KLASSISCHE VERSCHLÜSSELUNGSVERFAHREN

Schon seit langem werden Verschlüsselungen verwendet, um Nachrichten geheim zu übermitteln. Überlieferungen zufolge hat bereits Gaius Iulius Caesar (Ca. 50 n.Chr) ein Verschlüsselungsverfahren angewendet, das aus diesem Grund Caesar-Verschlüsselung genannt wird.

CAESAR-VERSCHLÜSSELUNG

Die Caesar-Verschlüsselung basiert auf einer einfach Verschiebung der einzelnen Buchstaben einer Nachricht. Zum Verschlüsseln wird dazu jeder einzelne Buchstabe im Alphabet um einen festen Buchstaben bzw. eine feste Anzahl N nach hinten verschoben. Zum Entschlüsseln werden die einzelnen Zeichen wieder um N nach vorne verschoben (Abb. 1).

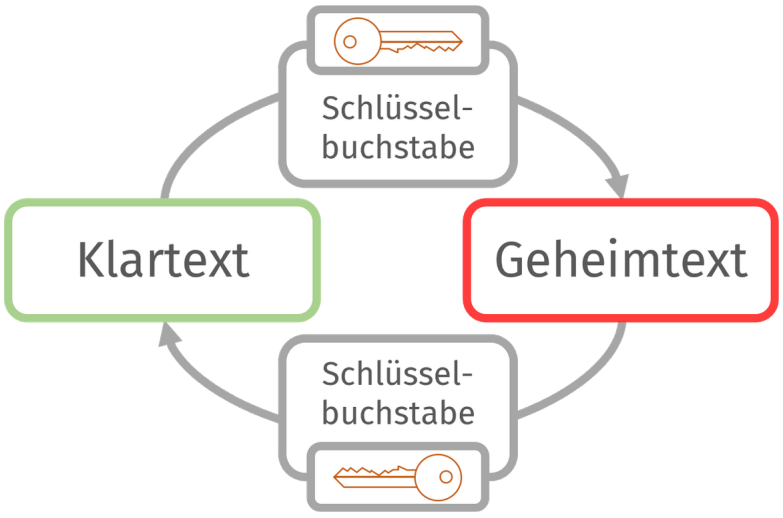


Abb. 1 — Prinzip der Caesar-Verschlüsselung

① Verschlüssele deinen eigenen Namen mit dem Buchstaben E!
Die Tabelle am Rand hilft dir.

Dein Name:

Verschlüsselter Name:

② Kommen in deinem Namen Buchstaben doppelt vor? Was fällt dir auf? Wie sicher findest du diese Verschlüsselung?

1	A
2	B
3	C
4	D
5	E
6	F
7	G
8	H
9	I
10	J
11	K
12	L
13	M
14	N
15	O
16	P
17	Q
18	R
19	S
20	T
21	U
22	V
23	W
24	X
25	Y
26	Z

Verschlüsseln

Entschlüsseln

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

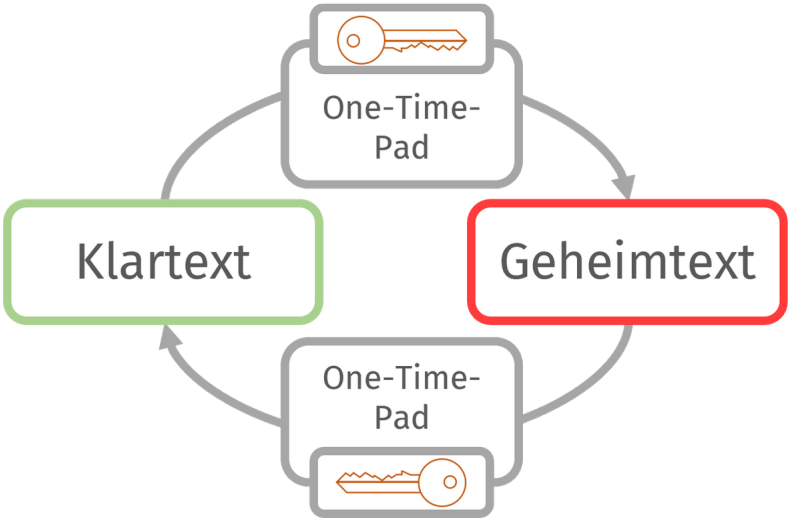
ONE-TIME-PAD

Die Sicherheit von symmetrischen Verfahren hängt stark von der **Länge** des Schlüssels ab. Aber auch die **Zufälligkeit** ist wichtig. Man sollte also nicht einfach einen Text aus einem Buch als Schlüssel benutzen. Besonders bei langen Nachrichten ergeben sich sonst Muster, die sich mit Computern relativ einfach entdecken lassen.
Tatsächlich sind sogar "Zufallszahlen", die mit einem Computer erzeugt wurden nicht gut als Schlüssel geeignet, weil oft noch eine gewisse Regelmäßigkeit enthalten ist. Der Schlüssel ist nicht **echt Zufällig**. Eine gute Möglichkeit, um echte Zufallszahlen zu erzeugen sind **Quanten-zufallsgeneratoren**.

③ Verschlüssele deinen eigenen Namen mit dem vorgegebenen Schlüssel!

Dein Name:										
Zufalls-schlüssel:	K	C	Y	J	R	E	C	N	W	E	W
Verschlüsselter Name:										

Um eine Nachricht mit symmetrischen Verfahren mathematisch sicher zu verschlüsseln, muss ein sogenanntes **One-Time-Pad** verwendet werden. Dazu wird für jede Nachricht ein neuer Schlüssel generiert, der (mindestens) so lang, wie die Nachricht, und echt zufällig ist.



Prinzip der Caesar-Verschlüsselung

Eine Nachricht, die mit einem **One-Time-Pad** verschlüsselt ist, kann aus mathematischer Sicht nicht geknackt werden.
Die **Schwierigkeit** bei der Verwendung eines One-Time-Pad ergibt sich beim **Schlüsselaustausch**. Besonders für den Austausch großer Datenmengen müssen lange Schlüssel generiert und geheim ausgetauscht werden. Dies ist in der Praxis nicht einfach durchzuführen. In der Kryptographie spricht man von dem Schlüsselverteilungsproblem.

1	A
2	B
3	C
4	D
5	E
6	F
7	G
8	H
9	I
10	J
11	K
12	L
13	M
14	N
15	O
16	P
17	Q
18	R
19	S
20	T
21	U
22	V
23	W
24	X
25	Y
26	Z

Verschlüsseln

Entschlüsseln

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

DIE IDEE ASYMMETRISCHER VERSCHLÜSSELUNGSVERFAHREN

In der Kryptografie unterscheidet man zwischen **symmetrischen** und **asymmetrischen** Verschlüsselungsverfahren. Symmetrische Verschlüsselungen zeichnen sich dadurch aus, dass der selbe Schlüssel zum Verschlüsseln und zum Entschlüsseln verwendet wird. Sowohl das *Caesar-Verfahren* als auch die Verschlüsselung mit dem *One-Time-Pad gehören* zu den symmetrischen Verfahren.
Im Gegensatz dazu werden bei asymmetrischen Verfahren unterschiedliche Schlüssel zum Ver- und Entschlüsseln verwendet, die der Empfänger der Nachrichten generiert. Einer der beiden Schlüssel ist für jeden öffentlich und wird zum Verschlüsseln verwendet. Den zweiten Schlüssel behält der Empfänger für sich. Er wird zum Entschlüsseln verwendet.
Natürlich müssen beide Schlüssel miteinander zusammenhängen, damit asymmetrische Verfahren funktionieren. In der Praxis werden dazu Rechenoperationen verwendet, die sich nicht einfach umkehren lassen. Die typischste Variante ist hier die Primfaktorzerlegung.

④ Dazu ein Rechenbeispiel (Taschenrechner erlaubt!):

a) Berechne das Produkt der Primzahlen 1307 und 6091

b) Berechnen Sie die Primfaktorzerlegung von 9113. (Hinweis: Es gibt genau 2 Primfaktoren.)

c) Vergleichen Sie die beiden Rechenaufgaben bzgl. der Schwierigkeit. Überlegen Sie, wie Sie die Primfaktorzerlegung des Ergebnisses aus a) berechnen würden.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

WIE SICHER SIND ASYMMETRISCHE VERSCHLÜSSELUNGSVERFAHREN?

Asymmetrische Verfahren nutzen aus, dass auch Computer sehr lange brauchen um Primfaktorzerlegungen zu berechnen. Dazu reicht es zwar nicht aus, vierstellige Primfaktoren zu verwenden, aber in der Praxis lassen sich auch sehr schnell sehr viel längere Primzahlen erzeugen, die dann multipliziert werden. Mit herkömmlichen Computern dauert es dann sehr lange die Zerlegung zu berechnen, so dass eine verschlüsselte Nachricht praktisch sicher ist.
Ein mögliches Sicherheitsrisiko ergibt sich durch den Shor-Algorithmus. Dieser besondere Algorithmus kann Primzahlzerlegungen im Vergleich zu den üblichen Algorithmen sehr schnell berechnen, muss dafür allerdings auf einem Quantencomputer ausgeführt werden, so dass er aktuell noch kein akutes Risiko darstellt. Es gibt aber schon Institutionen, die verschlüsslte Nachricht speichern, um diese entschlüsseln zu können, sobald Quantencomputer zur Verfügung stehen.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

DATEN ÜBERTRAGEN MIT EINZELNEN PHOTONEN

Eine Möglichkeit um Nachrichtenübertragungen sicherer zu machen, ist die Verwendung von einzelnen Photonen zur Datenübertragung. Dazu wird mit jedem Photon genau ein **Bit** der Informationen übertragen. Das Bit wird in der Polarisation codiert. Beispielsweise kann dabei die horizontale Polarisation ($|\rightarrow\rangle$) für die 0 und die vertikale Polarisation ($|\uparrow\rangle$) für die 1 stehen. Weil beide Polarisationen orthogonal zueinander sind, lässt sich der Zustand eines Photons so eindeutig bestimmen, wenn richtig gemessen wird. Man nennt zwei solcher orthogonaler Zustände eine Basis.

Bits
Das Bit ist die kleineste mögliche Dateneinheit, mit der ein Computer arbeiten kann. Es hat eine einzelne Stelle in der nur eine 1 oder eine 0 stehen kann.

TECHNISCHE HINDERNISSE BEIM ABHÖREN

Rein technisch ist es bereits sehr schwierig eine Nachricht dieser Art abzuhören, weil ein Spion die genaue Ausrichtung der Basis kennen muss, um zuverlässig messen zu können. Außerdem muss er jedes mal ein neues Photon zum eigentlichen Empfänger senden, damit diesem die Übertragung nicht auffällt, weil das Photon nach der Messung nicht mehr existiert.

DATENÜBERTRAGUNG BEIM BB84-PROTOKOLL

In der Praxis wird eine weitere Basis für die Kommunikation verwendet. Dazu werden zusätzlich die beiden Zuständen $|\nwarrow\rangle$ (-45°) und $|\nearrow\rangle$ (+45°) verwendet, die ein weiteres Paar orthogonaler Zustände bilden.
Wie auch für das andere Zustandspaar wird einem der Zustände die 1 und einem der Zustände die 0 zugeordnet. Insgesamt ergibt sich so die Zuordnung aus Tabelle 1.

Basis	Pol.	Bit
×	$\|\nearrow\rangle$	1
×	$\|\nwarrow\rangle$	0
+	$\|\uparrow\rangle$	1
+	$\|\rightarrow\rangle$	0

Tab. 1 – Basen, Polarisationszustände und zugeordnete Bitwerte

① Übersetze die folgenden Zustandsreihe mit Hilfe von Tab. 1 in eine Bitfolge.
$|\nearrow\rangle$ $|\rightarrow\rangle$ $|\uparrow\rangle$ $|\rightarrow\rangle$ $|\nearrow\rangle$ $|\nwarrow\rangle$

② Gib mindestens zwei Möglichkeiten an die folgende Zahlenfolge durch eine Reihe von Zuständen zu repräsentieren:
1100011

Im BB84-Protokoll wird zufällig zwischen den beiden Basen gewechselt, um ein Abhören unmöglich zu machen. Das genaue Protokoll lässt sich am besten an einem Modell nachvollziehen und wird auf den nächsten Seiten beschrieben.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

AUFBAU DES EXPERIMENTS

Zur Durchführung des BB84-Protokolls werden in der Realität einzelne Photonen als Informationsträger verwendet. Dies ist nötig, weil der Zufallsaspekt von einzelnen Photonen genutzt wird, um eine sichere Übertragung zu gewährleisten.
In der Praxis ist es sehr aufwendig einzelne Photonen zu erzeugen und noch aufwendiger diese zuverlässig wieder zu messen. Aus diesem Grund wird das BB84-Protokoll nur als Modellexperiment durchgeführt, bei dem keine einzelnen Photonen genutzt werden.

BENÖTIGTE BAUTEILE

① Legen Sie die auf Abb. 1 dargestellten Bauteile bereit. Zusätzlich benötigen Sie eine Grundplatte mit Mindestgröße 2x6 oder zwei Grundplatten mit Mindestgröße 2x3.

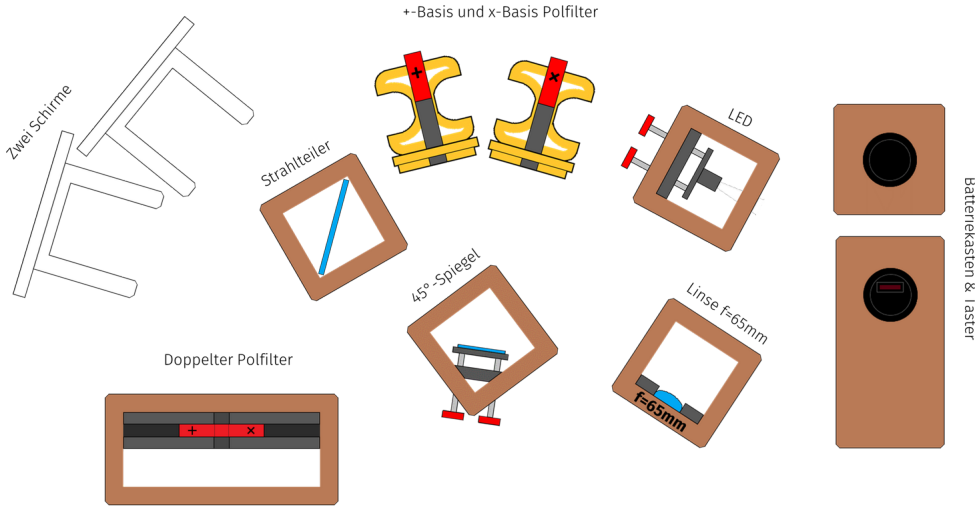
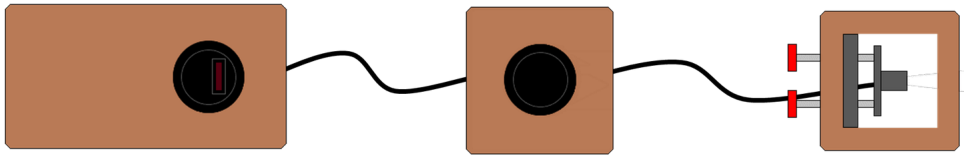


Abb. 1 — Benötigte Bauteile

② Stellen Sie sicher, dass die LED, der Batteriekasten und der Taster funktionieren. Die LED sollte (nur dann) leuchten, wenn..

- die LED im Taster und der Taster im Batteriekasten eingesteckt sind wie auf Abb. 2,
- der Batteriekasten eingeschaltet ist (LED im Schalter leuchtet) und
- der Taster gedrückt ist.



Ansclhießen der LED

Präparation von Einzelphotonen
Wenn Einzelphotonen erzeugt werden, befinden sie sich schon in einem Polarisationszustand. um diesen zu ändern, sind Polarisations-filter nicht gut geeignet, weil Sie viele Photonen absorbieren. Stattdessen werden Wellenplatten verwendet, die die Polarisation von Licht drehen können.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

AUFBAU DES SENDERS

Der Versuchsaufbau ist aufgeteilt in den Sender Alice und den Empfänger Bob. Zuerst wird der Sender Alice aufgebaut und erklärt.

③ Bauen Sie den Aufbau für Alice wie auf Abb. 2 auf.

- Es gibt zwei Polfilter, die sich leicht unterscheiden. Legen Sie beide bereit.

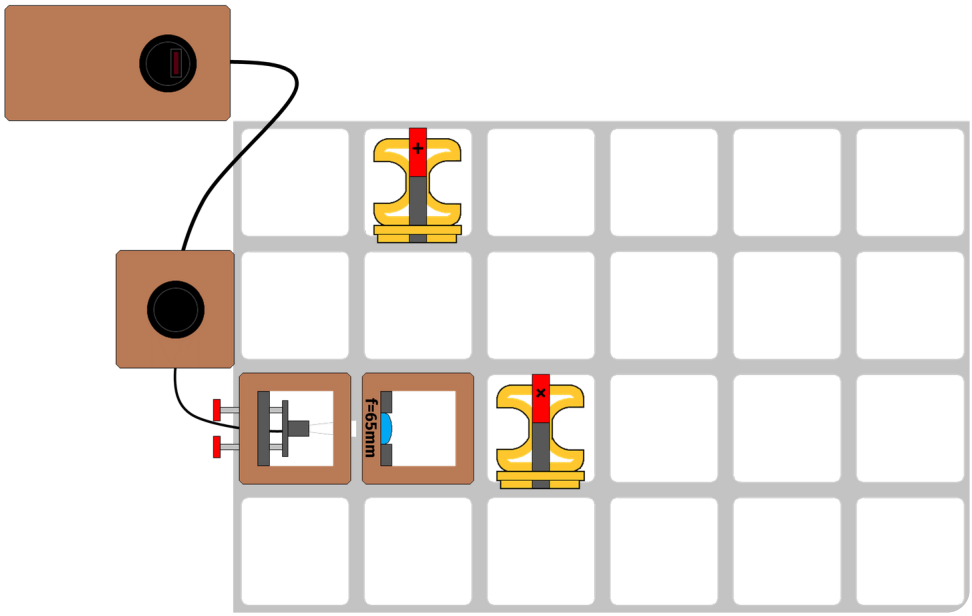


Abb. 2 — Sender Alice

PRÄPARATION EINES ZUSTANDS

Mit diesem Aufbau ist es jetzt möglich vier unterschiedliche Polarisationszustände zu „präparieren“. Dazu muss nur der richtige Polfilter in der richtigen Ausrichtung im Licht der LED positioniert werden. Der konkrete „Zustand“, der so erzeugt wird, kann von den Einprägungen des Polfilters abgelesen werden, wie auf Abbildung 3 dargestellt.

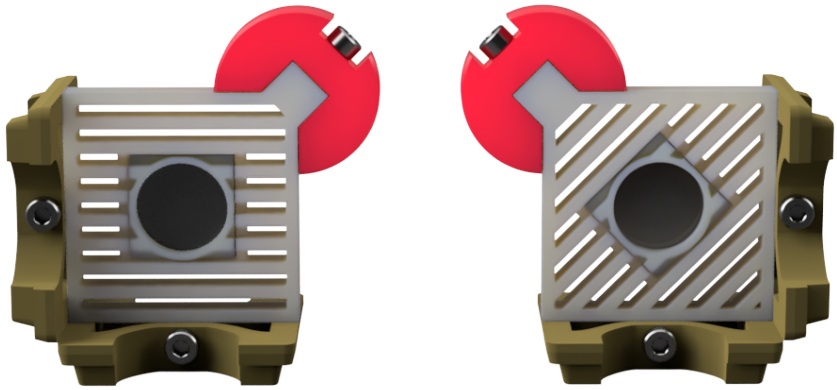


Abb. 3 — Polfilter links: $|\rightarrow\rangle$, Polfilter Rechts: $|\nearrow\rangle$.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

Beide Polfilter können um 90° gedreht werden um andere Zustände zu erzeugen. So ist es außerdem möglich die Zustände $|\uparrow\rangle$ (bzw. 0°) und $|\nwarrow\rangle$ (bzw. -45°) zu erzeugen.
Mit jedem Polfilter lassen sich dementsprechend zwei Zustände präparieren, die genau orthogonal zueinander sind. Gemeinsam werden zwei solcher orthogonalen Zustände *Basis* genannt.
Wir nennen den Polfilter, mit dem sich die Zustände $|\nearrow\rangle$ und $|\nwarrow\rangle$ erzeugen lassen X-Polfilter und die zugehörige Basis X-Basis. Den Polfilter, mit dem sich die Zustände $|\uparrow\rangle$ und $|\rightarrow\rangle$ erzeugen lassen nennen wir $+$-Polfilter.

DER EMPFÄNGER BOB

Der Aufbau von Bob dient dazu eine Messung der Polarisationszustände durchzuführen, die von Alice präpariert wurden.
Wie auch die Präparation wird die Messung technisch deutlich einfacher dadurch, dass keine einzelnen Photonen genutzt werden. Für die Messung kann aus diesem Grund ein einfacher Schirm (bzw. genau genommen das eigene Auge) als Detektor verwendet werden.

④ Ergänzen Sie Bob im Aufbau (Abb. 4). Sie können auch mit zwei 3x4-Grundplatten arbeiten und Alice und Bob getrennt aufbauen.

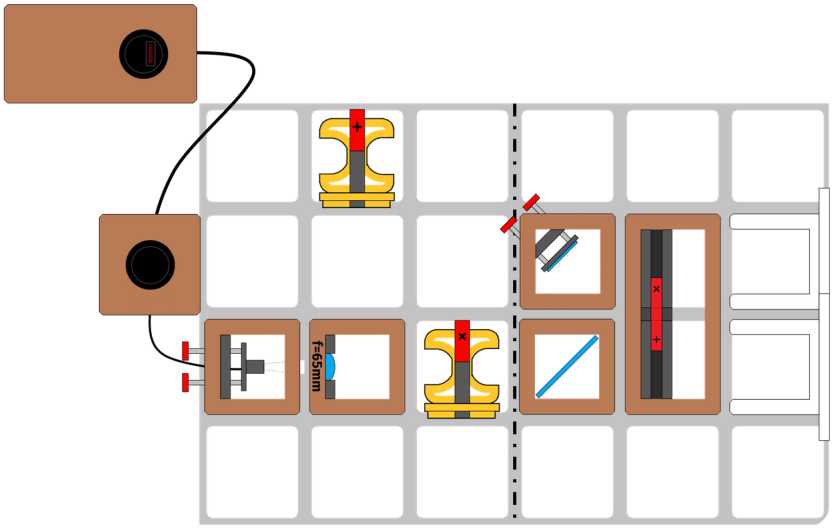


Abb. 4 — Vollständiger BB84 Modellaufbau.

DURCHFÜHREN EINER MESSUNG

Auf Bobs Seite fällt das Licht zunächst auf einen Strahlteiler, der das Licht in zwei Teilstrahlen aufteilt. Einer der Teilstrahlen wird durch einen Spiegel auf den Doppelten Polfilter reflektiert, der andere trifft direkt auf den doppelten Polfilter. Weil sowohl die Reflexion am Spiegel als auch die Reflexion und Transmission am Strahlteiler (nahezu) vollständig polarisationserhaltend sind, treffen zwei Strahlen der gleichen Polarisation auf den Doppelten Polfilter.
Im doppelten Polfilter sind zwei Polarisationsfolien enthalten, die um 90° gegeneinander gedreht sind (Abb. 5). Ähnlich wie beim X-Polfilter und beim $+$-Polfilter ist die Polarisationsrichtung hier vom Gitter vor dem Polfilter abzulesen. Auf (Abb. 5) sind also gerade die Polarisationen der $+$-Basis eingestellt.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

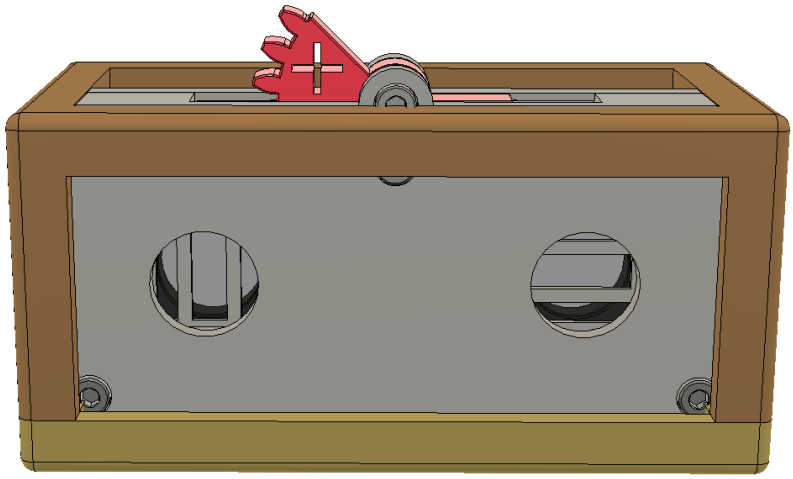


Abb. 5 — Doppelter Polfilter, links $|\uparrow\rangle$-Ausrichtung, rechts $|\rightarrow\rangle$-Ausrichtung.

Durch den roten Heben an der Oberseite des Würfels lässt sich die Ausrichtung beider Polarisationsfilter um 45° drehen. Auf diese Weise lässt sich der Polarisationsfilter auf die X-Basis einstellen. Abb. 6 zeigt den Polfilter in Einstellung auf X-Basis.

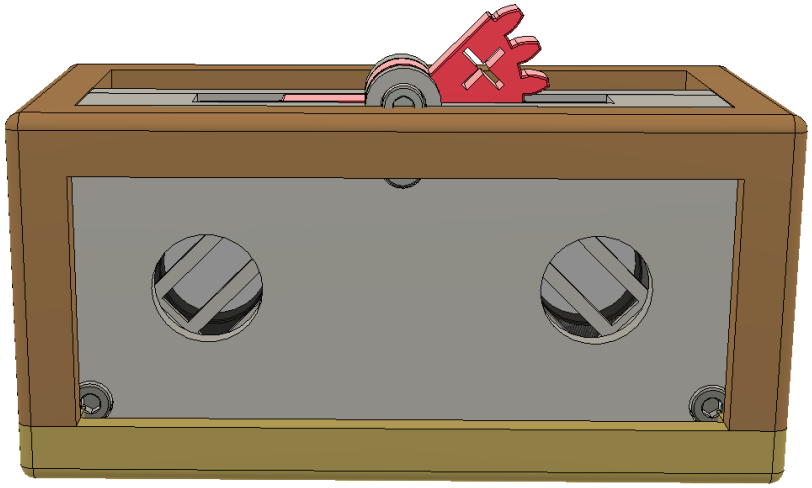


Abb. 6 — Doppelter Polfilter, links $|\nearrow\rangle$-Ausrichtung, rechts $|\nwarrow\rangle$-Ausrichtung.

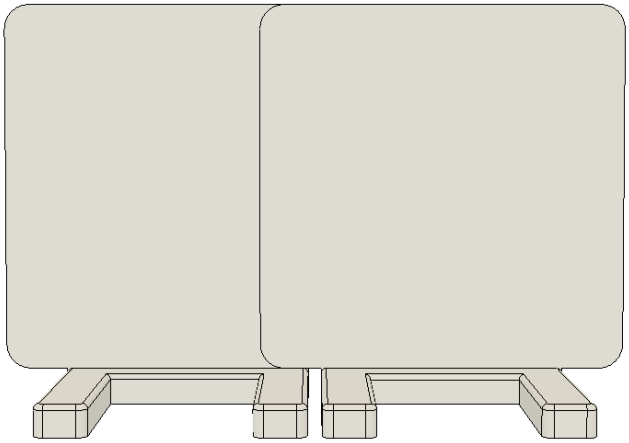
gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

MODELLCHARAKTER DES EXPERIMENTS

Wie bereits angemerkt ist das Experiment nur ein Modell für das BB84-Protokoll. Nachfolgend wirst du ausprobieren, welche Ergebnisse sich im Modell ergeben und welche Grenzen das Modell hat.

① Führe eine Messung durch, indem du die folgenden Schritte durchführst:

- Stelle den Doppelpolfilter auf Bobs Seite so ein, dass er in der +-Basis misst.
- „Präpariere“ dann einen $|\uparrow\rangle$-Zustand, indem du den entsprechenden Polfilter in der entsprechenden Basis auf dem Gitter positionierst und die LED mit dem Taster aktivierst.
- Skizziere das Bild, das auf dem Schirm entsteht.



Weil bei der Messung die Messbasis zum präparierten Zustand passt, kann ein eindeutiges Ergebnis gemessen werden.

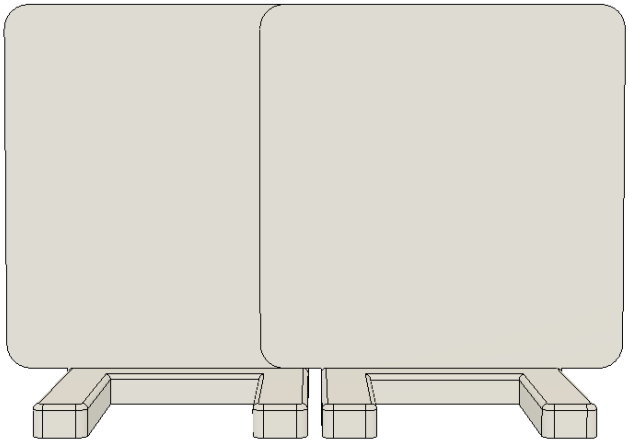
Modellgrenzen:
Im Modell wird das Licht am Strahlteiler in etwa gleichgroße Anteile aufgeteilt. Einer der Polfilter im Doppelpolfilter absorbiert das gesamte Licht, der zweite Polfilter transmittiert (nahezu) das gesamte Licht. Dieser zweite Teil ist dann auf dem Schirm zu erkennen.
Für den Fall eines einzelnen Photons ist das Aufteilen am Strahlteiler nicht möglich. Stattdessen entsteht eine Superposition, die durch die Messung an einem der Polarisationsfilter kollabiert. Am Ende könnte ein Photon mit einer Wahrscheinlichkeit von 50% an der Stelle gemessen werden, an der im Modell die Hälfte der Ausgangsintensität beobachtet werden kann. Mit einer Wahrscheinlichkeit von 50% wird das Photon bei der Messung am anderen Polfilter absorbiert.
Im Realexperiment wird aus diesem Grund stattdessen ein *polarisierender Strahlteiler* verwendet. Dieser transmittiert immer eine Polarisationsrichtung und reflektiert immer die dazu orthogonale Ausrichtung, sodass es nicht zu Schwierigkeiten mit der Absorption kommen kann.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

② Wie würde sich das Ergebnis im Modellexperiment ändern, wenn ein polarisierender Strahlteiler eingesetzt werden würde?

① Führe ein zweite Messung mit dem selben Aufbau durch.

- Stelle den Doppelpolfilter diesmal auf die $\times$-Basis ein.
- „Präpariere“ dann wieder einen $|\uparrow\rangle$ -Zustand.
- Skizziere das Bild, das auf dem Schirm entsteht.



Modellgrenzen (Vielleicht als Lückentext?)
Im Modell kann auf beiden Schirmen Licht beobachtet werden. Dies ist im Realen Experiment offensichtlich nicht möglich, das das einzelne Photon nicht an beiden Detektoren gleichzeitig gemessen werden kann. Stattdessen zerfällt die Superposition durch die Messung und es ist zufällig, an welchem Detektor das Photon gemessen wird.
Dies hat die wichtige Konsequenz, dass Bob in der Realsituation nicht unterscheiden kann, ob er ein zuverlässiges oder ein zufälliges Ergebnis gemessen hat, solange er nicht weiß, in welche Basis Alice das Bit verschlüsselt hat. Im Modell wird dies im Gegenteil dazu sofort deutlich und und hat keinen Zufallscharakter. Aus dem Grund müssen wir uns bei der Durchführung „dummstellen“ und so tun, als wenn wir nicht wüssten, ob das Ergebnis zuverlässig ist oder nicht. Auch den Zufall müssen wir nachstellen.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

SIMULATION EINER SCHLÜSSEL-GENERIERUNG NACH DEM BB84-PROTOKOLL

AUSTAUSCH VON DATEN

Die eigentlichen Informationen werden beim BB84-Protokoll in Form von Bit-Werten in der Polarisation verschlüsselt. Dafür ordnet man jeweils einem der beiden Polarisationszustände einer Basis den Bitwert 1 und dem anderen Zustand den Bitwert 0 zu. Die Zuordnung kann Beispielsweise wie rechts dargestellt aussehen.
Es gibt jetzt für jeden Bitwert zwei mögliche Kodierungen. Das ist genau so gewollt, um einen sicheren Schlüssel zu generieren.

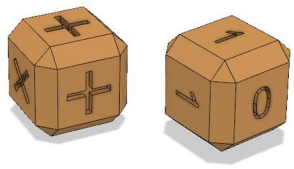
Basis	Pol.	Bit
×	$\|\nearrow\rangle$	1
×	$\|\nwarrow\rangle$	0
+	$\|\uparrow\rangle$	1
+	$\|\rightarrow\rangle$	0

EIN SICHERER SCHLÜSSEL

Damit ein Schlüssel sicher ist, dürfen nur Alice und Bob darauf Zugriff haben. Dazu muss im Wesentlichen dafür gesorgt werden, dass von der Kommunikation zwischen Alice und Bob nicht ausreichend Daten abgehört werden können, um den vollständigen Schlüssel daraus zu generieren. Außerdem sollte im Idealfall auffallen, wenn der Austausch des Schlüssels abgehört wird.
Mit dem BB84-Protokoll wird beides erreicht. Dazu nutzt man aus, dass Bob bei gleichen Basen ein verlässliches Messergebnis erhält und bei ungleichen Basen ein zufälliges Ergebnis misst. Durch die doppelte Belegung der Bitwerte können gerade beide Situationen auftreten. Durch eine zufällige Kombination beider Fälle kann dann ein sicherer Schlüsselaustausch erfolgen.

SIMULATION DES ZUFALLS

Weil bei dem vorhanden Experimentiermaterial keine Einzelphotonen genutzt werden, muss nachgeholfen werden, um den „Quantenzufall“ zu simulieren. Dazu werden Würfel (Siehe Abb. Rechts) verwendet. Es gibt einen Würfel, mit dem eine zufällig Basis gewählt werden kann und einen Würfel mit dem zufällig



Würfel zur Simulation des Zufalls

DURCHFÜHRUNG DES PROTOKOLLS

Auf den nächsten Seiten wird das BB84-Protokoll beispielhaft durchgespielt. Dazu wird in zwei Gruppen gearbeitet. Eine Gruppe bedient den Aufbau von Alice, eine den Aufbau von Bob.
Für die Durchführung des Protokolls wird neben dem vorhandenen Kommunikationskanal mit Einzelphotonen als Informationsträger noch ein zweiter Kanal benötigt. Dieser Kanal ist öffentlich und hat keine besonderen technischen Anforderungen. In der Realität könnte das beispielsweise eine Kommunikation durch das Internet sein. Im Modell können die entsprechenden Informationen einfach mündlich ausgetauscht werden.

1 Führt+ jetzt den Schlüsselaustausch durch.

- Teilt euch dazu in zwei Gruppen auf.
- Die erste Gruppe spielt die Rolle von Alice und orientiert sich an der entsprechenden Anleitung.
- Die zweite Gruppe spielt die Rolle von Bob. Auch dafür gibt es eine entsprechende Anleitung.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

ALICE' AUFGABE

ERZEUGUNG DES SCHLÜSSELS

Alice entscheidet sich für jedes übertragene Bit zufällig für einen Zustand. Dazu wählt sie jeweils eine Basis und einen Bitwert. Anschließend wird der entsprechende Polfilter in der korrekten Ausrichtung auf das Gitter gesetzt.

Basis	Pol.	Bit
×	$\lvert\nearrow\rangle$	1
×	$\lvert\nwarrow\rangle$	0
+	$\lvert\uparrow\rangle$	1
+	$\lvert\rightarrow\rangle$	0

① Versende zunächst 14 Bits in unterschiedlichen Basen an Bob. Gehe für jedes Bit wie folgt vor:

a) Wähle zufällig eine Basis und einen Bitwert (z.B. durch Würfeln).
b) Setze den entsprechenden Polfilter in der richtigen Ausrichtung auf das Gitter.
c) Sende den Bitwert, indem Du die LED aktivieren.
d) Notiere die Basis und den Bitwert in der Tabelle.

Messung	1	2	3	4	5	6	7
Basis							
Bitwert							

Messung	8	9	10	11	12	13	14
Basis							
Bitwert							

② Vergleiche für alle Bits die verwendete **Basis** mit der von Bob und streiche alle Spalten, in denen sich die Basis von Bobs Basis unterscheidet. Notiere die übrigen Bitwerte als *One-Time-Pad*.

One-Time-Pad
(Streng Geheim) _____

Schlüssellänge

Damit ein einzelner Buchstabe verschlüsselt werden kann, sind fünf Bits nötig. Bei 14 übertragenen Bits und einer Wahrscheinlichkeit für die gleiche Basis von 50%, liegt der Erwartungswert bei sieben Bits. Normalerweise sind also ausreichend viele Bits vorhanden. Sollte das One-Time-Pad zu kurz sein müssen weitere Bits ausgetauscht werden. Besonders bei sehr großen Mengen lässt sich über den Erwartungswert sehr gut abschätzen, wie viele Bits notwendig sind um einen ausreichend langen Schlüssel zu erzeugen, so dass die Zufallskomponente nicht zu Problemen in der Durchführung führt.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

VERWENDUNG DES SCHLÜSSELS

③ Verschlüssle einen beliebigen Buchstaben im (vereinfachten) ASCII-Format. Gehe dazu wie folgt vor:

a) Suche dir einen beliebigen Buchstaben aus und notiere die vereinfachte ASCII-Codierung (Tab. 1):

b) Addiere den Schlüssel zum gewählten Buchstaben (es gilt 1+0=1 und 1+1=0). So ergibt sich die verschlüsselte „Nachricht“.

Ausgewählter Buchstabe: ☐

Buchstabe in ASCII-Format: ☐☐☐☐☐

One-Time-Pad (Erste 5 Stellen) ☐☐☐☐☐

Verschlüsselter Buchstabe: ☐☐☐☐☐

c) Gib den verschlüsselten Buchstaben **öffentlich** an Bob weiter. Gleiche Deinen unverschlüsselten Buchstaben mit Bob ab, sobald er deine Nachricht entschlüsselt hat.

Schlüssel zu kurz?
Falls der Schlüssel weniger als 5 Stellen lang ist, werden die ersten Stellen des Schlüssels noch einmal verwendet.

Vereinfachte ASCII-Tabelle

A	00001	J	01010	S	10011
B	00010	K	01011	T	10100
C	00011	L	01100	U	10101
D	00100	M	01101	V	10110
E	00101	N	01110	W	10111
F	00110	O	01111	X	11000
G	00111	P	10000	Y	11001
H	01000	Q	10001	Z	11010
I	01001	R	10010	Φ	11011

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

BOBS AUFGABE

ERZEUGUNG DES SCHLÜSSELS

Bob entscheidet sich für jedes übertragene Bit zufällig für eine Basis, in der er Messen möchte. Falls das Ergebnis im Modellexperiment uneindeutig ist, muss er dann außerdem noch zufällig einen der beiden Bitwerte auswählen.

① Empfange 14 Bits von Alice. Gehe wie folgt vor.

a) Wähle zufällig eine Basis und stelle den Doppelpolfilter entsprechend ein. Notiere die Basis in der untenstehenden Tabelle
b) Gib Alice ein Zeichen, dass Du bereit für eine Übertragung bist.
c) Falls du ein eindeutiges Ergebnis misst, notieren den zugehörigen Bitwert in der untenstehenden Tabelle.
d) Falls du kein eindeutiges Ergebnis misst, entscheide dich zufällig für einen Bitwert und notieren diesen.

Basis	Pol.	Bit
×	$\|\nearrow\rangle$	1
×	$\|\nwarrow\rangle$	0
+	$\|\uparrow\rangle$	1
+	$\|\rightarrow\rangle$	0

Messung	1	2	3	4	5	6	7
Basis							
Bitwert							

Messung	8	9	10	11	12	13	14
Basis							
Bitwert							

② Vergleiche für alle Bits die verwendete **Basis** mit der von Alice und streiche alle Spalten, in denen sich die Basis von Alice' Basis unterscheidet. Notiere die übrigen Bitwerte als One-Time-Pad.

One-Time-Pad
(Streng Geheim) _____

Schlüssellänge
Damit ein einzelner Buchstabe verschlüsselt werden kann, sind fünf Bits nötig. Bei 14 übertragenen Bits und einer Wahrscheinlichkeit für die gleiche Basis von 50%, liegt der Erwartungswert bei sieben Bits. Normalerweise sind also ausreichend viele Bits vorhanden. Sollte das One-Time-Pad zu kurz sein müssen weitere Bits ausgetauscht werden. Besonders bei sehr großen Mengen lässt sich über den Erwartungswert sehr gut abschätzen, wie viele Bits notwendig sind um einen ausreichend langen Schlüssel zu erzeugen, so dass die Zufallskomponente nicht zu Problemen in der Durchführung führt.

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

VERWENDUNG DES SCHLÜSSELS

③ Alice verwendet jetzt den Schlüssel um einen Buchstaben zu verschlüsseln. An dieser Stelle musst du dich einen Moment gedulden. Entschlüssle dann den verschlüsselten Buchstaben, den Alice dir mitteilt, wie folgt:

a) Notiere den verschlüsselten Buchstaben, den Alice dir übermittelt.
b) Addiere den Schlüssel zum verschlüsselten Buchstaben (es gilt 1+1=0). So ergibt sich der unverschlüsselte Buchstabe im Ascii-Format. Falls der Schlüssel weniger als 7 Stellen lang ist, werden die ersten Stellen des Schlüssels noch einmal verwendet.
c) Nutze die ASCII-Tabelle (Tabelle 3), um den Buchstaben zu bestimmen, und gleiche diesen mit Alice ab.

Verschlüsselter Buchstabe: ☐

Verschlüsselter Buchstabe (ASCII): ☐☐☐☐☐☐☐

One-Time-Pad (Erste 7 Stellen) ☐☐☐☐☐☐☐

Entschlüsselter Buchstabe (ASCII): ☐☐☐☐☐☐☐

Entschlüsselter Buchstabe: ☐

Vereinfachte ASCII-Tabelle

A	00001	J	01010	S	10011
B	00010	K	01011	T	10100
C	00011	L	01100	U	10101
D	00100	M	01101	V	10110
E	00101	N	01110	W	10111
F	00110	O	01111	X	11000
G	00111	P	10000	Y	11001
H	01000	Q	10001	Z	11010
I	01001	R	10010	Φ	11011

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG

ABHÖRSICHERHEIT

Zu Beginn wurde angekündigt, dass das BB84 Protokoll theoretisch abhörsicher ist. Tatsächlich ist ein möglich einen Teil der Schlüsselübertragung abzuhören. Wenn das Protokoll korrekt durchgeführt wird, fällt dies aber immer auf. Nachfolgend wird erklärt, wie das möglich ist.

① *Alice schickt ein ／-polarisiertes Photon (Bitwert 1) an Bob, das Eve abfängt. Welche Bitwerte kann Eve messen, wenn sie in der ×-Basis misst und welche kann sie messen, wenn Sie in der +-Basis misst? Geben Sie jeweils die Wahrscheinlichkeiten an.*

×-Basis
P(1|×)=
P(0|×)=

+-Basis
P(1|+)=
P(0|+)=

② *Alice schickt wieder ein ／-polarisiertes Photon (Bitwert 1) an Bob, das Eve abfängt. Eve misst die Polarisation in der +-Basis. Sie misst den Bitwert 1. Und sendet deshalb ein \|-polarisiertes Photon zu Bob. Bob misst in der ×-Basis. Wie hoch ist die Wahrscheinlichkeit, dass Bob den Bitwert 1 misst? Wie hoch ist die Wahrscheinlichkeit für Bitwert 0? Welche Wahrscheinlichkeiten ergeben sich, wenn Eve den Bitwert 1 misst und ein \|-polarisiertes Photon zu Bob schickt?*

|-polarisiertes Photon
P(1|❙)=
P(0|❙)=

—-polarisiertes Photon
P(1|—)=
P(0|—)=

Um zu überprüfen, ob es einen Lauschangriff gab, vergleichen Bob und Alice (über einen offenen Kanal) die ersten Stellen ihres Schlüssels. Durch einen Lauschangriff würde eine große Fehlerquote entstehen, die dafür sorgt, dass der Lauschangriff aufgedeckt werden kann.

③ *Welcher Fehleranteil ist zu erwarten, wenn Alice, Eve und Bob die Basis für jedes Photon zufällig wählen?*

gefördert durch:
WILHELM UND ELSE HERAEUS-STIFTUNG