, the less likely it is that she will guess all the readings correctly.

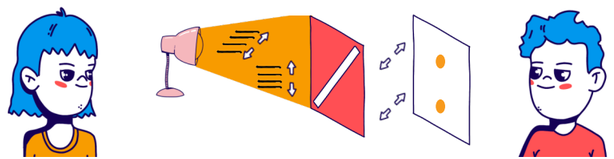
Polarisation

Light particles (photons) oscillate in all directions. With the help of a polarization filter, Alice only sends photons to Bob that oscillate in a certain direction, e.g. vertically, horizontally, left diagonally or right diagonally. They are then said to be polarized in that direction.



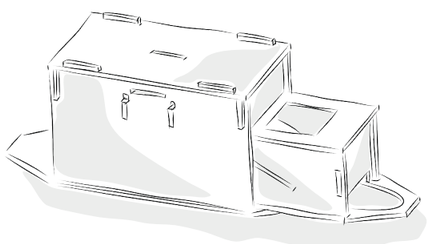
If they both had a modern laboratory, Alice could send photons, particles of light, with a certain polarization to Bob. Bob would then measure the photons in his laboratory by also sending the by sending the incoming photons through a filter as well. If he aligns his filter in the same way as Alice does, he can measure light. If, on the other hand, he holds his filter exactly perpendicular (90°) to Alice's polarization, he sees no light.

It is especially exciting if he aligns his filter only 45° twisted to Alice's filter. Then there is exactly a 50:50 chance that the photon comes through the filter or not. This is true chance. If Bob sees light, he could have held his filter the same way Alice did, or the photon got lucky and slipped through. If Bob does not see light, his filter could have been perpendicular to Alice's polarization, or the photon did not slip through. So Bob does not know yet if he has held his filter correctly before Alice tells him.



Now Bob guesses how Alice oriented her filter - either horizontally/vertically or diagonally.
Alice could lie, of course, and say she held her filter differently so she could eat sausage.
To prove that Alice is not lying, she can accurately predict Bob at each reading (light or no light) where he measured in her stated base. If Alice predicts all the readings correctly, she probably did not lie. If she were lying, she would have to guess. And the more readings they both compare, the less likely Alice is to guess them all.

To make a random decision, we flip a coin. But already Einstein said that this is not real coincidence. Because depending on the force with which we throw the coin, how the wind is, etc., the result is influenced. the result is influenced. If we knew everything exactly, we could even calculate it. Whether slightly twisted photons come through the filter - on the other hand, this is real coincidence. Nobody can predict or influence it.



And exactly this is used here to generate keys or to make a random decision at a greater distance.

The Qey-Gen game was developed as part of the project Quantum 1x1 by Junge Tüftler gGmbH and Tobias Schubert (Technische Universität Berlin). The project is funded by the German Federal Ministry of Education and Research through the measure "Quantum aktiv" (funding number: 13N15479), which is part of the German government's high-tech strategy.

Superposition and entanglement?

If you want to learn even more about the wondrous world of quanta then visit us on our website and check out the "Quantum Tiq Taq Toe"!

https://bit.ly/3v6Sc5E