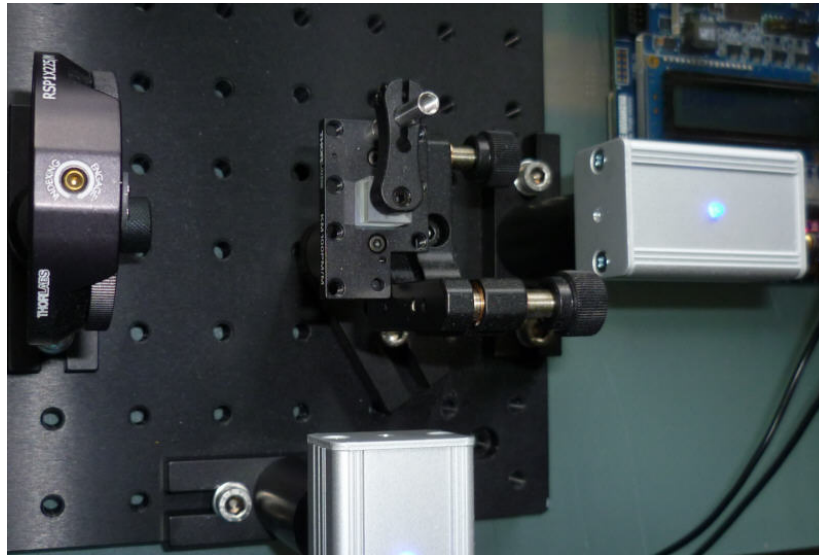


# Schrödingers Katze und Heisenbergs Würfel

Moderne Quantenexperimente in der Schule

vorgelegt von OStR Jörn Schneider

am Leibniz-Gymnasium Dormagen



- **Worum geht es? - Eine Kurzvorstellung**
- **So fing alles an - Von der ersten Idee zum fertigen Experiment**
- **Kooperationen – ohne sie geht es nicht**
- **Die Quantenkryptografie – sichere Datenübermittlung mit Quantenzuständen**
- **Schrödingers Katze lebt – Verschränkung als Schulexperiment**
- **Heisenbergs Würfel – Ganz nah an der aktuellen Forschung**
- **Und jetzt alles noch mal neu – Photonics aus dem 3D-Drucker**
- **Die Schüler mitnehmen – der Quantenwürfel**
- **Der Quantenchip – Quantenkryptografie auf dem FPGA**
- **Die Idee weitertragen – Schüler auf dem MINT-Tag am 26.11.2017**
- **Was kommt danach? - Ein Ausblick**

## 📌 Worum geht es? - Eine Kurzvorstellung

Die 1930iger Jahre waren nicht nur ein dunkles Kapitel in der deutschen Geschichte, es wurde auch Wissenschaftsgeschichte geschrieben. Mit der Entdeckung und Erklärung der Quantenwelt waren Namen wie Heisenberg, Planck, Schrödinger, Einstein und viele andere deutsche oder in Deutschland forschende Wissenschaftler verbunden. Viele grundlegende Experimente aus dieser Zeit haben Eingang in die Lehrpläne der Schulen gefunden und werden heute im Unterricht gezeigt. Die Entwicklung ist aber nicht stehen geblieben. Die Quantenphysik ist eine lebendige und aktive wissenschaftliche Forschungsdisziplin, davon ist an den Schulen bis heute aber kaum etwas angekommen.

Als Physiklehrer an einem Gymnasium fand ich diesen Zustand mehr als unbefriedigend und für den Wissenschaftsstandort Deutschland auch beschämend. Gesucht waren also Experimente der modernen Quantenphysik, die unter den Bedingungen des Schulalltages im Physikunterricht durchgeführt werden können. Dabei sollte das Schülerexperiment Vorrang vor einem Demoexperiment haben.

***Die Vorstellung der einzelnen Experimente habe ich teilweise aus früheren Publikationen entnommen, eine gewisse Doppelung der dargestellten Zusammenhänge ist dem zuzuschreiben.***

## 📌 So fing alles an – Von der ersten Idee zum fertigen Experiment

Die Heinrich-Heine Universität Düsseldorf veranstaltete im Oktober 2012 einen Informationstag für engagierte Lehrerinnen und Lehrer zu aktuellen Themen der Forschung, mit Laborführungen und Vorträgen. Am Ende besteht immer die Möglichkeit zu Gesprächen und einem offenen Austausch. Nach einer Laborführung in die optischen Labore der HH-Universität ergab sich die Gelegenheit mein Anliegen eines modernen Quantenexperiments an unserer Schule einmal vorzutragen. Dabei wurde ich auf das QuantumLab an der FAU Erlangen und auf Professor Meyn aufmerksam gemacht, der zum damaligen Zeitpunkt dort auch ein Schülerlabor unterhielt.

Friedrich-Alexander-Universität Erlangen-Nürnberg

# QuantumLab

🇩🇪 🇬🇧

Einführung:

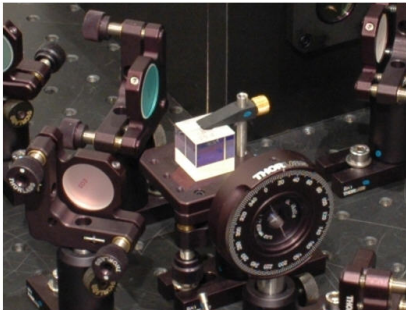
- Startseite
- Konzept
- Grundlagen

Experimente:

- Aufbau Optik
- Koizidenz
- Existenz Photon
- Quantenzufall
- Q-Kryptographie
- Verschränkung
- Interferenz
- Hong-Ou-Mandel
- Franson
- Photonenstatistik


Weiteres:

- Schülerlabor
- Unterricht
- Literatur
- Impressum



Besteht Licht aus unteilbaren Portionen?  
Gibt es Zufall in der Quantenwelt?  
Wie funktioniert Quantenkryptographie?  
Was sind verschränkte Photonen?

Ein interaktiver Zugang zur faszinierenden Welt der Quantenphysik ([Konzept](#)).

English version 

[www.quantumlab.de](http://www.quantumlab.de)

Die Kontaktaufnahme war zum Glück problemlos und im Februar 2013, als das Rheinland in den Ausnahmezustand des Karnevals verfiel, nutzte ich die Gelegenheit zu einem Besuch in Erlangen. Von den gezeigten Experimenten begeisterte mich vor allem die Quantenkryptografie und das Verschränkungsexperiment. Allerdings wurde mir auch schnell klar, dass die Finanzierung eines solchen Experiments nicht ganz einfach sein dürfte.

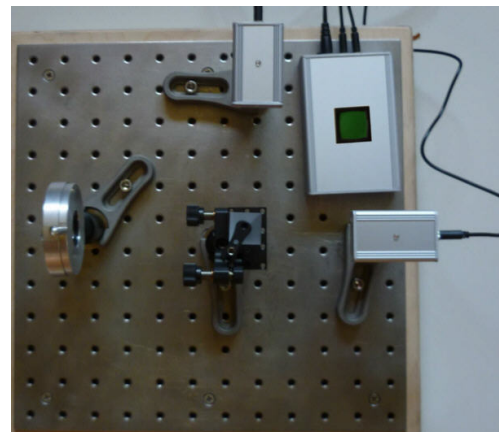
In den Herbstferien 2013 verbrachte ich dann eine ganze Woche in Erlangen und danach stand die Planung für das erste Experiment, die Quantenkryptografie.

Dormagen, als Bayer-Standort kann über die Bayer Science & Education Foundation Gelder für Projekte beantragen. Mit über 18.000€ Fördersumme war es uns möglich, sowohl 8 Michelson-Interferometer als auch 8 Schülerexperimente zur Quantenkryptografie zu finanzieren.



ALICE, BOB und EVE – Vorstellung des Projektes im Bayer-Bürgerbüro 2014

Die in Erlangen verwendeten Detektoren und die Auswertungs elektronik entsprach allerdings nicht mehr dem Stand der Technik und wurde komplett gegen moderne, mikroprozessorgesteuerte Systeme ausgetauscht. Anfang 2014 war unser System für den ersten Test soweit fertig und wurde erfolgreich in einem Informatik-Differenzierungskurs der Klasse 9 und in zwei Oberstufenkursen der Q2 (Klasse 13) in Physik getestet. Sowohl am Experiment, wie an der Anleitung wurden einzelne Verbesserungen vorgenommen und seit dem Schuljahr 2014/2015 ist die Quantenkryptografie fester Bestandteil unseres Lehrplanes in der Oberstufe.



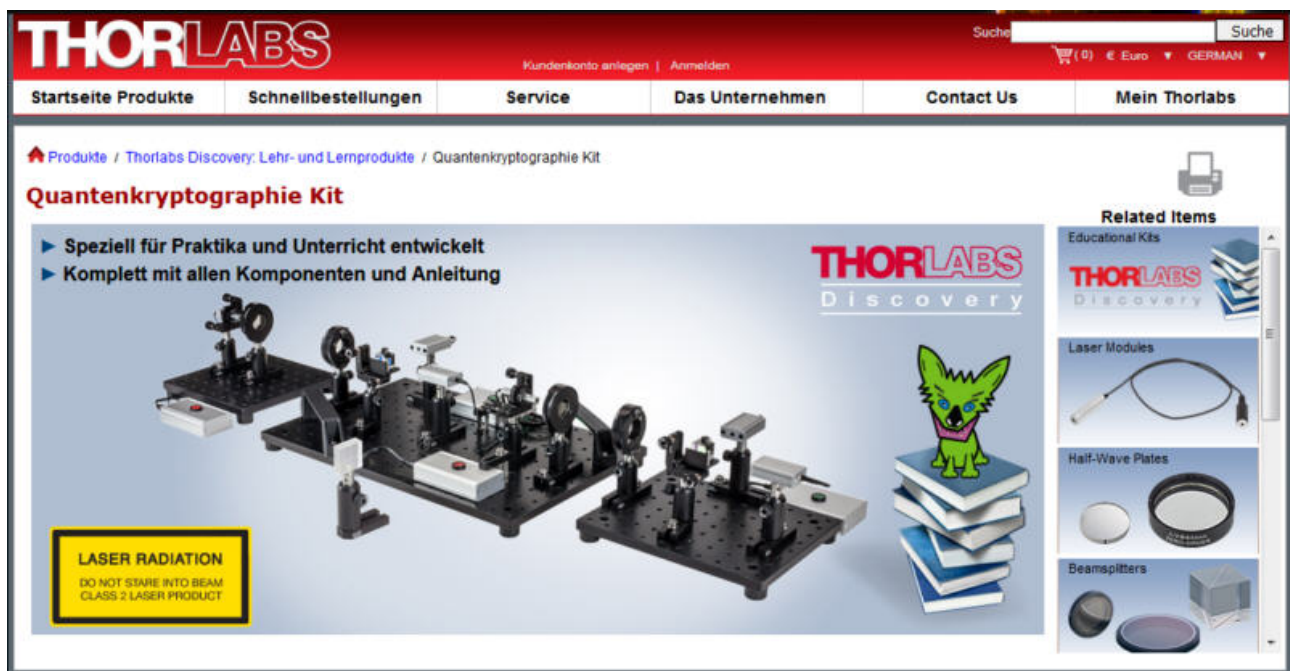
BOB mit neuer Sensorelektronik 2016

## 📌 Kooperationen – ohne sie geht es nicht

Ohne die Kooperation mit der Universität Erlangen und Professor Meyn wäre eine Umsetzung vermutlich sehr schwierig und deutlich langwieriger gewesen. Sowohl die Möglichkeit des Ausprobierens wie auch die Bereitstellung von technischen Informationen und letztendlich die Anfertigung der Rotationsdreher in der universitätseigenen Metallwerkstatt waren wichtige Bestandteile für das Gelingen der Umsetzung.

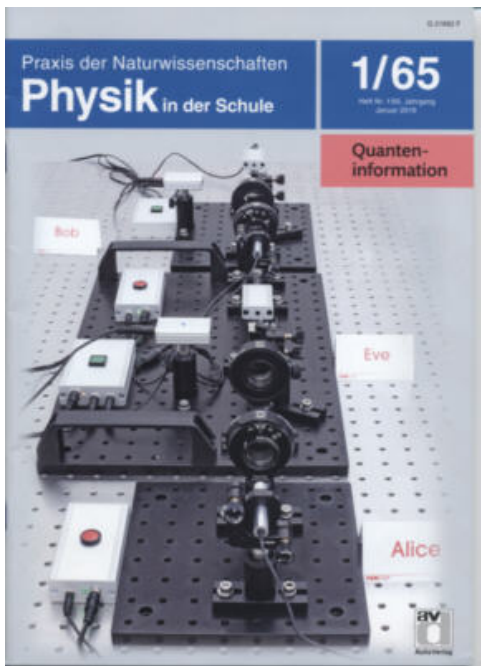
Im Jahr 2014 veranstaltete die Heisenberg-Gesellschaft einen Workshop zum Thema „Quantenphysik und Schule“, den ich als einer der wenigen teilnehmenden Lehrer besuchte. Der Workshop selbst war eher enttäuschend, dabei lernte ich aber einen Entwickler von didaktischem Material der Firma Thorlabs, Jens Küchenmeister, kennen.

Thorlabs ist einer der großen Hersteller von optischen Geräten und Geräte von Thorlabs sind in fast jedem optischen Labor weltweit zu finden. Für Universitäten und auch Schulen bietet Thorlabs eigene Education-Kits zu optischen Versuchen an. Von der Idee der Quantenkryptografie war Herr Küchenmeister sofort begeistert. Ende 2014 besuchte er unsere Schule und ließ sich das Experiment vorführen. Nach einem fast 10 Monate dauernden Entwicklungsprozess, der viele weitere Verbesserungen und Weiterentwicklungen brachte, kann die Quantenkryptografie nun auch als fertiges Set bei Thorlabs käuflich erworben werden.



[https://www.thorlabs.com/newgrouppage9.cfm?objectgroup\\_id=9869](https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=9869)





Dabei wurde auch in Zusammenarbeit mit Professor Meyn und mir didaktisches Material entwickelt, welches mit kleinen Änderungen bei uns an der Schule zum Einsatz kommt. Im Januar 2016 veröffentlichte der Aulis Verlag in der „Praxis der Naturwissenschaften“ 1/65 einen gemeinsamen Artikel von Professor Meyn und mir zur Quantenkryptografie.

Nach erfolgreichem Abschluss des ersten Projektes fingen die Vorarbeiten zu „Schrödingers Katze lebt“ an. Diesmal sollte es ein echtes Einzelphotonenexperiment sein, das transportabel und an normalen Schulen einsetzbar ist. Zu diesem Thema promovierte ein Doktorand in Erlangen bei Professor Meyn und stand kurz vor dem Abschluss seiner Doktorarbeit. Nachdem die Rütgers-Stiftung in NRW eine Förderzusage von immerhin 10.000€ gemacht hatte, sprang der Doktorand in Erlangen ohne Vorwarnung ab und hinterließ nur unzureichend und fehlerhaft dokumentierte Detektoren, die darüber hinaus nicht richtig arbeiteten. An diese Doktorarbeit angehängt war eine andere Doktorarbeit in Hannover, die ebenfalls die Detektoren benötigte und auch dort waren sie nicht einsatzfähig. Vom Prinzip her erforderte diese Situation eine komplette Nacharbeit der Doktorarbeit, die Entwicklung neuer bzw. die Modifikation der vorhandenen Detektoren und damit viel Zeit. Die beiden Betroffenen, Kim-Allessandro Weber und ich kooperierten daher in der Entwicklung eines funktionsfähigen Detektors und auch an der Verbesserung des gesamten Experiments. Inzwischen gibt es sowohl in Dormagen, wie auch in Hannover zwei gleiche Versuchsaufbauten, mit funktionsfähigen Detektoren und Auswertungselektroniken.

Die Schwierigkeiten bei den Einzelphotonen-Detektoren und auch die viel zu hohen Kosten des Experiments führten zur dritten Kooperation. Im Max-Planck-Institut „Science of light“ in Erlangen arbeitete eine Forschungsgruppe ebenfalls an einer Quantenkryptografie, allerdings mit einem komplett anderen Ansatz. In der Zeitschrift „Max Planck Forschung“ 1.2015 berichtete die Arbeitsgruppe um Gerd Leuchs davon. Im Jahr Februar 2016 stellte ich einen Kontakt dorthin her und bei einem Besuch im Institut wurde eine neue Kooperation ins Leben gerufen. Daraus entsteht das zur Zeit das aktuelle Experiment „Heisenbergs Würfel“

Neben diesen ausführlich beschriebenen Kooperationen waren noch viele andere Beteiligte an dem Gelingen beteiligt. Dazu gehören das **Bundesministerium für Bildung und Forschung (BMBF)** das die Finanzierung des Quantenchips ermöglichte, **Herr Heidemann vom ZDI** und **Frau Backes von der IHK Düsseldorf**, die Fortbildungen für Lehrer organisieren, **Dominique Elser vom MPI**, der den Heisenberg-Würfel mit betreut hat und viele Kollegen und Kolleginnen, die bei der Verfassung der Berichte mitgearbeitet haben.

## 📌 Die Quantenkryptografie – sichere Datenübermittlung mit Quantenzuständen

**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	$4,29 \cdot 10^9$	$1,84 \cdot 10^{19}$	$3,40 \cdot 10^{38}$

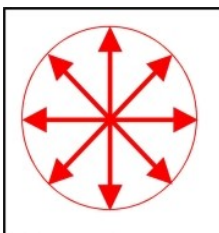
Ein Lauscher muss dabei im Prinzip alle Möglichkeiten ausprobieren um die Daten lesen zu können. Ein Schlüssel von 16 Bits kann noch durch einfaches Ausprobieren in wenigen Stunden geknackt werden. Geht man davon aus, dass ein Computer pro Sekunde 1 Milliarde Schlüssel testen kann, dann benötigt man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

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

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.

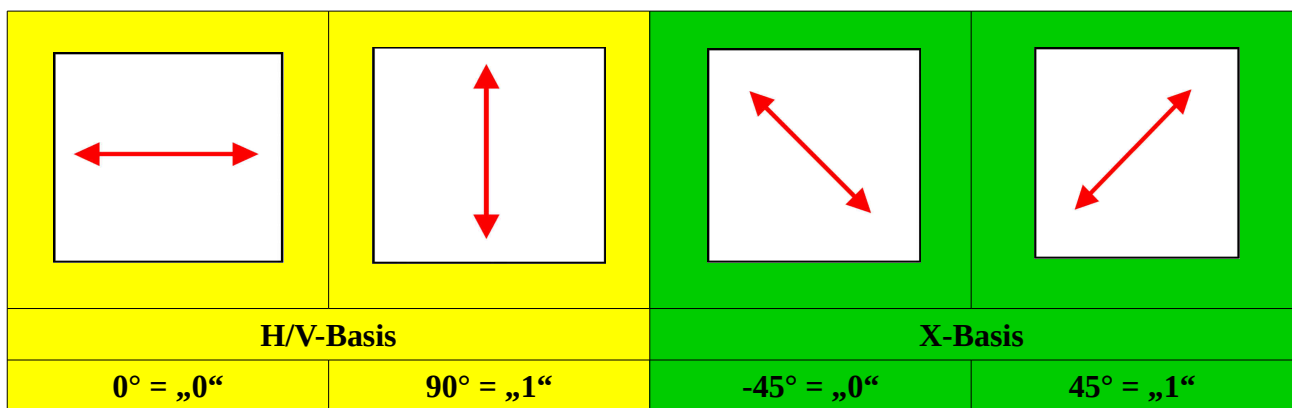
Bei Lasern mit Halbleiterdioden ist dies anders. Durch den Aufbau und die Lichterzeugung ist dieses Laserlicht immer polarisiert. Es schwingt nur in einer Richtung. Durch Drehen des Lasers kann man dann die Schwingungsebene festlegen.

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, die Helligkeit vom Maximum zur Dunkelheit abnimmt und wieder zunimmt. Zwischen maximaler Helligkeit und Dunkelheit liegt ein Winkel von  $90^\circ$ .

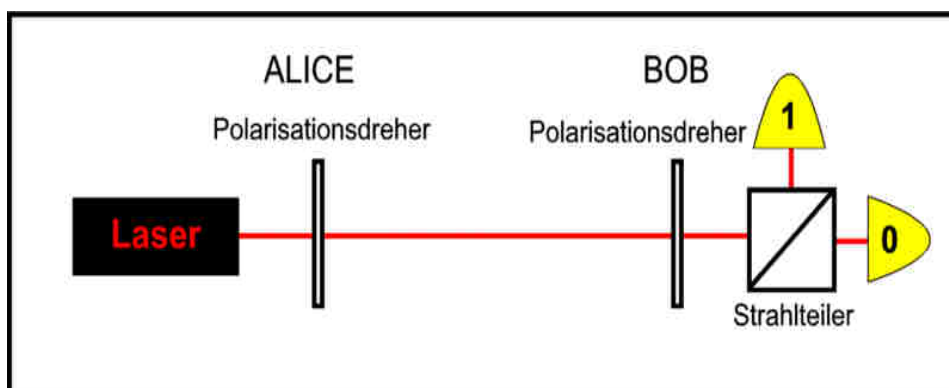
Quarzglas mit der Dicke von der Hälfte der Lichtwellenlänge (632nm!) hat eine interessante Eigenschaft. Beim Drehen eines solchen dünnen Quarzglasplättchen dreht sich auch die Polarisationsrichtung mit. Da ein solches Plättchen viel zu zerbrechlich wäre, wird es auf eine Glasplatte aufgebracht. Ein solches 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  $90^\circ$  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.

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.



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 (beide LEDs leuchten auf). Arbeitet man mit einzelnen Photonen oder mit dem Simulationsmodus wird ein zufälliger Wert erzeugt. Stimmen die Basen nicht überein, sind die Messwerte von BOB 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, bei denen die Basis nicht übereinstimmt.

Messprotokolle für BOB

BOB																											
U	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																											
U	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																											

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

BOB																											
V																											
S																											
D																											
W																											

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

Beispiel

BOB																											
U	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	X	X	X	X	X	X	X	X	X																		
S	1	1	0	1	1	0	1	1	0																		
U	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	

BOB																											
V	1	0	1	1	1																						
S	1	1	0	1	0																						
D	0	1	1	0	1																						
W																											

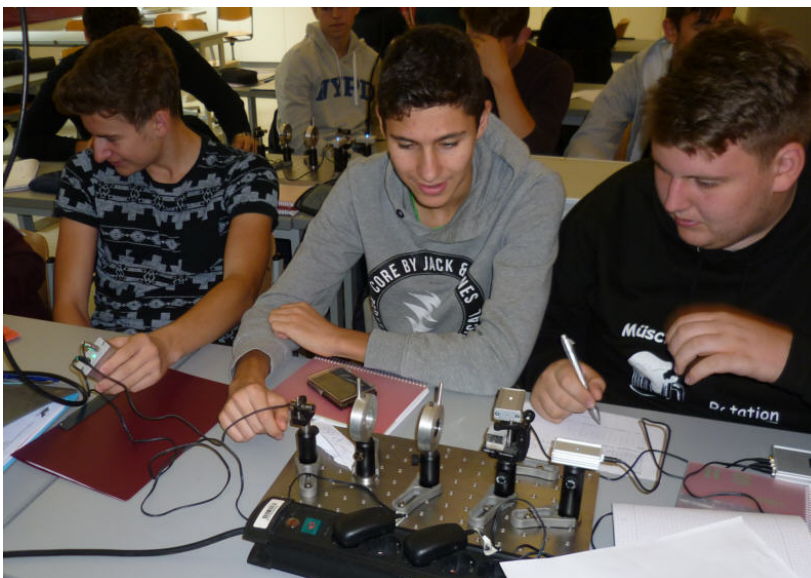
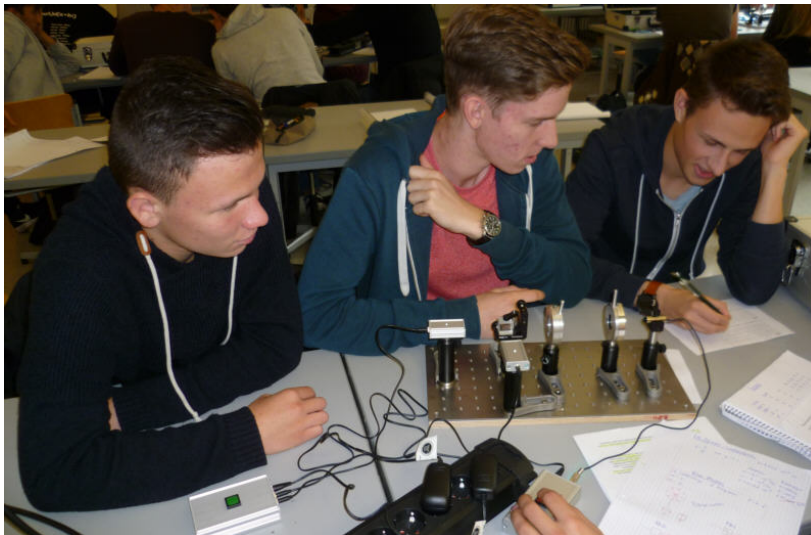
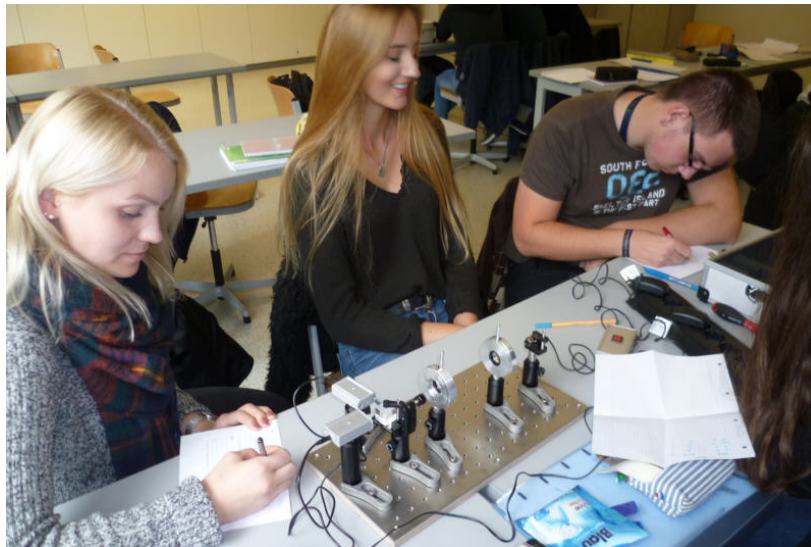
		Codetabelle (Auszug)					Verschlüsselung				
M	0	1	1	0	0	Verschlüsselt (V)	0	1	0	1	
N	0	1	1	0	1	Schlüsselbit (S)	0	0	1	1	
O	0	1	1	1	0	Datenbit (D)	0	1	1	0	

Auf der linken Seite ist das Messprotokoll für BOB abgebildet. Die Durchführung des Experiments erfordert mit Aufbau ungefähr 90 Minuten, mit fertig justiertem Aufbau 20-30 Minuten. Getestet wurde sowohl der Aufbau, wie auch die Durchführung in der Jahrgangsstufe 9, der Q1 (Klasse 12) und Q2 (Klasse 13).

Das Experiment kann bei uns in einem Koffer verpackt ausgeliehen werden, über das ZDI Neuss und Düsseldorf bieten wir auch Fortbildungen für Schüler und Lehrer an.



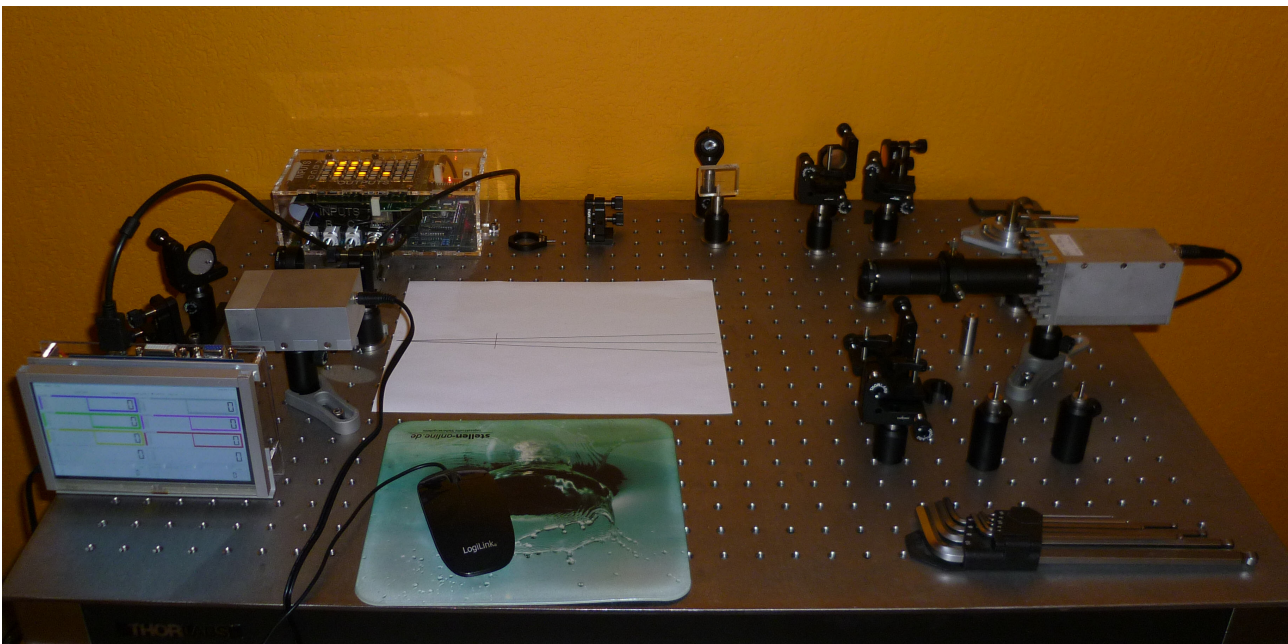
Quantenkryptographie im Physik Grundkurs Q2 (13) 2017  
mit neuem Breadboard



## 📌 Schrödingers Katze lebt – Verschränkung als Schulexperiment

Nach der erfolgreichen Umsetzung der Quantenkryptographie sollte es diesmal ein echtes Quantenexperiment sein, mit dem Nachweis einzelner Photonen. Dabei sollte auch die Verschränkung von Photonen experimentell gezeigt werden, wofür es in der klassischen Physik kein Analogieexperiment gibt. In Anlehnung an das berühmte Gedankenexperiment von Schrödinger, der ein Makroobjekt (Katze) mit einem Quantenobjekt (radioaktives Atom) verschränkte, lautete der Arbeitstitel für dieses Experiment „Schrödingers Katze lebt“.

Grundlage für das Experiment war ein transportables Quantenexperiment, das ein Doktorand im Rahmen seiner Doktorarbeit am Institut von Herrn Meyn entworfen hat. Die Finanzierung von erfolgte über die Rütgers-Stiftung.



Testaufbau für einen Einzelphotonendetektor

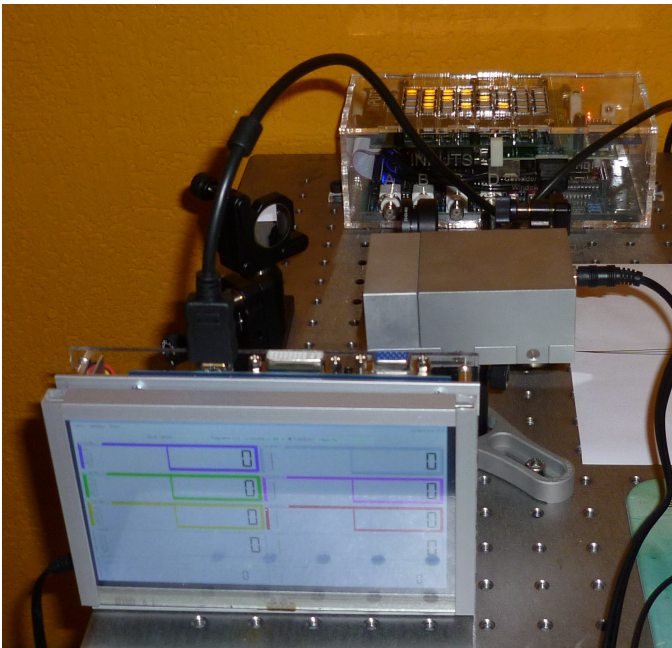
Unmittelbar nach der Zusage der Finanzierung teilte mir Herr Meyn mit, dass die von dem Doktoranden entworfenen Detektoren nicht richtig arbeiteten und besonders die mit rund 1000€ pro Stück teuren Avalanche-Photodioden nach kurzer Zeit erheblich an Empfindlichkeit einbüßten.

Die nächste schlechte Nachricht war dann, dass der Doktorand ohne Vorwarnung und Begründung die Arbeit vollständig eingestellt hatte und nicht mehr Erreichbar war. Dazu war seine Arbeit in großen Teilen nicht richtig dokumentiert. Aus dem geplanten Nachbau wurde daher eine langwierige Neuentwicklung, die in Detailfragen noch immer nicht ganz abgeschlossen ist.

Leidtragender dieser Entwicklung war auch ein Doktorand an der Universität Hannover, der vier dieser Detektoren im Einsatz hatte, von denen keiner richtig arbeitete. In einer konstruktiven Zusammenarbeit ist es uns gelungen, jeweils einen Satz Detektoren soweit umzubauen, dass sie sicher funktionieren und die Photodiode auch bei Überbelichtung nicht beschädigt wird.



An der Universität Hannover wird dieses Experiment inzwischen in der Ausbildung von Studenten eingesetzt, der Einsatz an einer Schule ist geplant.



Auswerteelektronik mit Rasp-Pi und Selbstbau Monitor

Daraus ergibt sich folgendes Fazit: Dieses Experiment hat gezeigt, dass es vom Prinzip her möglich ist, an einer normalen Schule Einzelphotonen-Experimente durchzuführen. Allerdings sind sowohl die Kosten für die Detektoren, als auch der Aufwand für den Aufbau und die Justierung viel zu hoch um ein solches Experiment realistisch im Unterricht einzusetzen.

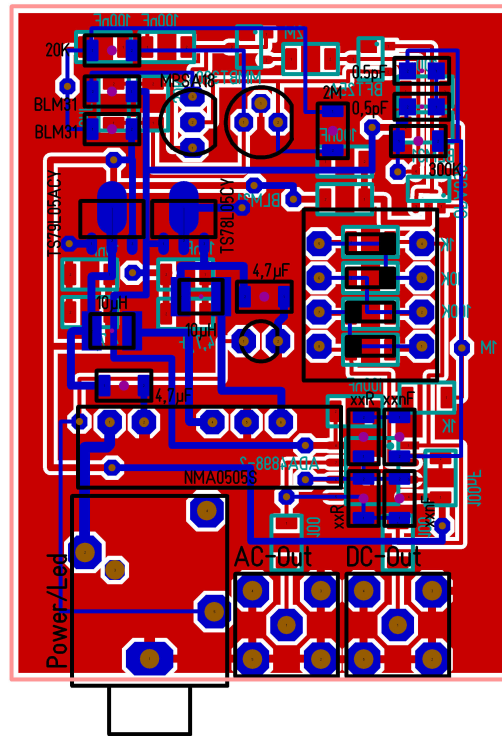
Geplant ist deshalb, dieses Experiment als interaktives Bildschirmexperiment für alle Schulen zugänglich zu machen. Dabei werden echte Messungen als Grundlage eingesetzt. Diese Umsetzung wird im Jahr 2018 online gehen.

### ➤ Heisenbergs Würfel – Ganz nah an der aktuellen Forschung

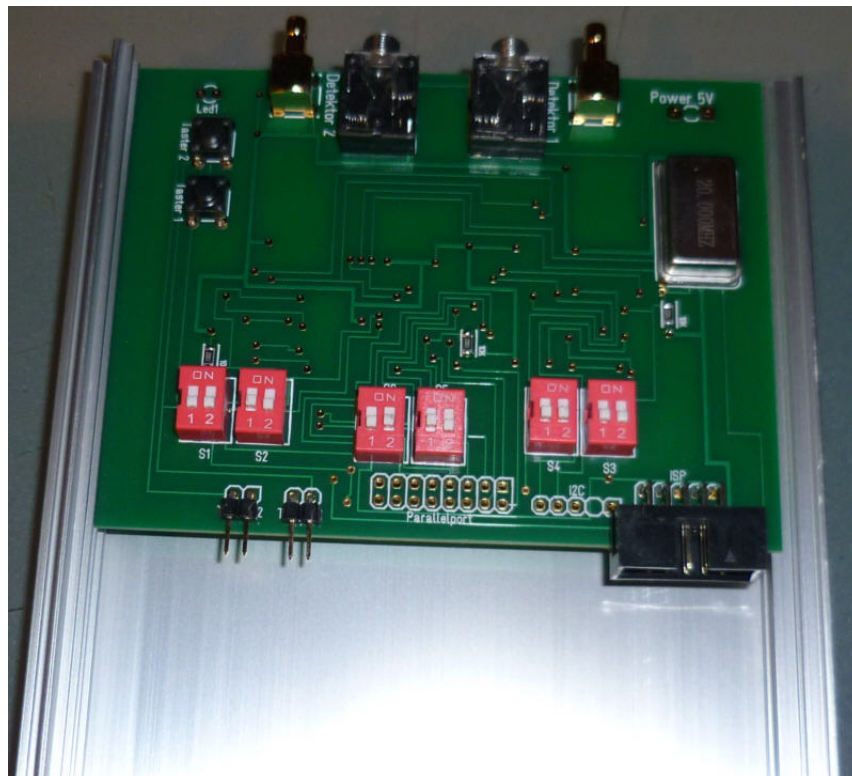


Anfang 2015 elektrisierte mich ein Bericht in der Max-Planck-Forschung. „Geheimcode im Laserblitz“ lautete der Artikel, worin die Forschungsgruppe um Christoph Marquardt und Gerd Leuchs über ein Quantenoptisches Verschlüsselungsverfahren mit einem Laserstrahl und nicht mit einzelnen Photonen berichteten. Nach einer Kontaktaufnahme und einem Besuch im Institut entstand daraus ein neues Quantenexperiment, „Heisenbergs Würfel“. Grundlage ist auch hier wieder ein Versuchsaufbau, der im Prinzip dem des BB84-Protokolls entspricht, allerdings mit zwei deutlichen Unterschieden. Zum einen werden aus dem Quantenvakuum virtuelle Photonen in den Laserstrahl eingekoppelt. Danach werden nicht einzelne Photonen, sondern ganze Pakete untersucht. Ist die Messzeit möglichst kurz gewählt, so ergeben sich nach der Heisenbergschen Unschärferelation zufällige Konfigurationen bei der Messung, man

spricht vom Quantenzufall. Das erste Experiment ist daher gar keine Datenübertragung, sondern ein Quantenwürfel, der eine Folge von Zufallszahlen erzeugt. Die Umsetzung erfolgte erstmals auf einem FPGA und ein Prototyp ist gerade fertig geworden. Dank der Förderung durch das BMBF konnten bis jetzt drei verschiedene Sensortypen, jeweils in zehnfacher Ausfertigung erstellt werden, sowie eine schnelle Auswerteelektronik auf Mikrocontroller-Basis mit einer Schnittstelle zum Raspberry Pi. An diesem Projekt will ebenfalls eine Schülergruppe aktiv mitarbeiten. Soweit ein Experiment fertiggestellt ist, möchte das Max-Planck Institut in Erlangen dieses für Ausstellungen und Messen benutzen. Dieses Experiment wurde schon erfolgreich an andere Schulen eingesetzt und kann von interessierten Lehrerinnen und Lehrern ausgeliehen werden.



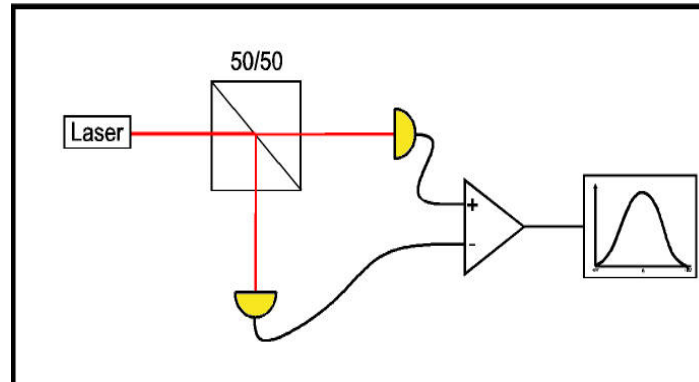
Sensorelektronik in zweiseitiger SMD-Technik Originalgröße 50x36mm



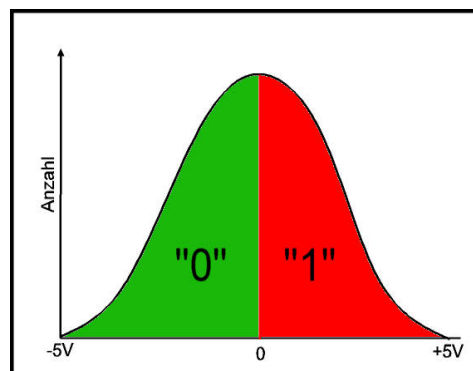
Auswertungselektronik mit 3 Mikrocontrollern im Parallelbetrieb für Datenraten bis 1 MHz / 16bit Auflösung und zwei Kanälen in Echtzeit vor dem Einbau in das Aluminiumgehäuse

## Zufall im quantenmechanischen Messprozess

Schickt man einen Laserstrahl durch einen 50/50 Strahlteiler, detektiert die Intensität der beiden erzeugten Strahlen und bildet aus den gemessenen Signalen die Differenz, so würde man beim Ausschluss aller Messfehler den Messwert Null erwarten.



Aufgrund der Heisenbergschen Unschärferelation erhält man Differenzwerte, die entweder größer oder kleiner Null sein können. Messungen über einen längeren Zeitraum zeigen eine gaußförmige Verteilung der Differenzwerte mit dem Maximum bei Null. Aussagen über die einzelnen Photonen aus dem Quantenvakuum sind aber nicht möglich, so dass die einzelnen Messungen zufällige Werte ergeben. In einem einfachen Fall kann man allen positiven Werten den logischen Wert „1“ zuordnen, allen negativen Werten den logischen Wert „0“.



Da jede Messung einen zufälligen Wert liefert, erhält man eine zufällige Abfolge von binären Werten, die man für die Erzeugung von Zufallszahlen nutzen kann.

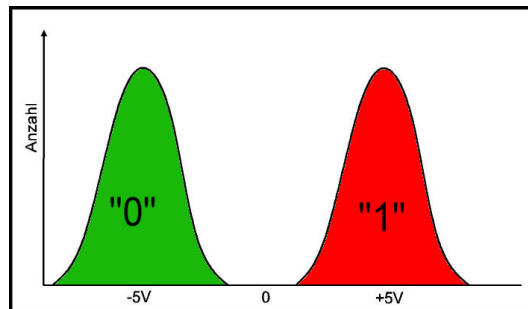
## Schlüsselübertragung mit Lauscher

Bei der Schlüsselübertragung mit Einzelphotonen und dem BB84 Protokoll nutzt man das „No Cloning Theorem“ aus. Das von EVE detektierte Photon kann nicht geklont werden, sondern EVE kann nur ein neu erzeugtes Photon an BOB weiterleiten. Dabei tritt zwangsläufig ein Fehler von 25% aller übertragenen Bits auf. Ist der Schlüssel lang genug, können ALICE und BOB den Lauscher so identifizieren. Sobald man den Schlüssel aber mit mehreren Photonen gleichzeitig überträgt, reicht EVE genau ein einzelnes Photon, um den Schlüssel abzuhören. Da zu BOB dann immer noch Photonen gelangen, bemerkt er den Lauscher nicht.

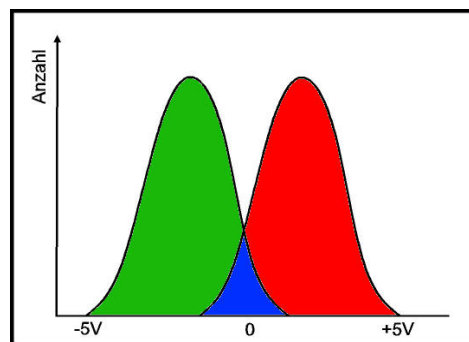


Nachteil der Einzelphotonen-Übertragung ist der große Messaufwand, da spezielle Detektoren benötigt werden. Die Methoden unterscheiden sich nicht prinzipiell in der Reichweite. Allerdings gibt es Protokolle mit Einzelphotonen, die sogar über größere Entfernungen Schlüssel erzeugen können als unsere Methode.

Bei der normalen Übertragung von Daten sind die Zustände für den logischen Wert „0“ und den logischen Wert „1“ praktisch eindeutig separiert. Im einfachsten Fall verwendet man für den Wert 1 die horizontale Polarisation, für den Wert 0 die vertikale. Durch den Quantenzufall würde man messtechnisch zwei deutlich getrennte Gaußkurven erhalten.



Wählt man für die beiden logischen Werte jetzt aber Polarisationszustände, die nicht wie im oben angeführten Fall um 90° auseinanderliegen, sondern sich nur um wenige Grad unterscheiden, dann überlappen sich die beiden Gaußkurven.



Misst man in dem blau markieren Überlappungsbereich, so ist keine eindeutige Aussage zu dem erhaltenen logischen Wert möglich. Nur in den beiden grün bzw. rot markierten Bereichen sind eindeutige Aussagen über den logischen Wert möglich. Jede einzelne Messung ist durch den Quantenzufall rein zufällig.

ALICE erzeugt eine zufällige Abfolge von binären Werten und überträgt diese an BOB. BOB führt dann jeweils eine Messung durch. Er notiert sich die erhaltenen Werte. Über eine öffentliche Leitung verständigen ALICE und BOB sich darüber, welche Messwerte bei BOB eindeutig waren. Alle anderen Werte werden verworfen. Der einzelne logische Wert wird bei dem Abgleich natürlich nicht erwähnt. Am Ende haben ALICE und BOB den gleichen Schlüssel. Um im Modellexperiment möglichst viele eindeutige Werte zu erhalten, darf die Überlappung nicht zu stark sein. Darunter leidet natürlich die Datensicherheit, dies ist aber in der Schule ohne Relevanz. Ist eine Lauscherin EVE in der Leitung macht sie das gleiche wie BOB. Da aber jede Messung einen zufälligen Punkt auf unserer Gaußkurve bedeutet, messen EVE und BOB niemals denselben Wert. EVE kann sogar bei dem öffentlichen Schlüsselabgleich lauschen. Der abgehörte Schlüssel ist

für EVE völlig unbrauchbar. In diesem Fall erkennen ALICE und BOB EVE zwar nicht, aber da EVE keinen sinnvollen Schlüssel erhält, ist der Lauscher für die Datensicherheit nicht relevant.

Der Vorteil dieses Verschlüsselungsverfahrens ist, dass großenteils Komponenten aus der optischen Telekommunikation verwendet werden können, was die Integration in bestehende Infrastruktur vereinfacht. In einer Freiraum-Übertragungstrecke stört Streulicht die Messung nicht, im Gegensatz zur Einzelphotonen-Detektion.

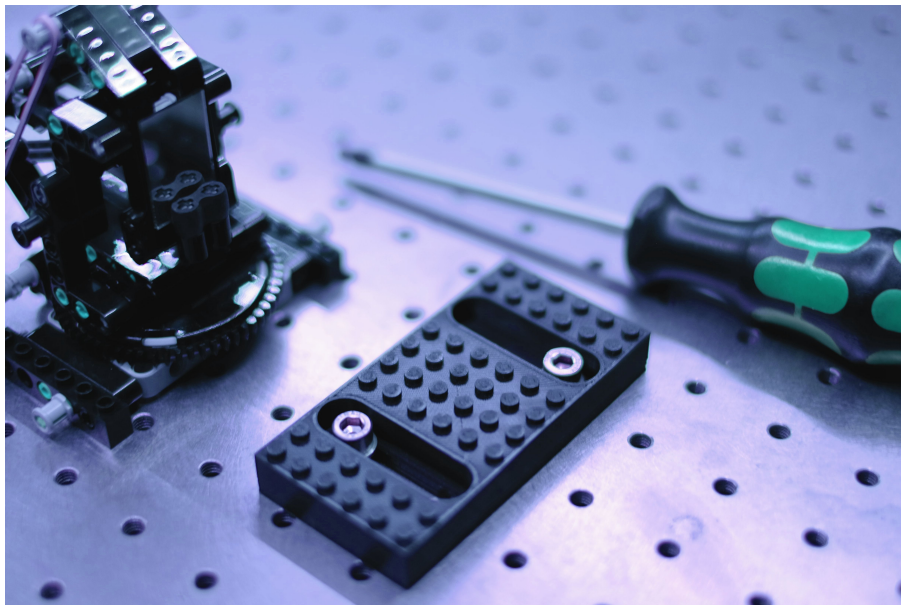
### 🔗 Und jetzt alles noch mal neu – Photonics aus dem 3D-Drucker

Ein Knackpunkt bei allen Experimenten ist, dass die Kosten pro Set über 1000€ liegen, was für die meisten Schulen viel zu teuer ist. Auf Anregung der Quantenchip-Schüler ist daher geplant, alle benötigten Komponenten aus 3D-Druckformen und Material, das in jedem normalen Baumarkt vorhanden ist, aufzubauen. Die Gesamtkosten sollten dabei 500€ pro Set nicht übersteigen. Für die benötigten Strahlteilerwürfel und die Lambda/2 Platten haben wir schon geeignete Bezugsquellen für preiswerten Ersatz gefunden.

Eine Schülergruppe plant entweder in diesem oder spätestens im nächsten Jahr damit an „Jugend forscht“ teilzunehmen.

Dieses Projekt soll dann auch im Internet frei verfügbar für alle Lehrkräfte sein und mit einem 3D-Drucker können alle Bauteile selbst hergestellt werden.

Als Erweiterung ist sogar geplant, die Rotationsdreher mit Motoren auszustatten, so dass eine halb- oder sogar vollautomatische Schlüsselübertragung möglich wird. Das Experiment wäre damit in der Praxis in einem Glasfasernetzwerk einsetzbar.

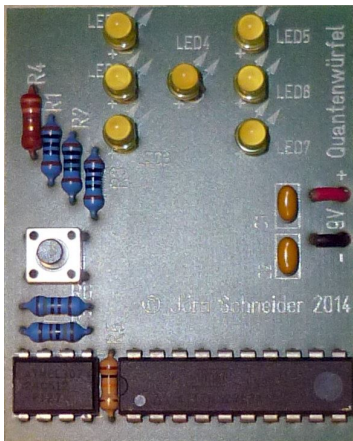


Beispiel eines Exponats von myphotonics der Uni Osnabrück

<https://www.ufp.uni-osnabrueck.de/en/education/myphotonics.html>

## ➤ Die Schüler mitnehmen – der Quantenwürfel

War die Entwicklung der Quantenkryptografie und auch von Schrödingers Katze noch weitgehend in Lehrerhand, so wurden bei Heisenbergs Würfel, wie schon beschrieben, die Schüler aktiv mit eingebunden.

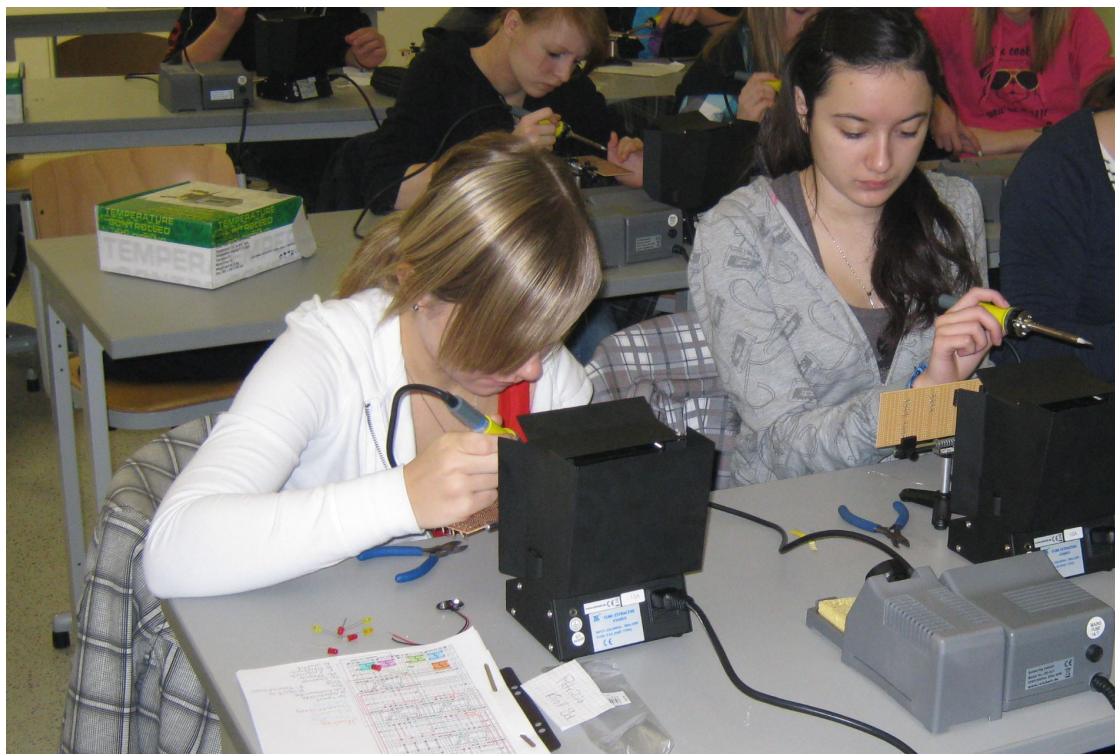


Ein ganz anderer Nebeneffekt von Schrödingers Katze war die Entwicklung eines „Quantenwürfels“ für die Klasse 9. In unserem Lehrplan ist der Bau eines kleinen elektronischen Geräts in der Klasse 9 im Rahmen des normalen Physikunterrichts vorgesehen. Dies war bis vor einigen Jahren ein elektronischer Würfel der Firma Pollin, den die Schüler selbst im Unterricht löteteten. Die Idee war, aus einer echten quantenphysikalischen Messung einzelne Würfe eines Würfels zu erzeugen und als „Würfelaugen“ auszugeben. Die Kosten sollten dabei 10€ nicht überschreiten. Im ersten Durchlauf konnten die Schüler zwischen einem „Pollin-Würfel“ zu 3,95€ und einem Quantenwürfel zu 8,50€ wählen. Fast alle Schüler hatten sich damals für den - *Originalzitat* „coolen Quantenwürfel“ - entschieden. Nach diesem Probelauf im Jahr 2013 konnten über die Joachim Herz-

Stiftung im Jahr 2014 500 Sätze angeschafft werden, so dass wir dieses Projekt kostenlos für unsere 9er anbieten können.

Dieses Projekt weckt schon früh die Neugierde auf die Physik in der Oberstufe. Und die Schüler in der Q2 (13) erinnern sich tatsächlich noch an das Projekt in der Klasse 9, was ich jetzt im dritten Jahrgang zu meiner Freude feststellen durfte.

Auch in Zukunft sollen die Schüler aktiv in die Entwicklung der Versuche mit eingebunden werden.



Erster Einsatz unserer Lötstationen im Jahr 2011 – damals gab es den Quantenwürfel noch nicht

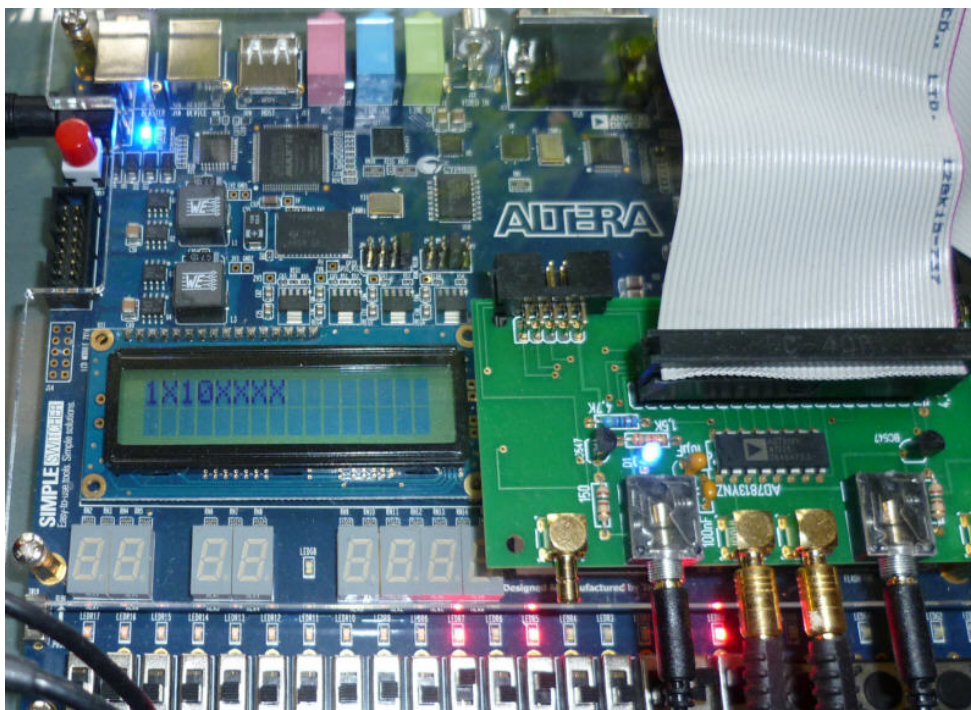


## 📌 Der Quantenchip – Quantenkryptografie auf dem FPGA

Das Leibniz-Gymnasium Dormagen dürfte weltweit die einzige Schule sein, die insgesamt 8 Schülerexperiment-Sets zur Quantenkryptografie im Unterricht der Oberstufe einsetzt. Da unsere Schule schon seit Jahren erfolgreich am Wettbewerb „Invent-a-chip“ teilnimmt, entstand die Idee eines „Quantenchips“ der die Quantenkryptografie auf einem FPGA umsetzt. Da die Idee von mir als Lehrer ausging, konnten wir nicht am Wettbewerb teilnehmen, aber die Macher des Wettbewerbes fanden die Idee ebenfalls sehr spannend und räumten uns die Möglichkeit einer Teilnahme außerhalb des Wettbewerbes ein.

Neben den 8 vorhandenen Schülerversuchen haben wir durch eine finanzielle Förderung von 3750€ der VR-Bank ein weiteres Experiment anschaffen können, das anders als unsere Schulexperimente bessere optische Komponenten besitzt und zwecks Transport komplett aufgebaut in eine Transportbox passt. Allerdings stellte sich schon am Anfang heraus, dass die vorhandenen Sensoren für die Umsetzung auf dem FPGA nicht brauchbar waren, es mussten also neue Sensoren entwickelt und gebaut werden. In dem gerade einmal 55x27x24mm großen Gehäuse ist die Photodiode, eine Verstärker und Filterschaltung untergebracht, die ein der Helligkeitsänderung proportionales Signal ausgibt und Störimpulse weitgehend eliminiert. Zusätzlich ist im Sensor eine LED als Signalquelle angebracht, die ein empfangenes Bit anzeigt. Die Ansteuerung erfolgt über das FPGA.

Das aufbereitete Signal wird einem 2-Kanal 8(10)bit ADC-Wandler mit einer 8bit breiten Schnittstelle und 400kSPS zugeführt, der auf einer extra für das FPGA entwickelten Platine sitzt. Im Laufe der Entwicklung zeigte es sich, dass die 8bit-Bandbreite völlig ausreichend ist, auf eine Erweiterung auf 10 Bit wurde daher verzichtet. Zusätzlich befindet sich auf der gleichen Platine noch zwei weitere ADCs mit 16 Bit Bandbreite bei 1MSPS und ISP-Schnittstelle, die für spätere Entwicklungen vorgesehen sind. Dies wurde ebenfalls mit Mitteln des **BMBF** umgesetzt.



Umsetzung auf dem Altera DE2-115 FPGA  
Im Vordergrund ist die ADC-Platine zu erkennen

Als Sonderpreisträger des Wettbewerbs „Invent-a-chip“ durften wir vom 23-26.10.2017 die Quantenkryptografie auf dem MST-Kongress bei München und bei IBM Watson vorführen.



Das Quantenkrypto-Team Mit John Cohn, einer der weltweit 10 kreativsten Köpfe hinter IBM.



Preisverleihung auf dem MST-Kongress



## 📌 Die Idee weitertragen – Schüler auf dem MINT-Tag am 26.11.2017

Das ZDI Neuss (<http://www.mint-machen.de/>) veranstaltet in diesem Jahr erstmals einen MINT-Tag, wo neben Firmen und Initiativen auch das Leibniz-Gymnasium mit der Quantenkryptographie vertreten sein wird. Unsere Schülerinnen und Schüler zeigen anderen Jugendlichen und Lehrerinnen und Lehrern aus dem Kreis Neuss und Umgebung unseren Quantenchip, zusätzlich können alle Besucher das Experiment selbst ausprobieren und für interessierte Lehrerinnen und Lehrer besteht die Möglichkeit, dieses Experiment danach auch auszuleihen.



Auch auf dem MINT-Tag der IHK Düsseldorf am 10. Oktober 2017 waren wir mit der Quantenkryptographie vertreten. Mehrere Schulen im Raum Düsseldorf zeigten großes Interesse an der Ausleihmöglichkeit und die Lehrer haben selbst mit viel Spaß das Experiment ausprobiert.

Auch die zukünftigen Informatik-Lehrer in NRW sollen in das Projekt mit eingebunden werden. Die Qualifizierungsmaßnahme für die Oberstufe in Informatik wird vom Kompetenz-Team in Wesel durchgeführt. Im Rahmen dieser Maßnahme wird es im Jahr 2018 erstmals auch einen Workshop zur Quantenkryptographie in Dormagen geben.



Auch zur MINT-Tagung der Heinrich-Heine-Universität in Kooperation mit der IHK-Düsseldorf im Frühjahr 2018 ist ein weiterer Workshop geplant.

Und zuletzt wird eine Schülerin aus dem Quantenkrypto-Team in diesem Jahr mit einem eigenen experimentellen Entwurf zur Quantenkryptographie am Wettbewerb „Jugend forscht“ teilnehmen.



### **Was kommt danach? - Ein Ausblick**

Die Quantenphysik steckt noch voller spannender Experimente, die nur darauf warten, in der Schule einmal eingeführt zu werden. Zusammen mit Schülern und auch unseren Kooperationspartnern planen wir ein Quanten-Experimentalset zu entwickeln, welches im normalen Unterricht in der Oberstufe zum Einsatz kommen soll. Dieses wird eng angelehnt an die Lehrpläne zur Quantenphysik sein und soll so aufgebaut sein, dass jeder Physiklehrer es einsetzen und auch jede Schule es finanzieren kann. Fachlich und didaktisch soll dies durch die Universität Erlangen begleitet werden. Grundsätzliche Überlegungen sind dazu schon getätigt worden.