Quantenkryptografie

Die experimentelle Realisation basiert auf der Doktorarbeit von Patrick Bronner, Didaktik der Physik, Universität Erlangen-Nürnberg
dieser Artikel ist downloadbar bei www.quantenphysik-schule.de unter „Schulexperimente“

1. Quantenkryptografie – die Idee

Kryptographie ist die Kunst eine Nachricht so zu verschlüsseln, dass sie für fremde Personen unlesbar und ohne jeglichen Informationsgehalt ist. Trotz vielfältiger Forschung gibt es bisher kein klassisches Kryptografieverfahren, das absolute Sicherheit bieten kann. Einen Ausweg aus dem Dilemma bietet die Quantenphysik, denn mit Hilfe von einzelnen Quanten kann ein absolut zufälliger Schlüssel erzeugt werden und dieser dann abhörsicher zwischen zwei Parteien ausgetauscht werden.

2. Verschlüsselung mit einem One Time Pad (Einmalblock)

Das Verfahren wurde 1918 von G. Vernam entwickelt. Ein Schlüssel wird erzeugt und auf zwei Blöcke für „Alice“ und „Bob“ geschrieben. Der Schlüssel selbst hat nichts mit der Nachricht zu tun. Diese wird vielmehr mit dem Schlüssel codiert und kann dann sogar auf einem öffentlich zugänglichen Kanal gesendet werden. Damit nun der Schlüssel nicht aus der Nachricht herausdestilliert werden kann (wie im 2. Weltkrieg geschehen), muss der Schlüssel 4 Bedingungen erfüllen:

- Bedingung 1: Der Schlüssel darf nur einmal verwendet werden.
- Bedingung 2: Der Schlüssel muss mindestens genauso lang wie die eigentliche Nachricht sein.
- Bedingung 3: Der Schlüssel muss absolut zufällig sein.
- Bedingung 4: Der Schlüssel darf nur zwei Personen bekannt sein.

Die Bedingungen 1 und 2 lassen sich relativ leicht (vom Sender bzw. Empfänger) erfüllen. Die Bedingung 3 kann jedoch mittels „klassisch“ erzeugter Zufallszahlen nicht in Strenge erfüllt werden. Solche Zufallszahlen basieren auf Computerprogrammen, wobei die Zufälligkeit von der Komplexität des Rechenprogramms anhängt. Sie werden deshalb als "Pseudozufallszahlen" bezeichnet und sind für die absolut zufällige Erzeugung eines Schlüssels nicht geeignet.
Die Quantenphysik bietet jedoch z.B. mittels eines Strahlteilers die Möglichkeit, dass ein einzelnes Photon an einem Strahlteiler entweder reflektiert (binär 1) oder transmittiert (binär 0) wird. Hinter dieser „Entscheidung“ steckt keine mathematische Rechenvorschrift, sondern der absolute Zufall.

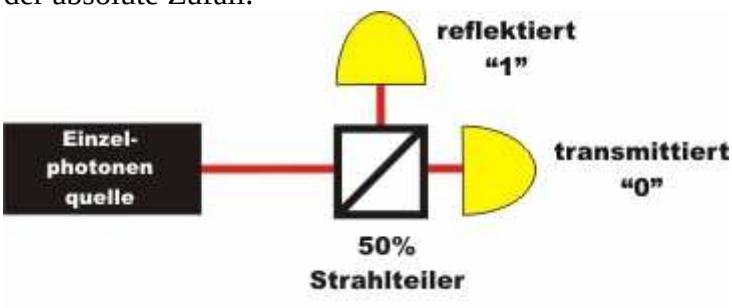

Abb.1 Versuchsaufbau Quantenzufall, Prinzip

Die Bedingung 4 lässt sich ebenfalls (nur) mit der Quantenphysik erfüllen, wie weiter unten gezeigt wird.

3. Das Prinzip der Verschlüsselung

Wir nehmen an, dass Bob und Alice geheime Nachrichten austauschen wollen, die aus einem binärer Code aus Nullen und Einsen bestehen. Wie kann man eine solche Nachricht einfach aber wirkungsvoll verschlüsseln? Probieren Sie es doch selbst einmal aus!

1. Schritt: Bobs Nachricht **(N)** ist z.B. die Folge **1010101010.** Ganz einfach zu merken.

wie kann er diese Nachricht so verschlüsseln, dass sie niemand erkennt?

2. Schritt: Bob nimmt einen Schlüssel **(S)**, der eine (mindestens) gleichlange Folge von Zufallszahlen ist, z.B. **0011011101**

3. Schritt: Bob addiert den Schlüssel (S) zur Nachricht (N) "modulo 2", d.h. er beachtet, dass 1+1= 0 ergibt.Bobs verschlüsselte Nachricht **(VN)** lautet also: **1001110111**. Da sie durch Addition einer Zufallsfolge gebildet wurde ist auch die verschlüsselte Nachricht selbst eine Zufallsfolge (auch wenn die originale Nachricht extrem periodisch war). Wie kann aber Alice die Nachricht entschlüsseln?

4. Schritt: Ganz einfach, Alice addiert denselben Schlüssel wieder modulo 2 und erhält die ursprüngliche Nachricht **(N)**

VN	**1001110111**
+ S	**0011011101**
= N	**1010101010**

Beispiel der Verschlüsselung eines Bildes

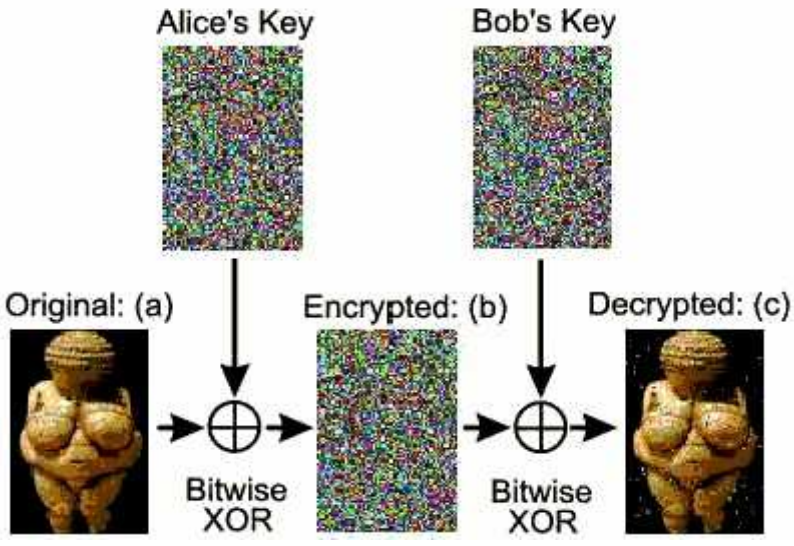

Abb.2 Verschlüsselung eines Fotos durch einen Zufallscode. Im entschlüsselten Foto (rechts) sind einige fehlerhafte Pixel zu erkennen, die aber durch Fehleralgorithmen (weitgehend) herausgefiltert werden können.

4. Experimentelle Realisierung

Grundsätzlich kann man (derzeit) in der Schule noch keine Experimente mit einzelnen Photonen durchführen. Das Prinzip der Quantenkryptographie lässt sich jedoch ansatzweise mit Laserpulsen realisieren und damit konkret darstellen. Im Schulalltag neu sind vermutlich die beiden Bauteile: Polarisationsdreher (λ/2-Platte) und polarisierender Strahlteilerwürfel.

Der Polarisationsdreher dreht die Polarisationsrichtung des (linear polarisierten Laserlichts) um einen definierten Winkel. Er besteht aus einer λ/2 Glasplatte. Polarisationsdreher besitzen eine Symmetrieachse, die als Spiegelachse für die Polarisation betrachtet werden kann. Daher führt eine Drehung der Platte um 45^0 zu einer Drehung der Polarisationsrichtung um 90^0.

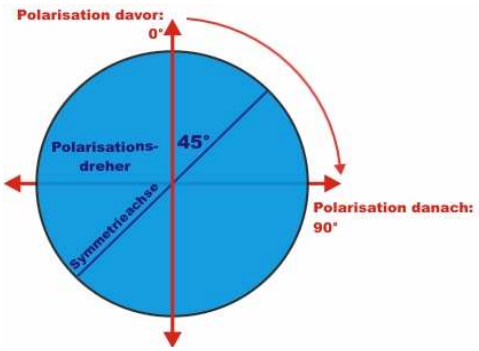

Abb.3 Wirkungsweise des Polarisationsdrehers
coyright www.quantumlab.de

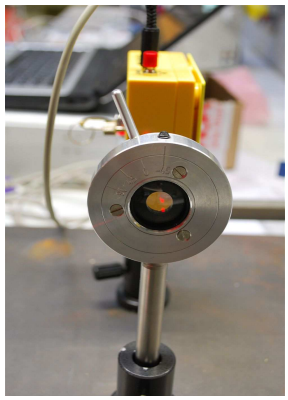

Abb.4 Polarisationsdreher in selbst gefertigter Halterung (UniErlangen)

Der polarisierende Strahlteilerwürfel transmittiert das Licht, wenn die Polarisationsrichtung parallel zur vertikalen Kante ist bzw. er reflektiert das Licht, wenn die Polarisationsrichtung horizontal ist.

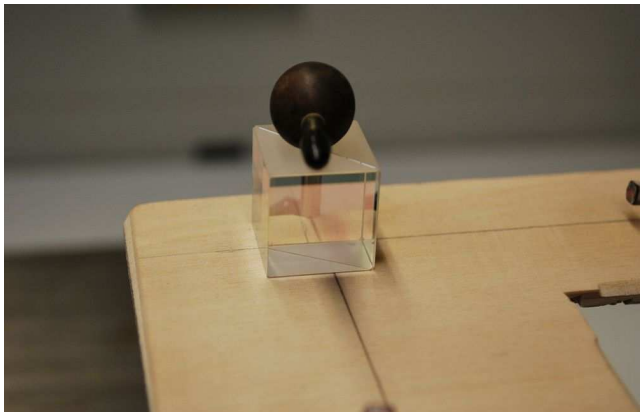

Abb.5 Polarisiernder Strahlteilerwürfel. Bezug www.thorlabs.com

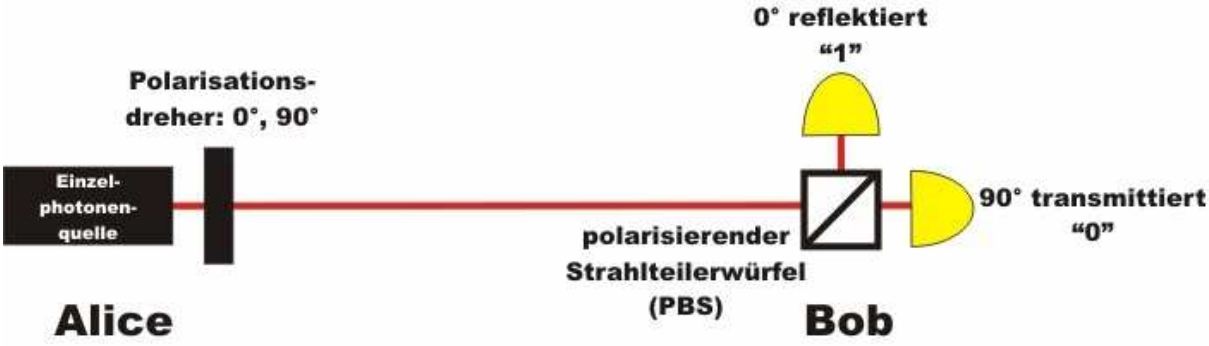

Abb.6 Versuchsaufbau Prinzip copyright www.quantumlab.de

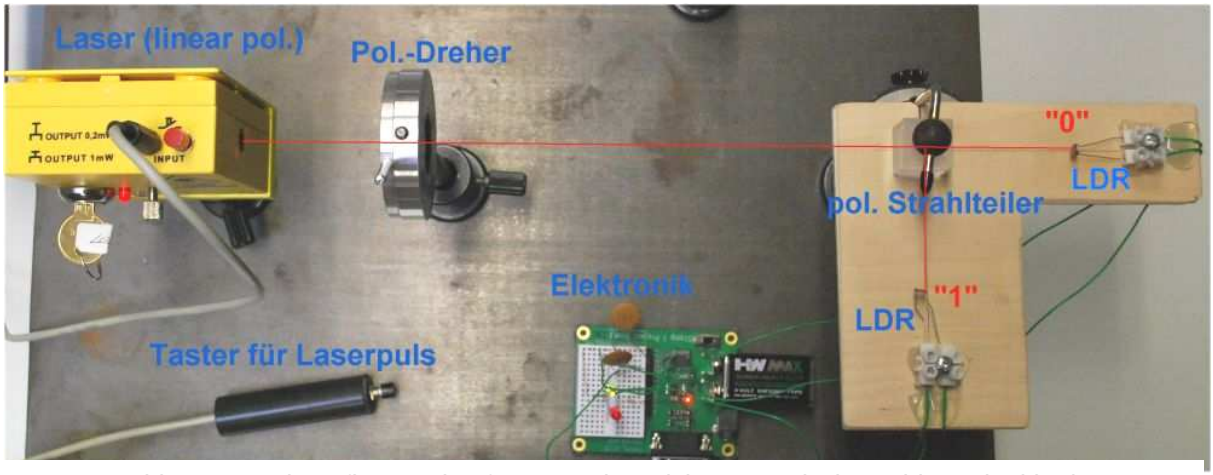

Abb.6 Versuchsaufbau real auf Magnetplatte (ebenso optische Schiene denkbar)

Mit dem Polarisationsdreher kann nun eine vorher erzeugte Zufallsliste aus „0“ und „1“ von Alice (linke Station) zu Bob (rechte Station) übertragen werden.
(Für die absolute Sicherheit muss die Quantenzufallszahl direkt parallel erzeugt werden und ohne Zwischenspeicherung auf einen automatischen Polarisationsdreher übertragen werden)

Detektoren und Elektronik

Als Lichtdetektoren wurden hier einfache LDR (light dependent resistor) verwendet. Ein Mikrocontroller (Basic Stamp1) schaltet je Strahlengang entweder eine rote oder eine gelbe LED an. Die Schaltschwelle kann per PC eingestellt werden. Falls die Polarisationsrichtung 45^0 beträgt (siehe unten bei 5.) leuchten beide LED’s. Dies ist der entscheidende Unterschied zur Detektion von einzelnen Photonen, die in diesem Fall zufällig (mit 50% Wahrscheinlichkeit) den einen oder den anderen „Weg gehen“. Anstelle eines Mikrocontrollers kann selbstverständlich eine einfache Transistorschaltung verwendet werden, wobei ein die Schaltschwelle mit einem Potenziometer eingestellt werden kann.


Abb.7 LDR als Detektor

5. Die Überlistung von „Eve“

Wäre es für einen Spion möglich, den geheimen Schlüssel unbemerkt zu kopieren? Leider ja. Der Spion Eve (von engl. eavesdropping = abhören) kann sich unbemerkt in den Strahlengang einschleichen. Die Einheit von Eve enthält die Empfangseinheit wie bei Bob und die gleiche Sendeeinheit wie bei Alice. Eve empfängt das Photon, kennt somit die Binärzahl und schickt ein entsprechendes Photon mit der gleichen Polarisation an Bob weiter. Bisher also absolut keine Sicherheit!

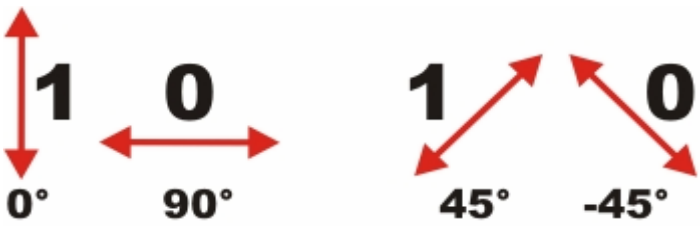

Abb.8 Definition von „0“ und „1“ in den beiden Basen **+**(links) und **x**(rechts) Copyright www.quantumlab.de

Um Spione bei der Quantenkryptographie aufdecken zu können, müssen zusätzliche Elemente in das System eingefügt werden. Bob und Alice benutzen deshalb **zwei Messbasen**: Eine Basis Plus (Bezeichung: +) und Basis X (Bezeichung: **x**). In jeder Basis gibt es eine fest definierte Polarisationsrichtung für die beiden Bits 1 oder 0. In der Basis + entspricht die Polarisation von 0° dem Bit "1" und die Polarisation von 90° dem Bit "0" (Abb. 1 links). In der Basis **x** entspricht die Polarisation 45° dem Bit "1" und die Polarisation -45° dem Bit "0" Für die Übertragung von einem Bit muss Alice nun **zweimal zufällig wählen**. Zunächst wählt sie zufällig, in welcher Basis sie das Bit versenden möchte: + oder **x**. Danach wählt sie zufällig, welches Bit sie in dieser Basis übertragen möchte: 1 oder 0. Alice benötigt somit vier verschiedene Winkel an ihrem Polarisationsdreher: 0°, 90° für die Basis + und 45°, -45° für die Basis **x** (Abb. 2). Auch Bob muss sich nun immer rein zufällig für eine Messbasis entscheiden: + oder **x**. Hierfür benötigt er einen Polarisationsdreher mit zwei festen Einstellungen in seiner Empfangseinheit. Auch Bob wählt rein zufällig entweder 0° für die Messbasis + oder 45 ° für die Messbasis **x**

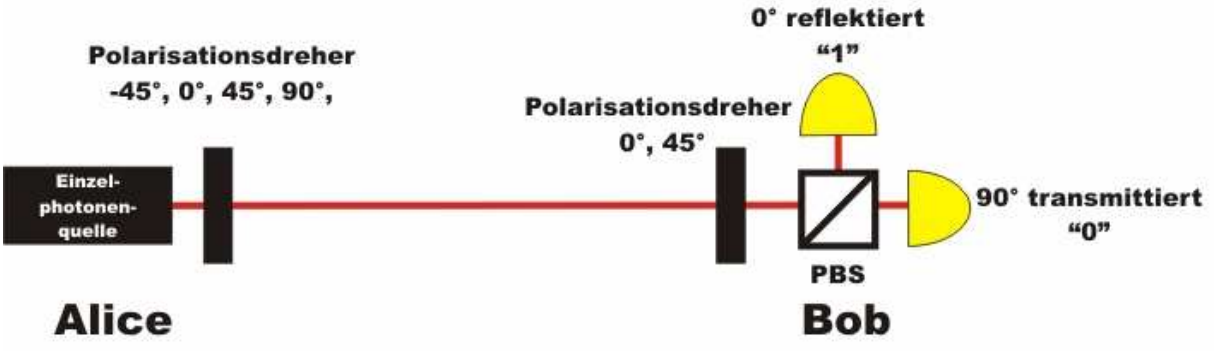

Abb.9 Versuchsaufbau abhörsichere Übertragung von Alice zu Bob, Prinzip Copyright www.quantumlab.de

Wenn Alice nun ein Photon in der Basis + mit der Polarisation 0° oder 90° verschickt und Bob die Basis + wählt, so gibt es eindeutige Ergebnisse. Wenn Alice das Photon in der Basis **x** mit der Polarisation -45° oder 45° verschickt und Bob die Basis **x** wählt, so gibt es wieder eindeutige Ergebnisse. Wenn Alice und Bob zufällig die gleichen Basen wählen, sind die übertragenen Daten eindeutig und können für den Schlüssel verwendet werden.
Wenn Alice aber ein Photon in der Basis + mit der Polarisation 0° oder 90° versendet und Bob die Basis **x** wählt, dann ist das Photon vor dem Strahlteiler diagonal polarisiert. Trifft ein diagonal polarisiertes Photon auf einen Polarisationsstrahlteiler, so wird das Photon mit der Wahrscheinlichkeit von 50% transmittiert oder mit der Wahrscheinlichkeit von 50% reflektiert. Das gleiche 50% zu 50% Verhalten am Strahlteiler ergibt sich, wenn Alice das Photon in der Basis **x** verschickt und Bob zur Messung die Basis + wählt. Wenn Alice und Bob verschiedene Basen wählen, sind die übertragenen Daten absolut zufällig und nicht zu gebrauchen.

Praktisches Vorgehen:

Bei jedem gesendeten Photon notiert Alice in ihrer Liste, welche Basis sie gewählt hat und welches Bit sie übertragen hat. Bob notiert bei jedem Photon in seiner Liste, welche Basis er zur Messung gewählt hat und welcher Detektor das Photon registrierte. Alice und Bob besitzen somit zwei Listen mit den Einträgen: Photonnummer - Basis – Bit. Nach z. B. 100 Photonen telefonieren Alice und Bob miteinander und erzählen sich nur, bei welcher Photonnummer sie in welcher Basis gemessen haben. Stimmen die Basen überein, so werden

die Ergebnisse behalten. Stimmen die Basen nicht überein, so werden die Ergebnisse gelöscht Beim Telefonieren werden nur die verwendeten Basen verraten, nicht das Bit. Ein Spion könnte bei diesem Telefonat mithören, wobei ihm diese Information aber nichts bringt. Das eigentliche Ergebnis - die eindeutig übertragenen Bits - werden nicht verraten und sind noch immer geheim. Der Kontakt zwischen Alice und Bob und das Löschen der falschen Ergebnisse kann natürlich auch durch einen Computer erfolgen. Mit Quantenzufallsgeneratoren und den beiden automatischen Polarisationsdrehern arbeitet das System völlig selbstständig. Eine Bitrate mit bis zu einigen Millionen Bit pro Sekunde ist mit elektrooptischen Polarisationsdrehern möglich, da diese keine mechanisch bewegten Teile haben. Können sich Alice und Bob nun wirklich sicher sein, dass nur sie beide den Schlüssel kennen? Der Spion Eve kann nun auch rein zufällig eine Basis wählen und das Photon messen. Eve muss allerdings sofort wieder ein neues Photon an Bob senden. In etwa 50% der Fälle wählt Eve zur Messung die falsche Basis. Diesen durch Eve verursachten Fehler können Alice und Bob allerdings nur dann bemerken, wenn Alice und Bob die gleiche Basis gewählt haben. Bei gleicher Wahl der Basis sollten Alice und Bob immer eindeutige Ergebnisse erhalten. Um Eve zu entdecken, müssen Alice und Bob also einige der eindeutigen Messergebnisse (öffentlich) überprüfen. Bei einem Fehler der eigentlich eindeutigen Daten können Alice und Bob die Eve enttarnen. Eve kann allerdings erst nach der Schlüsselübertragung entdeckt werden. Allerdings wurde bisher lediglich der Schlüssel generiert und noch nicht die geheime Nachricht übertragen. Im Fall der Enttarnung von Eve wird dieser Schlüssel einfach gelöscht und nicht zur Verschlüsselung der eigentlichen Nachricht verwendet.

6. Bezugsquellen

www.lasercomponents.de	polarisierender Strahlteilerwürfel für rotes Laserlicht (633nm). Kantenlänge 2cm. Low cost Produkt auf Anfrage ca. 100€ in China produziert λ/2 Platte für 632,8nm, Durchmesser 12,7mm in Fassung 0,5’’ ebenfalls auf Anfrage als low cost Produkt in China gefertigt
www.thorlabs.de	der Ausstatter der Quantenoptik-Labors. Sehr schnelle Lieferung in ca. 2 Tagen aber evt. teuer.
Conrad electronic	Lasermodule mit Steuerelektronik, sodass mit einem Taster Laserpulse gesendet werden können.
Vereinfachte Variante:	Rote Laserpointer produzieren (annähernd) linear polarisiertes Licht. Der Versuch nach Abb.5/6 kann auch ohne Polarisationsdreher durchgeführt werden, wenn man stattdessen den Laserpointer dreht. Durch einen anmontierten Drehgriff lässt sich dies sicherlich gut bewerkstelligen.

7. Dank

Die Idee zu dieser Abhandlung basiert auf der Doktorarbeit von Patrick Bronner vom Institut Didaktik der Physik, Universität Erlangen-Nürnberg. Aus seiner Website www.quantumlab.de sind zudem mehrere Abbildungen und Textpassagen entnommen.