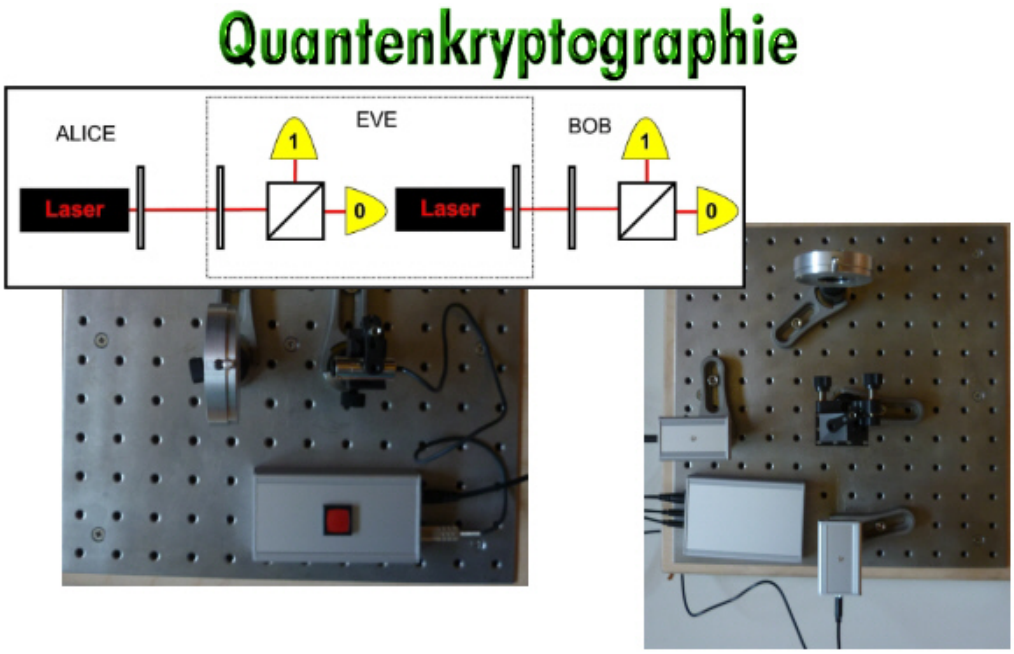
Moderne Quantenphysik in der Schule



Ein Modellexperiment zum BB84-Protokoll

von Jörn Schneider

Grundlagen:

Kryptografie ist die Wissenschaft der Verschlüsselung von Nachrichten. Benutzte man dafür früher einfaches Vertauschen von Buchstaben oder sogenannte Gitter, so sind im Zeitalter des Computers kompliziertere Verfahren erforderlich. So wie im normalen Leben ein Schlüssel fremde Personen daran hindert, unsere Wohnung zu betreten, so hindert ein digitaler Schlüssel fremde Personen daran, unsere Daten zu lesen. Ein digitaler Schlüssel besteht aus einer Reihenfolge von Bits. Dabei gilt: Je mehr Bits ein Schlüssel hat, umso mehr Möglichkeiten gibt es.

Bits	2	4	8	16	32	64	128
Schlüssel	4	16	256	655364	$4{,}29\ 10^{9}$	$1{,}84\ 10^{19}$	$3{,}40\ 10^{38}$

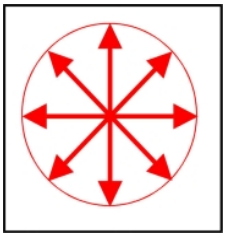
Ein Lauscher muss dabei im Prinzip alle Möglichkeiten ausprobieren um die Daten lesen zu können. Ein Schlüssel von 16 Bits kann noch durch einfaches Ausprobieren in wenigen Stunden geknackt werden. Geht man davon aus, dass ein Computer pro Sekunde 1 Milliarde Schlüssel testen kann, dann benötigt man für

32 Bit	64 Bit	128 Bit
4,29s	585 Jahre	$1{,}08\ 10^{22}$ Jahre

Ein 128 Bit-Schlüssel würde also mehr Zeit benötigen, als Zeit in unserem Weltalls mit seinem Alter von 13,8 Milliarden Jahren vergangen ist. Immer schnellere Rechner ermöglichen allerdings auch immer mehr Schlüssel in der gleichen Zeit zu testen, so dass dies ein klassisches Hase-Igel-Problem wird. Heutige Großrechner könnten rund 10^{15} Schlüssel in einer Sekunde testen und die Rechenleistung steigt ständig an.

Aber es gibt auch prinzipiell unknackbare Schlüssel. Und zwar dann, wenn ein Schlüssel unendlich lange ist oder nur einmal benutzt wird. Die Quantenphysik stellt uns dabei eine Möglichkeit zur Verfügung, einen einmaligen Schlüssel zu erzeugen, den wir auch nur einmal benutzen und der damit völlig unknackbar ist.

Was ist Polarisation?



Licht ist ein wichtiges Werkzeug in der Quantenkryptografie. Neben der Farbe (der Physiker spricht hier von der Wellenlänge) hat das Licht noch eine weitere Eigenschaft, die man nicht sofort sehen kann. Licht kann man als Welle auffassen. Dabei sendet eine normale Lichtquelle (z.B. eine Glühlampe) Wellen in alle Richtungen aus. Schauen wir von vorne auf solch eine Welle, so kann diese in jede Richtung eines Kreises schwingen. Glühlampenlicht ist nicht polarisiert.
Bei Lasern mit Halbleiterdioden ist dies anders. Durch den Aufbau und die Lichterzeugung ist dieses Laserlicht immer polarisiert. Es schwingt nur in einer Richtung. Durch Drehen des Lasers kann man dann die Schwingungsebene festlegen.

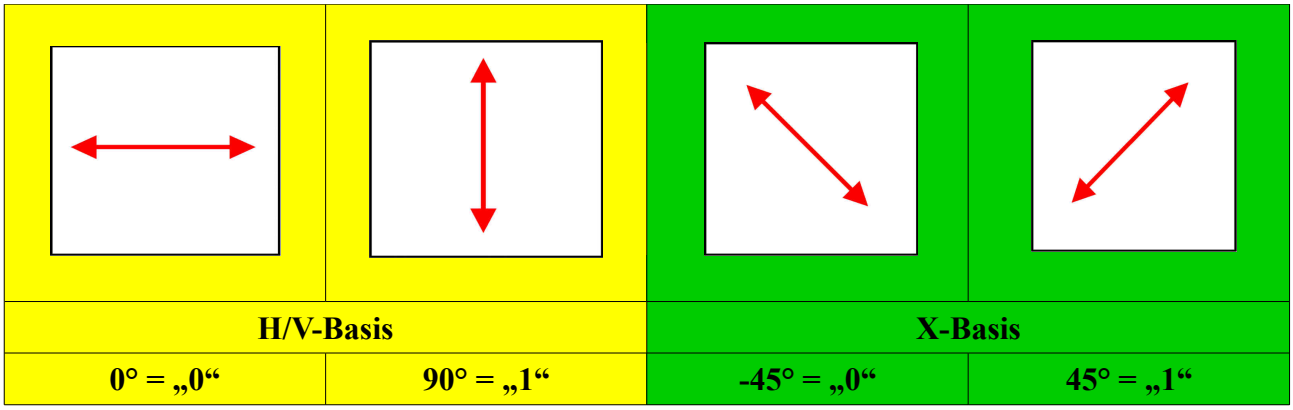
Mit Hilfe von Polarisationsfolien können wir nachweisen, dass Licht polarisiert ist. Betrachten wir das Laserlicht durch eine solche Folie, so sehen wir, dass beim Drehen der Folie, das Licht von maximaler Helligkeit auf (idealerweise) Dunkelheit sich verändert. Zwischen maximaler Helligkeit und Dunkelheit liegt ein Winkel von 90°.

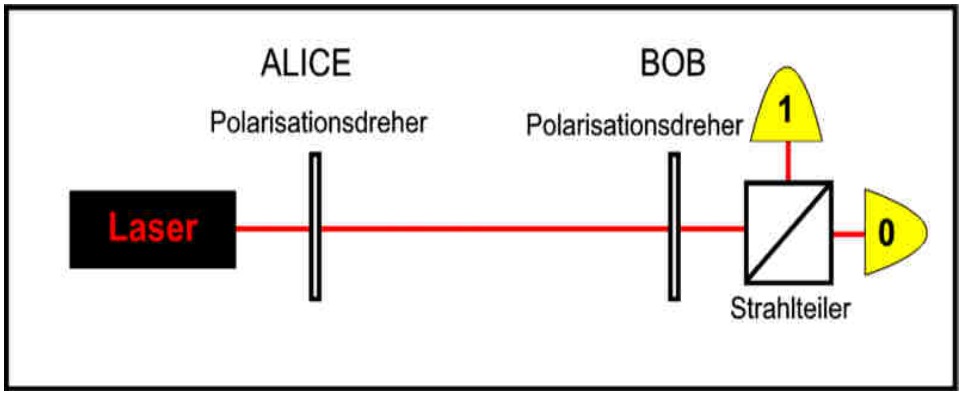
Quarzglas mit der Dicke von der Hälfte der Lichtwellenlänge (632nm!) hat eine interessante Eigenschaft. Beim Drehen eines solchen dünnen Quarzglasplättchen dreht sich auch die Polarisationsrichtung mit. Da ein solches Plättchen viel zu zerbrechlich wäre, wird es auf eine Glasplatte aufgebracht. Ein solches Plättchen wird als lambda/2-Waveplate bezeichnet. In unserem Versuch werden wir diese benötigen.

Klebt man zwei Prismen zu einem Würfel zusammen und schickt Licht durch eine der horizontalen Flächen, so teilt sich der Strahl in zwei Teilstrahlen auf. Durch eine geeignete Beschichtung kann man erreichen, dass in gerader Richtung nur horizontal polarisiertes Licht durchgelassen wird und in der um 90° gekippten Richtung nur vertikal polarisiertes Licht. Ein solcher polarisierender Strahlteilerwürfel wird als PBS-Cube (polarised-beam-splitter-cube) bezeichnet. Diesen werden wir auch in unserem Versuch einsetzen.

Die Grundlagen der Quantenkryptografie

Bei der Quantenverschlüsselung gibt es zwei Basen, die jeweils die logische „0“ und die logische „1“ durch die Polarisation kodiert enthalten. Die erste Basis wird als H/V-Basis und die zweite als Diagonal-Basis bezeichnet. Für die Basen verwendet man die Symbole H/V und X.





Der Sender ALICE stellt mit seinem Polarisationsdreher einen der 4 oben abgebildeten Zustände ein. Damit wählt er automatisch auch einen logischen Wert aus.

Beispiel: -45° = X-Basis mit dem logischen Wert „0“

Der Polarisationsdreher bei BOB kennt nur zwei Einstellungen, 0° (H/V) und 45° (X). Damit erhält man folgende Ergebnisse:

ALICE	0°	90°	0°	90°	-45°	45°	-45°	45°
BOB	0° (HV)		45° (X)		0° (H/V)		45° (X)	
Bit	0	1	✖	✖	✖	✖	0	1

Das "✖" bedeutet, dass bei unserem Experiment sowohl eine logische "0" als auch eine logische "1" angezeigt wird. Arbeitet man mit einzelnen Photonen wird ein zufälliger Wert erzeugt. Stimmen die Basen nicht überein, sind die Messwerte von BOB also unbrauchbar.

Da ALICE und BOB nicht wissen, welche Basis sie gewählt haben, müssen sie sich darüber noch austauschen. Das kann öffentlich geschehen, da die Basis nichts über den Bitwert verrät. ALICE und BOB streichen alle Werte, wo die Basis nicht übereinstimmt.

Verschlüsselung:

Die Verschlüsselung und auch die Entschlüsselung erfolgt durch binäre Addition von Datenbit (D) und Schlüsselbit (S).

D	S	V
0	0	0
0	1	1
1	0	1
1	1	0

Wie man an der Tabelle oben sieht, kann man mit D+S=V und V+S=D verschlüsseln und entschlüsseln.

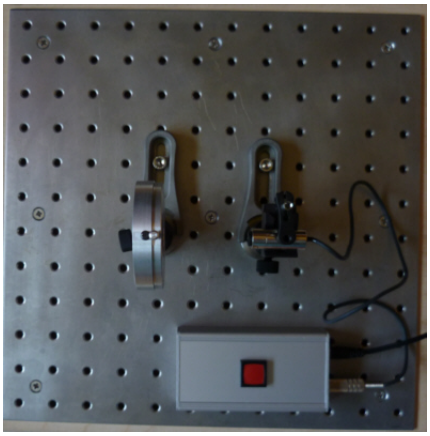
Datenübertragung:
Die Übertragung der verschlüsselten Daten erfolgt ebenfalls mit dem Versuchsaufbau. Dabei wird nur die H/V-Basis benutzt. Bei BOB wird der Phasendreher fest auf 0° eingestellt. ALICE verwendet für die „0“ 0° und die „1“ 90°.

Versuchsaufbau:

Geräte:

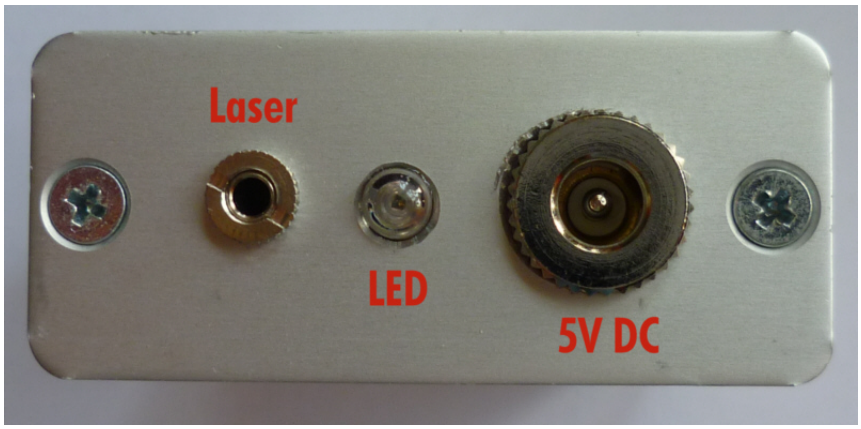
 2 x Phasendreher	 Polarisierender Strahlteilerwürfel	 Laser	 2x Sensor
 Auswertungselektronik	 Laserelektronik	 5x Klammer	2x Breadboard

Aufbau ALICE:

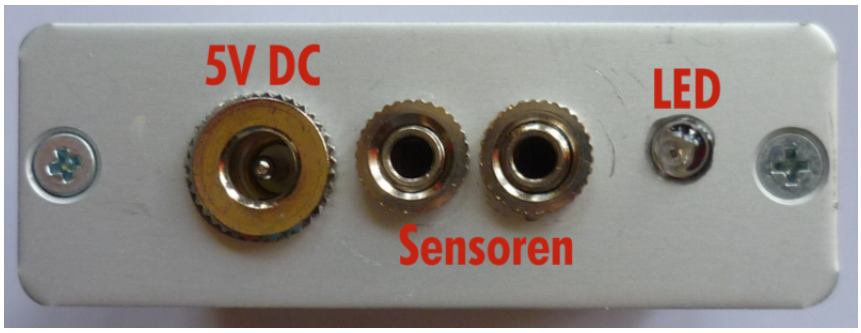


Aufbau BOB:

Bedienelemente Lasersteuerung:



Bedienelemente Sensorsteuerung:



Es ist unerheblich, welcher Sensor an welchen Eingang angeschlossen wird.

Laser und der Polarisationsdreher werden auf dem ersten Breadboard aufgebaut. Am Anfang ist es ausreichend, die Bauteile mit den Magnetfüßen einfach aufzustellen. Auf dem zweiten Breadboard kommt der Polarisationsdreher, der Strahlteiler und die beiden Sensoren. Der Laser wird mit der Ansteuerungselektronik verbunden und für ca. 2 Sekunden der rote Knopf gedrückt. Der Laser leuchtet nun permanent. Zuerst wird ALICE einjustiert. Dazu wird der Laser so auf dem Breadboard platziert, dass sein Strahl möglichst mittig auf das lambda/2 Waveplate des Polarisationsdrehers fällt. Das Waveplate dabei niemals berühren! Der Polarisationsdreher wird auf 0° eingestellt.
Nun wird BOB justiert. Der Laserstrahl soll auch hier möglichst mittig auf das Waveplate des Rotationsdrehers fallen. Dieser wird auf 45° eingestellt. Nun wird der Strahlteiler so in den Strahl geschoben, dass aus einer der Seitenkanten und in gerader Richtung jeweils ein Laserstrahl austritt. An diese Postionen werden die beiden Sensoren gerückt. Der Laserstrahl soll dabei mittig auf die kleine Öffnung in den Sensoren fallen. Sind alle Bauteile justiert, können sie mit den Klammern fixiert werden. Zusätzlich kann ALICE und BOB mit Schraubzwingen am Tisch fixiert werden, das ist aber nicht unbedingt erforderlich.

Der Laser muss vor der ersten Benutzung justiert werden. Dazu wird ALICE auf 0° und BOB auf 90° eingestellt. An der Laserhalterung ist eine kleine Inbus-Schraube, die wird soweit gelöst, bis das runde Lasergehäuse drehbar wird. In den gerade ausgehenden Strahl wird ein weißes Papier gestellt und der Laser so lange gedreht (ganz langsam und mit sehr kleinen Schritten) bis der rote Laserpunkt die minimale Intensität erreicht. Nun die Inbusschraube wieder festziehen.

Durch kurzes Drücken auf den roten Knopf wird der Laser wieder in den Pulsmodus versetzt. Nun werden beide Sensoren an die Auswertungselektronik angeschlossen. Ein kurzer Druck auf den Knopf sollte dazu führen, dass beide Leds an den Sensoren aufleuchten. Falls das nicht geschieht, müssen die Sensoren vorsichtig nachjustiert (Höhe und Position) werden, bis beide Leds leuchten. Nun werden beide Rotationsdreher auf 0° eingestellt. Es darf nur die Led in gerade Position aufleuchten. Zuerst wird der Rotationsdreher bei ALICE auf 90° (gewinkelte Led leuchtet) und beide 45° Einstellungen (beide Leds) leuchten durchprobiert. BOB steht dabei immer auf 0°. Danach wird das Gleiche für BOB gemacht. ALICE steht dabei immer auf 0°. Wenn alle 8 Positionen richtig sind, kann mit dem Versuch begonnen werden.

ALICE steht auf 0°				**BOB steht auf 0°**			
BOB 0°	BOB 90°	BOB 45°	BOB -45°	ALICE 0°	ALICE 90°	ALICE 45°	ALICE -45°
LED „0“	LED „1“	Beide LEDs	Beide LEDs	LED „0“	LED „1“	Beide LEDs	Beide LEDs

Problembehebung:

Die Justierung und der Aufbau ist manchmal etwas schwierig, falls es mal nicht klappen will, hier ein paar Fehlerquellen und ihre Behebung

ALICE und BOB stehen auf 0° trotzdem leuchten beide Leds auf
In diesem Fall ist der Laser nicht richtig justiert.

ALICE und BOB haben unterschiedliche Basen, trotzdem leuchtet nur eine Led auf
Ist sichergestellt, dass der Laser richtig justiert ist, so ist der Sensor an dem die Led leuchtet nicht perfekt justiert. Den Laser auf Dauerlicht umschalten und den Sensor nachjustieren. Das muss ggf. mehrfach geschehen bis beide Leds leuchten.

Der Versuch klappt perfekt, nach einiger Zeit aber nicht mehr

Falls der Laser nicht richtig festgeschraubt war, kann er sich verstellt haben. Oder ALICE und BOB wurde bewegt. Dann stimmt die Justierung nicht mehr.

Versuchsdurchführung:

Bei den Arbeitsblättern weiter unten sind zwei Messwerttabellen für ALICE und BOB zu finden. Die ALICE-Gruppe füllt vor dem Versuch 52mal die gewählte Basis (H/V oder X) und das logische Schlüsselbit ("1" oder "0") aus. Diese Tabelle darf die BOB-Gruppe natürlich nicht sehen. Die BOB-Gruppe legt vor dem Versuch die jeweiligen Basen 52 mal fest. Nun kann die Datenübertragung beginnen.

ALICE stellt den Rotationsdreher nach folgender Vorschrift ein

Basis	**H/V**		**X**	
Bit	**0**	**1**	**0**	**1**
Winkel	**0°**	**90°**	**-45°**	**45°**

BOB stellt seine gewählte Basis ein

Basis	**H/V**	**X**
Winkel	**0°**	**45°**

Sind beide Gruppen fertig, drückt ALICE kurz auf den roten Knopf und BOB notiert sich sein Ergebnis. Für die Led in gerade Position den Bitwert "0" und für die Led in gewinkelter Position den Wert "1". Leuchten beide Leds, trägt BOB ein "x" ein. Das Ganze wird insgesamt 52 mal durchgeführt.

Nun tauschen sich ALICE und BOB über die Basen aus. ALICE liest nur die Basis (H/V oder X) vor und BOB antwortet mit "Ja" (Basis stimmt überein) oder "Nein" falls das nicht der Fall ist. ALICE und BOB streichen alle Messwerte mit falscher Basis. Es sollten am Ende mindestens 20 Messwerte übrigbleiben, ansonsten muss noch mal mit der Übertragung begonnen werden.

Je nach Zeitaufwand kann an dieser Stelle der Versuch beendet werden. ALICE und BOB vergleichen ihre Messwerte und finden bei allen nicht gestrichenen Übereinstimmung. Spannender ist es aber, wenn jetzt ein verschlüsseltes Datenwort übertragen wird und am Ende ALICE und BOB dieses Wort vergleichen.

ALICE denkt sich ein Wort aus 4 Buchstaben aus und notiert sich dieses in seinem Arbeitsblatt. Mit Hilfe der beiliegenden Code-Tabelle für die Buchstaben A-Z erzeugt es einen 20bit langen Binärcode. Unter diesen Code trägt ALICE nun den mit BOB abgestimmten Schlüssel ein und verschlüsselt Bitweise. ALICE erhält eine 20bit langes verschlüsseltes Datenwort, das nun an BOB übertragen wird. Dazu wählen ALICE und BOB die H/V-Basis aus, die Übertragung geschieht genauso wie bei der Schlüsselübertragung.

BOB notiert sich die gemessenen Werte in seine Messwerttabelle. Mit dem Schlüssel entschlüsselt er nun das Wort und kann mit Hilfe der Code-Tabelle daraus wieder die 4 Buchstaben gewinnen. Nun können ALICE und BOB ihr Wort vergleichen.

Arbeitsaufträge:

1. Schlüsselerzeugung:
   Es werden insgesamt 52 Bit Schlüsselwerte nach der oben stehenden Vorschrift von ALICE nach BOB übertragen.

2. Schlüsselüberprüfung:
   ALICE und BOB vergleichen die gewählten Basen. Stimmen diese nicht überein, wird das Ergebnis aus dem Schlüssel gestrichen. (Hinweis: Das ist immer der Fall, wenn bei BOB beide LEDs aufleuchten).

3. ALICE denkt sich ein Wort mit 4 Buchstaben aus. Es kann auch ein sinnloses Kunstwort sein. Mit Hilfe der an der Station bereitliegenden Codetabelle erzeugt er ein 20Bit langes Datenwort. Dieses verschlüsselt er mit den mit BOB überprüften Schlüssel.

4. ALICE sendet das verschlüsselte Wort an BOB. Dieser entschlüsselt die Daten und hat damit das ursprünglich von ALICE gesendetes Wort.

Messprotokolle für ALICE und BOB

ALICE

Ü	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
B																										
S																										
Ü	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
B																										
S																										

Ü = Übertragene Bits B = Basis (+) oder (X) S = Schlüsselbits

ALICE

W																				
D																				
S																				
V																				

W = Wort D = Datenbit (4x5 Bit) S = Schlüsselbit V = Verschlüsselte Datenbits

✂----------

BOB

Ü	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
B																										
S																										
Ü	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
B																										
S																										

Ü = Übertragene Bits B = Basis (+) oder (X) S = Schlüsselbits

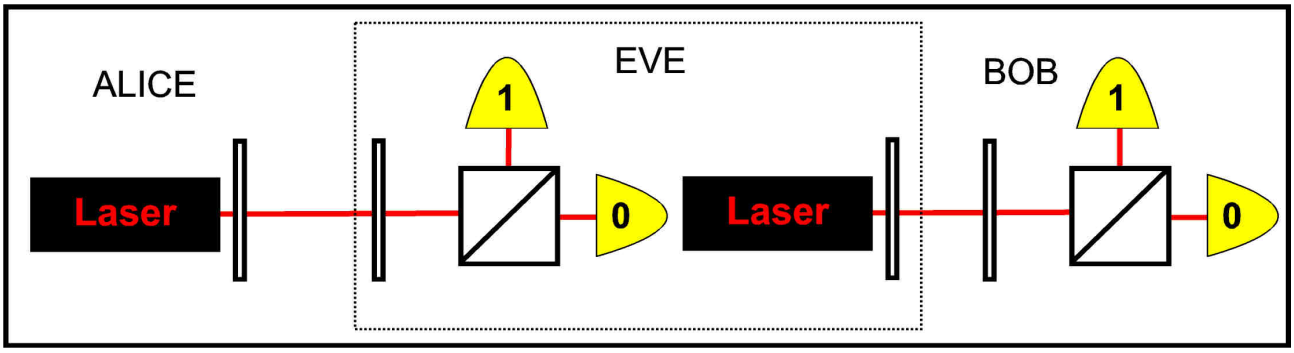
BOB

V																				
S																				
D																				
W																				

W = Wort D = Datenbit (4x5 Bit) S = Schlüsselbit V = Verschlüsselte Datenbits

EVE – Der Lauscher

Bis jetzt sind wir davon ausgegangen, dass kein Lauscher in der Leitung vorhanden ist. Doch wie können wir einen solchen Lauscher finden? Dazu erweitern wir den Versuch um einen Lauscher EVE.



Wie man sieht, besteht EVE aus einer Kombination von ALICE und BOB. Da EVE nicht beide Basen gleichzeitig messen kann, liegt EVE bei 50% aller Messungen statistisch gesehen falsch. EVE muss dann den Bitwert erraten. Dafür hat er ebenfalls eine 50% Chance. Insgesamt sind statistisch gesehen 25% aller übertragenen Bitwerte falsch.

ALICE und BOB müssen also nur den übertragenen Schlüssel vergleichen, ohne diesen dann zu benutzen. Sind im Schlüssel Fehler vorhanden, so ist der Lauscher EVE erkannt.

Natürlich kann ALICE und BOB auch die übertragenen Daten immer wieder auf Fehler überprüfen. Da der Schlüssel bei ALICE und BOB nicht identisch ist, wird der Lauscher EVE so auch erkannt.

Möchte man mit EVE arbeiten, dann müssen sich zwei Gruppen zusammentun. Eine Gruppe ist ALICE und BOB, die zweite Gruppe ist zusammen EVE. Die Schlüsselerzeugung bei ALICE und BOB geschieht genauso wie im Versuch ohne EVE. Die Vorgehensweise bei EVE ist folgendermaßen:

EVE wählt für den Eingang eine beliebige Basis aus. Die Ausgangsbasis ist immer die gleiche wie die Eingangsbasis. Wird ein eindeutiger Wert erhalten (nur ein Sensor spricht an) wird dieser Wert wieder ausgegeben. Wird kein eindeutiger Wert erhalten (beide Sensoren sprechen an) wird einfach geraten.

Zum Schluss überprüfen ALICE und BOB den übertragenen Schlüssel. Die Fehler im Schlüssel verraten den Lauscher EVE.

Hinweis: Unser Versuch arbeitet mit einem Laserpuls und damit mit Milliarden von Photonen. Die echte Quantenkryptografie arbeitet mit einzelnen Photonen. Trotzdem ist der Versuchsaufbau und die Messmethode völlig identisch. Die Abhörsicherheit ist allerdings nur bei einzelnen Photonen gewährleistet, da bei vielen Photonen EVE nicht alle Photonen zum Lauschen benötigt, sondern prinzipiell nur ein einziges von den Milliarden. ALICE und BOB würden einen solchen Lauscher dann nicht finden.

Anhang: Codetabelle und Beispiele

Codetabelle

A	0	0	0	0	0
B	0	0	0	0	1
C	0	0	0	1	0
D	0	0	0	1	1
E	0	0	1	0	0
F	0	0	1	0	1
G	0	0	1	1	0
H	0	0	1	1	1
I	0	1	0	0	0
J	0	1	0	0	1
K	0	1	0	1	0
L	0	1	0	1	1
M	0	1	1	0	0
N	0	1	1	0	1
O	0	1	1	1	0
P	0	1	1	1	1
Q	1	0	0	0	0
R	1	0	0	0	1
S	1	0	0	1	0
T	1	0	0	1	1
U	1	0	1	0	0
V	1	0	1	0	1
W	1	0	1	1	0
X	1	0	1	1	1
Y	1	1	0	0	0
Z	1	1	0	0	1

Beispiele

Schlüsselüberprüfung

ALICE

Ü	0	0	1	0	1
B	X	X	+	X	+
S	✖	0	1	✖	1
Ü					
B					
S					

BOB

Ü	✖	0	1	✖	1
B	+	X	+	+	+
S	✖	0	1	✖	1
Ü					
B					
S					

Verschlüsselung (ALICE)

W	M				
D	**0**	**1**	**1**	**0**	**0**
S	**0**	**1**	**1**	**1**	**0**
V	**0**	**0**	**0**	**1**	**0**

Entschlüsselung (BOB)

V	**0**	**0**	**0**	**1**	**0**
S	**0**	**1**	**1**	**1**	**0**
D	**0**	**1**	**1**	**0**	**0**
W	M				

Probleme: Falls bei der Schlüsselerzeugung und nachfolgender Überprüfung weniger als 20 Schlüsselbits übrig bleiben, so müssen weitere Schlüsselbits erzeugt werden.