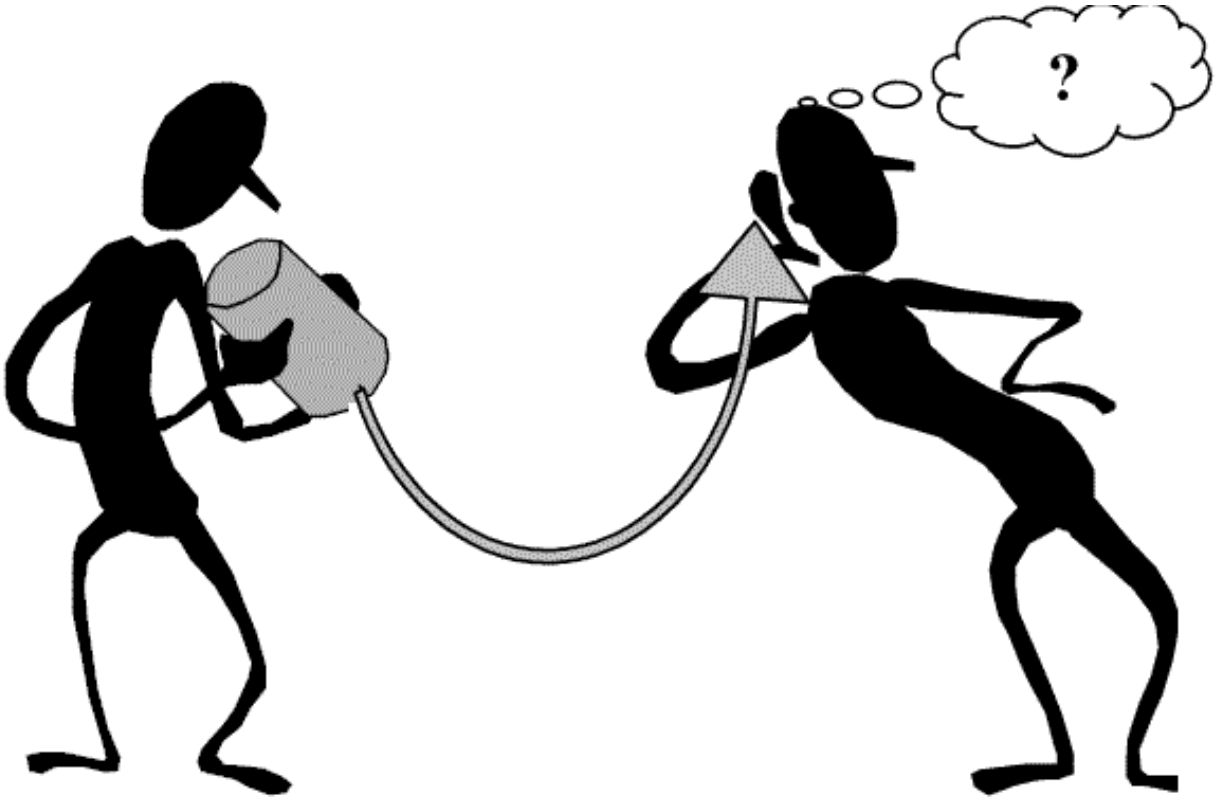
Unterrichtsszenario zum Thema Quantenkryptographie

(abhörsichere Datenübertragung)



Erstellt im Rahmen der LV „Didaktik der theoretischen Physik“ im SS 2011
(Prof. Franz Embacher)
von
Katharina Putzer und Christine Reiter

Inhaltsverzeichnis

1 Vorschau und Gliederung

Unser Unterrichtsszenario ist konzipiert für SchülerInnen (S) der 12. Schulstufe und umfasst drei Doppelstunden. Wir sind uns bewusst, dass im Standardunterricht wohl selten die Zeitressourcen zur Verfügung stehen, sich über mehrere Wochen nur mit dem „Randthema“ Quantenkryptographie auseinanderzusetzen. Deshalb haben wir dieses Szenario als Erweiterung zum Standardunterricht – etwa als Thema für „Physik vertiefend“ oder ein Wahlfach Physik entworfen.
In der ersten Unterrichtseinheit werden wir den S eine vielseitige Lernumgebung anbieten, um ihnen die Möglichkeit zu geben, sich eigenständig einen Zugang zum Thema Kryptographie zu erschließen.
Die zweite Einheit behandelt dann, mit einer Mischung aus für die S aktiven und passiven Komponenten, die Sicherheitsproblematik der klassischen Kryptographie und führt zum BB84 Protokoll hin.
In der dritten Einheit schließlich können die S anhand eines Computersimulationsprogramm die einzelnen Schritte des BB84 Protokolls selber nachvollziehen. Als Abschluss dieser Einheit ist dann noch eine Diskussionsrunde über Eves Abhörmöglichkeiten geplant, um das Thema endgültig abzuschließen.

2 Skizze des fachlichen Hintergrunds

Wir beschränken uns hier darauf den fachlichen Hintergrund des BB84 Protokolls zu skizzieren, da die historischen Kryptographieverfahren bereits auf den entsprechenden Arbeitsblättern ausführlich behandelt sind.
Des Weiteren wird die in der Quantenphysik verbreitete Diracnotation verwendet um Zustände und ihre Veränderung im zugehörigen zweidimensionalen Hilbertraum (das genügt für unsere Zwecke) zu beschreiben.

2.1 Polarisation

Der Diracvektor $|0\rangle =: |h\rangle$ soll horizontale Polarisation, $|1\rangle =: |v\rangle$ soll vertikale Polarisation bezeichnen. Allgemein bezeichnet man einen Zustand $|\Psi\rangle = \alpha|0\rangle+\beta|1\rangle$ mit $\alpha,\beta \in \mathbf{C}$ als Überlagerung der Basisvektoren $|0\rangle,|1\rangle$ =: „Superposition“.
Ausserdem benötigen wir noch die Orthonormiertheit der Basisvektoren:
$\langle 0|0\rangle = \langle 1|1\rangle = 1$ (Normierung) und $\langle 0|1\rangle = \langle 1|0\rangle = 0$ (Orthogonalität)
Die Wahrscheinlichkeit bei der Messung eines Zustands $|\Psi\rangle = \alpha|0\rangle+\beta|1\rangle$ in der Basis h/v den Zustand $|0\rangle$ zu erhalten ist gegeben durch $p_{|0\rangle} = \langle\Psi|0\rangle\langle 0|\Psi\rangle = (\alpha^*\langle 0|0\rangle+\beta^*\langle 0|1\rangle)(\alpha\langle 0|0\rangle+\beta\langle 0|1\rangle) = |\alpha|^2$ (analog ist die Wahrscheinlichkeit $|1\rangle$ zu messen gegeben durch $|\beta|^2$). Das Betragsquadrat der Amplituden vor den Zuständen $|0\rangle$, $|1\rangle$ gibt also die Wahrscheinlichkeit an, den Zustand $|0\rangle$, $|1\rangle$ nach einer Messung mit Basis $|0\rangle$, $|1\rangle$ vorzufinden. Das impliziert die Forderung $|\alpha|^2+|\beta|^2 = 1$

Aus Superposition der Zustände $|0\rangle$ und $|1\rangle$ erhalten wir weiters

$|+\rangle =: \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ um den Zustand eines im Winkel 45° polarisierten P hotons zu beschreiben,

und

$|-\rangle =: \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ um den Zustand eines im Winkel -45° polarisierten Photons zu beschreiben.

Damit gilt weiters: $|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$ sowie $|1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$

2.2 Messung

In der Quantenphysik entspricht eine Messung einer Wechselwirkung der Messapparatur mit dem Quantensystem – die Messung kann also den Zustand verändern (und tut dies im Allgemeinen auch). Die Messung eines Zustands $|\Psi\rangle = \alpha|0\rangle+\beta|1\rangle$ in Richtung $|0\rangle$ beschreibt man durch den Projektor in Messrichtung: $M|\Psi\rangle = |0\rangle\langle 0| \, |\Psi\rangle$.
Nach der Messung befindet sich das Quantensystem im gemessenen Zustand (in diesem Fall im Zustand $|0\rangle$ mit der Wahrscheinlichkeit $|\alpha|^2$) – eine Messung bedeutet also gleichzeitig auch eine Präparation.
Diesen Umstand macht man sich zu Nutze, um Schlüssel mittels Quantenkryptographie sicher übertragen zu können:
Wenn eine mögliche Lauscherin (üblicherweise „Eve“ genannt) ein gesendetes Photon abfängt, müsste sie eine größere Anzahl von Kopien des Zustands des Photons haben, um die Amplituden α,β bestimmen zu können. Da sie aber nur ein Photon zur Verfügung hat kann sie nur raten, ob Alice (die Senderin) das Photon in der h/v oder in der +/- Basis präpariert hat. Wenn sie richtig rät, erhält sie den gesendeten Zustand als Ergebnis und kann ein Photon im selben Zustand an Bob (Empfänger) weitersenden ohne entdeckt zu werden. Das wird aber nur in 50% der Fälle zutreffen. Wenn Eve zur Basis h/v misst und Alice z. B den Zustand $|+\rangle$ präpariert hat, so misst Eve mit einer Wahrscheinlichkeit von jeweils 50% ($|\alpha|^2=|\beta|^2=1/2$) den Zustand $|1\rangle$ oder $|0\rangle$. Danach ist ihr Photon aber horizontal oder vertikal polarisiert – ihre Messung hat den Quantenzustand verändert. Sie kann also nur einen veränderten Zustand an Bob weiterschicken, der wiederum in der Messbasis +/- mit einer Wahrscheinlichkeit von 50% den von Alice gesendeten Zustand $|+\rangle$ erhält. In einem Viertel der Fälle wird Eve also enttarnt, wenn Alice und Bob einige ihrer Schlüsselbits vergleichen.
Das man einen unbekannten Quantenzustand nicht kopieren kann, ist auch unter dem Begriff „non-cloning Theorem“ in der Literatur zu finden, und wird unter diesem Begriff auch in unserem Unterrichtsszenario vorkommen.

2.3 BB84 – Protokoll

Zusammenfassend basiert die Abhörsicherheit der Quantenkryptographie auf folgenden Punkten:

- Messungen an einem Qubit verändern den Zustand
- Non – Cloning – Theorem
- Es ist unmöglich einen unbekannten Quantenzustand durch eine einzige Messung vollständig zu bestimmen

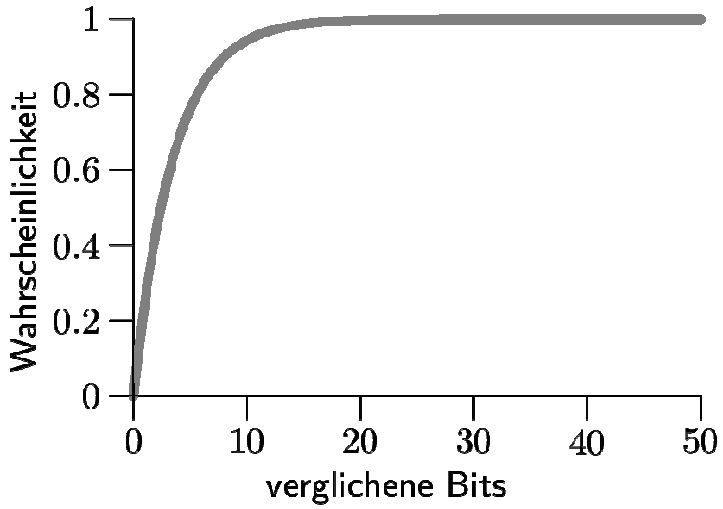
Dass ein möglicher Lauscher bei Alice oder Bob über die Schulter schaut, kann aber auch durch die Verwendung von Quantenkryptographie nicht ausgeschlossen werden.

Das von uns behandelte BB84 Protokoll wurde von Charles Benett (IBM) und Gilles Brasset (Universität Montreal) 1984 entwickelt und wurde inzwischen bereits mehrmals angewendet und erprobt.
Das Ziel der Quantenkryptographie besteht darin, einen abhörsicheren Schlüssel zu erzeugen, ohne dass sich Sender (Alice) und Empfänger (Bob) treffen müssen.

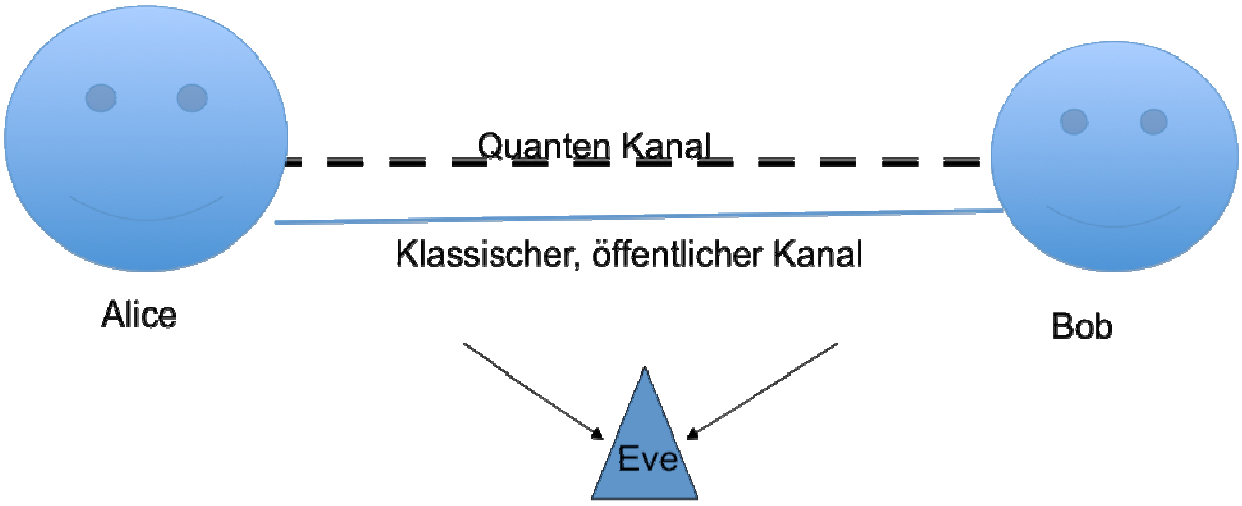
Das BB84 Protokoll sieht dafür folgende Schritte vor:

1. Alice präpariert Qubits zufällig in einem der Zustände $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, indem sie beliebig aus den Basen h/v, +/- sowie aus den Bitwerten 0,1 auswählt. (In jeder Basis kann sie ein Bit zum Wert 0 oder 1 präparieren → insgesamt 4 Möglichkeiten.)
2. Alice schickt das präparierte Bit an Bob.
3. Bob wählt eine Zufallsfolge von Basen $\in$ {h/v, +/-} und misst die von Alice empfangenen Qubits.

4. Alice und Bob vergleichen die von ihnen gewählten Messbasen (auf klassischen Kanälen) und tauschen sich auch darüber aus, welche Photonen erfolgreich erhalten wurden.
5. Die nicht erfolgreich gesendeten Bits, sowie die in unterschiedlichen Basen gemessenen Bits werden gestrichen – die übrigen bilden den Schlüssel.
6. Alice und Bob tauschen k der nicht gelöschten Bits aus und ermitteln die Fehlerrate. Ist diese zu hoch, so muss ein neuer Schlüssel erzeugt werden, da der Verdacht auf einen Lauschangriff besteht. Die folgende Abbildung zeigt den Zusammenhang zwischen der Anzahl der verglichenen Bits und der Wahrscheinlichkeit einen Lauschangriff zu entdecken. (Quelle: Diplomarbeit von Heidemarie Knobloch S 67)
7. Alice verschlüsselt ihre Nachricht und übermittelt die verschlüsselte Nachricht an Bob
8. Bob entschlüsselt die Nachricht mit dem zuvor erzeugten Schlüssel



Das BB84 Protokoll verwendet also sowohl einen „geheimen“ Quantenkanal (Versenden der Schlüsselbits), als auch einen klassischen sogar öffentlichen Kanal (Austausch über verwendete Messbasen) für die Kommunikation.



3 Unterrichtseinheiten

3.1 1. Unterrichtseinheit:

Zeiteinteilung: (Doppelstunde – 100min)
10min: Einstieg, Historischer Rückblick, Gruppeneinteilung
40min: Stationenbetrieb: Plakat anfertigen, Aufgabe lösen
15min Besuch pro Station
5min: Schlussbesprechung

Unterrichtseinstieg:

Als Motivation stehen die folgenden beiden Sätze zu Stundenbeginn an der Tafel:
guten morgen kinder _ iwvgp optigp mkpfgt
das ist eine geheime nachricht _ fcu kuv gkpg igjgkog pcejtkejv

Mit den Schülern soll gemeinsam überlegt werden, wo verschlüsselte Nachrichten notwendig waren und auch heute noch sind.

Stationenbetrieb

Gruppeneinteilung: Den Schülern werden zusammengefaltete Zettelchen gegeben, auf denen jeweils die Nummern 1-4 stehen, um so die Klasse bunt zusammengewürfelt in 4 verschiedene Gruppen zu unterteilen.

Es stehen jeweils 4 Tische (1 Tisch ist ein Computertisch) mit Unterlagen bereit, an denen jeweils eine Minipräsentation aufgearbeitet werden soll. Die Schüler sollen, mit den von der Lehrperson gestellten Hintergrundinformationen, ein Plakat so anfertigen, dass ihre Mitschüler neben dem Kennenlernen und Verstehen des jeweiligen Verfahrens auch einen aktiven Part ausführen können (Satz entschlüsseln, Cäsarscheibe basteln etc.). Die 4 verschiedenen Arbeitsaufträge sind im Anhang aufgeführt.

Wie soll der Stationenbetrieb in die Benotung mit einfließen?
Für die Schüler sind an den jeweiligen Stationen Arbeitsaufträge notiert, welche gesammelt in Reinschrift in ein Lernjournal geschrieben werden sollten, welches dann nach einer vordefinierten Zeit (2 Wochen) zur Kontrolle/Benotung abgegeben werden muss. Damit die Benotung der Arbeitsaufträge für die Schüler durchsichtig erscheint, sind die einzelnen Abschnitte mit Punktezahlen angeführt, sodass die Schüler selbst entscheiden können, wie viel Prozent sie erreichen wollen. Für besondere Kreativität, Ausführlichkeit etc. werden Bonuspunkte vergeben. Details zur Benotung erfolgen im abschließenden Kapitel.

3.2 2. Unterrichtseinheit:

Zeiteinteilung: (Doppelstunde – 100min)
20min: Wiederholung Quantenphysik allgemein: Superposition, Polarisation, Zustände, Messung, Bedingungen an „absolut sicheren Schlüssel“
40min: Expertengruppen: Zufallszahl, Schlüsselverteilung mit einzelnen Photonen
20min: Zusammenfassung und Diskussion – haben wir schon eine sichere Schlüsselübertragung?
20min: Lehrerinput – Verwendung von 2 Messbasen – BB84 Protokoll

Stundeneinstieg
Dieses Unterrichtsszenario setzt voraus, dass die Grundlagen der Quantenphysik bereits zuvor im Unterricht behandelt wurden und somit prinzipiell zur Verfügung stehen. Trotzdem erachten wir es als sinnvoll, die im Weiteren benötigten Begriffe wie Superposition, Polarisation, Zustände und Messung noch einmal zusammenfassend zu behandeln und zu festigen. Da in dieser Unterrichtssequenz von den Schülerinnen und Schülern bereits sehr viel Eigenleistung verlangt wird, um den akustischen Lerntypen gerecht zu werden, und nicht zuletzt auch aus Gründen der Zeitökonomie, haben wir diesen Teil als Lehrerinput konzipiert.
Wir verwenden dafür die Zusammenfassung der Quantendimensionen DVD auf U1 Station 8/08.

Expertengruppen
In der vorangegangenen Unterrichtseinheit wurden bereits die vier Bedingungen an eine „abhörsichere Schlüsselübertragung“ formuliert:

1) Die Länge des Schlüssels muss mindestens der Länge der zu übertragenden Nachricht entsprechen
2) Der Schlüssel darf NUR Sender (Alice) und Empfänger(Bob) bekannt sein
3) Jeder Schlüssel muss unvorhersagbar und absolut zufällig sein
4) Der Schlüssel darf nur einmal verwendet werden

Wie wohl auch die S unmittelbar erkennen, liegt die Erfüllung der Bedingungen 1) und 4) in der Verantwortung von Sender und Empfänger.

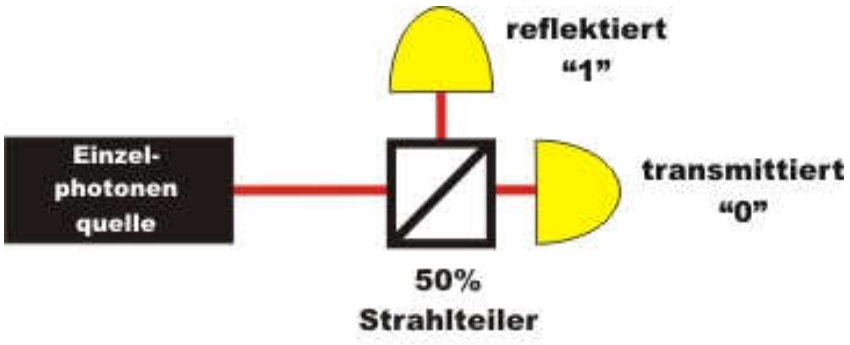
Schwieriger wird es schon die Forderung nach einer absolut zufälligen Folge von Bits zu erfüllen, was für die S wahrscheinlich nicht unmittelbar einsichtig ist (schließlich können vermutlich einige S eine „Zufallszahl“ vom Computer generieren lassen, die aber tatsächlich nicht rein zufällig ist, sondern vom Startwert und der verwendeten mehr oder weniger komplexen Rechenvorschrift abhängt – die quantumlab – homepage bezeichnet solche Zahlen auch als „Pseudozufallszahlen“).

Einsichtiger ist da schon, dass die Bedingung 2) nicht so ohne weiteres erfüllbar ist, denn der Schlüssel darf nicht nur keiner weiteren Person bekannt sein, er muss natürlich auch zwingend Alice und Bob zur Verfügung stehen. Da jede Form von klassischer Datenübertragung nicht sicher ist (Boten können abgefangen, bestochen etc. werden, Telefonate können abgehört werden...) müssten sich Alice und Bob zur Erzeugung des Schlüssels an einem einsamen Ort treffen und sich den Schlüssel jeweils auf geheimen Blöcken notieren („one time pad“) – und zwar jedes Mal, wenn der letzte Schlüssel aufgebraucht ist. Dass diese Methode wegen des hohen Zeitaufwands für den alltäglichen Gebrauch wie z.B. für Bankgeschäfte nicht praktikabel ist, liegt schon ziemlich nahe (oder noch näher).

Nachdem also diese vier Bedingungen von der Lehrperson zusammengefasst wurden, kann sich die Klasse in zwei Gruppen aufteilen (hier dürfen sich die Schüler unter der Auflage, dass beide Gruppen möglichst gleich viele Mitglieder haben, selbst organisieren – sollte das auch für angehende Maturanten noch zu viel verlangt sein, teilt die Lehrperson die Gruppen ein (z.B.: abzählen, alphabetisch etc.)).

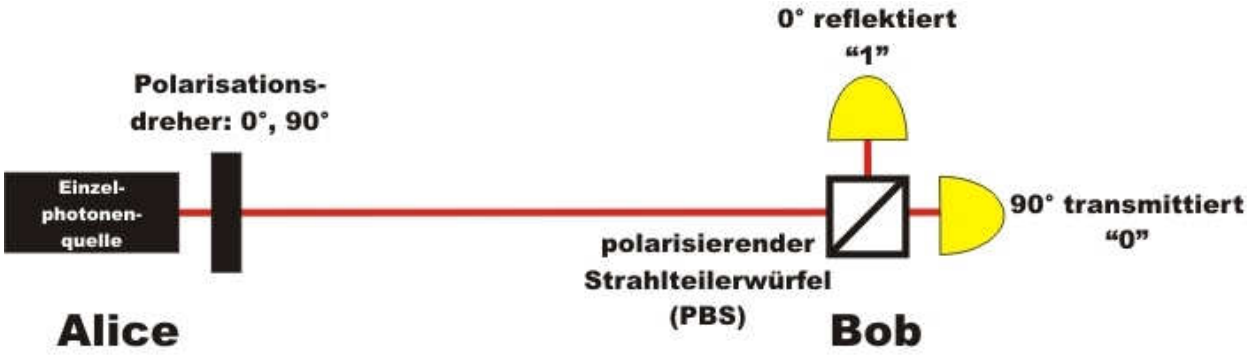
Beide Gruppen benötigen Computer!

Gruppe eins beschäftigt sich mit der Generierung von Zufallszahlen mittels Strahlteilerwürfel. Dazu können sie die Haltestelle 3/03 der U1 der DVD „Quantendimensionen“ (Klett – Verlag) sowie den Abschnitt „Welche Bedingungen lassen sich bisher erfüllen“ im Unterpunkt „Quantenkryptographie“ verwenden.



Quelle: URL: http://www.didaktik.physik.uni-erlangen.de/quantumlab/index.html?/quantumlab/Kryptographie/index.html (28.4.2011)

Gruppe zwei beschäftigt sich mit der „Schlüsselverteilung mit einzelnen Photonen" und hat dafür die Quantumlab – homepage Kapitel 2 zur Verfügung.
Für den Fall eines Technikausfalls, sollte das Material auch in gedruckter Form vorliegen, was aber v.A. für Gruppe zwei ein echter Verlust wäre, da sie um die Bildschirmpräsentation umfallen würde.



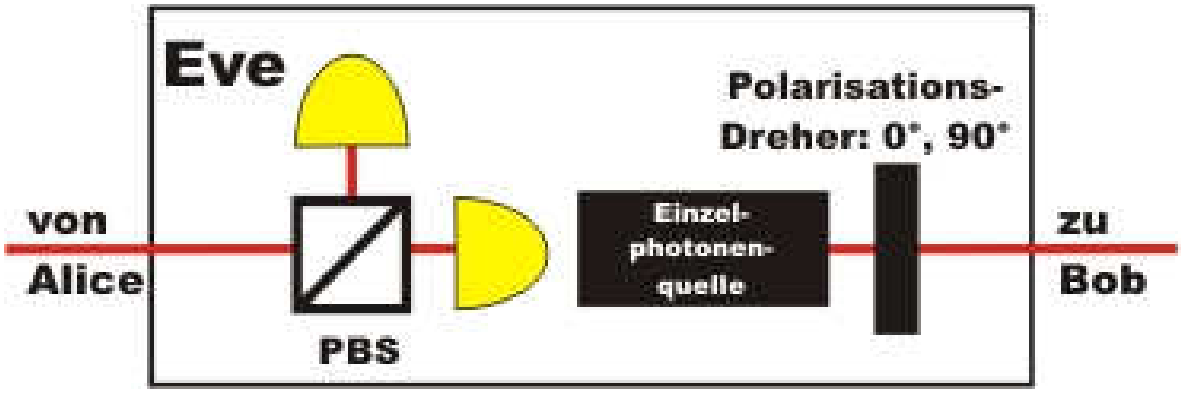
Quelle: URL:http://www.didaktik.physik.uni-erlangen.de/quantumlab/index.html?/quantumlab/Kryptographie/index.html (28.4.2011)

Nach etwa 20 min. sollten die Gruppen mit dem jeweiligen Thema so vertraut sein, dass sich jeweils zwei Schüler aus den unterschiedlichen Gruppen gegenseitig das Thema erklären können sollten. In der Folge sucht sich also jeder Schüler einen Partner aus der jeweils anderen Gruppe, erklärt was er zum eigenen Thema weiß, und bekommt erklärt, was das Gegenüber zum jeweils anderen Thema zu erzählen hat. (Das soll die Kommunikation über physikalische Themen sowie die Ausdrucksfähigkeit fördern, und zudem wieder den kommunikativen Schülern zugute kommen.)

Dafür stehen insgesamt 10 min zur Verfügung. Um den Lernertrag zu sichern, und um allen S die Möglichkeit eines entsprechenden Lernjournaleintrags zu geben (auch wenn der „Expertenpartner" kein echter Experte gewesen sein sollte), stehen noch einmal 10min zur Präsentation vor der ganzen Klasse zur Verfügung. Das heißt, dass jeweils ein Vertreter der beiden Gruppen für die ganze Klasse eine kurze Zusammenfassung gibt (wenn es Freiwillige gibt, dann freiwillig, sonst von der Lehrperson bestimmt) – zum Einen, um den Stoff noch einmal zu wiederholen und zum Anderen, um einen Konsens über das Besprochene zu erlangen und um der Lehrperson die Möglichkeit zu geben, falls nötig korrigierend einzugreifen (um „stille Post - Effekte" zu minimieren und Verständnisprobleme aufzudecken).

Lehrerinput

Im Anschluss daran sollte die Lehrperson thematisieren, warum durch die eben behandelte Methode noch keine sichere Schlüsselübertragung möglich ist (Eve könnte das gesendete Photon abfangen, messen, kopieren und weiterschicken – s. quantumlab – homepage, von der auch die folgende Abb. stammt: URL:
http://www.didaktik.physik.uni-erlangen.de/quantumlab/index.html?/quantumlab/Kryptographie/index.html (28.4.2011))



Dieses Problem lässt sich jedoch lösen, indem man zwei Messbasen verwendet (h/v – horizontal/vertikal und +/- - um 45° zur h/v Basis gedreht) – wenn man weiß, dass folgende 3 Punkte gelten:

- Messungen an einem Qubit verändern den Zustand
- Es ist unmöglich einen unbekannten Quantenzustand durch eine einzige Messung vollständig zu bestimmen
- non – cloning – Theorem

(die ersten zwei Punkte sollten eigentlich schon bekannt sein, wurden am Anfang der Stunde noch einmal wiederholt, und werden jetzt noch einmal ins Gedächtnis gerufen)

Das non-cloning-Theorem wird ebenfalls in der Form eines Lehrerinputs thematisiert werden. Dass ein unbekannter Quantenzustand nicht durch eine einzige Messung vollständig bestimmt werden kann, könnte den S dabei quantitativ mit den Bildern von Polarisationsfiltern und Polarisationsrichtungen veranschaulicht werden (durchaus auch während der folgenden Powerpointpräsentation). Wenn Eve den Ausgangszustand nicht genau kennt, kann sie ihn auch nicht so einfach „kopieren“. Dass es auch keine Apparatur in der Art eines „Quantenkopierers“ gibt, in die man ein Photon in einem bestimmten Zustand reinschickt, und zwei Photonen identischen Zustands rauskriegt, würden wir einfach als Tatsache präsentieren.
Danach werden die möglichen Fälle für Eves' Lauschangriff besprochen.

Im Weiteren würden wir uns an die bereits sehr anschaulich gestaltete Powerpointpräsentation und Ausarbeitungen von Frau Heidemarie Knobloch halten, da wir diesen Vorschlag als sehr gut und anschaulich erachten, und im weiteren auch das Spiel „geheime Quanten“ von Frau Knobloch verwenden wollen, welches dem Design der folgenden Präsentation – die verspielt und optisch klar strukturiert dieses komplizierte Thema aufgreift - entspricht. Ihre Arbeit wie auch das Programm finden sich auf der Homepage
http://homepage.univie.ac.at/heidemarie.knobloch/wordpress/. (28.4.2011)
Den von uns verwendeten Teil, sowie die zugehörigen Overheadfolien, füge ich hier als komplettes Zitat (Mit freundlicher Genehmigung von Frau Knobloch) ein S33– 37, 43 - 44:

II
Umsetzung in der Schule

In diesem Kapitel geht es darum, wie man das Grundkonzept der Quantenkryptographie in der Schule verständlich machen kann. Im ersten Abschnitt »Einführung in die Quantenkryptographie« wird eine Möglichkeit vorgestellt, das Thema einzuführen und die wichtigsten Begriffe den SchülerInnen verständlich zu machen. Um das Gelernte zu vertiefen wird im Abschnitt »Ein Programm zur Demonstration der Quantenkryptographie« ein Lernspiel für den Computer präsentiert, in dem alle wichtigen Schritte der Quantenkryptographie simuliert werden. Im dritten Abschnitt »Diskussion« werden einige Punkte angeführt, über die man im Anschluss an das Lernprogramm mit den SchülerInnen zur Erhöhung des Verständnisses diskutieren sollte.

4 Einführung in die Quantenkryptographie

In diesem Kapitel werden Methoden vorgestellt, wie man den SchülerInnen die Grundlagen der Quantenkryptographie beibringen kann. Als Voraussetzung sollten sie schon über die Polarisation etwas Bescheid wissen. Auch die Kenntnis des Binärsystems wird vorausgesetzt. Natürlich können diese Punkte auch an den entsprechenden Stellen während des Kurses kurz eingeführt werden.

Die Methoden, die hier vorgeschlagen werden, können auch beliebig durch andere ersetzt werden. Sie sind eher als Vorschläge zu sehen. Da man mit dem Computer viel bessere Graphiken erstellen kann, eignet sich einiges gut für eine Präsentation. Falls kein Beamer vorhanden ist, wurden die Folien auch zum Kopieren auf Overheadfolie auf CD beigelegt (siehe Anhang B). Der Vortrag für den Computer findet sich als pdf auf der CD. Wenn Folien eingesetzt werden, werden diese in den jeweiligen Kapiteln genau erklärt.

4.1 Grundprinzipien

4.1.1 Erste Folie: Akteure

Die erste Folie (siehe Abb. 4.1, 4.2 und 4.3) dient als Einstieg und stellt die wichtigsten Komponenten dar. Zuerst haben wir die drei Personen Alice, Bob und Eve. Alice möchte Bob eine geheime Nachricht übermitteln. Eve – der Name kommt vom englischen Wort *eavesdropper* (= Lauscher) – möchte diese Nachricht abhören. Diese Namensgebung ist die in der Kryptographie übliche.

Während wir es in der klassischen Kryptographie mit Bits zu tun haben, treten in der Quantenkryptographie die Qubits (kurz für Quantenbits) auf. Meistens sind das polarisierte Photonen. Von den polarisierten Photonen gibt es vier wichtige, die immer wieder verwendet werden. Das sind die horizontal, vertikal, $+45°$ und $-45°$ polarisierten.

Um sie wieder als klassische Bits umzuinterpretieren, schreibt man dem horizontalen und dem $+45°$ Teilchen die 0 und dem vertikalen und dem $-45°$ Teilchen die 1 zu.

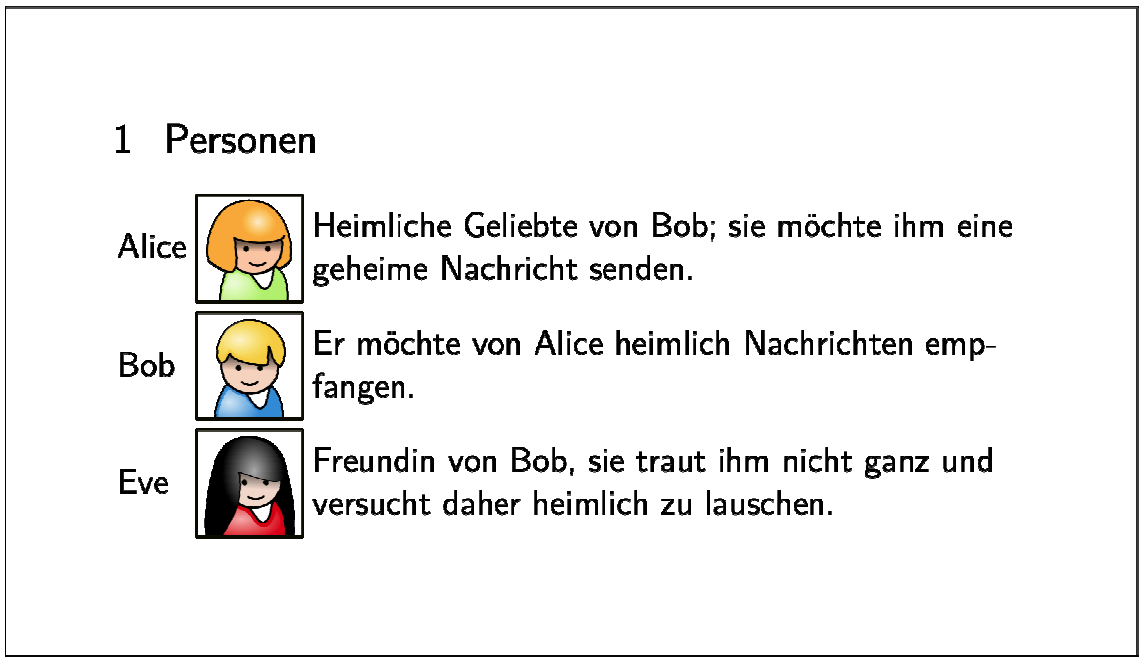


Abbildung 4.1 Ausschnitt aus der ersten Folie

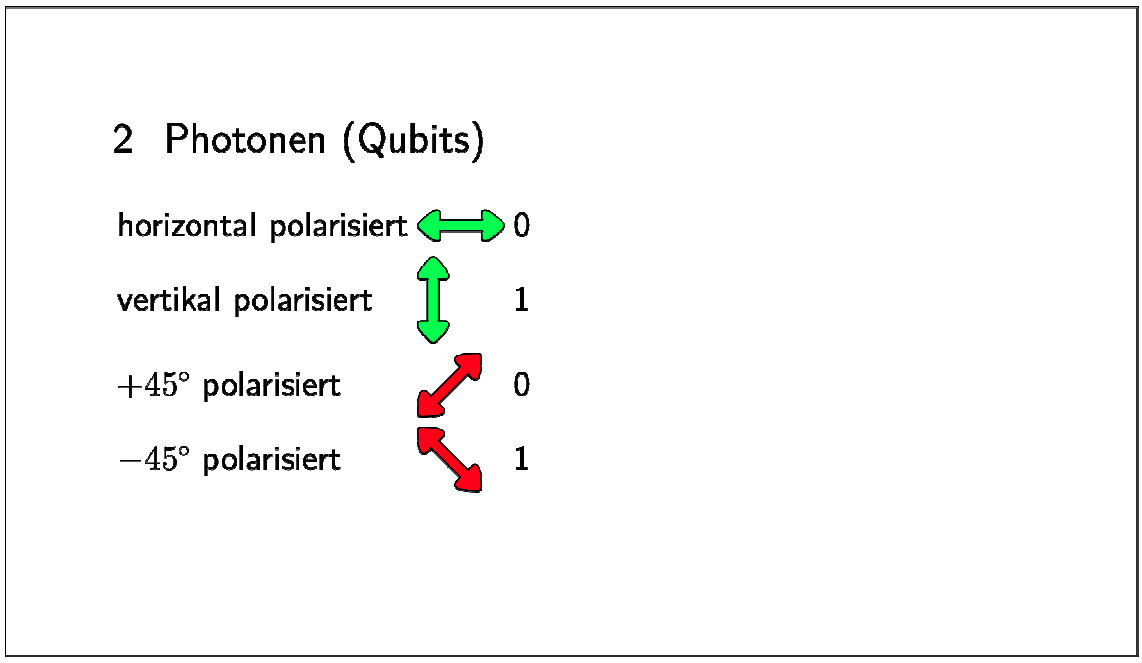


Abbildung 4.2 Ausschnitt aus der ersten Folie

Als drittes haben wir noch die Mess- und Präparationsapparate. Für uns reichen zwei verschiedene Basen. Die Basis h/v steht für die horizontal-vertikal Messung und die Basis $+/-$ für die Messung der Polarisation $+45°$ und $-45°$. Messen kann man das Teilchen mit einem Zweikanalanalysator. Dies ist ein doppelbrechender Kristall (z.B. Kalkspat), der die durchgehenden Teilchen entweder nach unten oder nach oben ablenkt, je nachdem wie sie zuvor

polarisiert waren (siehe Abb. 4.4). Im Folgenden verwenden wir  oder  als Symbol für so einen Messapparat.

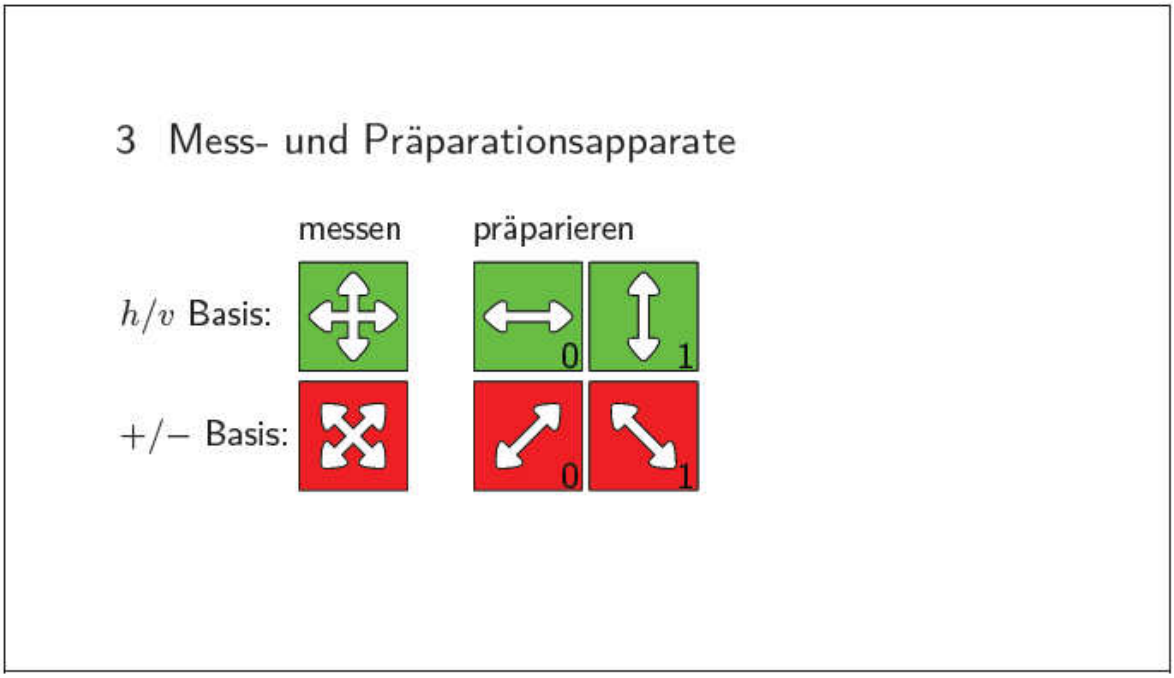


Abbildung 4.3 Ausschnitt aus der ersten Folie

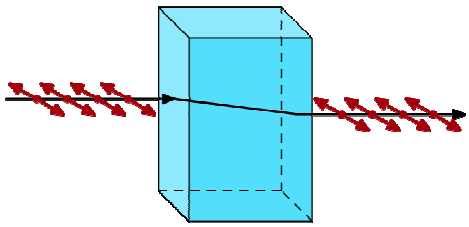
Für die Präparation von Zuständen kann man zum Beispiel Polarisationsfilter verwenden. Diese werden einfach in die gewünschte Richtung gedreht, sodass dann einer dieser vier Zustände herauskommt. Wir bezeichnen eine Präparation eines Photons in horizontaler bzw. vertikaler Richtung als in der Basis h/v präpariert und eine in $+45°$ bzw. $-45°$ in der Basis $+/-$ präpariert.

4.1.2 Zweite Folie: Messung

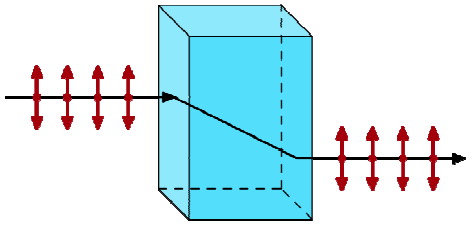
In dieser Folie (siehe Abb. 4.5 und 4.6) spielen die Komponenten nun zusammen. Ein Photon wird zuerst präpariert und anschließend gemessen. Dabei werden verschiedene Fälle untersucht.

In den ersten zwei Fällen werden Photonen in der Basis präpariert, in der sie anschließend auch gemessen werden. Als Ergebnis kommt klarerweise wieder der gleiche Zustand heraus.

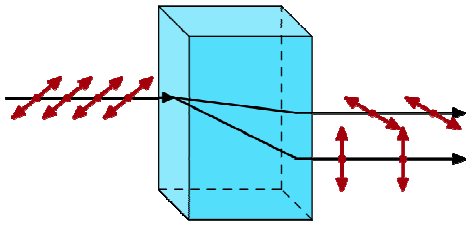
Wie sieht das aber aus, wenn ich ein Photon in einer anderen Basis messe, als ich es präpariert habe? Nehmen wir den Fall, in dem das Photon vertikal präpariert wird, aber in der Basis $+/-$ gemessen wird. Da das Teilchen nicht durch den Messapparat durchgehen kann, ohne verändert zu werden, geht es in einen der beiden Zustände $+$ oder $-$ über. Da die horizontale Polarisation genau zwischen der $+45°$ und $-45°$ Polarisation liegt, ist die Wahrscheinlichkeit für die beiden Richtungen je $\frac{1}{2}$. Analog funktionieren alle anderen Fälle, bei denen man in einer anderen Basis präpariert als man misst.



Horizontal polarisierte Photonen kommen im oberen Teil des Kristalles heraus.



Vertikal polariserte Photonen treten weiter unten aus.



Diagonal polarisierte Photonen können entweder oben oder unten aus dem Kristall herauskommen. Wo ein einzelnes Photon austritt hängt vom Zufall ab. Hier sind die Wahrscheinlichkeiten für beide Fälle je 50%

Abbildung 4.4
Zweikanalanalysator

Das Wesentliche daran ist der Zufall, der dabei auftritt. Dieser ist im Gegensatz zur klassischen Mechanik (wo der Zufall nur durch unsere Unkenntnis der einzelnen Parameter zustande kommt) wirklich zufällig, indem Sinn, dass es nur Wahrscheinlichkeitsaussagen für die Ausgänge der Messungen gibt. So ist die Wahrscheinlichkeit dafür, dass ein Photon im Zweikanalanalysator im oberen Bereich austritt $\cos^2 \alpha$ und im unteren Bereich $\sin^2 \alpha$, wobei α der Winkel zwischen dem Photon und dem Messapparat ist.

Betrachtet man nochmals Abbildung 4.4, so ist im ersten Fall der Winkel 0. Da $\cos^2 0 = 1$, kann das Photon nur im oberen Teil austreten. Im zweiten Fall ist der Winkel $\frac{\pi}{2}$ und das Photon tritt im unteren Bereich aus. Im dritten Bild sind die Teilchen im Winkel $\frac{\pi}{4}$ zum Messapparat verdreht. Daher erhält man folgende Wahrscheinlichkeiten für den Austritt:

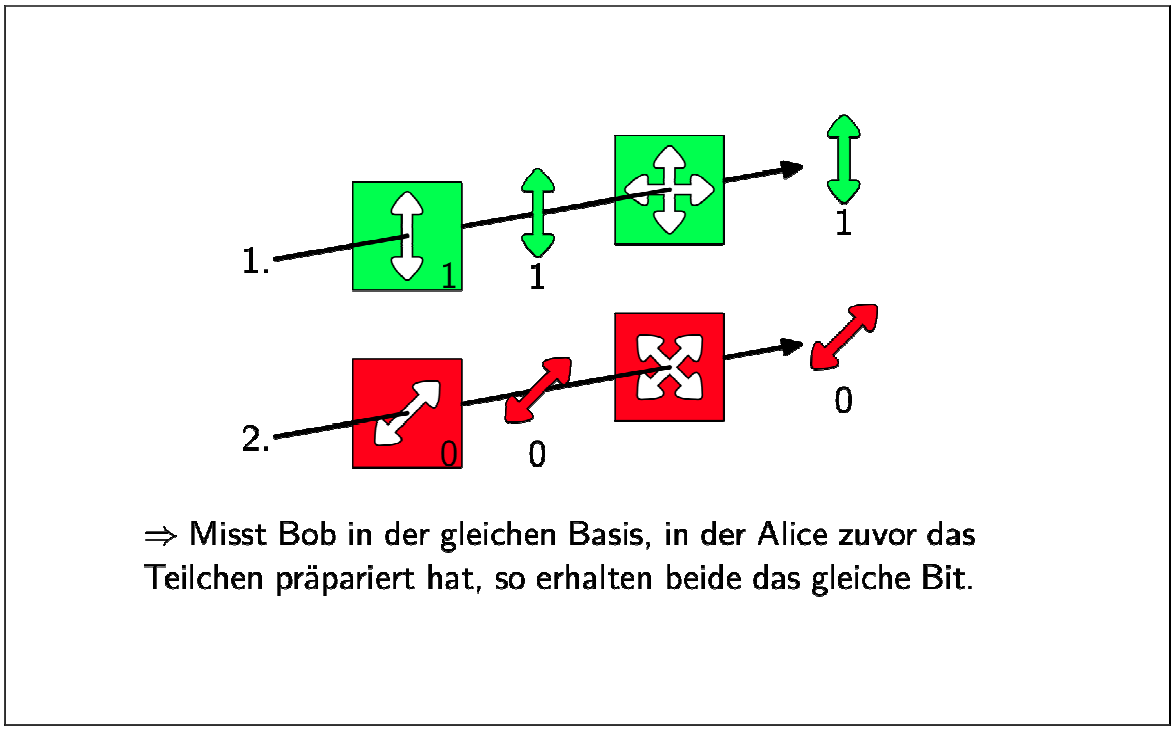


Abbildung 4.5 Ausschnitt aus der zweiten Folie

im oberen Bereich	$\cos^2(\frac{\pi}{4}) = \frac{1}{2}$
im unteren Bereich	$\sin^2(\frac{\pi}{4}) = \frac{1}{2}$

Auf diese Weise erhält man mathematisch das intuitive Ergebnis von oben.

4.3 Quantenkryptographie

Nun sollte man sich entscheiden, welches Quantenkryptographie-Protokoll im Unterricht besprochen werden soll: Das BB84-Protokoll oder das Verschränkung nutzende (vereinfachte) Ekert-Protokoll. Natürlich kann man auch beides machen. Dabei empfiehlt es sich zuerst das BB84-Protokoll durchzunehmen, dann die Verschränkung einzuführen und anschließend das Ekert-Protokoll zu erklären. Beim Simulationsprogramm sollte man allerdings nur eines herzeigen, da sich die Programme ziemlich ähnlich sind.

4.3.1 Dritte Folie: Quantenkryptographie-Einstieg

Die Quantenkryptographie baut direkt auf den Vernam-Code auf. Dieser ist zwar sicher, allerdings ist das Problem der Schlüsselaustausch, da es ja sehr kompliziert sein würde, wenn sich ein Bankangestellter mit seinem Kunden immer auf einer einsamen Insel treffen müsste, um einen Code für die nächsten Geschäfte auszumachen. Dieses Problem des Schlüsselaustausches lösen die Quantenkryptographieprotokolle (siehe Folie 4.12).

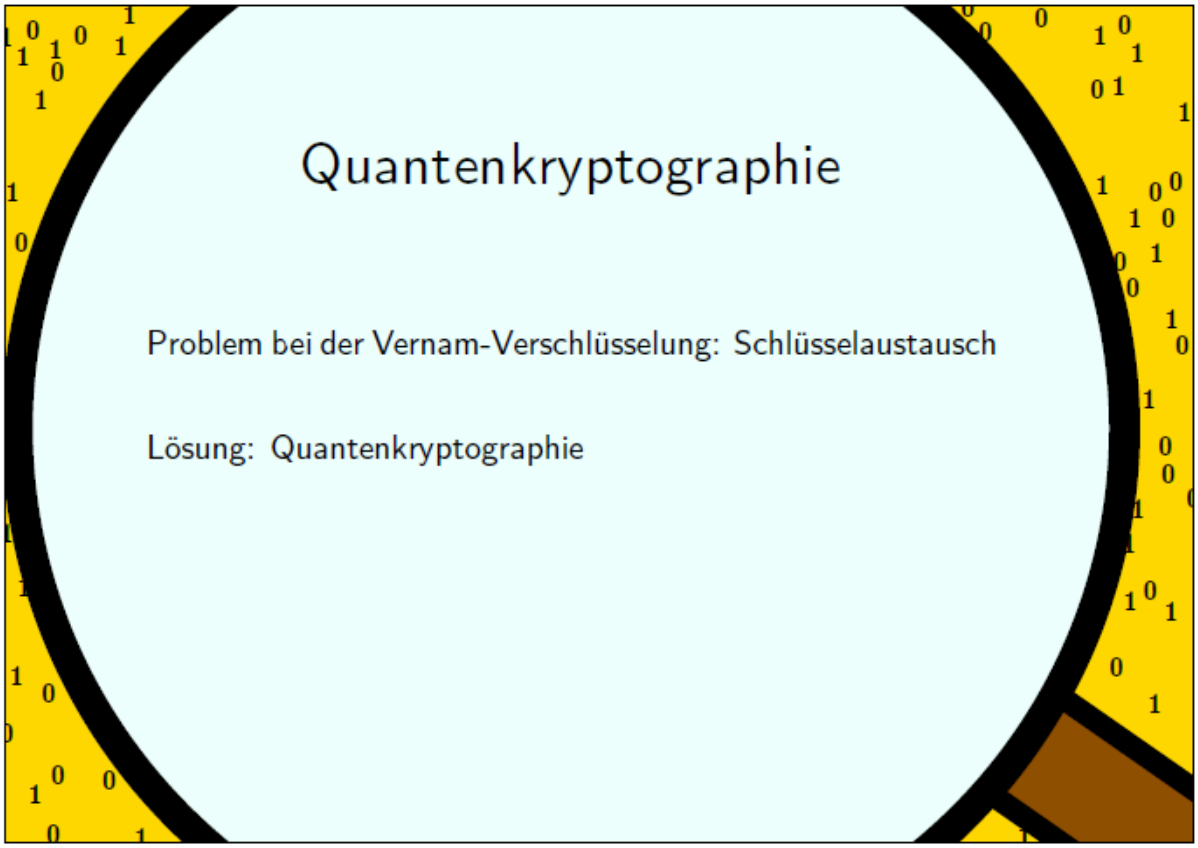


Abbildung 4.12 Dritte Folie

4.3.2 Vierte Folie: BB84-Protokoll

Auf der Folie (siehe Abb. 4.13) befinden sich auf der rechten Seite die Präparationsapparate von Alice. Aus diesen wählt sie *zufällig* aus und schickt die erhaltenen polarisierten Photonen an Bob, der sie mit seinen beiden Messapparaten, die auch er *zufällig* auswählt, messen kann.

In der Tabelle darunter sind nochmals die Bits, die Alice gesendet hat, sowie ihre Präparationsbasis eingetragen und zwar zur besseren Übersicht genau unter den jeweiligen versendeten Teilchen. Die h/v Basis wurde als grüner Punkt und die $+/-$ Basis als roter Punkt symbolisiert. Bobs zufällige Wahl seiner Basen und die dazugehörigen Bits wurden darunter eingetragen (in der Graphik oben allerdings nicht dargestellt).

Nun müssen Alice und Bob ihre Präparations- bzw. Messbasen vergleichen. Dies kann durchaus auch über einen öffentlichen Kanal (z.B.: Telefon, etc.) geschehen. Wird ein Teilchen zufällig in der gleichen Basis gemessen, in der es zuvor präpariert wurde, so wird, wie wir vorher schon gesehen haben, der Zustand des Teilchens nicht verändert. Das heißt, dass Alice und Bob dann das gleiche Bit haben. Sind die Basen allerdings unterschiedlich, so stimmen die Ergebnisse nur zu 50% überein. Durch den Basisvergleich können Alice und Bob diese Fälle streichen und können nun sichergehen, dass sie die gleichen Schlüsselbits haben ohne die Bits selbst ausgetauscht zu haben.

Um aber noch herauszufinden, ob jemand gelauscht hat, müssen die beiden eine gewisse Anzahl der Bits, die sie nachher aber klarerweise nicht mehr für den Schlüssel verwenden dürfen, vergleichen. Stimmen zu viele Bits nicht überein, so wurde höchstwahrscheinlich gelauscht und sie müssen von vorne anfangen, da jeder Lauschversuch eine gewisse Anzahl der Bits verändert (näheres zum Lauschen findet sich im Kapitel 6.2). Stimmen die ausgetauschten Bits überein, so haben sie erfolgreich einen gemeinsamen Schlüssel erzeugt und können nun eine Nachricht geheim übermitteln.

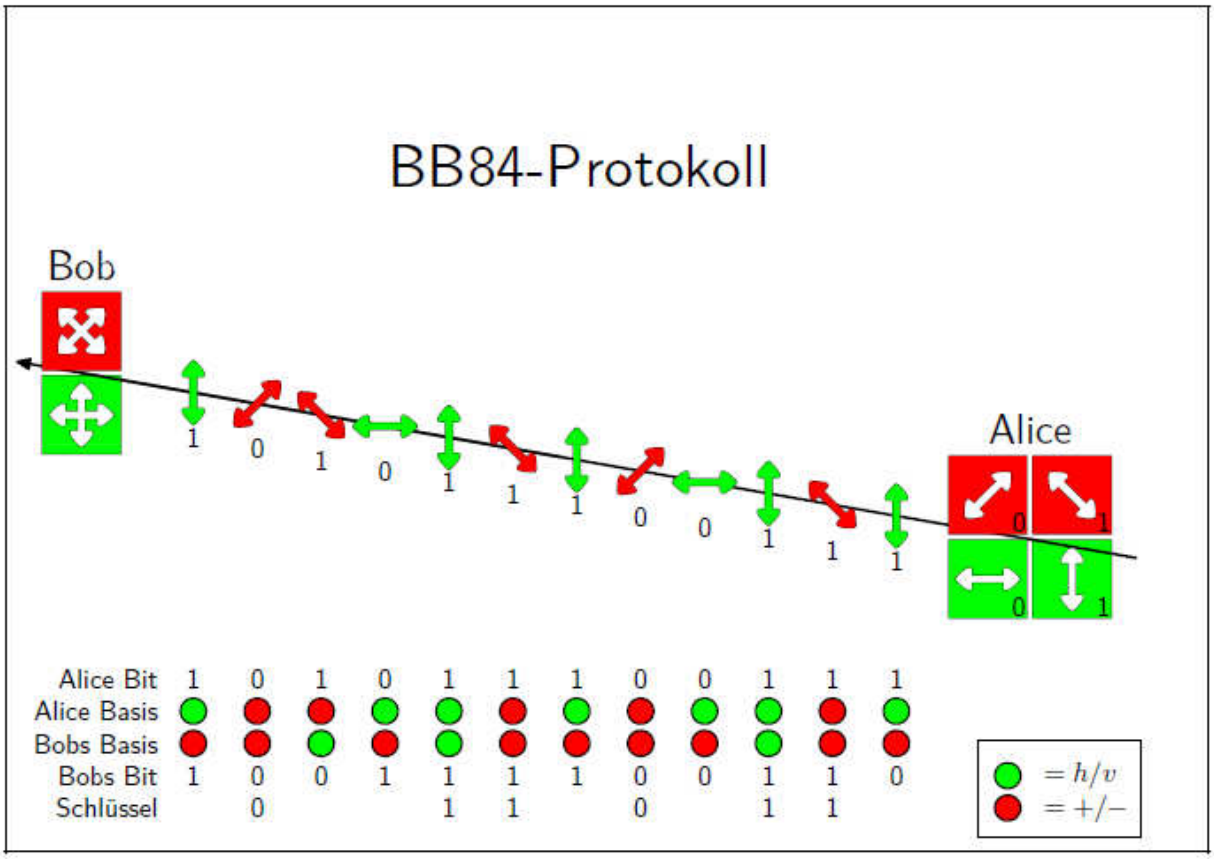


Abbildung 4.13 Vierte Folie

Im Anschluss an die Powerpointunterstützte (geht alternativ auch mit Overheadprojektor) Präsentation sollen mit den Schülern noch einmal die einzelnen Schritte der Schlüsselerzeugung des BB84 Protokolls zusammengefasst, und Lerntagebuchtauglich aufbereitet werden: siehe Unterpunkt 2.3: Schritte beim *BB84* – Protokoll bzw. Arbeitsblatt im Anhang.

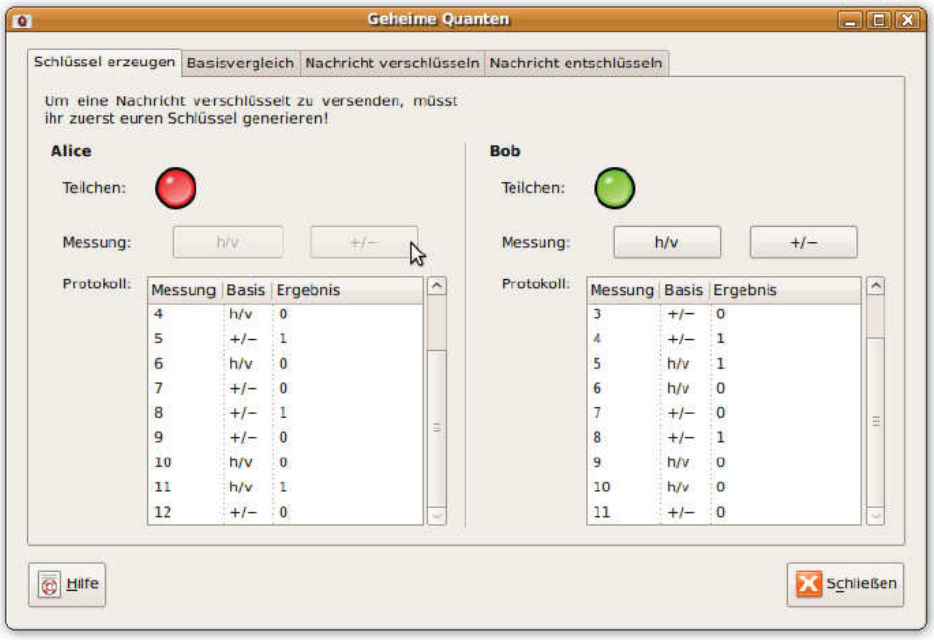
3.3 3. Unterrichtseinheit

Zeiteinteilung: (Doppelstunde – 100min)
10min: Wiederholung und Erklärung „Geheime Quanten“
40 min: Spiel
50 min: Lauschmöglichkeiten, Rekorde, aktuelle Forschungsergebnisse, Abschluss

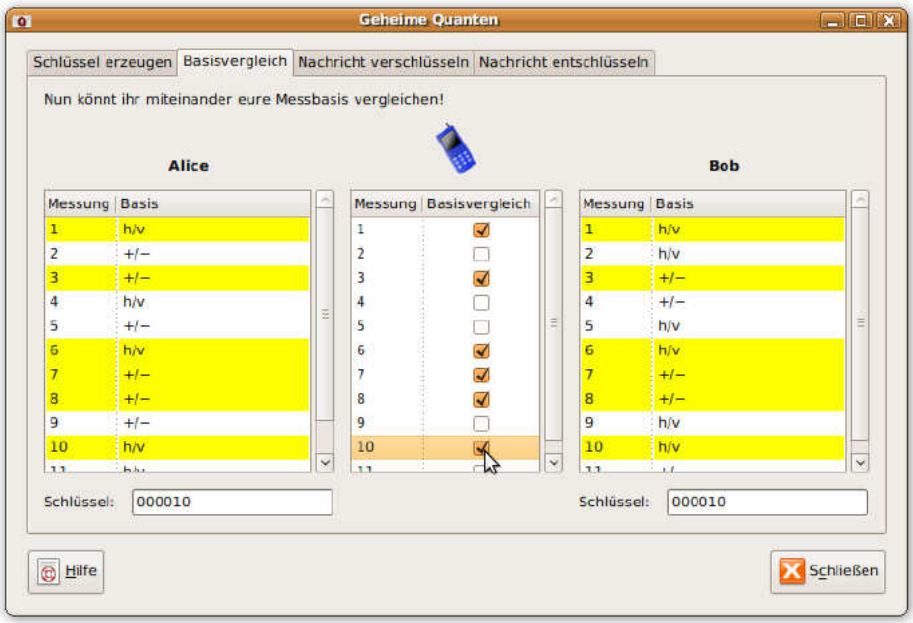
Wiederholung und Erklärung „Geheime Quanten“
Für diese Unterrichtseinheit benötigen je zwei S einen Computer.
Als Einstieg soll gemeinsam mit den S noch einmal der Ablauf des BB84 Protokolls besprochen werden – parallel dazu kann den S exemplarisch das Programm „geheime Quanten“ erläutert und vorgestellt werden.

Spiel
Anschließend sollen sich die S in 2er Gruppen organisieren (wiederum eigenständig, oder durch die Lehrperson festgelegt) – einer übernimmt den Part von Alice, der andere den Part von Bob. Dann sollen die S einander mit dem Programm Nachrichten übermitteln, und alles in ihrem Lerntagebuch dokumentieren. (Als Vorlage haben wir uns hier wieder an die Vorlage von Frau Knobloch gehalten)
Dadurch erhoffen wir uns besonders für die haptischen Lerntypen einen großen Lernfortschritt, denn die Schüler können hier „selbst“ und Schritt für Schritt das gesamte Prozedere der Übermittlung Verschlüsselter Botschaften nachvollziehen.
Allerdings muss die Lehrperson hier ausdrücklich darauf hinweisen, dass es sich bei dem Spiel um eine reine Simulation handelt, da sonst bei den S leicht der Eindruck entstehen könnte, auf jedem „normalen Computer“ sei Quantenkryptographie realisierbar.

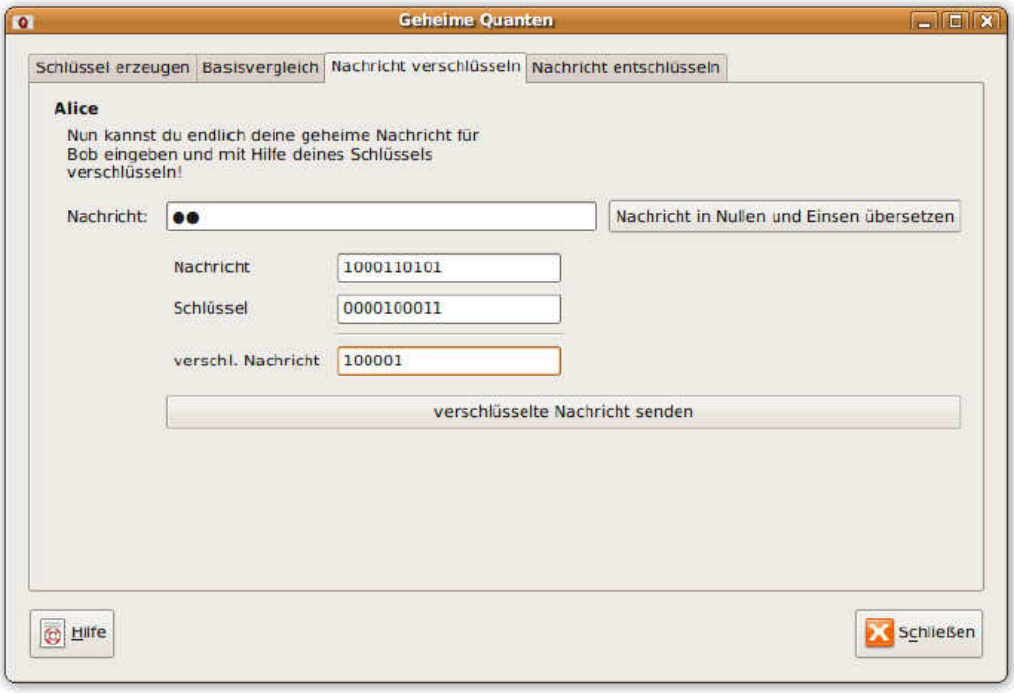
1. Schritt: Schlüssel erzeugen. Hier wählen die beiden Schüler, hier Alice und Bob, jeweils intuitiv ihre Basen um einen Schlüssel zu erzeugen. Dieser Part ist natürlich nur spannend, wenn in dieser Version des Spiels, die Schüler nicht schwindeln und immer die gleichen Basen verwenden um schneller einen Schlüssel zu erhalten.



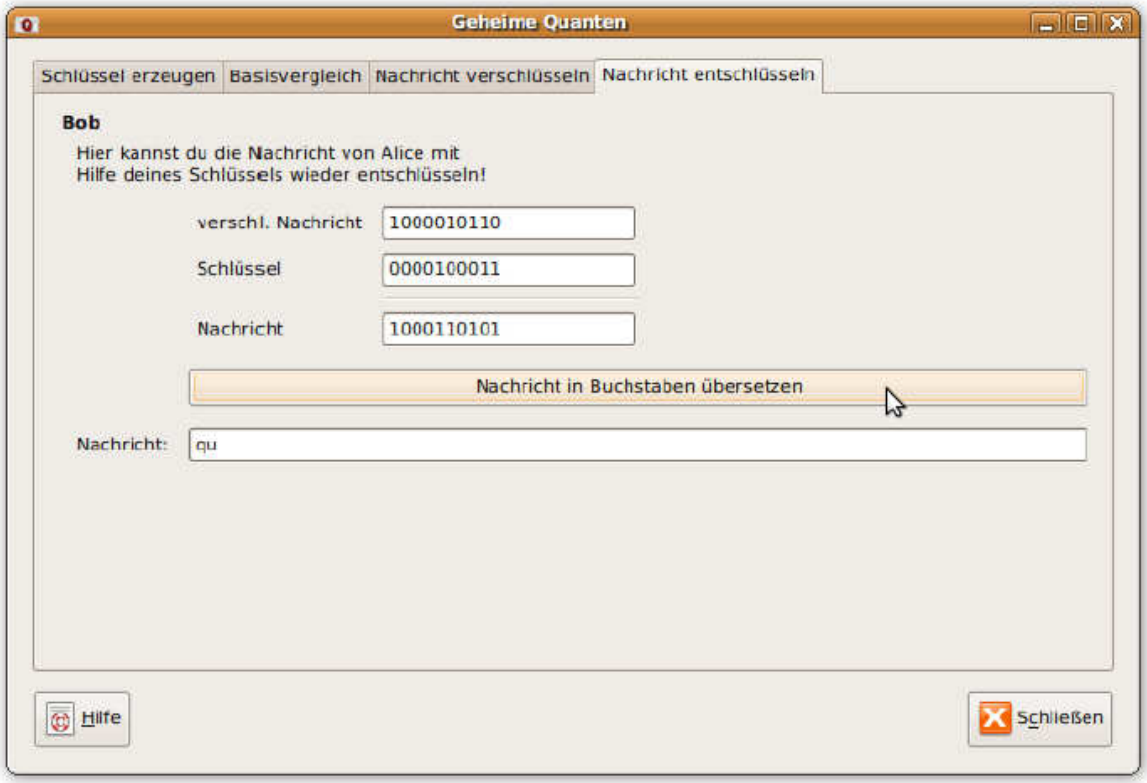
Im **zweiten Schritt**, dem Basisvergleich, sollen Alice und Bob schauen, bei welcher Messung sie die gleiche Basis verwendet haben. Diese Messung wird mit einem Häkchen gekennzeichnet und zur Schlüsselerzeugung verwendet. Dieser Basisvergleich erfolgt, wie bereits auf den Folien von Heidemarie Knobloch zum BB84 Protokoll erwähnt, über einen öffentlichen Kanal (Handy). An dieser Stelle sollen die Schüler begreifen, dass es einen Schlüssel von einer Länge von mindestens 5 Bits benötigt, damit zumindest ein Buchstabe übermittelt werden kann. Somit kann abermals eine Verknüpfung zur ersten Einheit gefunden werden, da auf dem Arbeitsblatt Vernam Code bereits die jeweiligen Buchstaben- Bit Kombinationen angeführt wurden.



Im **dritten Schritt** erfolgt nun das eigentlich „geheime“. Je nach Länge ihres konstruierten Schlüssels können sich die Schüler nun eine kodierte Nachricht übermitteln.
Gerade Punkt 3, welcher in der folgenden Abbildung zu sehen ist, eignet sich abermals zur Überprüfung des bereits gelernten Wissens der Schüler. Hier sollen sie, um ihre Nachricht zu verschlüsseln die Addition von Binärzahlen anwenden, welche in der ersten Unterrichtseinheit beim Arbeitsblatt Vernam Code gelernt wurde.



Der **vierte und letzte Schritt**: Nachricht entschlüsseln funktioniert ähnlich wie der vorangehende. Abermals muss der Schlüssel zu der verschlüsselten Nachricht addiert werden um die entschlüsselte Nachricht zu erhalten, welche dann wieder mittels des Ascii Code in Buchstaben umgewandelt werden muss.



An das Spiel anschließend, möchten wir mit den Schülern gemeinsam diskutieren, wie denn Eve doch noch Möglichkeiten für einen Lauschangriff finden könnte. Falls das Quantenspiel selbst noch nicht Anregung genug für diese Diskussion bieten sollte, so kann die Lehrperson auf die Gefahr des Abhörens hinweisen, und die Schüler beispielsweise in 5er Gruppen Ideen sammeln lassen. Diese werden nach einer 20minütigen Überlegungsphase gemeinsam in der Klasse diskutiert und gegebenenfalls aufgeklärt und falsifiziert (20min).

Aus der Arbeit von Heidermarie Knobloch möchten wir nur einige zu diskutierende Möglichkeiten kurz anführen:

Idee: „Eve könnte das Teilchen abfangen, kopieren und das Original an Bob weiterschicken. Nun hätte Eve ihr eigenes Teilchen an dem sie messen kann, ohne den Zustand von Bobs Photon zu verändern."
Diese Idee wurde bereits in der 2. Unterrichtseinheit unter der Thematik „no cloning theorem" behandelt. Unserer Meinung nach ist es allerdings kein Schaden, wenn eine kurze Wiederholung stattfindet. Deshalb könnte diese Idee beispielsweise von der Lehrperson vorgebracht werden um zu testen, wie viele Schüler die Verbindung an die vorhergehende Einheit anknüpfen können.

Einige weitere Ideen:
Idee: „Eve könnte doch einfach das Teilchen abfangen, messen und an Bob weiter schicken."
Idee: „Eve könnte sich bei Alice als Bob ausgeben und bei Bob als Alice (sogenannte „Man in the mittle attack")".

Damit die letzte Diskussionsrunde auch einen arbeitsmotivierenden Aspekt hat, haben wir dafür ein Arbeitsblatt konzipiert, indem ein Zeitungsartikel über die einzelnen Möglichkeiten von Eve geschrieben werden soll.

In den letzten 10 Minuten möchten wir einen weiteren Aspekt der Quantenkryptographie ansprechen, der unserer Meinung nach nicht ungesagt bleiben sollte. Den Schülern soll die Tatsache näher gebracht werden, dass Verschlüsselungsverfahren keine reine Spielerei sind, so wie wir es in der 3. Unterrichtseinheit ausgeführt haben, sondern sich in der Realität bereits Anwendungen finden lassen. An dieser Stelle möchten wir großes Augenmerk darauf legen, dass die Lehrperson die jeweils aktuellsten Forschungsergebnisse kennen sollte, um auch eine entsprechend kompetente Diskussion leiten zu können. Ist dies nicht der Fall, geht unserer Meinung nach der wichtigste Aspekt verloren: die aufgebaute Begeisterung wird durch das Nichtwissen der Lehrperson wieder genommen.

Einige faszinierende Rekorde seien als Motivation zum selber Weiterforschen angeführt:
2004: Banküberweisung über eine Distanz von 650m von der Bank- Austria Kreditanstalt in die Stadthalle in Wien
2007: Distanz von 144km wurde mittels Glasfaserkabel überwunden La Palma- Teneriffa (diese Distanz ist vergleichbar mit erdnahen Satelliten)
2008: Wahlresultate wurden mittels Quantenkryptographie in die Zentrale geleitet
2009: auf über 250km wurden Quanteninformationen übertragen

4 Abschließende Bemerkungen

Warum ziehen wir ein Lernjournal für die Benotung heran? Welche Erwartungen bestehen an den „Lernertrag“?

Die Schüler können sich mit dem möglicherweise rein theoretischen Wissen in einer kreativen Weise auseinandersetzten und das Gelernte persönlich reflektieren.

Durch die Methode des Lerntagebuchs werden unterschiedliche Lerntypen besonders gut miteinbezogen. Der haptische Typ z.B. kann etwas Basteln oder eigene (Bildschirm-) Experimente ausführen und diese im Lernjournal dokumentieren. Für den visuellen Lerntyp kann es von Vorteil sein, Lerneindrücke noch einmal niederzuschreiben (um diese beim Lernen vor sich zu sehen) und dabei Mindmaps oder Diagramme anzufertigen. Dem auditiven Typ kann es möglicherweise eine Hilfestellung sein, wenn man ihm vorschlägt, das Gelernte in eine Geschichte zu packen oder als Dialog auszuformulieren.

Durch gezielte Fragestellungen, welche im Lernjournal ausgeführt werden sollen, kann die Lehrperson den Rahmen der Arbeit festlegen und den Schülern einen Anhaltspunkt bieten. (Was hat mir besonders gut gefallen, mich am meisten interessiert? Was habe ich noch nicht so ganz verstanden?

Die Lehrperson bekommt somit von jedem Schüler ein persönliches Feedback, über sowohl über die eigenen, als auch die Schwächen und Stärken der Schüler. Die Benotung erscheint uns dadurch recht vereinfacht und gerecht zu sein, da für die Lehrperson 1. ein Vergleich zur jeweiligen Zielsetzung gegeben ist und 2. durch die unterschiedliche Ausführung der jeweiligen Anforderungskriterien jeder Schüler eine individuelle Punktezahl erreichen kann und so eigenständiges Lernen gefördert wird.

Zudem muss in jedem Fall in irgendeiner Form eine schriftliche Dokumentation des Lernstoffes erfolgen (klassischerweise geschieht dies in einem „Physik-Heft“ indem die Lehrperson die entsprechenden Inhalte ausformuliert zur Verfügung stellt). Im Gegensatz dazu bietet das Lerntagebuch die Möglichkeit eigene, physikalisch richtige Formulierungen zu finden. Das stellt für die S natürlich eine Herausforderung dar, der S einer Maturaklasse aber gewachsen sein

sollten. Die Ausarbeitungen werden sich, je nachdem welcher Lerntyp der jeweilige S ist, individuell sehr stark unterscheiden.
So erwarten wir z.B.: von S des eher akustischen Lerntyps Formulierungen wie „ich habe gehört", „wir haben gesagt..."
Von S des eher optischen Lerntyps könnten Formulierungen der Art „wie man sieht...", „es ist einsichtig dass...", sowie bunte und optisch ansprechend gestaltete Lernjournale abgegeben werden.
Von Schülern des haptischen Lerntyps könnten hingegen Formulierungen der Form „wir versuchen zu begreifen...", „wir haben gemacht..." verwendet werden, usw.
Wir glauben, dass die S intuitiv jene Formulierungen und Form der Ausarbeitung wählen, die ihrem individuellen Lerntyp am besten entspricht, wodurch das Gelernte noch zusätzlich zu den selbständig gefundenen eigenen Formulierungen gefestigt wird.
In den eigenständigen Formulierungen der S liegt zusätzlich die Chance, falsche Schülervorstellungen zu entdecken, die verborgen blieben, wenn alle Formulierungen von der Lehrperson vorgegeben würden.

Wie schaut die Benotung im Detail aus?
Für alle 3 Arbeitsblätter gibt es im Gesamten 38 Punkte. Wir haben uns einen möglichst schülerfreundlichen Notenschlüssel ausgedacht, sodass diese selbst entscheiden können, welche und wie viele Arbeitsschritte sie machen wollen und nicht Gefahr laufen gleich eine schlechte Note zu erhalten, wenn sie einen Schritt auslassen. Die Begründung dafür ist, dass wir bei diesem Unterrichtsprojekt nicht den Leistungsdruck in den Vordergrund stellen möchten, sondern die Schüler dazu motivieren wollen, Physik einmal anders zu erlernen – mit eigener Mitgestaltung. Zudem versuchen wir mit dem „speziellen" Benotungsschema den Schülern die Möglichkeit zu lassen, ihren Interessen entsprechend zu arbeiten. Aus diesem Grund ist für die Note sehr gut ein verhältnismäßig großer Schwankungsbereich von 8 Punkten ausgelegt.

Punkteschlüssel:
45 Pkt. – 38 Pkt.: Sehr Gut
37 Pkt. – 32 Pkt.: Gut
31 Pkt. – 26 Pkt.: Befriedigend
25 Pkt. – 20 Pkt.: Genügend
19 Pkt. oder weniger: Nicht Genügend

Was erwarten wir uns?
Quantenkryptographie ist ein aktuelleres Thema denn je. Dadurch erwarten wir uns von den Schülern eine gewisse Grundmotivation und Begeisterung. Durch die abwechslungsreiche Aufarbeitung sollen die Schüler nicht das Lernen im Vordergrund sehen, sondern Spaß am spielerischen Entdecken von neuem Wissen haben. Die entsprechenden Lernfortschritte werden im Lernjournal dokumentiert, sodass eine Benotung erfolgen kann. Nach dieser Unterrichtseinheit sollen die Schüler verstehen, warum die historischen Kryptographieverfahren heute nicht mehr sicher sind, sowie ein Verständnis dafür entwickeln, wie heute Geheimbotschaften verschlüsselt und versendet werden. Auch die grundlegenden Vorteile des verwendeten BB84 Protokolls gegenüber rein klassischen Kryptographieverfahren sollten prinzipiell verstanden worden sein, sowie die Grundgedanken, die diese Vorteile begründen.
Wir sind uns bewusst, dass möglicherweise nicht alle S mit Begeisterung an dieses Thema herangehen werden – aber wir hoffen dass auch weniger motivierte S die Chance des Lernjournals nutzen, ihre Note selbst mitzubestimmen, und vielleicht über die Arbeit am Lernjournal doch noch Interesse an diesem Thema gewinnen können. In jedem Fall setzt unser Unterrichtsszenario ein hohes Maß an Eigenverantwortung und Kooperation der S voraus, was wir uns in dieser Jahrgangsstufe aber erwarten.

Wie berücksichtigen wir die einzelnen Sozialformen?

Hierbei werden folgende 4 Grundtypen unterschieden:
Klassenarbeit, Gruppenarbeit, Partnerarbeit, Einzelarbeit

In unserer Unterrichtseinheit über Quantenkryptographie haben wir versucht alle 4 Typen möglichst ausgeglichen zu berücksichtigen.

1. Doppelstunde:
Der Unterrichtseinstieg mit dem gemeinsamen Brainstorming über Kryptographie früher und heute bezieht die ganze Klasse mit ein. Im nächsten Unterrichtsteil sind alle gefordert, sich in einer Gruppe zu organisieren um ihr jeweiliges Thema zu erarbeiten. Dabei ist eine konstruktive Argumentation untereinander notwendig, damit während dem vorgegebenen Zeitrahmen der Arbeitsauftrag erledigt werden kann. Im anschließenden Stationenbetrieb können die Schüler in Gruppen- oder Einzelarbeit die weiteren Themengebiete selbst entdecken und erforschen. Zuhause soll dann in Einzelarbeit die Ausarbeitung mit dem neu Gelernten geschehen.

2. Doppelstunde:
Zu Beginn der zweiten Einheit (abermals einer Doppelstunde) erfolgt ein LehrerInnen – Input, welches eine kurze Wiederholung entscheidender Elemente beinhaltet (Superposition, Polarisation, Messung). Der Frontalunterricht als Einstieg geht dann im nächsten Abschnitt in die Gruppenarbeit der Expertenrunde über. Hier haben die Schüler wieder die Möglichkeit in gemeinsamer Arbeit ein eher komplexes Thema zu erarbeiten und sich so gegenseitig zu unterstützen. Gerade für den visuellen und den haptischen Lerntyp wird das Arbeiten am Computer und insbesondere die Bildschirmexperimente den Lernerfolg unterstützen. Damit auch der auditive Typ nach der 40 minütigen Arbeitsphase wieder auf seine Kosten kommt, und vor Allem als Überprüfung des Lernerfolgs für die Lehrperson, haben wir eine abschließende Zusammenfassungsphase sowie eine Diskussion eingeplant. Damit auch der auditive Typ genug gefordert ist, wird an dieser Stelle ein LehrerInnen Input erfolgen, welcher die Sicherheit beim Übertragen von Nachrichten thematisiert.

3. Doppelstunde
Um einen runden Abschluss zu erhalten, wird zum Abschluss der Unterrichtssequenz der Unterrichtseinheit das gelernte Wissen in der Form eines Simulationsprogramms von Heidemarie Knobloch umgesetzt. Dabei wird dann wohl auch der haptische Lerntyp seine Fähigkeiten ausspielen können und somit einen optimalen Lernerfolg mitnehmen können. Insgesamt erwarten wir uns aber für alle Schüler eine Festigung des zuvor erarbeiteten Wissens, da das Programm den Schülern ermöglicht, die einzelnen Punkte des BB84 Protokolls eigenständig nachzuvollziehen, und Schritt für Schritt anzuwenden.
Im Anschluss daran ist dann wieder die Kreativität der Schüler gefordert, wenn es um die Frage geht, wie Eve doch noch lauschen könnte, und bei der Argumentation, warum außer dem klassischen „über die Schulter schauen“ nichts bleibt, kann dann noch einmal das eigene Verständnis auf Konsistenz geprüft werden.

Wie werden unterschiedliche Kompetenzen und Interessen von SchülerInnen berücksichtigt?
Wir haben versucht, eine möglichst abwechslungsreiche Unterrichtseinheit zu dem Thema Quantenkryptographie zu entwickeln, damit möglichst viele Schülerinteressen berücksichtigt werden. Vom gemeinsamen Diskutieren, über eigenes forschendes Lernen, hin zu Arbeiten, bzw. „Spielen“ am Computer ist ein kunterbuntes Lernen möglich.
Insbesondere das Lernjournal soll den S Raum geben, ihren individuellen Interessen und Kompetenzen entsprechend zu arbeiten.
Auch zu diesem Aspekt beziehen wir bei den jeweiligen Punkten ausführlich Stellung.

Welche SchülerInnen – Vorstellungen und besondere Probleme erwarten Sie?
Da das Thema Quantenkryptographie sehr aktuell ist, dürften die jeweiligen Vorstellungen kaum vorhanden sein, bzw. werden im Unterrichtseinstieg entdeckt. Die Arbeitsaufträge lassen keinen großen Spielraum offen, sodass entsprechende Vorstellungen kein Problem in der Ausarbeitung darstellen sollten. Die größte Problematik wird im allgemeinen Verständnis der Quantenwelt zu finden sein, welche wir hoffen in den entsprechenden (vorangegangenen) Unterrichtsstunden bereits berücksichtigt zu haben.
Die Homepage der Uni Erlangen (http://www.didaktik.physik.uni-erlangen.de/quantumlab/index.html?/quantumlab/Kryptographie/index.html) ist zudem nicht unbedingt auf den ersten Blick selbsterklärend, sodass hier wohl einerseits eine Einführung von Seiten der Lehrperson nötig ist, andererseits bietet die Seite besonders motivierten und interessierten Schülern ein breites „Forschungsfeld" – weswegen wir sie auch in die Unterrichtsplanung eingebaut haben.
Mit Technikausfällen etc. muss immer gerechnet werden, der Plan B besteht hier darin, möglichst viele Materialien in gedruckter Form (bzw. die Powerpointpräsentation auch als Overheadfolie) bereitzuhalten, wobei aber besonders bei den Bildschirmexperimenten schon mit Qualitätsverlusten zu rechnen ist.

Im Detail äußern wir uns zu den jeweils erwarteten Vorstellungen und Problemen bei den einzelnen Punkten weiter oben in der Ausarbeitung.

Als letzte abschließende Bemerkung möchten wir noch einige Vorschläge andeuten, wie Quantenkryptographie fächerübergreifend unterrichtet werden könnte.

Kombination mit Deutsch, Englisch:
Passt es gerade zum behandelnden Inhalt, könnten folgende Filme eine Verbindung zu unserem Thema schaffen:

- "A beautiful Mind": John Nash entschlüsselt für die US-Regierung Geheimbotschaften
- "The Mercury Puzzle": Der 9-jährige Simon knackt per Zufall den militärischen Geheimcode „Mercury" der Vereinigten Staaten beim Kreuzworträtseln in einem Magazin".
- "The Da Vinci Code": Der Symbolforscher Robert und Sophia, eine Kryptologin der Dechiffrierabteilung der Pariser Polizei versuchen immer wieder verborgene Zeichen und Symbole in den Werken Leonardo da Vincis zu lösen.

Eine weitere Möglichkeit wäre die Auseinandersetzung mit dem amerikanischen Schriftsteller Edgar Allan Poe (*1809 †1849). Er prägte entscheidend die Genres der Kriminalliteratur, der Science Fiktion und der Horrorgeschichte. In seinem Werk „Der Goldkäfer", Originaltitel The Gold-Bug, wird im Rahmen einer Schatzsuche ausführlich die Dechiffrierung einer Geheimschrift anhand von Häufigkeitszahlen der einzelnen Buchstaben in englischen Texten erläutert. Poe hat zudem einmal die Leser einer Zeitung herausgefordert, ihm chiffrierte Nachrichten zuzusenden, die er dann knacken würde. Nach eigenen Angaben (in dem Aufsatz "Geheimschreibekunst") hat er dabei alle rund 100 Einsendungen geknackt.

Ein Zitat (aus "Geheimschreibekunst") von Poe: „Es wäre deshalb gar nicht so unangebracht, die Lösung von Geheimschriften in den Lehrplan unserer Hochschulen aufzunehmen, um der wichtigsten aller Geisteskräfte Spielraum zur Entfaltung zu geben."

Kombination mit Geschichte:
Neben den historischen Verschlüsselungsverfahren, welche ja auch in dieser Arbeit behandelt wurden, wäre ein weiterer interessanter Aspekt speziell die verwendeten Verfahren in der Kriegsführung zu betrachten, hierbei sei speziell die Verschlüsselungsmaschine ENIGMA des deutschen Militärs im zweiten Weltkrieg zu erwähnen.

5 Resümee

Mit diesem Unterrichtskonzept hoffen wir für die Schüler spannende Einheiten gestaltet zu haben. Für uns stand im Vordergrund, dass die Schüler dabei spielerisch in Eigenarbeit lernen können, weshalb wir weitgehend auf Frontalunterricht verzichtet haben um ein möglichst abwechslungsreiches Programm bieten zu können – speziell im Vergleich zu dem sonst so trockenen Tafelunterricht im Fach Physik.

Die Arbeit selbst hat uns gezeigt, wie während eines Randthemas doch viele entscheidende Pflichtthematiken eingebaut und so im Wahlpflichtfach oder einer Form Projektunterricht spannend wiederholt und gefestigt werden können.

Leider konnten wir die von uns gestalteten Einheiten bisher noch nicht selbst erproben, aber wir sind gespannt auf das Ergebnis, wenn es dann einmal so weit sein wird.

6 Quellverzeichnis

6.1 Bildquellen

Deckblatt:
URL: http://www.aprillwitz.de/lib/exe/detail.php/images:kommunikation.gif?id=kommunikation (28.4.2011)

S. 8,9
URL: http://www.didaktik.physik.uni-erlangen.de/quantumlab/index.html?/quantumlab/Kryptographie/index.html (28.4.2011))

S.5, 11 - 19
http://homepage.univie.ac.at/heidemarie.knobloch/wordpress/. (28.4.2011)

Arbeitsblatt Internetrecherche:
URL: www.microsoft.com (21.4.2011)

6.2 Verwendete Literatur

URLs:

http://homepage.univie.ac.at/heidemarie.knobloch/wordpress/. (28.4.2011)
http://www.didaktik.physik.uni-erlangen.de/quantumlab/index.html?/quantumlab/Kryptographie/index.html (28.4.2011)
http://www.blinde-kuh.de/geheim/geschichte.html (21.4.2011)
http://de.wikipedia.org/wiki/Atbasch (21.4.2011)
http://de.wikipedia.org/wiki/Skytale (21.4.2011)
www.physik.hu-berlin.de/nano/lehre/folder_qPhys/qk2.pdf (30.4.2011)
http://de.wikipedia.org/wiki/Edgar_Allan_Poe (30.4.2011)

DVD:

Quantendimensionen – Doppelspalt · Verschränkung · Quantencomputer, Münster 2010: SCIENCeMOTION und Ernst Klett Verlag Stuttgart, ISBN: 978-3-12-772611-4

Artikel aus Fachzeitschriften/ Diplomarbeiten etc.:

- Knobloch Heidemarie: „Quantenkryptographie in der Schule“(Diplomarbeit, Universität Wien, 2009)
- Müller, Rainer: Quantenphysik in der Schule. Studien zum Physiklernen. Bd.26. – Berlin: Logos 2003 Kapitel 1.3.
- Vorlesungsnotizen von Wolfgang Dür aus der Vorlesung *Quanteninformation und Quantencomputer* WS2009/10
- Seminararbeit Kryptographie aus Methoden des Mathematikunterrichts WS 08/09 von Juliane Schuster für die fächerübergreifenden Ideen

Anhang

Arbeitsblätter der 3 Unterrichtseinheiten

1. Einheit: Quantenkryptographie

Name:

Arbeitsaufträge für die Gruppe:
Verfasst ein Plakat so, dass eure Mitschüler das Verschlüsselungsverfahren kennen lernen und anwenden können. Vergesst nicht euch Notizen bei den jeweils anderen Stationen zu machen, damit ihr die Lernjournalaufträge ausführen könnt.

Atbash

Atbash-Verschlüsselung beruht auf dem Hebräischen Alphabet. Es ist die älteste (600 v.Chr.) und einfachste Verschlüsselungstechnik. Dabei werden die Buchstaben einfach rückwärts aus dem Alphabet aufgezählt.

Verschlüsselungsart:

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

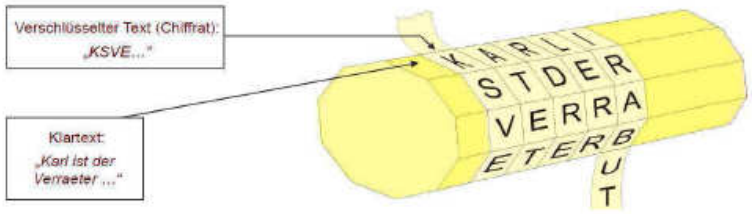
Vervollständigt die obige Tabelle.

Könnt ihr die folgenden Sätze ver- und entschlüsseln?
Hallo! Wie geht es dir? Szool! Drv tvsg vh wri?
Heute regnet es. _____
Nri tvsg vh tfg. _____

Skytale

Ein Zylinder mit spindelförmigem Band gilt als das älteste bekannte militärische Verschlüsselungsverfahren und wurde bereits von den Spartanern vor mehr als 2500 Jahren verwendet. Sender und Empfänger müssen einen Zylinder mit demselben Durchmesser haben, um die Nachricht lesen zu können.

Überlegt euch jeweils einen spannenden Beispielsatz für beide Verfahren, sodass eure Mitschüler ihre Entschlüsselungskünste üben können.
Es liegen dazu 2 Zylinder mit unterschiedlichem Durchmesser bereit.



Arbeitsauftrag für euer Lernjournal:
Findest du diese beiden Verschlüsselungsmethoden sicher? Wenn nein, warum nicht? Was könnte man besser machen? Überleg dir, warum so „einfache" Verschlüsselungsverfahren zur damaligen Zeit sicher genug waren. (3 Pkt.)

1. Einheit: Quantenkryptographie

Name:

Arbeitsaufträge für die Gruppe:
Verfasst ein Plakat so, dass eure Mitschüler das Verschlüsselungsverfahren kennen lernen und anwenden können. Vergesst nicht euch Notizen bei den jeweils anderen Stationen zu machen, damit ihr die Lernjournalaufträge ausführen könnt.

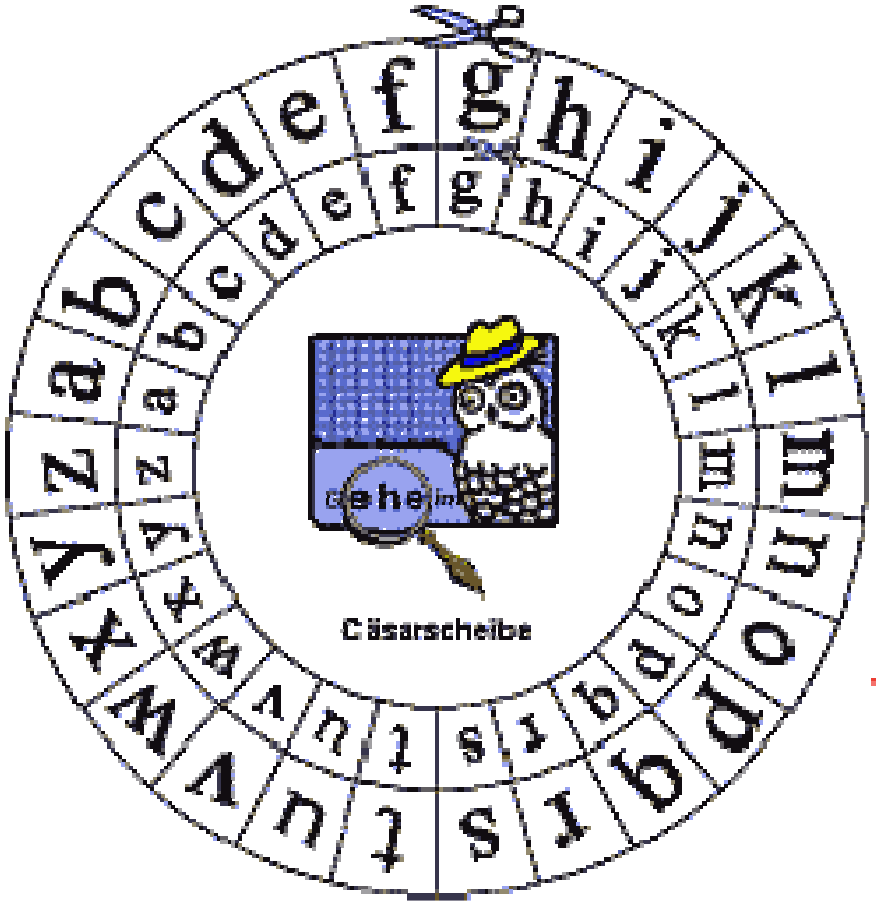
Cäsarcode

Auch Cäsar (100 – 44 v.Chr.) verwendete für seine geheimen Nachrichten eine eigene Verschlüsselungsmethode. Dazu verschob er das Alphabet um genau drei Buchstaben nach rechts. So wurde z.B. das A zu einem D, das B zu einem E und so weiter. Diese Art von Verschlüsselung wurde nach ihm benannt: Cäsar Chiffre.

Entschlüsselt gemeinsam die zwei Sätze, die zu Beginn der Stunde an der Tafel geschrieben worden sind.

Bastelt die Cäsarscheibe nach und legt ein Exemplar eurem Plakat bei. Überlegt euch eine kleine Rede, wie sie Cäsar hätte schreiben können. Dieser kodierten Satz ist als Arbeitsauftrag von euren Mitschülern zu lösen.

Arbeitsauftrag für euer Lernjournal:
Was muss man wissen, um einen Text, der auf diese Art und Weise verschlüsselt wurde, wieder zu entschlüsseln? (1 Pkt.)
Wie könnte man die Verschlüsselung auch ohne den Schlüssel zu wissen, brechen (wenn Zeit keine Rolle spielt)? (2 Pkt. pro Idee)



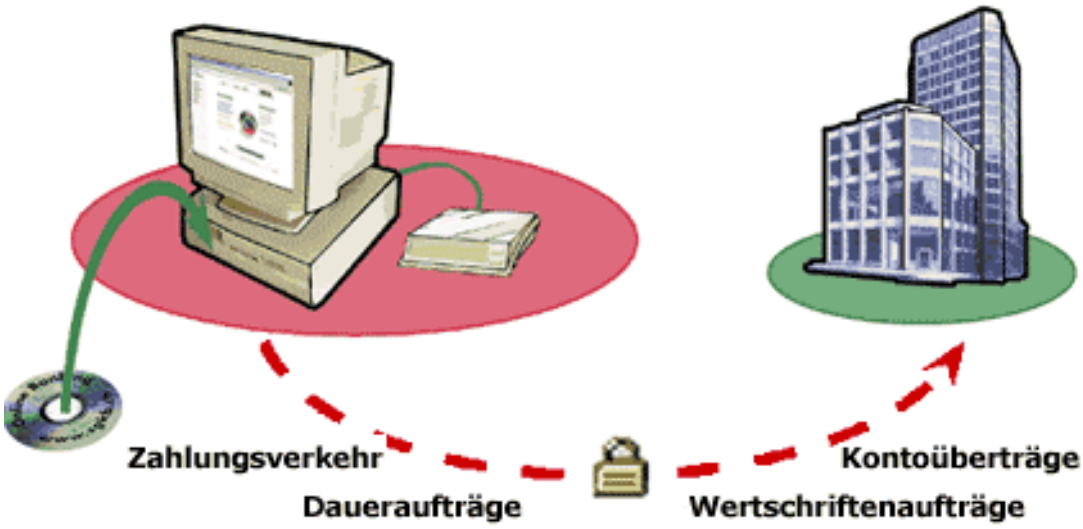
1. Einheit: Quantenkryptographie

Name:

Arbeitsaufträge für die Gruppe:
Verfasst ein Plakat so, dass eure Mitschüler allgemein etwas über Kryptographie erfahren. Vergesst nicht euch Notizen bei den jeweils anderen Stationen zu machen, damit ihr die Lernjournalaufträge ausführen könnt.

Internetrecherche

Informiert euch im Internet
1. über die Bedeutung des Wortes „Kryptographie“ und versucht 2. etwas über den Unterschied zwischen symmetrischer und asymmetrisches Verschlüsselung zu erfahren. Gebt dazu 3. die Vor- bzw. Nachteile an und erwähnt 4. in ein paar Stichworten einige Beispiele. (Die Nummerierung dient als Vorschlag zur Arbeitsaufteilung.)



1. Einheit: Quantenkryptographie

Name:

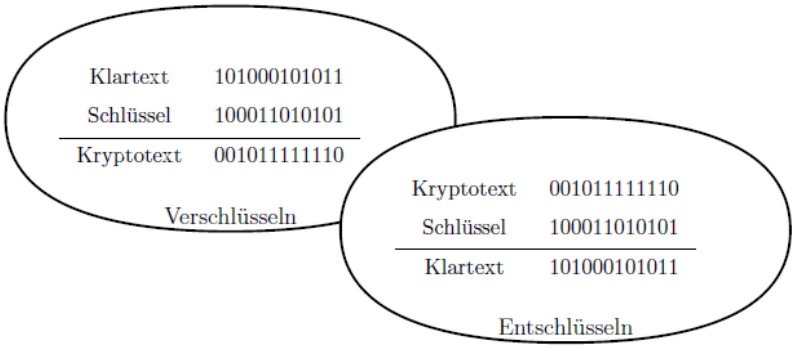
Arbeitsaufträge für die Gruppe:
Verfasst ein Plakat so, dass eure Mitschüler das Verschlüsselungsverfahren kennen lernen und anwenden können. Vergesst nicht euch Notizen bei den jeweils anderen Stationen zu machen, damit ihr die Lernjournalaufträge ausführen könnt.

Vernam- Code

1919 entwickelte der Mathematiker Gilbert Vernam (1890-1960) ein sehr einfaches und effektives Verfahren zur sicheren Verschlüsselung. Auf dieses Grundprinzip stützt sich auch die Quantenkryptographie.
Alice will an Bob eine geheime Nachricht übermitteln. Dazu treffen sie sich auf einer einsamen Insel und schreiben auf einen Notizblock auf jedem Zettel je ein zufälliges Bit (also 0 oder 1). Anschließend fahren sie nach Hause und bewahren den erstellten Schlüssel gut für die Übertragung der Nachricht auf.
Zuerst muss die Nachricht natürlich in Nullen und Einsen verwandelt werden. Dies kann man zum Beispiel machen, indem man die Buchstaben von 1 bis 26 nummeriert und anschließend die jeweilige Zahl in Binärcode umwandelt. Da die nächst höhere Zweierpotenz 32 (= 25) ist, benötigt man zur Darstellung eines Buchstaben genau fünf Bits.

Beispiele:

Buchstabe	Nummer	Binärzahl
a	1	00001
b	2	00010
r	18	10010
x	26	11010



Dann addiert Alice ihren Schlüssel zu der Nachricht (Klartext) mit folgender Rechenvorschrift:

- 0 + 0 = 0
- 0 + 1 = 1
- 1 + 0 = 1
- 1 + 1 = 0

Den nun erhaltenen Kryptotext schickt sie an Bob. Wird die Nachricht am Weg abgefangen, so kann der Lauscher ohne den Schlüssel nichts damit anfangen, da die verschlüsselte Nachricht eine zufällige Folge von Bits ist.
Hat Bob den Kryptotext erhalten, so addiert er nach der gleichen Rechenvorschrift wieder den Schlüssel dazu. Es kommt wieder der Klartext heraus.

Der Vernam- Code ist absolut sicher, wenn
- der Schlüssel genauso lang wie die Nachricht ist.
- nur Alice und Bob den Schlüssel kennen.
- der Schlüssel wirklich zufällig erzeugt wurde.
- der Schlüssel nur einmal benutzt wird.

Überlegt euch gemeinsam ein Wort, welches ihr mit dem Vernam Code für eure Mitschüler verschlüsselt. Dabei dürft ihr nicht vergessen ihnen den Schlüssel mitzuteilen.

Arbeitsauftrag für euer Lernjournal:
Was muss man wissen um einen Text, der auf diese Art und Weise verschlüsselt wurde, wieder zu entschlüsseln? (1 Pkt.)
Wie funktioniert die Umrechnung von Zahlen vom Dezimalsystem ins Binärsystem und umgekehrt? (4 Pkt.)

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

2. Einheit: Lerntagebuch zur Quantenkryptographie

Welche 4 Bedingungen müssen unbedingt erfüllt werden, um eine absolut sichere Schlüsselübertragung zu gewährleisten? –Welche lassen sich mit klassischen Methoden erfüllen? (2 Punkte)

Beschreibe in kurzen Sätzen, wie eine Zufallszahl mit Hilfe eines Strahlteilers generiert werden kann. (evtl. Skizze) (2 Punkte)

Beschreibe in kurzen Sätzen, wie die Schlüsselübertragung mittels polarisierter Photonen funktioniert. (3 Punkte)

Warum ist dadurch noch keine abhörsichere Übertragung möglich? (1 Punkt)

Was besagt das non-cloning Theorem? (1 Punkt)

Wie können wir dieses Theorem zur sicheren Schlüsselübertragung nutzen? (2 Punkte)

Welche Punkte enthält das BB84 – Protokoll? (4 Punkte)

3. Einheit: Quantenkryptographie

A. Arbeitsblätter

Name: _____

Protokoll zu Geheime Quanten

1 Notiere hier die ersten zehn Einträge von deinem Protokoll und dem deines Partners:

Messung	Basis Alice	Basis Bob	Ergebnis Alice	Ergebnis Bob
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

2 Punkte

2 Vergleiche nun die Messergebnisse:

Wie sehen die Ergebnisse aus, wenn Bob in der gleichen Basis gemessen hat, in der Alice ihr Teilchen präpariert hat?

2 Punkte

Erklärung:

Wie sehen die Ergebnisse aus, wenn Bob in der anderen Basis gemessen hat?

2 Punkte

Erklärung:

3 Trage hier den Schlüssel, den du erhalten hast ein! Vergleiche ihn mit deinem Partner!

Schlüssel:

1 Punkt

4 Trage hier die Rechnung, die du durchgeführt hast vollständig ein!

3 Punkte

5 Welche Nachricht wurde übertragen?

2 Punkte

Nachricht, die Alice gesendet hat:

Nachricht, die Bob erhalten hat:

81

3. Einheit: Lerntagebuch zur Quantenkryptographie

Schreib für die 3. Einheit einen Zeitungsartikel, mit Schlagzeile, Unter- bzw. Dachzeile, Quelle, Vorspann und Nachrichtenkörper. Darin soll beschrieben werden, wie Eve lauschen könnte (so wie wir es in der Abschlussdiskussion besprochen haben). Für dieses Arbeitsblatt werden, wenn min. 3 Punkte korrekt angeführt wurden und eine schöne Form gegeben ist, mindestens 7 Punkte vergeben (bis zu 3 Bonuspunkte sind für besondere Kreativität zu erlangen).

-

-

-

-

Quellen:

Autor: