

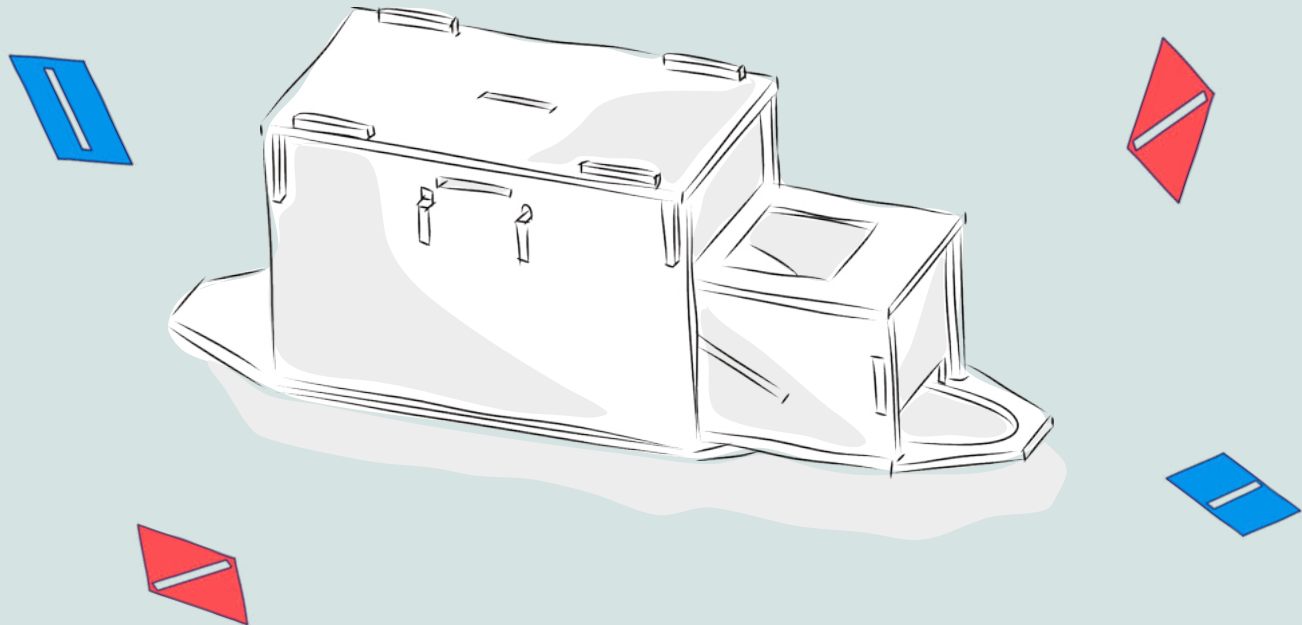
Anleitung



TüftelAkademie

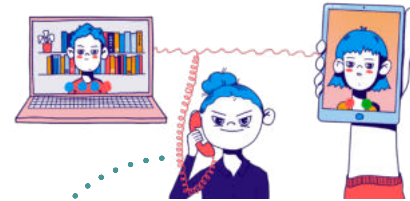
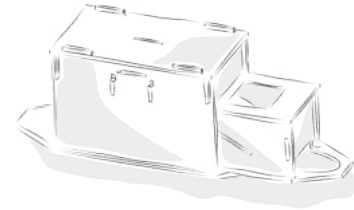
Quanten Verschlüsselung

Qey-Gen - Der Quantenschlüssel Generator



Inhaltsverzeichnis

Inhalt	3
Einleitung	4
Bauplan für den Qey - Gen	5
Spielanleitung	15
Hat vielleicht jemand mitgehört?	20
Verschlüsseln mit der Caesar Chiffre	21
Geheime Nachrichten erstellen	22
Zusatz: Spielvariante mit einem Spion	24
Polarisation und Filter	26
Funktionsweise der Box	30
Der Quantum Coin-Toss	34
Der echte Zufall	38
Impressum	39



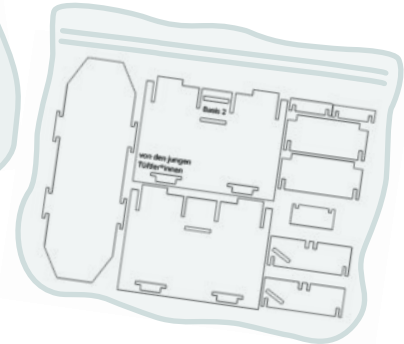


Tüte 2



22 Bauteile
2 Tüten

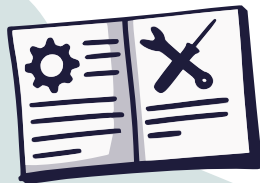
Tüte 1



Münze



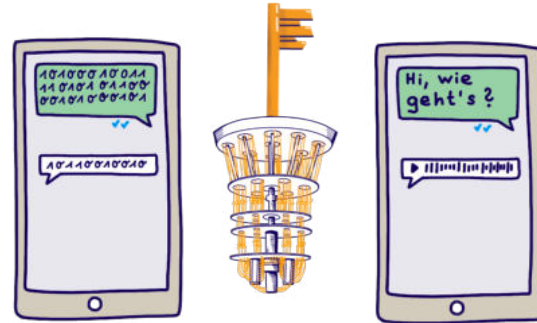
Anleitung



Der Qey-Gen wird übrigens händisch mit einem Lasercutter in Berlin produziert! Das ist auch der Grund, warum er ein bisschen nach Lagerfeuer riecht.

Einleitung

Ein großes Anliegen der heutigen Zeit ist die Übermittlung von vertraulichen Nachrichten. Dafür erzeugt man oft einen geheimen Schlüssel, mit dem man Nachrichten für fremde Personen unlesbar machen kann. Doch das Problem ist, beide Personen müssen sich vorher auf einen Schlüssel einigen. Aber wie soll das funktionieren, ohne dass schon jemand beim Schlüsselaustausch mithört?



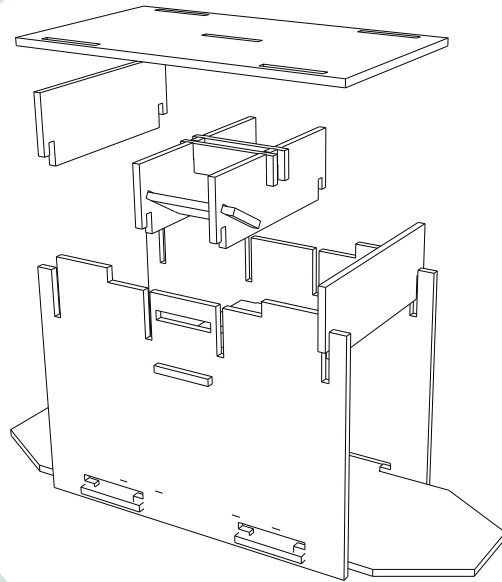
Um unsere Nachrichten in Zukunft abhörsicher zu machen, schaut man sich seit einiger Zeit in einem Teilgebiet der Physik um, der Quantenmechanik. Denn wir werden sehen, dass man mit Hilfe von quantenmechanischen Phänomenen extrem sichere (Quanten-)Schlüssel erzeugen kann.



Was bedeutet eigentlich Qey-Gen?

Der Qey-Gen
(Quantenschlüssel-Generator)
Quantum-**K**ey-**G**enerator

Bauplan für den Qey-Gen

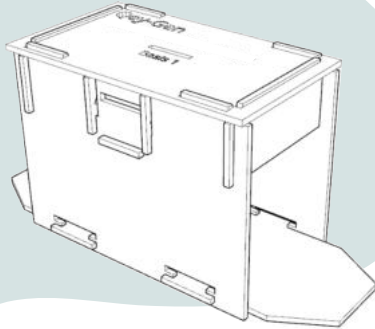


Im folgenden Abschnitt bekommst du eine Schritt-für-Schritt Anleitung, um die Box zusammenzubauen oder du schaust dir einfach unser **Video** an.

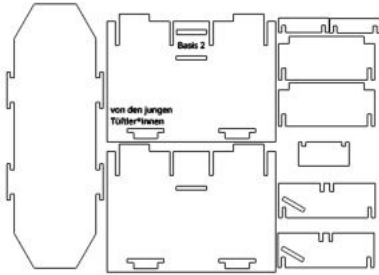


<https://bit.ly/3CB0Lst>

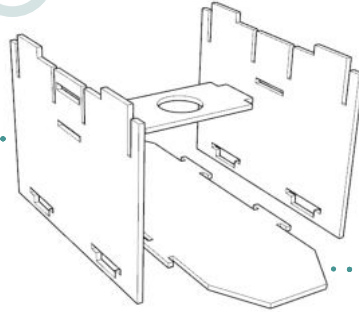
Aufbau - Teil 1 - Außenbox



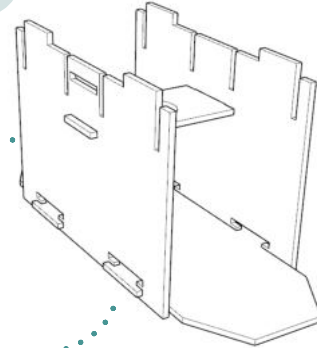
Tüte 1



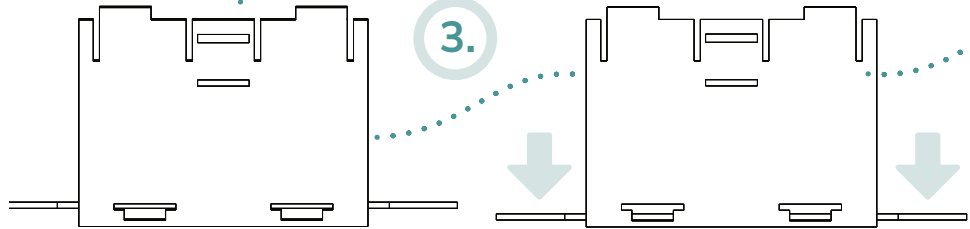
1.



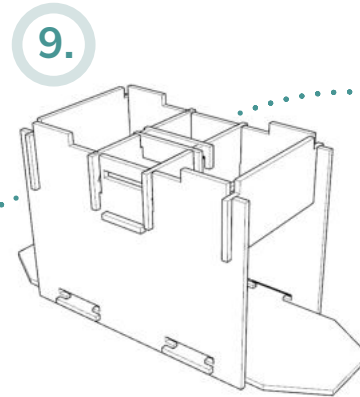
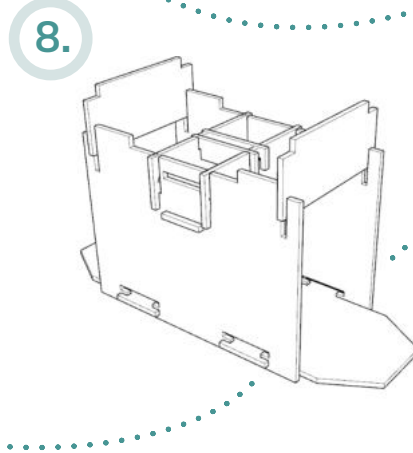
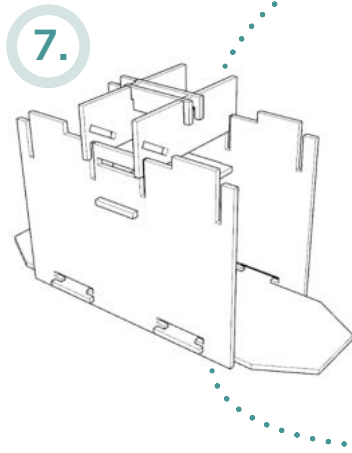
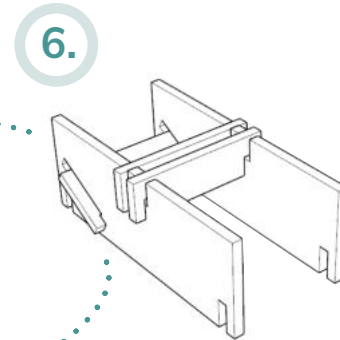
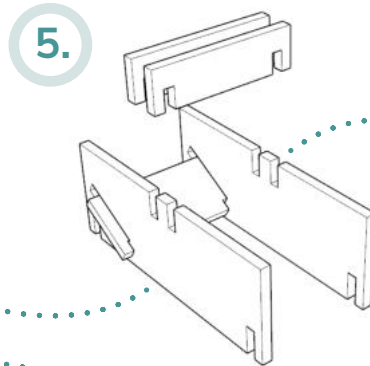
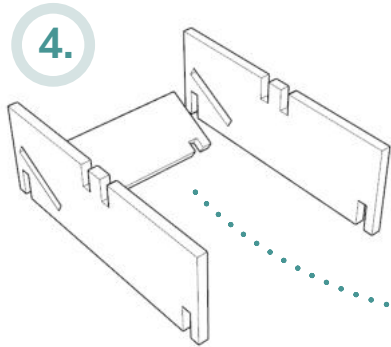
2.



3.

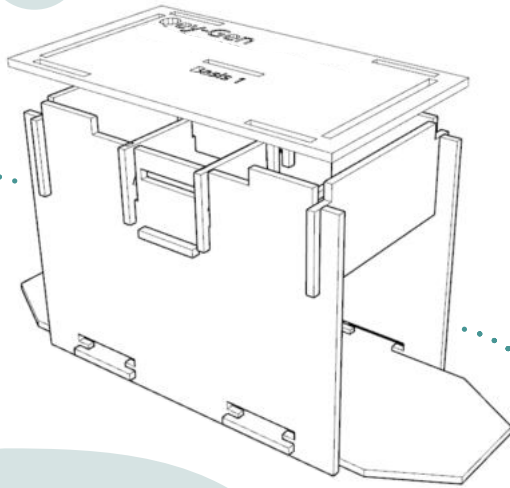


Aufbau - Teil 1 - Außenbox

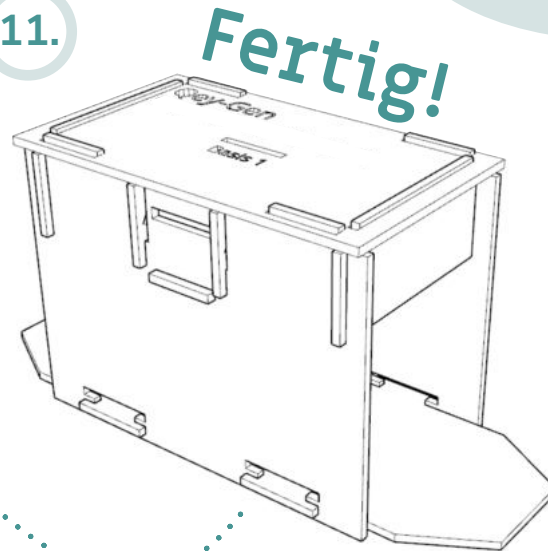


Aufbau - Teil 1 - Außenbox

10.



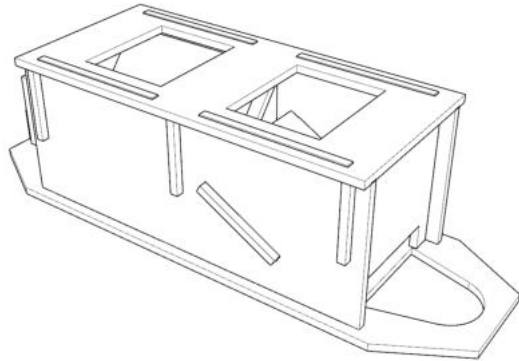
11.



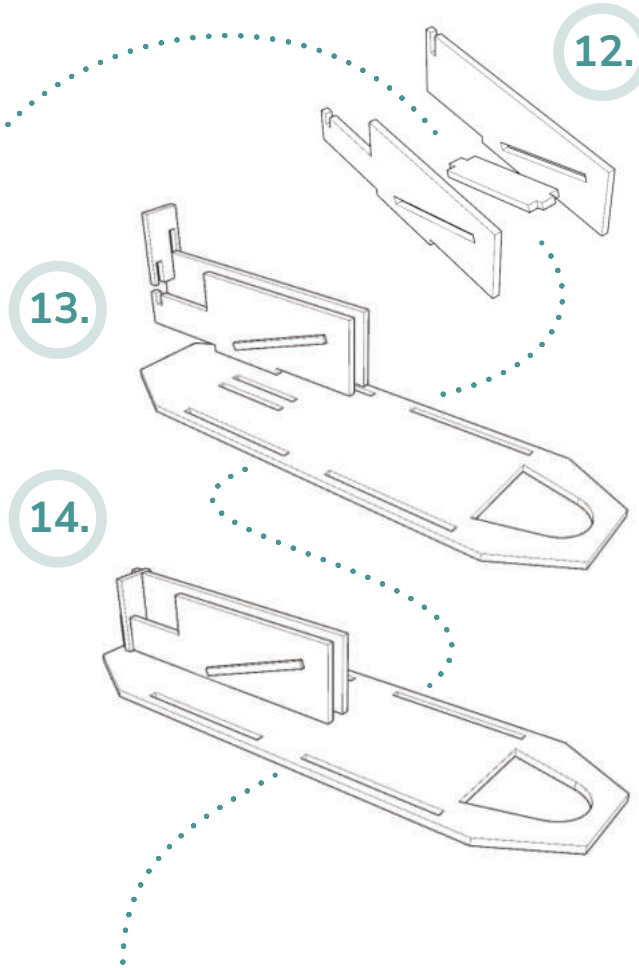
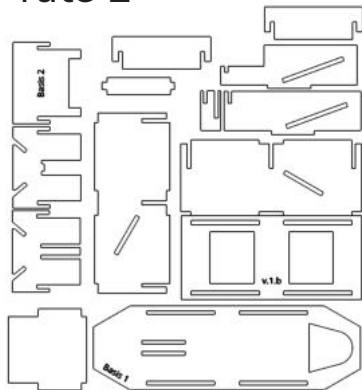
Jetzt kommt
die Innenbox



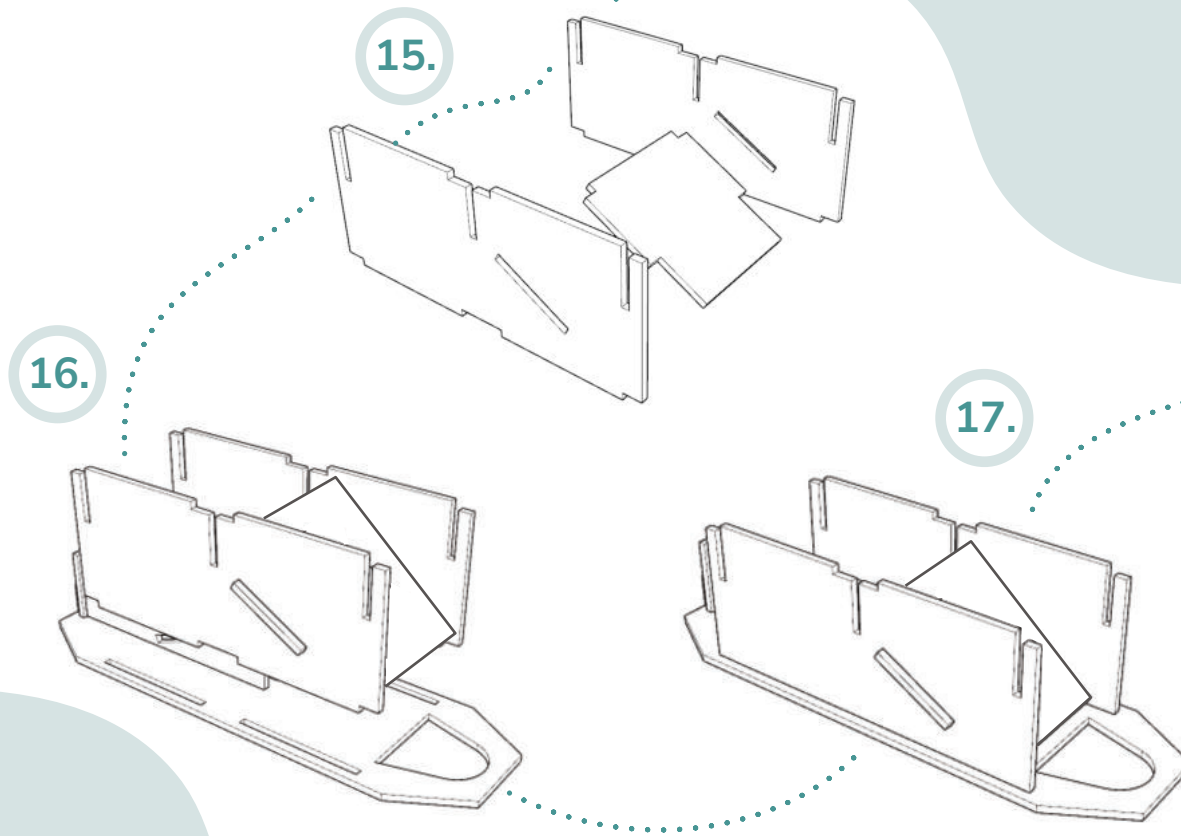
Aufbau - Teil 2 - Innenbox



Tüte 2

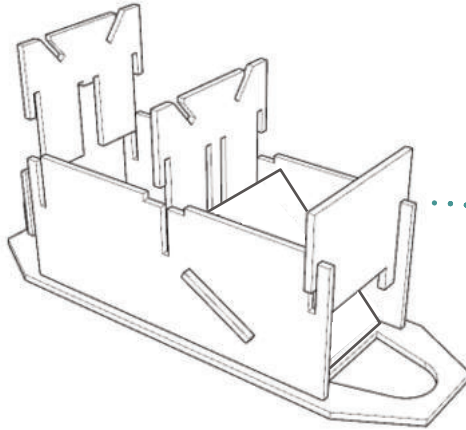


Aufbau - Teil 2 - Innenbox

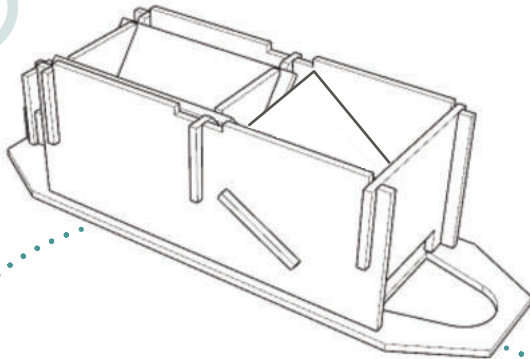


Aufbau - Teil 2 - Innenbox

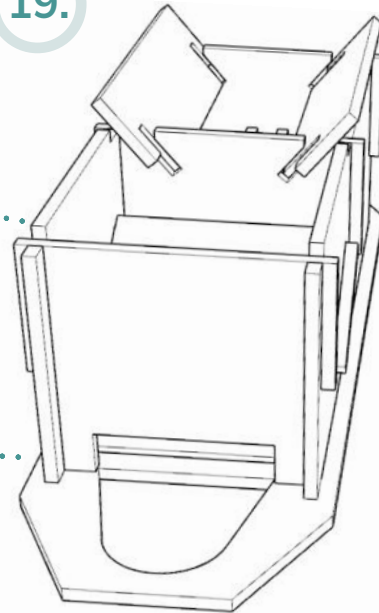
18.



20.

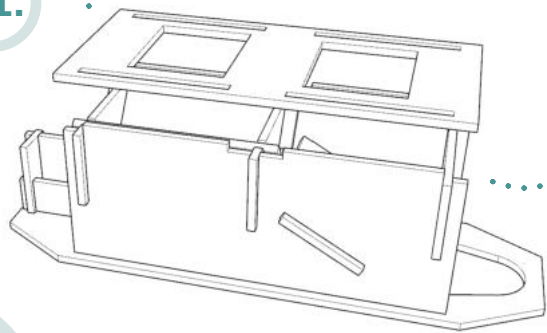


19.

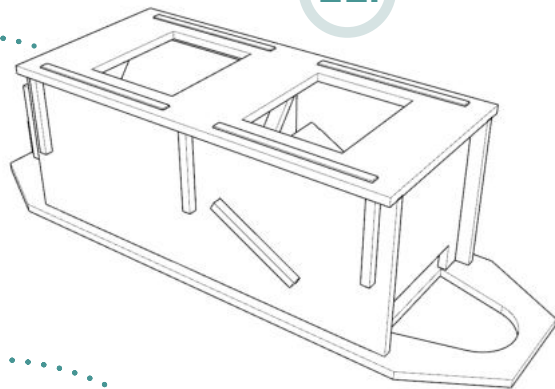


Aufbau - Teil 1 + Teil 2 - Zusammenbau

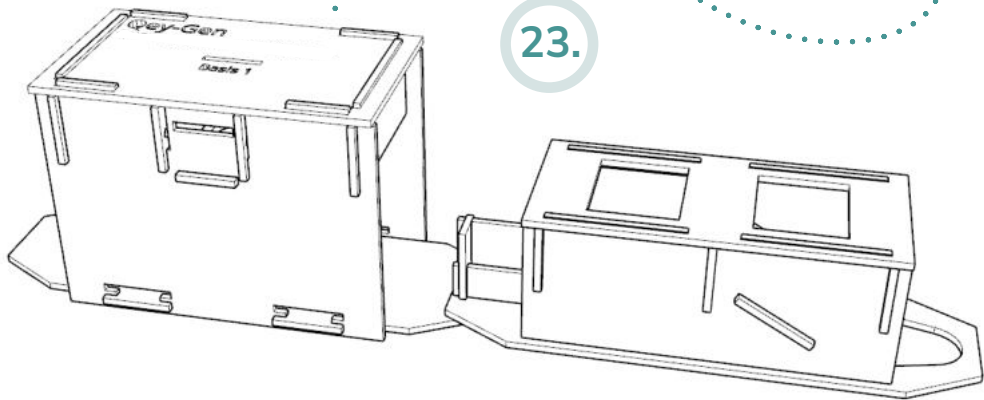
21.



22.



23.



Qey-Gen



Juhu! Du hast es geschafft!

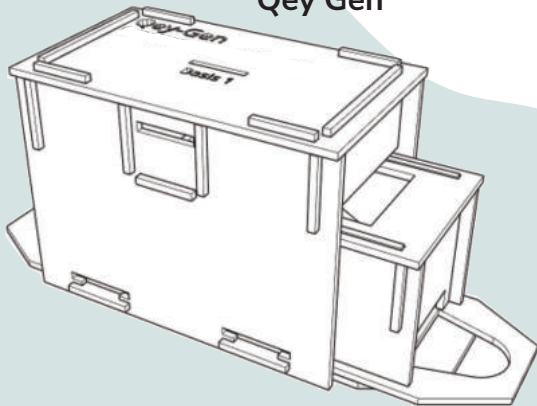


Spielmünze

Eure Quantenspielmünze findet ihr in einer der Tüten. Der Qey-Gen ist genau auf das Gewicht und die Größe einer 50ct Münze ausgelegt. Falls ihr eure Original Münze verlieren solltet, könnt ihr ganz einfach eine eigene benutzen.

Um zu starten benötigt ihr folgende Sachen:

Qey Gen



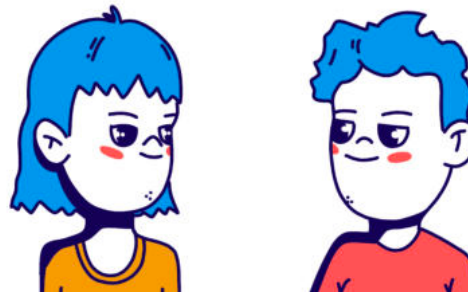
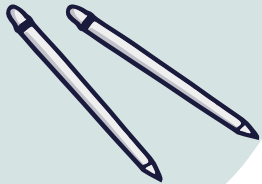
Spielmünze



Zwei Spielblätter



Zwei Stifte



Mindestens zwei Mitspieler*innen

Spielanleitung

Alice



Bob

Das erstellen von abhörsicheren Schlüsseln ist tatsächlich gar nicht mal so einfach zu verstehen. Wir haben dir aber eine Schritt-für-Schritt-Anleitung als Beispiel zur Verfügung gegeben.

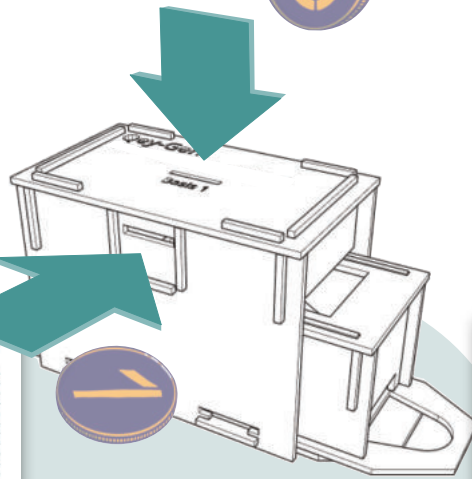
In unserem Beispiel nennen wir einfachheitshalber Spielerin 1 "Alice" und Spieler 2 "Bob".

1.

Alice



Bob



Wurf	Basis	Wert
1.	1	1
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		

Wurf	Basis	Wert	Wurf	Basis	Wert	Wurf	Basis	Wert
1.			1.			1.		
2.			2.			2.		
3.			3.			3.		
4.			4.			4.		
5.			5.			5.		
6.			6.			6.		
7.			7.			7.		
8.			8.			8.		
9.			9.			9.		
10.			10.			10.		
11.			11.			11.		
12.			12.			12.		

Wurf	Basis	Wert	Wurf	Basis	Wert	Wurf	Basis	Wert
1.			1.			1.		
2.			2.			2.		
3.			3.			3.		
4.			4.			4.		
5.			5.			5.		
6.			6.			6.		
7.			7.			7.		
8.			8.			8.		
9.			9.			9.		
10.			10.			10.		
11.			11.			11.		
12.			12.			12.		

Alice schiebt geheim die Münze in Basis 1 oder 2 und notiert sich auf ihrem Tabellenblatt die Basis und den Wert der Münze. Der „Wert“ der Münze ist welche Zahl zu **dir (wenn Basis 1)** oder welche Zahl nach **oben (im Fall Basis 2)** zeigt.

Während Alice ihre Münze einwirft, muss Bob wegsehen!

2.

Nun führt Bob eine Messung durch und notiert sich jetzt das Ergebnis.



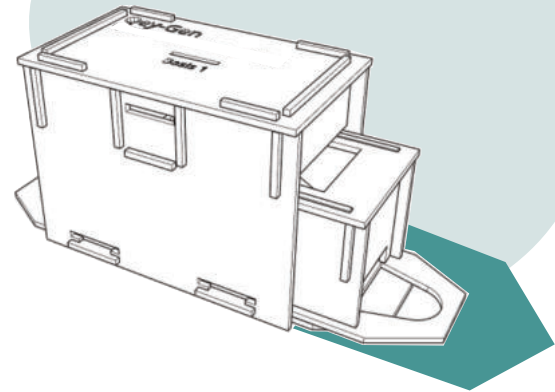
Wurf	Basis	Wert
1.	1	1
2.		
3.		
4.		
5.		
6.		
7.		

Wurf	Basis	Wert
1.	2	0
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		

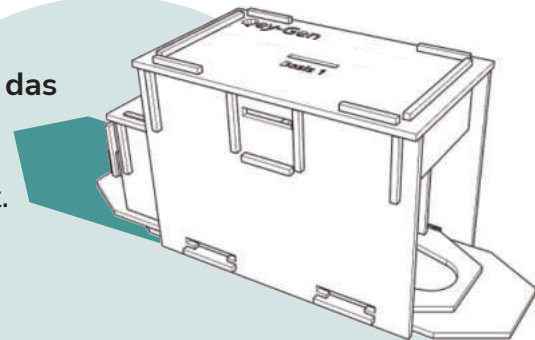


Alice muss natürlich wegsehen!

Wenn er nach **Basis 1** ausmessen will, muss er die **innere Box nach rechts** verschieben.



Bei **Basis 2** muss er das **innere nach links** verschieben bis die Münze herunter fällt.



3.

Wurf	Basis	Wert
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

12x

Alice legt immer die Münze ein und Bob liest sie aus. Diesen Vorgang wiederholen sie 12 Mal.



Doch Moment. Wie könnt ihr euch sicher sein das niemand heimlich gelauscht hat?



In den nächsten Schritten nutzt ihr eure Werte um einen Schlüssel zu bauen und um auf Lauscher zu testen

Wurf	Basis	Wert
1.	2	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



4.



Wurf	Basis	Wert
1.	-	
2.	1	0
3.	-	-
4.	1	1
5.	-	-
6.	-	-
7.	-	-
8.	1	0
9.	2	0
10.	2	1
11.	-	-
12.	1	0

Wurf	Basis	Wert
1.	-	-
2.	1	0
3.	-	-
4.	1	1
5.	-	-
6.	-	-
7.	-	-
8.	1	0
9.	2	0
10.	2	1
11.	-	-
12.	1	0

Damit baut ihr euren Schlüssel und führt den Lauschtest durch.



Jetzt besprechen Alice und Bob offen, bei welchem Wurf sie welche Basis gewählt haben, ohne den Wert zu verraten. Alle Würfe mit unterschiedlichen Basen streichen sie durch.

5.

Hat vielleicht jemand mitgehört?

Wurf	Basis	Wert
1.	-	-
2.	1	0
3.	-	-
4.	1	1
5.	-	-
6.	-	-
7.	-	-
8.	1	0
9.	2	0
10.	2	1
11.	-	-
12.	1	0



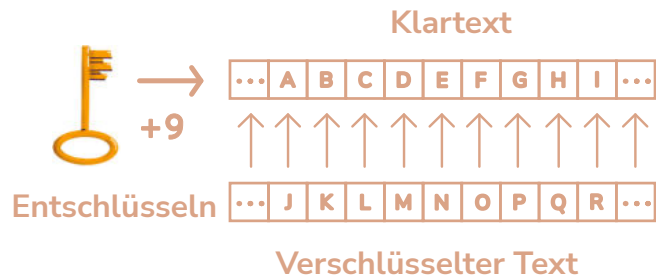
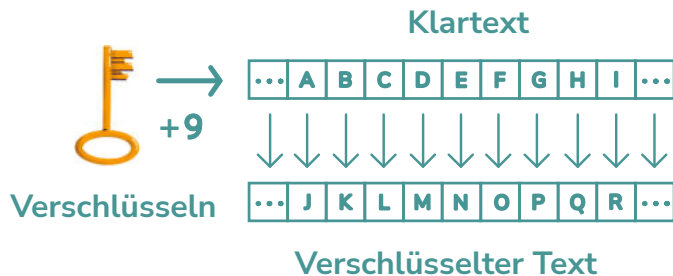
Doch Moment mal. Wie können wir sicher sein, dass niemand gelauscht hat? Alice und Bob benötigen nur vier Werte für den Schlüssel. Solange sie nie den Wert laut sagen, können sie zusammen frei wählen, welche sie benutzen wollen (hier 8, 9, 10 und 12).

Über die übrigen Werte können sie sich laut austauschen (hier 2 und 4). Sie müssen richtig, also gleich sein. Sind sie nicht gleich, hat jemand gelauscht. Je mehr Werte sie vergleichen, desto sicherer ist, dass niemand gelauscht hat. Ihr könntet auch mehr als zwölf Münzwürfe machen, um mehr Werte für den Lauschtest zu haben.

6.

Verschlüsseln mit der Caesar Chiffre

Mit eurem abhörsicheren Schlüssel könnt ihr nun eine geheime Nachricht erzeugen. Dafür benutzen wir die Caesar Chiffre. Die Caesar Verschlüsselung ist eine der ältesten Verschlüsselungsmethoden. Dabei ersetzt man Buchstaben eines Wortes mit anderen im Alphabet. Um möglichst leicht zu ver- und entschlüsseln kann man sich das Alphabet auf zwei Streifen aufschreiben und das obere um die Länge des Schlüssels nach rechts verschieben.



Geheime Nachrichten erstellen

7.

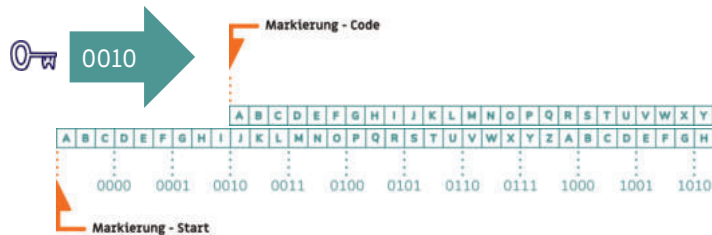
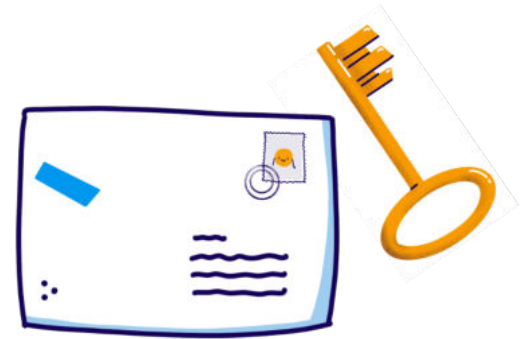
Jetzt braucht ihr die Markierungen auf euren Listenblättern!



Um die Caesar-Verschlüsselung mit eurem bereits erzeugten Zahlen-Schlüssel „0010“ (siehe S.22) anzuwenden, könnt ihr die beiden rechts abgebildeten Streifen nutzen. Neben Buchstaben sind auch Zahlen-Markierungen darauf angebracht, damit ihr euren Schlüssel aus Nullen und Einsen nutzen könnt, um Buchstaben zu verschlüsseln.

So wird zum Beispiel aus dem Wort „QUANTASTISCH“ → „ZDJWCDBCRBLQ“

Legt zuerst beide Streifen so untereinander, dass die Markierung „Code“ und „Start“ sich treffen.
 Verschiebt nun den oberen Streifen nach rechts, bis die Markierung „Code“ auf den passenden Schlüssel zeigt, also „0010“ in diesem Fall.



Hurra! Jetzt habt ihr abhörsicher euren Quanten-Schlüssel erzeugt und die Möglichkeit euch geheime Nachrichten zu verschicken.

Achtung: Die Caesar-Chiffre ist heute sehr unsicher. Wir haben sie genutzt, da sie leicht per Hand durchführbar ist. Wenn du aber für jeden Buchstaben einen neuen Schlüssel erstellst, wird sie Einmalverschlüsselung genannt. Es wurde bewiesen, dass die Einmalverschlüsselung unknackbar ist.

Zusatz: Spielvariante mit einem Spion

Ihr könnt auch mal ausprobieren wie sich das Spiel verändert wenn ihr **einen Spion** mitspielen lasst.

Dabei gebt ihr einer dritten Person die Möglichkeit, während Schritt 3 (Alice wirft die Münze ein, Bob liest sie aus) mal selbst, heimlich auszulesen. Am besten spielt ihr es so, das ihr selbst nicht wisst, ob jemand mitgehört hat.

8.



Ihr könnt zum Beispiel jeweils in einem anderen Raum sitzen und euch den Qey-Gen zum einwerfen und auslesen von einer Person bringen lassen. Diese Person hat dann in der Zwischenzeit die Möglichkeit, geheim bei der Erzeugung eures Schlüssels mitzuhören. Probiert es einfach mal aus!

Alice

Wurf	Basis	Wert
1.	-	-
2.	1	0
3.	-	-
4.	1	①
5.	-	-
6.	-	-
7.	-	-
8.	1	0
9.	2	0
10.	2	1
11.	-	-
12.	1	0

Bob

Wurf	Basis	Wert
1.	-	-
2.	1	0
3.	-	-
4.	1	①
5.	-	-
6.	-	-
7.	-	-
8.	1	0
9.	2	0
10.	2	1
11.	-	-
12.	1	0

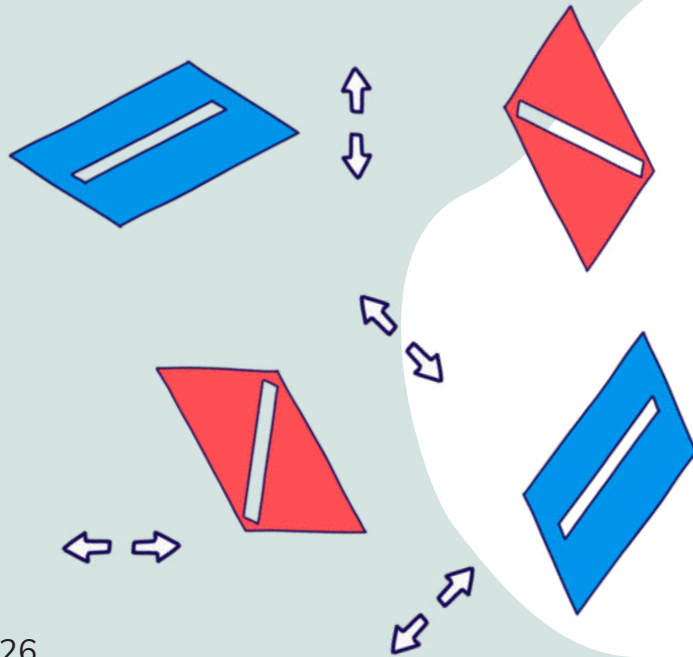
Danach streicht ihr wieder eure unterschiedlichen Basen durch (Schritt 4) und benutzt ein paar Werte für den Lauschtest (Schritt 5). Stimmt der Wert nicht überein, hat euch jemand belauscht!

**Das kann nicht sein!
Jemand hat euch belauscht!**

Mit jeder Zahl, die ihr vergleicht, verringert sich die Wahrscheinlichkeit richtig zu raten um 50%!

Polarisation und Filter

Funktionsweise Quantenkommunikation

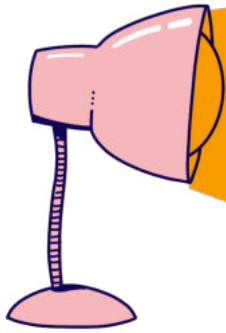


Wunderbar! Nun hast du verstanden wie ihr euch abhörsichere Nachrichten schicken könnt! Aber was hat das jetzt eigentlich mit Quanten zu tun? Im folgenden Abschnitt wollen wir euch erklären, wie diese Art der Schlüsselerzeugung in der Welt der Quanten funktioniert. Dort können wir natürlich keine Münzen verwenden sondern Lichtquanten (Photonen). Um dir zu zeigen wie das funktioniert, führen Alice und Bob ein Experiment durch.



<https://bit.ly/3Q9Uh9p>

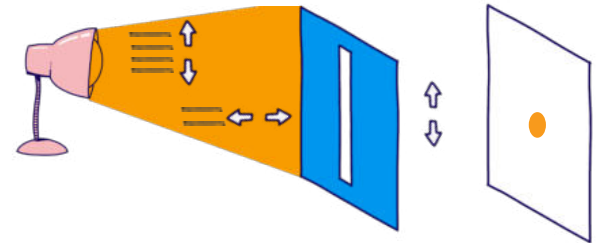
Polarisation und Filter



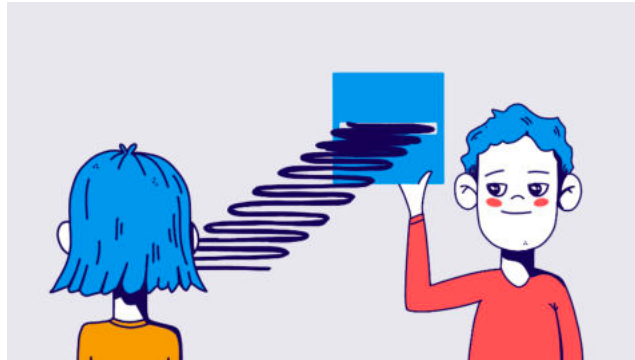
Lichtquanten (Photonen) schwingen in alle Richtungen.



Mit Hilfe eines Polarisationsfilters sendet Alice nur Photonen an Bob, die in eine bestimmte Richtung schwingen, z.B. senkrecht, waagrecht, links diagonal oder rechts diagonal. Man sagt dann, sie sind in diese Richtung polarisiert.



Falls beide ein modernes Labor hätten, könnte Alice Photonen, also Lichtteilchen, mit einer bestimmten Polarisation zu Bob schicken. Bob misst die Photonen dann in seinem Labor, indem er die ankommenden Photonen ebenfalls durch einen Filter sendet.



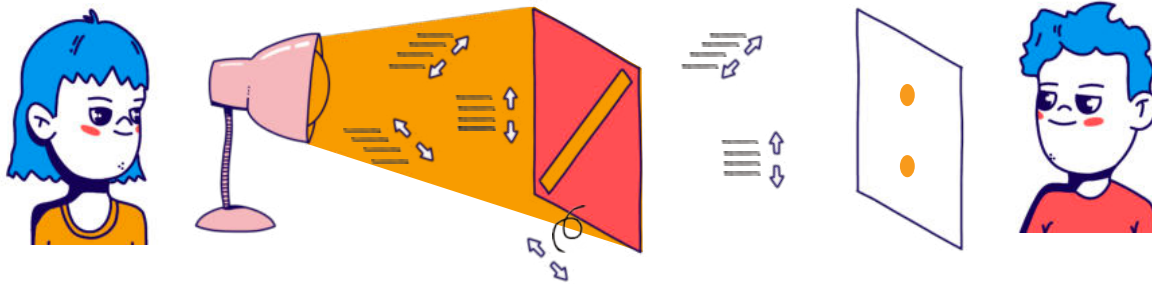
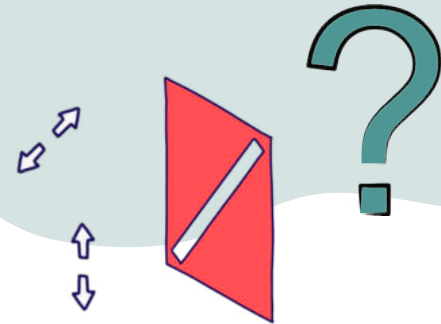
Wenn er seinen Filter dabei genauso ausrichtet wie Alice, kann er Licht messen.



Wenn er seinen Filter dagegen genau senkrecht (90°) zur Polarisation von Alice hält, sieht er kein Licht.

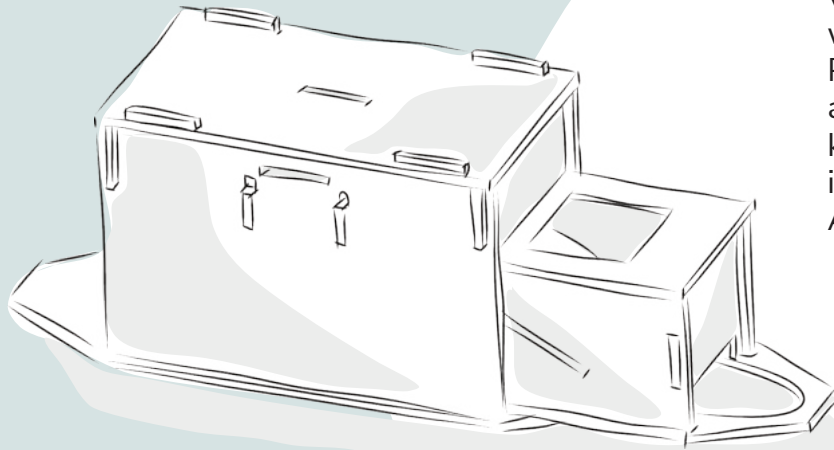
Polarisation und Filter

Besonders spannend ist es, wenn er seinen Filter nur um 45° zu dem Filter von Alice verdreht ausrichtet. Dann besteht genau eine 50:50 Chance, dass das Photon durch den Filter kommt, oder nicht. Dies ist echter Zufall. Sieht Bob Licht, könnte er seinen Filter genauso wie Alice gehalten haben, oder das Photon hatte Glück und ist durchgerutscht. Sieht Bob dagegen kein Licht, könnte sein Filter senkrecht zu Alice Polarisation gewesen sein, oder das Photon ist eben nicht durchgerutscht. Bob weiß also noch nicht, ob er seinen Filter richtig gehalten hat, bevor Alice es ihm verrät. Genau nach diesem Prinzip funktioniert der Qey-Gen! Wie wir das umgesetzt haben, zeigen wir euch jetzt.



Qey-Gen

Funktionsweise der Box

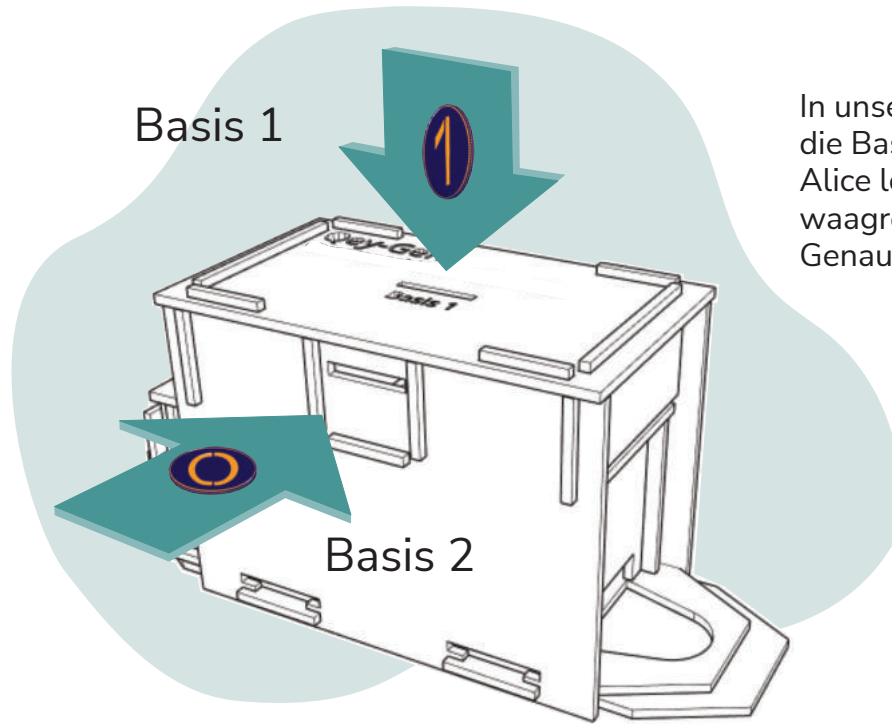


Macht euch keine Sorgen, wenn ihr anfangs nicht sofort versteht, worum es geht, oder wie die Box funktioniert. Probiert es einfach ein paar Mal aus, dann macht es irgendwann klick, versprochen! Hier findet ihr außerdem ein Anleitungsvideo:

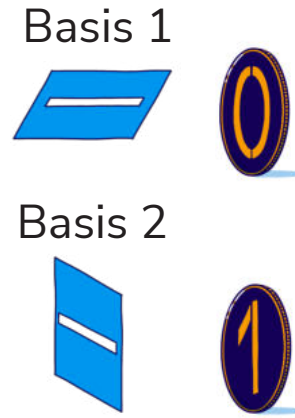


<https://bit.ly/3k3tqjx>

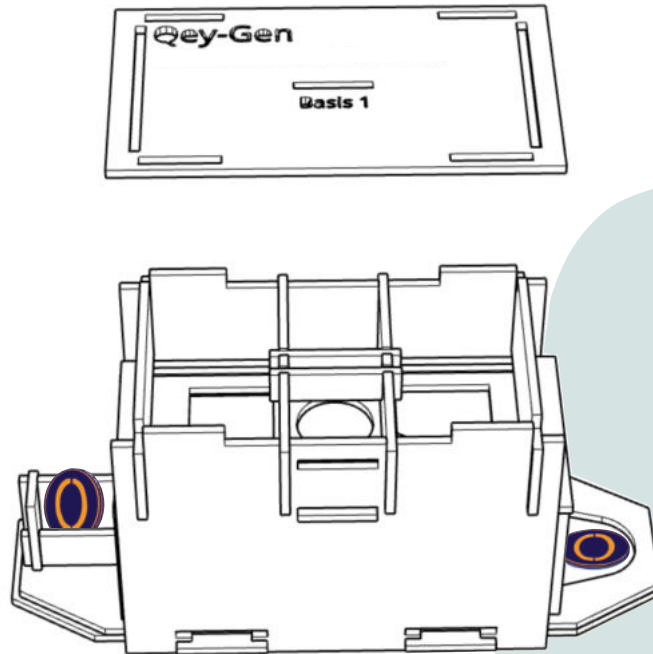
Die Box hat zwei Schlitz, in die man eine 50 Cent Münze einwerfen kann. Wenn wir uns für einen entscheiden und die Münze einwerfen ist sie in „Basis 1 oder Basis 2“ präpariert.



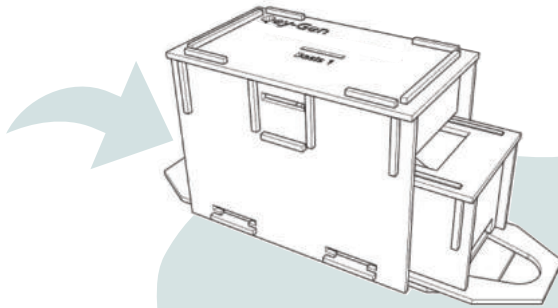
In unserem Experiment beschreiben die Basen, welche Art von Photonen Alice losschickt. Also senkrecht oder waagrecht, mit dem Wert 1 oder 0. Genau wie bei unserer Box.



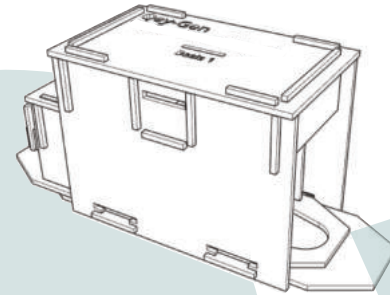
Funktionsweise der Box



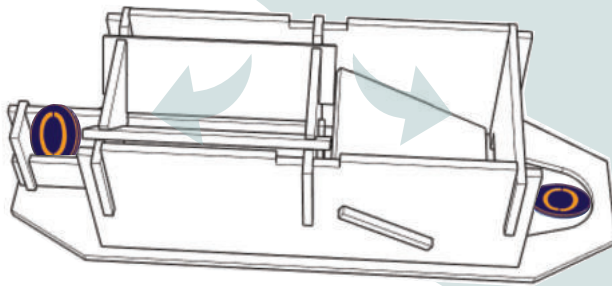
Wenn wir den Qey-Gen öffnen, sehen wir, dass die Münze in einer Vorrichtung gehalten wird, je nachdem, in welcher Basis wir sie einwerfen. Die innere Box lässt sich nach links oder rechts verrücken, wobei die Münze entweder eine Rampe runter rutscht und flach auf dem Boden liegen bleibt, oder einen Art Trichter herunterfällt und auf der Kante endet. Ähnlich wie bei dem Einwerfen nennt man dies eine Messung in Basis 1 (waagrecht) oder in Basis 2 (senkrecht).



Messung in Basis 1



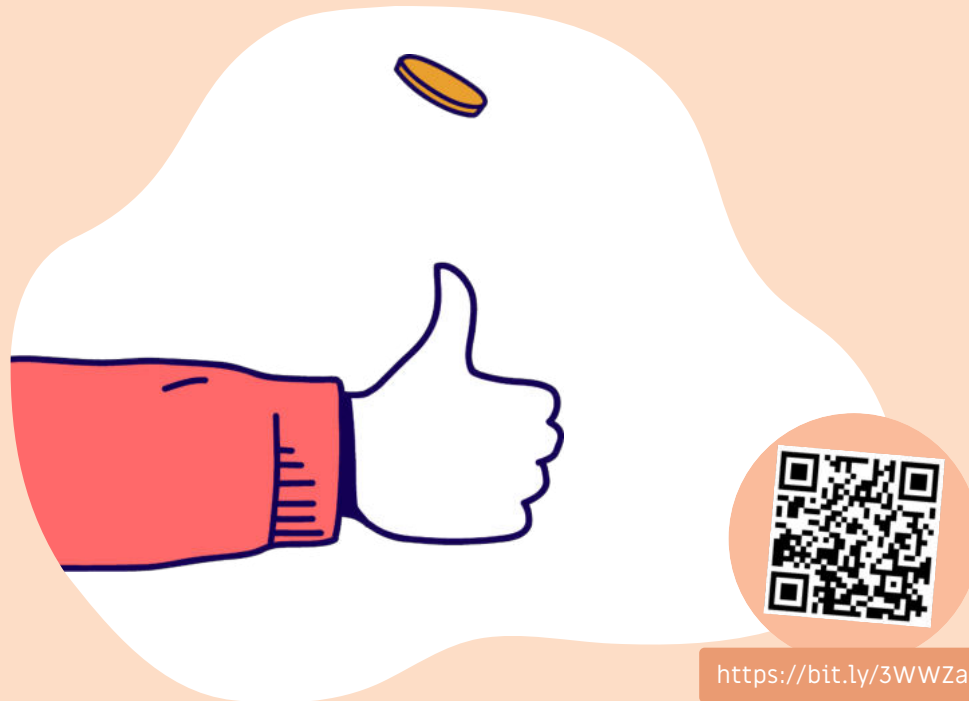
Messung in Basis 2



Wenn man also eine Münze in Basis 2 einsetzt und auch in Basis 2 misst, bleibt der Zustand der Münze unverändert. Falls Zahl nach oben zeigt, so zeigt beim Messen auch Zahl nach oben. Sollte man jedoch in Basis 1 messen, so kippt die Münze auf eine Kante, und zu 50% zeigt eine 0 und zu 50% eine 1 zu dir. So entsteht genau der gleiche Effekt wie bei den Quanten. Bei gleicher Basis bleibt der Wert gleich, bei unterschiedlichen entscheidet der Zufall über den Wert.

Der Quantum Coin Toss

Zufällige Entscheidungen über große Distanzen

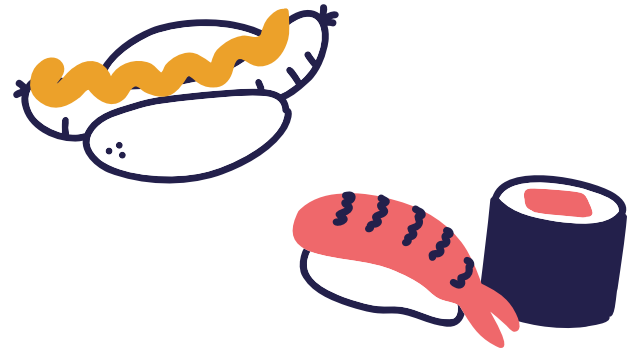


Was ist der Quantum Coin Toss?

Der Quantenmünzwurf ist ein Verfahren in der Quantenkryptografie, bei dem zwei Parteien, die sich nicht vertrauen, eine zufällige Entscheidung Analog zum klassischen Münzwurf über große Distanzen durchführen können.

Die Grundidee ist folgende:

Alice und Bob telefonieren, weil sie später gemeinsam Essen gehen wollen. Alice möchte Bratwurst essen, aber Bob hat mehr Lust auf Sushi. Alice schlägt vor, eine Münze zu werfen um zu entscheiden. Aber Bob zweifelt an der Methode und befürchtet, dass Alice einfach lügt, damit sie ihre Bratwurst bekommt. Schließlich hat Bob keine Möglichkeit zu überprüfen, ob Alice die Wahrheit sagt, weil er die Münze ja nicht sieht. Alice und Bob verwenden dafür den Qey-Gen und führen den Quantum CoinToss durch.



Quantum Coin Toss

1.

Alice wirft dabei eine Münze in immer den **selben Schlitz**, nur mit unterschiedlichen Werten. Bob misst nun die Münze indem er jedesmal zufällig entweder in Basis 1 oder Basis 2 ausliest. Beide notieren sich jeweils ihre Basen und Werte.

Ihre Listen sehen nun so aus:



2.

Bob kann nun raten, welche Basis Alice gewählt hat. Alice muss die Wahrheit sagen sonst fliegt sie auf!

Alice

Wurf	Basis	Wert
1.	1	0
2.	1	0
3.	1	1
4.	1	1
5.	1	1
6.	1	1
7.	1	1
8.	1	0
9.	1	0
10.	1	1
11.	1	0
12.	1	0

Bob

Wurf	Basis	Wert
1.	1	0
2.	0	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



Stell dir vor Bob rät Basis 1 und Alice behauptet, sie habe Basis 2 gewählt. Somit hätte Bob also falsch geraten. Wie kann Bob jetzt sicher sein, dass Alice nicht lügt?



Ganz einfach. Alice verrät nun die Werte der Münze, die sie Bob geschickt hat und Bob vergleicht diese mit den Werten, die er bei Basis 2 gemessen hat.



1x ... 50%

2x ... 25%

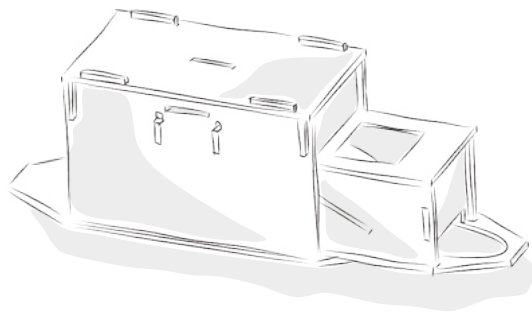
5x ... 0,031%

10x ... 0,001%

Bei Einem Messwert wäre die Chance 50% dass sie richtig rät. Bei zwei Messwerten wäre die Chance bei 25%, bei drei wären es 12,5% und bei zehn sogar 0,001%. Nun sehen wir uns den Qey-Gen an, der funktioniert nämlich nach dem selben Prinzip.

Einstein und der echte Zufall

Um eine zufällige Entscheidung zu treffen, werfen wir eine Münze. Aber schon Einstein hat gesagt, dass es sich hier nicht um echten Zufall handelt. Denn je nachdem mit wie viel Kraft wir die Münze werfen, wie der Wind steht, etc. Wird das Ergebnis beeinflusst. Wenn wir alles ganz genau wüssten, könnten wir es sogar berechnen. Ob leicht verdrehte Photonen durch den Filter kommen - dabei hingegen handelt sich um echten Zufall. Keiner kann es voraussagen oder beeinflussen.



Und genau das wird hier ausgenutzt um Schlüssel zu erzeugen oder auf größere Distanz eine zufällige Entscheidung zu treffen.



Das Qey-Gen Spiel wurde als Teil des Projekts Quanten 1x1 von der Junge Tüftler gGmbH und Tobias Schubert (Technische Universität Berlin) entwickelt. Das Projekt wird vom Bundesministerium für Bildung und Forschung durch die Maßnahme “Quantum aktiv” (Fördernummer: 13N15479) gefördert, die Teil der Hightech-Strategie der Bundesregierung ist.

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung





Superposition und Verschränkung?

Wenn du noch mehr über die wundersame Welt der Quanten lernen willst dann besuch uns doch auf unserer Webseite und sieh dir das „Quanten Tiq Taq Toe“ an!



<https://bit.ly/3v6Sc5E>

