universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

Quantenkryptographie in der Schule

angestrebter akademischer Grad

Magistra der Naturwissenschaften (Mag. rer.nat)

Verfasserin:	Heidemarie Knobloch
Matrikel-Nummer:	0506207
Studienrichtung:	Lehramtsstudium UF Physik UF Mathematik
Betreuerin:	Univ. Doz. Dr. Mag. Beatrix Hiesmayr

Wien, am 3. Juni 2009

Zusammenfassung

Wie kann man Quantenkryptographie in der Schule behandeln? Dieser Frage soll hier nachgegangen werden. Es wird eine Möglichkeit gezeigt, die Einführung in dieses Thema auch den SchülerInnen zugänglich zu machen. Zusätzlich dazu wurde ein Lernprogramm entwickelt, mit Hilfe dessen sie das Konzept auch selbst am Computer ausprobieren können. Dieses wurde auch schon im Gymnasium in der Draschestraße (Wien) im Unterricht ausprobiert.

Neben dem schülerorientierten Teil gibt es auch einen Theorieteil, bei dem sich die LehrerInnen selbst in das Thema vertiefen können.

Abstract

How can Quantum Cryptography be teached in secondary education? The present study tries to find answers to this question. A teaching modality that makes the understanding of the subject more accessible to the pupils is proposed. A dedicated learning application is described, which assists the pupils to test the concept on their own at the computer. It has been tested in a school in Vienna.

In addition to the pupil-oriented part the study also contains a theoretical section, which offers profound information to the teachers.

Inhalt

Vorwort

Diese Arbeit richtet sich an Lehrer und Lehrerinnen, die den Unterricht der Quantenphysik etwas spannender gestalten wollen oder auch einfach nur neugierig auf die moderne Physik sind. Wie es schon der Titel sagt, wird hauptsächlich die Quantenkryptographie als Beispiel eines der Anwendungsgebiete der Quantenphysik behandelt. Die Arbeit besteht aus zwei großen Abschnitten: Einerseits die Theorie, in der sich die LehrerInnen das nötige Wissen erarbeiten können und andererseits die Umsetzung in der Schule. In diesem Teil finden sich auch einige Materialien, die direkt im Unterricht verwendet werden können. Dazu gehören einige Arbeitsblätter, ein Foliensatz (sowohl für den Beamer als auch für den Overheadprojektor) sowie ein Simulationsprogramm zur Quantenkryptographie. Alle Materialien finden sich einerseits auf der beigelegten CD und im Anhang als auch auf der Seite http://homepage.univie.ac.at/heidemarie.knobloch zum freien Download. Falls es Neuerungen gibt, wird dies auf der Homepage bekanntgegeben. Zusätzlich gibt es dort auch eine Seite für eigene Kommentare, wo ich mich über Feedback freuen würde.

Abbildung 1 Homepage

Der Unterrichtsteil der Arbeit ist aber nicht als fertiges Unterrichtskonzept zu verstehen, das man genauso in die Realität umsetzen muss, sondern als Vorschlag für den Unterricht. So darf man sich auch trauen, das eine oder andere wegzulassen oder auch auszubauen und intensiver zu behandeln. Auch die Arbeitsblätter können einerseits so verwendet werden, wie sie sind, dürfen aber auch nach Belieben verändert und weitergegeben werden (legal!). Der Source-Code sowie alle Bilder befinden sich auf der Homepage.

Die vorgeschlagenen Unterrichtsideen können durchaus auch fächerübergreifend mit Mathematik durchgeführt werden, da gerade die klassische Kryptographie gut in den Mathematikunterricht passt. Es eignet sich aber auch für den Physikunterricht alleine.

Warum aber soll die Quantenkryptographie überhaupt im Unterricht behandelt werden? Dafür gibt es viele Gründe. Einerseits steht die Quantenphysik ja auch im Lehrplan. Warum soll man daher nicht auch die Anwendungen zeigen. Außerdem sind, glaube ich, genau diese Themen für SchülerInnen interessant, da sie einerseits sehr aktuell und teilweise auch in den Medien vertreten sind und andererseits sich den Alltagserfahrungen so stark entziehen, dass man darüber leicht ins staunen kommt. Ein wichtiger Punkt ist auch, dass die SchülerInnen in der klassischen Physik meist das geboten bekommen, was die Wissenschaftler schon lange zuvor entdeckt haben. Hier sehen sie ein Beispiel, woran noch immer stark geforscht wird und so manche Fragen noch nicht geklärt sind. Die Physik ist also noch nicht abgeschlossen.

I
Theorie

Dieser Abschnitt ist ein Einblick in die Theorie der Quantenkryptographie. Er ist für LehrerInnen gedacht, um grundlegendes Verständnis der Theorie der Quantenkryptographie zu gewinnen, sowie auch die mathematischen Hintergründe zu verstehen.

1 Mathematischer Rahmen

In diesem Abschnitt wird der mathematische Formalismus, der in der Quantenkryptographie üblich ist, eingeführt. Dabei wollen wir Zustände und deren Veränderung sowie den dazugehörigen Raum beschreiben können. Es ist dazu ausreichend, wenn wir uns auf den zweidimensionalen Hilbertraum beschränken.

1.1 Hilbertraum

Um beginnen zu können, brauchen wir zuerst einmal einen mathematischen Raum. In der Quantenphysik ist dies der sogenannte Hilbertraum, benannt nach dem Mathematiker David Hilbert (1862-1943). Im Allgemeinen ist dieser Raum unendlichdimensional. Für die meisten Betrachtungen in der Quantentheorie reichen aber endlich viele Dimensionen aus.

1.1 Definition Ein zweidimensionaler Hilbertraum $\mathcal{H}$, ist ein linearer (vollständiger) Vektorraum über dem Körper der komplexen Zahlen $\mathbb{C}$ mit einem Skalarprodukt.

Jetzt haben wir einen Raum definiert. Wir wollen aber auch noch wissen, wie die Elemente, die darin leben, aussehen. Ganz einfach, es sind dies zweidimensionale komplexe Vektoren, also

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \qquad \text{mit } a_1, a_2 \in \mathbb{C}.$$

Um diese Vektoren nicht immer ausschreiben zu müssen, hat Paul Adrian Maurice Dirac (1902-1984) im Jahre 1930 einen Formalismus eingeführt. Dieser bringt einige Vorteile mit sich, wie wir später noch sehen werden. Es ist dies der heutzutage in der Quantentheorie übliche Formalismus. Bekannt wurde er unter Dirac-Notation oder auch Bra-ket Notation.

1.2 Dirac-Notation

Wie funktioniert nun dieser Formalismus? Beginnen wir einmal mit der Bezeichnung von unseren Vektoren im Hilbertraum. Sie werden dargestellt als *ket*-Vektor

$$|\psi\rangle := \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} \in \mathcal{H}.$$

Da der Hilbertraum ein Vektorraum ist, gibt es dazu auch einen dualen Vektorraum $\mathcal{H}^*$. Die Elemente darin sind die *bra*-Vektoren. Sie entsprechen den adjungierten (= komplex konjugierten; im Folgenden mit $*$ bezeichnet) und transponierten Vektoren

$$\langle\psi| := (\psi_1^*, \psi_2^*) \in \mathcal{H}^*.$$

Betrachten wir nun das Skalarprodukt, welches wir ja auch in unserer Definition für den Hilbertraum gefordert haben. Wir bekommen es, indem wir *bra* und *ket* zusammensetzen. Dies ergibt nicht nur zufällig das englische Wort »braket« (= Klammer). Das Symbol sieht dann genauso aus, wie wir es schon immer für das Skalarprodukt verwendet haben:

$$\langle\psi|\varphi\rangle = (\psi_1^*, \psi_2^*)\begin{pmatrix}\varphi_1\\ \varphi_2\end{pmatrix} = \psi_1^* \cdot \varphi_1 + \psi_2^* \cdot \varphi_2$$

Die bekannten Rechenregeln für das Skalarprodukt gelten auch hier. Es sind dies

1. $\langle\varphi|\varphi\rangle \geq 0 \qquad \forall|\psi\rangle \in \mathcal{H}, \qquad \langle\varphi|\varphi\rangle = 0 \iff |\varphi\rangle = \begin{pmatrix}0\\0\end{pmatrix}$
2. $\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^*$
3. $\langle\varphi|(c_1|\psi_1\rangle + c_2|\psi_2\rangle) = c_1\langle\varphi|\psi_1\rangle + c_2\langle\varphi|\psi_2\rangle, \qquad c_1, c_2 \in \mathbb{C}$
4. $(c_1\langle\varphi_1| + c_2\langle\varphi_2|)|\psi\rangle = c_1^*\langle\varphi_1|\psi\rangle + c_2^*\langle\varphi_2|\psi\rangle, \qquad c_1, c_2 \in \mathbb{C}$

Das war auch schon der ganze Trick für den Formalismus. Nun folgen ein paar Beispiele.

1.2 Beispiele

1. Sei $|\psi\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. Dann ist $\langle\psi| = (0^*, 1^*) = (0, 1)$.
2. Sei $|\psi\rangle = \begin{pmatrix}2-4i\\3+7i\end{pmatrix}$ und $|\varphi\rangle = \begin{pmatrix}5+4i\\3+2i\end{pmatrix}$. Dann ist $\langle\psi| = (2+4i, 3-7i)$ und das Skalarprodukt $\langle\psi|\varphi\rangle = (2+4i, 3-7i)\begin{pmatrix}5+4i\\3+2i\end{pmatrix} = (2+4i)(5+4i) + (3-7i)(3+2i) = 17+13i$

Für ein paar Vektoren gibt es spezielle Bezeichnungen, die in der Literatur immer wieder verwendet werden.

1.3 Vereinbarungen

$$\begin{pmatrix}1\\0\end{pmatrix} =: |0\rangle =: |h\rangle$$

$$\begin{pmatrix}0\\1\end{pmatrix} =: |1\rangle =: |v\rangle$$

Die Bezeichnung $|h\rangle$ steht dabei für horizontale, $|v\rangle$ für vertikale Polarisation. Die beiden Zustände bilden eine Orthonormalbasis (d.h. sie sind normiert und stehen normal aufeinander). Es gilt also

$$\langle 0|0\rangle = \langle 1|1\rangle = 1$$
$$\langle 0|1\rangle = \langle 1|0\rangle = 0.$$

1.3 Zustände

Nun haben wir bereits den Grundraum und dessen Elemente kennen gelernt. Für die meisten Anwendungen in der Quantentheorie betrachten wir aber nur einen Teilmenge davon: die normierten Vektoren, die wir Quantenzustände oder schlampig auch Zustände nennen.

1.4 Definition Seien $|0\rangle$ und $|1\rangle$ die zwei normierten, zueinander orthogonalen Vektoren im Hilbertraum von oben und $\alpha, \beta \in \mathbb{C}$ mit $|\alpha|^2 + |\beta|^2 = 1$, dann nennen wir

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

einen Quantenzustand (auch Quantenbit oder Qubit). Die Zahlen α und β heißen dabei Amplitude.

Man sagt $|\psi\rangle$ ist eine Linearkombination oder eine Überlagerung der beiden Basisvektoren $|0\rangle$ und $|1\rangle$. Diese nennt man auch *Superposition*. Die reellen Zahlen $|\alpha|^2$ und $|\beta|^2$ geben dabei die Wahrscheinlichkeiten an, mit der bei einer Messung in der Basis h/v der Zustand $|0\rangle$ bzw. $|1\rangle$ erhalten wird. Daher ist es auch klar, dass gefordert wird, dass sie bei Addition immer den Wert 1 ergeben müssen.

1.5 Beispiele

1. $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$
2. $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$
3. $|0\rangle = 1|0\rangle + 0|1\rangle = \begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$
4. $|1\rangle = 0|0\rangle + 1|1\rangle = \begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$

Der Zustand $|+\rangle$ repräsentiert bei Photonen die Polarisation im Winkel 45° und $|-\rangle$ die im Winkel $-45°$. In der Graphik 1.1 wurden die vier Zustände $|0\rangle$, $|1\rangle$, $|+\rangle$ und $|-\rangle$ am Einheitskreis dargestellt. Genau genommen müssten wir eigentlich eine dreidimensionale Darstellung wählen. Da wir es hier aber nur mit Zuständen, die reell darstellbar sind (ohne komplexe Phasen) zu tun haben, reicht eine zweidimensionale Darstellung zur Anschauung aus.

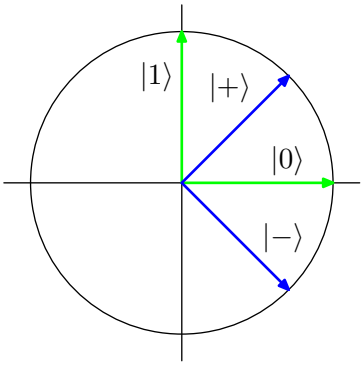


Abbildung 1.1 Die Zustände am Einheitskreis eingezeichnet

1.4 Operatoren

Nun wollen wir aber nicht nur fixe Zustände am Hilbertraum betrachten, sondern auch deren Veränderung. Mathematisch lässt sich dies durch Operatoren, die auf den jeweiligen Zustand wirken, darstellen. Im zweidimensionalen Hilbertraum sind dies 2×2 Matrizen, die beschreiben, wie sich ein isoliertes Quantensystem ändert.

1.6 Wirkung eines Operators auf einen Zustand Sei $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ und $A = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$. Um den Operator auf den Zustand wirken zu lassen, müssen wir ihn einfach auf den Vektor $|\psi\rangle$ anwenden. Daraus erhalten wir den Folgezustand $|\psi'\rangle$.

$$|\psi'\rangle = A \cdot |\psi\rangle = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}a\alpha + b\beta\\ c\alpha + d\beta\end{pmatrix}$$

So ein Operator ist zum Beispiel die sogenannte Hadamard-Matrix, die als

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

definiert ist. Wie diese Matrix nun unsere Zustände verändert sieht man in den folgenden Beispielen.

1.7 Beispiele

1. $H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = |+\rangle$
2. $H|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}2\\ 0\end{pmatrix} = |0\rangle$
3. $H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = |-\rangle$
4. $H|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}0\\ 2\end{pmatrix} = |1\rangle$

Aus den Beispielen können wir erkennen, dass die Hadamard-Matrix die Zustände $|0\rangle$ und $|1\rangle$ in die Zustände $|+\rangle$ und $|-\rangle$ überführt und umgekehrt. Zweimal angewendet ergibt sie wieder den ursprünglichen Zustand. Es gilt also $H \cdot H = I_2$ und damit $H^{-1} = H$.

Die Hadamard-Matrix ist ein besonderer Operator, da die Länge des Vektors bei dessen Anwendung erhalten bleibt. Operatoren mit dieser Eigenschaft nennt man unitär.

1.8 Definition Sei $A = (a_{ij})_n$ eine $n \times n$ Matrix mit $a_{ij} \in \mathbb{C}$. Falls

$$A^\dagger = A^{-1}$$

gilt, heißt A unitär.

Dabei ist $A^\dagger$ die komplex konjugierte und transponierte (also $(A^*)^t$) und A^{-1} die Inverse der Matrix A. Dazu ein paar Beispiele.

1.9 Beispiele

1. Sei $A = \begin{pmatrix} 1-i & 3 \\ 0 & 7+4i \end{pmatrix}$. Dann ist $A^\dagger = (A^*)^t = \begin{pmatrix} 1+i & 3 \\ 0 & 7-4i \end{pmatrix}^t = \begin{pmatrix} 1+i & 0 \\ 3 & 7-4i \end{pmatrix}$

2. Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Dann ist $A^{-1} = \frac{1}{bc-ad}\begin{pmatrix} -d & b \\ c & -a \end{pmatrix}$.

1.10 Beispiele für unitäre Matrizen

1. Die Hadamard-Matrix H ist unitär, da $H^\dagger = (H^*)^t = H^t = H = H^{-1}$.

2. Auch $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ist unitär, denn $I_2^\dagger = I_2 = I_2^{-1}$.

1.11 Definition Sei A eine unitäre 2×2 Matrix und $|\psi\rangle \in \mathcal{H}$ ein Zustand. Dann nennt man die Abbildung

$$|\psi\rangle \mapsto A \cdot |\psi\rangle$$

eine unitäre Transformation.

1.5 Messung

Eine Messung ist nichts anderes als die Wechselwirkung eines Quantensystems mit einem (klassischen) Messapparat. Jede messbare Größe (auch Observable genannt) wird durch eine Projektion im Hilbertraum beschrieben.

1.12 Definition Sei P eine quadratische-Matrix. Falls

$$P^2 = P$$

gilt, nennt man P eine Projektion.

Jede Projektion $P \neq 0, I_2$ lässt sich eindeutig darstellen als

$$P = |\psi\rangle\langle\psi|$$

wobei $|\psi\rangle$ ein (normierter) Vektor im Hilbertraum ist, der die Messrichtung vorgibt.

1.13 Satz Sei α die Richtung in der man ein Teilchen messen möchte. Dann ist der dazugehörige Messoperator

$$M_\alpha = \begin{pmatrix} \cos^2\alpha & \cos\alpha\sin\alpha \\ \cos\alpha\sin\alpha & \sin^2\alpha \end{pmatrix}.$$

Beweis Der Vektor $|\psi\rangle = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}$ repräsentiert eine beliebige Richtung im Einheitskreis. Nun kann der Projektor dazu gebildet werden:

$$P = |\psi\rangle\langle\psi| = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}(\cos\alpha, \sin\alpha) = \begin{pmatrix} \cos^2\alpha & \cos\alpha\sin\alpha \\ \cos\alpha\sin\alpha & \sin^2\alpha \end{pmatrix}$$

□

1.14 Bemerkung Genau genommen würde beim Messoperator wieder eine komplexe Phase in der Offdiagonalen dazukommen. Da wir uns aber nur mit den reellen Zuständen befassen, kann man diese auch weglassen.

Der Operator mit dem man in horizontaler Richtung ($\alpha = 0$) messen kann lautet somit $M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. In vertikaler Richtung ($\alpha = \frac{\pi}{2}$) ist es $M_{\frac{\pi}{2}} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Ich bezeichne nun mit $\emptyset$ den Vektor $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

1.15 Beispiele

1. $M_0|0\rangle = |0\rangle$
2. $M_0|1\rangle = \emptyset$
3. $M_{\frac{\pi}{2}}|0\rangle = \emptyset$
4. $M_{\frac{\pi}{2}}|1\rangle = |1\rangle$

M filtert quasi den Anteil der in α-Richtung polarisierten Photonen. Der Folgezustand ist dabei allerdings nicht immer normiert.

1.16 Beispiel Polarisation Betrachten wir nun die Polarisation als Zustand eines Teilchens. Um Photonen in einen gewünschten linear polarisierten Zustand zu bringen verwendet man einen Polarisationsfilter (kurz: Polarisator). Diesen kann man ebenfalls für die Messung verwenden. Dann wird er Analysator genannt. Möchte man also Teilchen mit der Orientierung α haben, so lässt man sie einen Polarisator mit Neigung α passieren.

Stellt man einen Analysator dem Photon in den Weg, so wird es mit einer gewissen Wahrscheinlichkeit, die vom Winkel abhängt, durchgelassen und mit der Gegenwahrscheinlichkeit absorbiert. Kommt ein Photon durch, so nimmt es anschließend die Polarisation in Richtung des Polarisators an. Ob ein Teilchen nun durchgelassen wird oder nicht, ist aber wegen den Wahrscheinlichkeiten nicht vorhersagbar und völlig vom Zufall bestimmt (außer man hat zuvor den Zustand im gleichen Winkel oder dazu orthogonal wie den Analysator präpariert). Dies ist ein wichtiger Punkt der Quantenmechanik, den man zum Beispiel für einen perfekten Zufallsgenerator ausnützen kann.

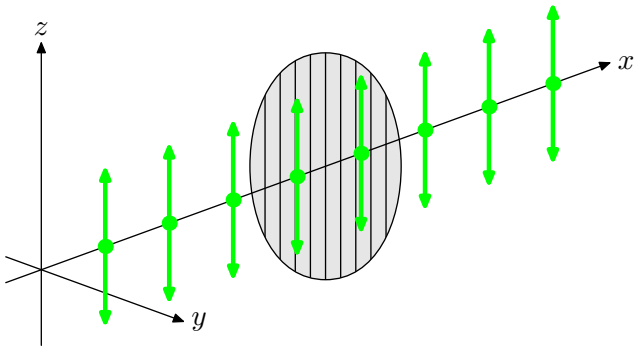


Abbildung 1.2 Die Polarisation der Photonen ist parallel zum Polarisator. Sie werden alle durchgelassen.

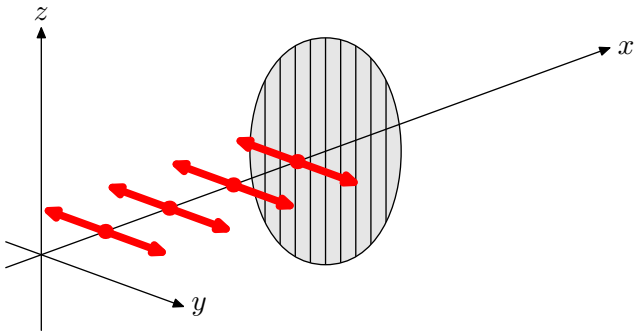


Abbildung 1.3 Die Polarisation der Photonen ist orthogonal zum Polarisator. Sie werden alle absorbiert.

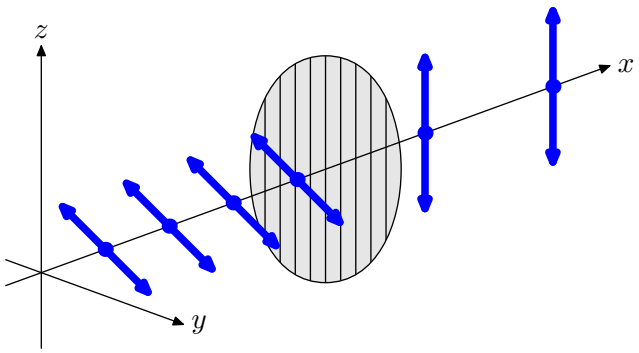


Abbildung 1.4 Die Polarisation der Photonen ist um 45° zum Polarisator geneigt. Die Hälfte der Teilchen werden durchgelassen, die andere Hälfte absorbiert. Die Wahrscheinlichkeiten sind für beide Fälle 50%.

Formal kann man die Wahrscheinlichkeiten über den Erwartungswert berechnen.

1.17 Definition Sei $|\psi\rangle \in \mathcal{H}$ ein Zustand und M_α ein Messoperator in Richtung α. Dann ist der Erwartungswert $\langle M_\alpha \rangle$ dafür, den Zustand nach der Messung in α Richtung vorzufinden, gleich

$$\langle M_\alpha \rangle = \langle \psi | M_\alpha | \psi \rangle.$$

1.18 Beispiele Sei $|\psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$.

1. $\langle H_0 \rangle = \langle \psi | H_0 | \psi \rangle = (a^*, b^*) \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = (a^*, 0) \begin{pmatrix} a \\ b \end{pmatrix} = a^* a = |a|^2$

2. $\langle H_{\frac{\pi}{2}} \rangle = \langle \psi | H_{\frac{\pi}{2}} | \psi \rangle = (a^*, b^*) \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = (0, b^*) \begin{pmatrix} a \\ b \end{pmatrix} = b^* b = |b|^2$

Anhand des Beispiels kann man erkennen, dass das Quadrat der Amplitude vor dem Zustand $|0\rangle$ bzw. $|1\rangle$ immer die Wahrscheinlichkeit angibt, mit der man den Zustand $|0\rangle$ bzw. $|1\rangle$ nach einer Messung in dieser Basis vorfindet.

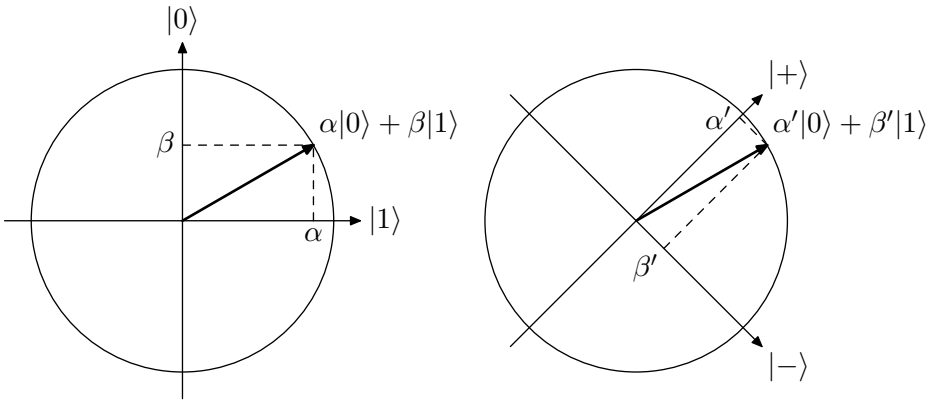


Abbildung 1.5 Wahrscheinlichkeiten bei einer Messung

1.19 Beispiel Spin

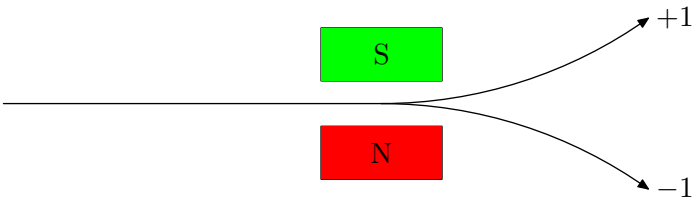


Abbildung 1.6 Stern-Gerlach-Experiment

Den Spin eines Teilchens kann man mit dem Stern-Gerlach-Experiment in verschiedene Richtungen messen. Dazu lässt man zum Beispiel ein Elektron ein Magnetfeld passieren. Anschließend kann man beobachten, dass die Teilchen nach oben oder nach unten abgelenkt werden. Bei anderen Teilchen kann nicht nur eine Aufteilung in zwei Strahlen sondern auch in mehrere oder gar keine beobachtet werden. Wir beschränken uns hier auf die Aufspaltung in zwei Möglichkeiten und bezeichnen den Zustand für Teilchen, die nach oben abgelenkt werden als Spin-up und die nach unten abgelenkt werden als Spin-down. Die Teilchen selbst werden als Spin-$\frac{1}{2}$-Teilchen bezeichnet. Dazu gehören zum Beispiel Neutronen, Protonen und Elektronen. Formal werden die Zustände als

$$|\uparrow\rangle = \begin{pmatrix}1\\0\end{pmatrix} \text{ und } |\downarrow\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

bezeichnet.

1.6 Zweiteilchensysteme

Betrachtet man nun anstatt nur einem Teilchen gleich zwei gemeinsam, so kann man dies mathematisch mit einem Tensorprodukt ausdrücken. Dies ist auch ein Postulat der Quantenmechanik. Für die Teilchen $|a\rangle$ und $|b\rangle$ kann man den gemeinsamen Zustand als $|a\rangle \otimes |b\rangle$ anschreiben. Das Zeichen zwischen den beiden ket-Vektoren ist das sogenannte Tensorprodukt. Da es einen Isomorphismus zwischen $\mathbb{R}^2 \otimes \mathbb{R}^2$ und dem $\mathbb{R}^4$ gibt, kann man den gemeinsamen Zustand von $|a\rangle$ und $|b\rangle$ auch durch einen vierdimensionalen Vektor anschreiben.

$$|a\rangle \otimes |b\rangle = \begin{pmatrix}a_1\\a_2\end{pmatrix} \otimes \begin{pmatrix}b_1\\b_2\end{pmatrix} = \begin{pmatrix}a_1 \cdot b_1\\a_1 \cdot b_2\\a_2 \cdot b_1\\a_2 \cdot b_2\end{pmatrix}$$

1.20 Schreibweisen Anstatt $|a\rangle \otimes |b\rangle$ schreibt man abkürzend oft auch $|a\rangle|b\rangle$ oder überhaupt $|ab\rangle$.

1.21 Beispiele

1. $|00\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$ Diese vier Zustände bilden eine mögliche Standardbasis für Zweiteilchensysteme.

1.6.1 Messung eines einzelnen Bits in einem Zweiteilchensystem

Einen allgemeinen Zustand in einem Zweiteilchensystem in der Standardbasis kann man anschreiben als

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle.$$

Angenommen wir messen das erste Bit. Mit Wahrscheinlichkeit $|\alpha|^2 + |\beta|^2$ erhalten wir als Ergebnis 0. Der Operator für diese Messung ist

$$P = |0\rangle\langle 0| \otimes I_2.$$

Dieser Projektor misst das erste Bit in der horizontalen Richtung ($|0\rangle\langle 0|$) und lässt das zweite Bit im ursprünglichen Zustand (I_2). Nun können wir ihn auf unseren Zustand anwenden (der Nenner ist für die Normierung notwendig):

$$\frac{(|0\rangle\langle 0| \otimes I_2)|\psi\rangle}{|(|0\rangle\langle 0| \otimes I_2)|\psi\rangle|}.$$

Berechnen wir uns zuerst den Zähler (der Nenner läuft ja analog).

$$(|0\rangle\langle 0| \otimes I_2)(\alpha|0\rangle \otimes |0\rangle + \beta|0\rangle \otimes |1\rangle + \gamma|1\rangle \otimes |0\rangle + \delta|1\rangle \otimes |1\rangle) =$$
$$\alpha|0\rangle \underbrace{\langle 0|0\rangle}_{1} \otimes|0\rangle + \beta|0\rangle \underbrace{\langle 0|0\rangle}_{1} \otimes|1\rangle + \gamma|0\rangle \underbrace{\langle 0|1\rangle}_{0} \otimes|0\rangle + \delta|0\rangle \underbrace{\langle 0|1\rangle}_{0} \otimes|1\rangle =$$
$$\alpha|00\rangle + \beta|01\rangle$$

Somit lautet unser Folgezustand

$$|\psi'\rangle = \frac{\alpha|00\rangle + \beta|01\rangle}{\sqrt{|\alpha|^2 + |\beta|^2}}.$$

Wie man sieht verschwinden die Anteile $|10\rangle$ und $|11\rangle$ und übrig bleiben klarerweise die, bei denen das erste Qubit $|0\rangle$ war.

Das Messergebnis $|1\rangle$ für das erste Bit erhält man mit Wahrscheinlichkeit $|\gamma|^2 + |\delta|^2$. Der Folgezustand ist hier (Rechnung analog wie oben)

$$|\psi'\rangle = \frac{\gamma|10\rangle + \delta|11\rangle}{\sqrt{|\gamma|^2 + |\delta|^2}}.$$

1.7 Verschränkte Systeme und Bell-Ungleichung

1.22 Experiment Eine Photonenquelle emittiert ein Teilchenpaar (siehe Abb. 1.7). Die Teilchen verlassen die Quelle in entgegengesetzter Richtung. Nun lässt sich folgendes beobachten:

Werden anschließend beide Teilchen in der gleichen Basis gemessen, so sind die Ergebnisse immer antikorreliert. Das heißt, messe ich bei einem Teilchen 0, so erhalte ich beim anderen Teilchen 1 und umgekehrt. Die Teilchen scheinen gegenseitig zu wissen, wie sich der jeweils andere während der Messung verhält. Die Messergebnisse waren aber vor der Messung unbestimmt. Diesen Zustand, bei dem das Messergebnis des einen Teilchens, egal in welcher Richtung gemessen wird, vom anderen abhängt, nennt man Verschränkung. Wie kann man das nun erklären?

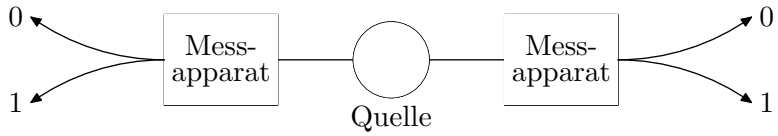


Abbildung 1.7 Eine Quelle emittiert ein Teilchenpaar

1.7.1 Erster Erklärungsversuch

Wird Teilchen A gemessen, so schickt es eine Information an Teilchen B, wie es sich bei der Messung verhalten hat. Allerdings ist klar, dass dies nicht funktionieren kann, da sich die Teilchen instantan entscheiden, wie sie sich verhalten. Misst man diese beiden Photonen nämlich sehr weit voneinander entfernt, so könnte nach der Relativitätstheorie das zweite Teilchen beschränkt durch die Lichtgeschwindigkeit erst später reagieren. Es zeigt sich aber, dass die beiden bei der Messung gleichzeitig antikorrelierte Ergebnisse liefern.

1.7.2 Zweiter Erklärungsversuch

Nachdem es im getrennten Zustand der Teilchen keinen Austausch, der schnell genug ist, geben kann, bleibt nur noch die Möglichkeit, dass sie sich direkt an der Quelle ausmachen, wie sie bei den Messungen reagieren werden. Das bedeutet Photon A und Photon B bekommen beide eine lange Liste mit Verhaltensregeln mit auf den Weg. Dazu gibt es eine Theorie, die auf diesen Verhaltensregeln basiert. So eine Theorie nennt man auch »lokal realistische Theorie mit verborgenen Parametern«, das heißt sie stützt sich lediglich auf die Annahme der Lokalität und die der Realität. Nun müssen aber die Kombinationen von Wahrscheinlichkeiten, die alle mit dieser Theorie berechnet werden, eine bestimmte Ungleichung erfüllen. Das ist die sogenannte Bell-Ungleichung (benannt nach John S. Bell im Jahre 1964).

1.7.3 Bell-Ungleichung

Die folgende Version (nach [1]) der Bellschen Ungleichung stammt von Eugene P. Wigner. Dies ist die Original Ungleichung nur mit Wahrscheinlichkeiten an Stelle von Erwartungswerten angeschrieben (dies wäre daher auch schülerInnentauglicher). Wir betrachten wieder den antikorellierten Zweiteilchenzustand wie oben. Diese können wir in drei verschiedenen Richtungen (α, β und γ) messen. Die Richtungen geben dabei den Winkel an, um den die jeweilige Messbasis zur Standardbasis gedreht ist. Unsere einzige Annahme ist, dass sich die Teilchen über eine Strecke hinweg nicht gegenseitig beeinflussen können (Lokalität). Dazu gibt es acht (zwei mögliche Ergebnisse hoch drei Richtungen) mögliche Messergebnisse (siehe Tabelle 1.1). Die Ergebnisse wurden mit 0 oder 1 bezeichnet. In einer Klammer stehen alle drei Ergebnisse für die Messungen in den drei Richtungen. Der erste Eintrag repräsentiert die Messung der ersten Richtung α, der zweite der Richtung β, und der dritte der Richtung γ. Da die Teilchen antikorreliert sind, müssen die Ergebnisse von Teilchen B genau entgegengesetzt zu Teilchen A sein.

Häufigkeit	Teilchen A (α, β, γ)	Teilchen B (α, β, γ)
N_1	$(0, 0, 0)$	$(1, 1, 1)$
N_2	$(0, 0, 1)$	$(1, 1, 0)$
N_3	$(0, 1, 0)$	$(1, 0, 1)$
N_4	$(0, 1, 1)$	$(1, 0, 0)$
N_5	$(1, 0, 0)$	$(0, 1, 1)$
N_6	$(1, 0, 1)$	$(0, 1, 0)$
N_7	$(1, 1, 0)$	$(0, 0, 1)$
N_8	$(1, 1, 1)$	$(0, 0, 0)$

Tabelle 1.1 Mögliche Ergebnisse der Messungen

Da wir es mit Häufigkeiten zu tun haben (also $N_i > 0, \forall i$), muss gelten

$$N_2 + N_4 \leq N_2 + N_4 + N_3 + N_6 = (N_2 + N_6) + (N_3 + N_4). \tag{1.1}$$

Die Wahrscheinlichkeit, dass nun Alice bei der Messung in Richtung α und Bob bei der Messung in Richtung β das Ergebnis 0 erhalten, ist dann

$$P_{00}(\alpha, \beta) = \frac{N_3 + N_4}{\sum_i^8 N_i}.$$

Auf die gleiche Art kann man auch folgende Wahrscheinlichkeiten berechnen:

$$P_{00}(\alpha, \gamma) = \frac{N_2 + N_4}{\sum_i^8 N_i}$$
$$P_{00}(\beta, \gamma) = \frac{N_2 + N_6}{\sum_i^8 N_i}$$

Setzt man nun in Formel (1.1) ein und multipliziert mit $\sum_i^8 N_i$, so erhält man

$$P_{00}(\alpha, \gamma) \leq P_{00}(\beta, \gamma) + P_{00}(\alpha, \beta).$$

Dies ist auch schon die Bell-Ungleichung (in Wigner Form). In der Quantenphysik kann man die Wahrscheinlichkeiten für die einzelnen Ereignisse durch die Formel

$$P_{00}^{QM}(\alpha, \beta) = \frac{1}{2} \sin^2(\alpha - \beta)$$

berechnen.

Herleitung Sei $|0_\alpha\rangle\langle 0_\alpha|$ der Messoperator in Richtung α mit

$$|0_\alpha\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle = \begin{pmatrix}\cos\alpha \\ \sin\alpha\end{pmatrix}.$$

Angenommen unsere Teilchen befinden sich im Zustand

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Die quantenmechanische Wahrscheinlichkeit in Richtung α und in Richtung β das Ergebnis 0 zu erhalten ist gegeben durch

$$P_{00}^{QM}(\alpha, \beta) = P^{QM}(0_\alpha, 0_\beta) = |(|0_\alpha\rangle\langle 0_\alpha| \otimes |0_\beta\rangle\langle 0_\beta|)|\psi^-\rangle|^2.$$

Einsetzen ergibt nun

$$|(|0_\alpha\rangle\langle 0_\alpha| \otimes |0_\beta\rangle\langle 0_\beta|)\frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)|^2 =$$
$$\frac{1}{2}||0_\alpha\rangle\langle 0_\alpha|0\rangle \otimes |0_\beta\rangle\langle 0_\beta|1\rangle - |0_\alpha\rangle\langle 0_\alpha|1\rangle \otimes |0_\beta\rangle\langle 0_\beta|0\rangle|^2 =$$
$$\frac{1}{2}|\cos\alpha \sin\beta|0_\alpha\rangle \otimes |0_\beta\rangle - \sin\alpha\cos\beta|0_\alpha\rangle \otimes |0_\beta\rangle|^2 =$$
$$\frac{1}{2}(\cos\alpha\sin\beta - \sin\alpha\cos\beta)^2 \underbrace{||0_\alpha\rangle \otimes |0_\beta\rangle|^2}_{1} =$$
$$\frac{1}{2}\sin^2(\alpha - \beta)$$

□

Wählen wir nun die Winkel wie folgt

$$\alpha = -\frac{\pi}{6}$$
$$\beta = 0$$
$$\gamma = \frac{\pi}{6}$$

Dann erhalten wir für die Wahrscheinlichkeiten

$$P_{00}(\alpha, \beta) = \frac{1}{8}$$
$$P_{00}(\beta, \gamma) = \frac{1}{8}$$
$$P_{00}(\alpha, \gamma) = \frac{3}{8}.$$

Somit lautet unsere Ungleichung

$$\frac{3}{8} \leq \frac{2}{8}$$

was offensichtlich falsch ist. Daraus folgt, dass die Quantenphysik die Ungleichung verletzt. Jetzt kann nur ein Experiment entscheiden, welche Theorie stimmt. Tatsächlich zeigen Versuche mit Photonen, Ionen und Protonen, dass die Quantenphysik die richtige ist und wir daher die Lokalitätsannahme aufgeben müssen. Das bedeutet, dass unsere Theorie von den verborgenen Parametern nicht stimmen kann und sich die Teilchen scheinbar doch auch über die Entfernung hinweg gegenseitig beeinflussen können.

1.7.4 Verschränkung

1.23 Definition Sei $|\psi\rangle$ ein Zweiteilchenzustand. Der Zustand heißt separabel (= nicht verschränkt), wenn er sich als Tensorprodukt der einzelnen Qubits hinschreiben lässt:

$$|\psi\rangle = |a_1\rangle \otimes |a_2\rangle$$

Andernfalls heißt er verschränkt.

1.24 Beispiele

1. Der Zustand $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ ist seperabel, da man ihn umschreiben kann als $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$.
2. Hingegen ist der Zustand $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ verschränkt, da man ihn nicht als Produkt aufspalten kann.

Die Beispiele kann man auch anschaulicher betrachten. Angenommen Alice besitzt im zweiten Beispiel das erste und Bob das zweite Bit. Egal in welcher Basis Alice ihr Bit misst, Bob wird immer das gegenteilige Ergebnis erhalten, falls er in der gleichen Richtung misst. Misst also Alice in der Basis h/v, so kann der Zustand in einen der beiden Folgezustände $|01\rangle$ (hier

hätte Alice das Ergebnis 0 und Bob 1) oder $|10\rangle$ übergehen. Misst sie in der Basis $+/-$, so ist der Folgezustand[1] entweder $|-+\rangle$ oder $|+-\rangle$ und wieder erhält Bob das gegenteilige Ergebnis, falls er zufällig in der gleichen Basis misst. Das Ergebnis war vor der Messung aber immer unbestimmt. Die Teilchen sind somit verschränkt. Misst Bob nun im ersten Beispiel sein Teilchen (sein Ergebnis kann nur 0 sein) in der Basis h/v, so kann der Zustand entweder in

$$|\psi'\rangle = |00\rangle$$

oder in

$$|\psi'\rangle = |10\rangle$$

übergehen. Alice kann also bei Messung in gleicher Basis sowohl 0 oder 1 als Ergebnis erhalten. Der Zustand war somit nicht verschränkt. Genauso ist der Zustand

$$|00\rangle$$

nicht verschränkt, da zwar Alice und Bob immer das gleiche Resultat bekommen, das Ergebnis (Bit 0) aber schon vor der Messung mit Sicherheit feststeht.

1.7.5 Bell-Zustände

Die vier Bell-Zustände sind die einzigen maximal verschränkten Zweiteilchenzustände. Es sind dies:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Benannt sind sie nach dem Physiker John Bell (1928–1990), der auch für die Bell-Ungleichung berühmt geworden ist.

Neben den maximal verschränkten Zuständen gibt es natürlich auch solche, die nur teilweise verschränkt sind. Zum Beispiel ist der Zustand

$$|\psi\rangle = \frac{2}{\sqrt{5}}|00\rangle + \frac{1}{\sqrt{5}}|11\rangle$$

nicht maximal verschränkt. Bei der Messung in der Basis h/v bekommen zwar Alice und Bob stets das gleiche Ergebnis, allerdings nicht mit gleicher Wahrscheinlichkeit. So tritt hier das Ergebnis 0 viel häufiger als 1 auf.

[1] es gilt $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|-+\rangle - |+-\rangle)$, wie man leicht nachrechnen kann

2 Allgemeines zur klassischen Kryptographie

Kryptographie (von griechisch: $\kappa\rho\upsilon\pi\tau o\sigma$ = verborgen, $\gamma\rho\alpha\phi\epsilon\iota\nu$ = schreiben) wurde bereits nachweislich 400 Jahre vor Christi Geburt verwendet. 1949 wurde von C. Shannon der erste Artikel zu diesem Thema veröffentlicht. Ab diesem Zeitpunkt wurde Kryptographie ein Teil der Mathematik und der Informationstheorie. Allerdings benötigt man für die Schlüsselübertragung immer ein physikalisches System. Das bedeutet, dass man die mathematische Struktur von den zugrunde liegenden physikalischen Gesetzen nicht trennen kann. Die Quantenkryptographie ist aber selbst ein physikalisches System.

Gewöhnlicherweise wollen zwei Personen eine geheime Nachricht austauschen. Wir möchten diese zwei Personen gleich Alice und Bob nennen, wie es jetzt in der Quantenkryptographie üblich geworden ist. Ein Lauscher oder eine Lauscherin trägt den Namen Eve (englisch: to eavesdrop = lauschen).

2.1 One-Time-Pads

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.

2.1 Erster Schritt: Schlüssel erzeugen Um eine Nachricht geheim zu Überbringen muss zuerst ein Schlüssel generiert werden. Dieser sollte aus einer Folge von zufälligen Bits bestehen.

$$k_1, \ldots, k_m \in \{0, 1\}$$

Im klassischen Fall treffen sich die zwei Personen dazu auf einer einsamen Insel und vereinbaren den Schlüssel. Die Folge der Nullen und Einsen wird (zumindest in Filmen) auf einem Abreißblock notiert. Auf jedem Zettel findet sich ein Bit. Daher stammt auch der Name One Time Pad (wörtlich übersetzt: Einmalblock). Anschließend fahren beide wieder nach Hause und verwahren den Schlüssel sicher bis zur Verwendung. War der Schlüssel aufgebraucht, mussten sie sich wieder treffen, denn die Verschlüsselung ist nur sicher, wenn der Schlüssel genauso lange wie die Nachricht selbst ist und nur einmal verwendet wird.

2.2 Zweiter Schritt: Verschlüsseln Alice hat eine Nachricht, die sie an Bob senden möchte. Diese muss sie nun in eine Binärfolge (zum Beispiel mit dem ASCII-Code) umwandeln. Sie erhält dann den Klartext $a_1, \ldots, a_m$. Mit der binären Addition $\oplus$ addiert sie nun den Schlüssel dazu:

$$a_1 \oplus k_1, \ldots, a_m \oplus k_m \in \{0, 1\}$$

$\oplus$	0	1
0	0	1
1	1	0

Klartext	101000101011
Schlüssel	100011010101
Kryptotext	001011111110

Dadurch erhält Alice den Kryptotext, den sie weiter an Bob schickt.

2.3 Dritter Schritt: Entschlüsseln Bob hat nun die verschlüsselte Nachricht erhalten. Er erhält den Klartext, den Alice ihm geschickt hat, indem er nochmals den Schlüssel addiert.

$$a_1 \oplus k_1 \oplus k_1, \ldots, a_m \oplus k_m \oplus k_m = a_1, \ldots, a_m$$

Kryptotext	001011111110
Schlüssel	100011010101
Klartext	101000101011

Wenn nun Eve den Kryptotext ohne Kenntnis des Schlüssels irgendwo abfängt, so kann sie nichts damit anfangen, da dies genauso wie der Schlüssel eine zufällige Folge von Bits ist.

Die Vernam Verschlüsselung ist also 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.

Der Nachteil dieser Art von Verschlüsselung ist allerdings, dass es so gut wie gar nicht für Bankgeschäfte, e-mails oder sonstiges geeignet ist, da man sich immer treffen muss, um den Schlüssel auszumachen. Denn sendet man den Schlüssel über einen klassischen Kanal (z.B. Telefon), so kann jederzeit ein Lauscher die Information mithören. Diese Lücke schließt die Quantenkryptographie. Dabei kann der Schlüssel mittels einen Quantenkanal generiert werden, der absolut sicher gegen Lauschattacken aufgrund der Quantengesetze ist.

3 Quantenkryptographie – Protokolle

Bei der Quantenkryptographie geht es hauptsächlich um die sichere Erzeugung eines Schlüssels zwischen zwei oder mehreren Personen, ohne dass diese sich an einem Ort treffen müssen. Die Sicherheit bei der Übertragung von Qubits über einen Quantenkanal ist im Gegensatz zum klassischen Kanal durch zwei physikalische Tatsachen gesichert:

1. No Cloning Theorem: Quantenzustände können nicht kopiert werden (siehe Abschnitt 6)
2. Messung an einem Qubit verändert den Zustand

Zwei Nachteile bleiben aber dennoch bestehen.

1. Die Nachricht ist vor der Verschlüsselung und nach der Entschlüsselung unsicher. D.h. Eve könnte zum Beispiel Alice oder Bob über die Schulter schauen.
2. Die Sicherheit hängt von der technischen Umsetzung jeder einzelnen Komponente ab.

Für die Umsetzung gibt es mittlerweile schon mehrere Ideen (Protokolle). Ein Protokoll nennt man die Abfolge der Schritte zur Durchführung eines kryptographischen Schemas. Die bekanntesten Quantenkryptographieprotokolle sind das BB84- und das Ekert-Protokoll, die nun genauer erklärt werden.

3.1 BB84-Protokoll

1984 wurde von Charles Bennett (IBM) und Gilles Brassard (Universität Montreal) ein Quantenkryptographie-Protokoll entwickelt. Mittlerweile wurde es auch schon öfters in der Realität erprobt und ist bekannt unter dem Namen BB84.

Das Schema beinhaltet zwei wichtige Teile. Im ersten werden über den Quantenkanal geheime Schlüsselqubits von Alice an Bob gesendet. Im zweiten tauschen sich die beiden darüber aus, welche Basen sie jeweils verwendet haben. Dies kann durchaus öffentlich erfolgen (z.B. in der Zeitung).

Im Folgenden werden die einzelnen Teile genauer erklärt werden. Ein durchgerechnetes Beispiel zu allen Schritten findet sich in den Tabellen 3.1, 3.2 und 3.3 (nach [2]).

3.1 Erster Schritt: Alice erstellt zwei Zufallsfolgen Alice erzeugt im ersten Schritt eine zufällige Folge von Bits

$$a_1, \dots a_m \in \{0, 1\}$$

und eine zufällige Folge von Messbasen

$$a'_1, \dots a'_m \in \{\oplus, \otimes\},$$

wobei $\oplus$ für die Messbasis h/v und $\otimes$ für die Messbasis $+/-$ steht. Diese Folgen kann man sowohl mit einem klassischen- oder auch mit einem Quantenzufallsgenerator erstellen.

3.2 Zweiter Schritt: Alice erstellt und versendet ein Qubit In diesem Schritt möchte Alice einen der vier Zustände $|0\rangle$, $|1\rangle$, $|+\rangle$ oder $|-\rangle$ erzeugen. Dazu kombiniert sie die zuvor generierten Zufallsfolgen wie folgt:

	$a_i = 0$	$a_i = 1$
$a'_i = \oplus$	$\|0\rangle$	$\|1\rangle$
$a'_i = \otimes$	$\|+\rangle$	$\|-\rangle$

Die vier Zustände erhält sie jeweils mit Wahrscheinlichkeit $\frac{1}{4}$. Ist zum Beispiel ihr erstes Zufallsbit $a_1 = 1$ und ihre erste Zufallsbasis $a'_1 = \oplus$, so bekommt sie den Zustand $|1\rangle$.

Anschließend schickt Alice das erhaltene Zufallsbit an Bob. Dabei kann es allerdings auch passieren, dass Bob ein Bit nicht bekommt. Ihre zwei Zufallsfolgen merkt sie sich. Diese wird sie später beim öffentlichen Austausch wieder brauchen.

3.3 Dritter Schritt: Bob misst das Qubit Nun wählt Bob eine Zufallsfolge von Messbasen

$$b'_1, \dots b'_m \in \{\oplus, \otimes\}.$$

Das erhaltene Qubit misst er in eben dieser Basis. Als Ergebnis bekommt er ein klassisches Bit $\in \{0, 1\}$, das er als b_i abspeichert. Die Messergebnisse hängen folgendermaßen von Alice gesendeten Qubit, das Bob natürlich nicht kennt, ab:

	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$b'_i = \oplus$	0	1	$0 \vee 1$	$0 \vee 1$
$b'_i = \otimes$	$0 \vee 1$	$0 \vee 1$	0	1

Hat zum Beispiel Alice den Zustand $|+\rangle$ gesendet und Bob misst ihn in der Basis $\otimes$, so erhält er das Bit $b_i = 0$. Hätte er in der Basis $\oplus$ gemessen, so hätte er mit jeweils gleicher Wahrscheinlichkeit das Ergebnis $b_i = 0$ oder $b_i = 1$ erhalten.

Die Wahrscheinlichkeit dafür, dass Bob die gleiche Zufallsbasis wie Alice wählt ist genau $\frac{1}{2}$, da es nur zwei Basen zur Auswahl gibt. Daher wird Bob auch nicht immer das gleiche Zufallsbit erhalten. Dazu muss es noch einen weiteren wichtigen Schritt geben, um die erhaltenen Bits auch verwenden zu können. Dies kann über einen öffentlichen Kanal geschehen.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Alice Zufallsbit	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Alice Zufallsbasis	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$
Photon, das Alice an Bob schickt	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Bobs Zufallsbasis	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\oplus$
Bits, die Bob erhält	1	—	1	—	1	0	0	0	—	1	1	1	—	0	1

Tabelle 3.1 Senden und Messen der Photonen

3.4 Vierter Schritt: Alice und Bob vergleichen ihre Basen Da Bob mit Wahrscheinlichkeit $\frac{1}{2}$ ein anderes Bit als Alice erhält, wenn er mit einer anderen Basis misst, können diese Bits nicht für den Schlüssel verwendet werden. Dazu vergleichen sie ihre Zufallsfolge der Messbasen. Ist $a'_i = b'_i$, so wird das dazugehörige Bit a_i $(= b_i)$ zu den Schlüsselbits hinzugefügt. Gilt $a'_i \neq b'_i$, so wird das entsprechende Bit von der Liste gelöscht, da diese Bits ja nicht übereinstimmen müssen.

Zusätzlich teilt Bob Alice mit, wann er überhaupt ein Bit erhalten hat. Es kann durchaus vorkommen, dass ein Qubit auf dem Weg verloren geht. Diese müssen klarerweise ebenfalls von der Liste gelöscht werden.

Die Messungen, bei denen Bob ein Bit erfolgreich erhalten hat und auch die Basis stimmt, wurden in der Tabelle 3.2 zur besseren Übersicht gelb gefärbt.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Alice Zufallsbit	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Alice Zufallsbasis	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$
Photon, das Alice an Bob schickt	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$
Bobs Zufallsbasis	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\oplus$
Bits, die Bob erhält	1	—	1	—	1	0	0	0	—	1	1	1	—	0	1

Tabelle 3.2 öffentlicher Vergleich der Basen

3.5 Fünfter Schritt: Alice und Bob testen, ob sie belauscht wurden Zusammenfassend folgt nach den Postulaten der Quantenmechanik, falls es einen Lauschangriff von Eve gibt, dass jede Messung, die nicht zufällig in der gesendeten Basis (die Eve nicht kennt) erfolgt, den Zustand verändert. Das bedeutet, dass Bob trotz Messung in gleicher Basis zu einer gewissen Wahrscheinlichkeit ein falsches Bit b_i erhält.

Um also einen Lauschangriff zu entdecken, müssen sie nur ein paar zufällige Schlüsselbits (z.B. jedes dritte) auswählen und miteinander vergleichen (siehe Tabelle 3.3). Die verglichenen Bits müssen sie aber klarerweise von der Liste streichen. Stimmen sie überein, so wurde mit hoher Wahrscheinlichkeit nicht gelauscht. Ist die Fehlerrate zu hoch[2], so könnte Eve gelauscht haben und daher müssen sie alle Bits verwerfen und nochmals neu beginnen. Die Fehlerrate erhält man, indem man die fehlerhaften Bits durch die Anzahl aller Bits dividiert.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
erhaltene Information nach dem Basisvergleich			1		1			0				1		0	1
Bob wählt ein paar Schlüsselbits zufällig für den Vergleich aus					1									0	
Alice prüft sie					✓									✓	
Alice und Bobs geheime Schlüsselbits			1					0				1			1

Tabelle 3.3 Vergleich von zufällig ausgewählten Schlüsselbits

3.1.1 Zusammenfassung

Nun folgt eine kurze Zusammenfassung (nach [3]) aller Schritte für die Schlüsselerzeugung.

1. Alice erzeugt eine zufällige Folge von Bits $a_1, \dots a_m \in \{0, 1\}$ und eine zufällige Folge von Messbasen $a'_1, \dots a'_m \in \{\oplus, \otimes\}$.

2. Alice kombiniert ihre Folgen von Zufallsbits wie folgt:

	$a_i = 0$	$a_i = 1$
$a'_i = \oplus$	$\|0\rangle$	$\|1\rangle$
$a'_i = \otimes$	$\|+\rangle$	$\|-\rangle$

[2] eine gewisse Fehlerrate ist durch die Geräte immer gegeben. Genaueres findet man im Kapitel 6.1

und schickt den erhaltenen Zustand anschließend an Bob.

3. Bob wählt eine zufällige Folge von Messbasen $b'_1, \ldots b'_m \in \{\oplus, \otimes\}$ und misst das i-te Qubit von Alice in der jeweiligen Basis. Das erhaltene Ergebnis speichert er unter b_i ab.

4. Alice und Bob tauschen sich öffentlich darüber aus, welche Photonen erfolgreich erhalten wurden und welche in der korrekten (= gleichen) Basis gemessen wurden. Ist $a'_i \neq b'_i$ werden a_i und b_i nicht verwendet.

5. Alice und Bob tauschen k der nicht gelöschten Bits aus und ermitteln die Fehlerrate. Ist diese zu hoch, so verwenden sie diese Bits nicht, da hier Verdacht auf einen Lauschangriff besteht.

3.2 Ekert-Protokoll

Das Ekert-Protokoll wurde unabhängig vom BB84-Protokoll von Artur K. Ekert 1991 entwickelt, ist ihm aber trotzdem sehr ähnlich. Das Schema ist auch unter E91-Protokoll bekannt. Der große Unterschied zum BB84 besteht darin, dass hier die Verschränkung für die Schlüsselverteilung genutzt wird. In Ekerts Originalveröffentlichung [4] misst Ekert nicht die Polarisation sondern den Spin. Wir verwenden aber wieder die Polarisation. Ein Beispiel zu den einzelnen Schritten ist wiederum in den Tabellen 3.4 und 3.5 zu finden.

Außerdem werden hier vier verschiedene Messbasen für die Photonen verwendet. Anstatt der Basen werden aber der Übersicht halber nur die Winkel in der sie bezüglich der h/v-Basis gedreht sind angegeben (siehe auch Abb. 3.1). Nur zwei Winkel haben Alice und Bob gemeinsam, der dritte ist verschieden. α_1 bis α_3 sind die Winkel von Alice und β_1 bis β_3 die von Bob.

$$\begin{aligned} \alpha_1 &= \frac{\pi}{8} & \beta_1 &= \frac{\pi}{8} \\ \alpha_2 &= \frac{\pi}{4} & \beta_2 &= \frac{\pi}{4} \\ \alpha_3 &= 0 & \beta_3 &= \frac{3\pi}{8} \end{aligned}$$

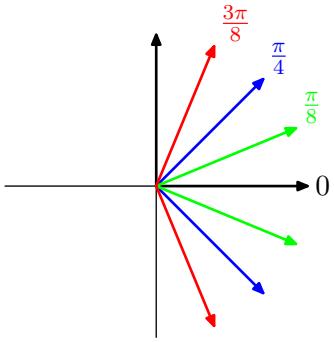


Abbildung 3.1 Die vier verschiedenen Messbasen

3.6 Erster Schritt: Ein verschränkter Zustand wird erzeugt Zuallererst muss ein verschränktes Teilchenpaar für die Übertragung zur Verfügung stehen. In der Praxis wird der Bell-Zustand

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

verwendet. Anschließend erhält Alice das erste und Bob das zweite Teilchen. Ihre Ergebnisse bei Messung in gleicher Basis werden antikorreliert sein, das bedeutet, dass entweder Alice oder Bob die erhaltenen Bits invertieren muss.

3.7 Zweiter Schritt: Alice und Bob wählen ihre Zufallsfolgen Alice wählt eine zufällige Folge von ihren Richtungen

$$a'_1, \ldots, a'_m \in \{\alpha_1, \alpha_2, \alpha_3\}.$$

Auch Bob wählt eine zufällige Folge aus seinen Richtungen

$$b'_1, \ldots, b'_m \in \{\beta_1, \beta_2, \beta_3\}.$$

Beide führen nun Polarisations-Messungen in der jeweiligen Richtung durch. Als Messergebnisse erhalten sie dann eine Folge von Bits $a_1, \ldots, a_m$ bzw. $b_1, \ldots, b_m$.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Alice Zufallsbasis	α_1	α_1	α_2	α_1	α_3	α_1	α_1	α_2	α_1	α_3	α_2	α_1	α_2	α_2	α_1
Bits, die Alice erhält	0	—	1	0	1	1	0	—	1	0	1	1	0	0	0
Bobs Zufallsbasis	β_2	β_2	β_2	β_3	β_2	β_2	β_3	β_1	β_2	β_1	β_2	β_3	β_1	β_1	β_1
Bits, die Bob erhält	1	—	1	—	1	0	0	0	—	1	1	1	—	0	0

Tabelle 3.4 Messen der Photonen

3.8 Dritter Schritt: Alice und Bob vergleichen ihre Basen Wie auch im BB84-Protokoll können sie für die Schlüsselbits nur diejenigen verwenden, bei denen sie auch in denselben Richtungen gemessen haben. Daher vergleichen sie diese über einen öffentlichen Kanal. Diesmal muss sowohl Bob als auch Alice die Nummer der Teilchen bekannt geben, die sie auch wirklich registriert haben, denn es kann hier im Gegensatz zu BB84 auch vorkommen, dass Alice kein Teilchen erhält. Als Schlüsselbits nehmen sie also nur diejenigen, bei denen beide Teilchen erhalten haben und wo sie in der gleichen Richtung gemessen haben.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Alice Zufallsbasis	α_1	α_1	α_2	α_1	α_3	α_1	α_1	α_2	α_1	α_3	α_2	α_1	α_2	α_2	α_1
Bits, die Alice erhält	0	—	1	0	1	1	0	—	1	0	1	1	0	0	0
Bobs Zufallsbasis	β_2	β_2	β_2	β_3	β_2	β_2	β_3	β_1	β_2	β_1	β_2	β_3	β_1	β_1	β_1
Bits, die Bob erhält	1	—	1	—	1	0	0	0	—	1	1	1	—	0	0
Alice und Bobs geheime Schlüsselbits			1								1				0

Tabelle 3.5 öffentlicher Austausch

3.9 Vierter Schritt: Alice und Bob testen, ob sie belauscht wurden Den anderen Teil der Bits, bei denen sie in unterschiedlichen Richtungen gemessen haben, verwenden sie, um zu testen, ob jemand gelauscht hat. Die einzige halbwegs sinnvolle Möglichkeit die Eve

hier hat, ist ein drittes Teilchen mit dem versendeten Bell-Zustand zu verschränken. Da aber bei zwei maximal verschränkten Teilchen kein drittes dazu verschränkt werden kann, sondern nur reparabel zu den anderen zwei sein kann, fällt diese Lauschattacke durch Eve auf. Dazu testen Alice und Bob mit den Bits, bei denen sie in unterschiedlichen Richtungen gemessen haben, die CHSH-Ungleichung. Dies ist eine Variante der Bell-Ungleichung. Wird diese nicht verletzt, so wurde mit hoher Wahrscheinlichkeit gelauscht. Eine genauere Erklärung zur CHSH-Ungleichung findet sich im Kapitel 6.

3.2.1 Zusammenfassung

Hier findet der Leser das ganze Protokoll nochmals kurz zusammengefasst.

1. Ein Quantenpaar im verschränkten Zustand

   $$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

   wird erzeugt. Ein Teilchen davon erhält Alice, das andere Bob.

2. Alice wählt eine Zufallsfolge von Messbasen $a_1, \dots a_m \in \{\alpha_1, \alpha_2, \alpha_3\}$.

   Bob wählt eine Zufallsfolge von Messbasen $b_1, \dots b_m \in \{\beta_1, \beta_2, \beta_3\}$.

   Beide messen ihre erhaltenen Qubits in der jeweiligen Basis.

3. Alice und Bob tauschen sich über einen öffentlichen Kanal aus, welche Teilchen sie erhalten haben und bei welchen sie in der gleichen Basis gemessen haben. Diese behalten sie für die Schlüsselbits.

4. Alice und Bob testen mit den Bits, bei denen sie in unterschiedlichen Basen gemessen haben die CHSH-Ungleichung. Besteht Verdacht auf Lauschen, so werden alle schon erhaltenen Schlüsselbits verworfen.

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.

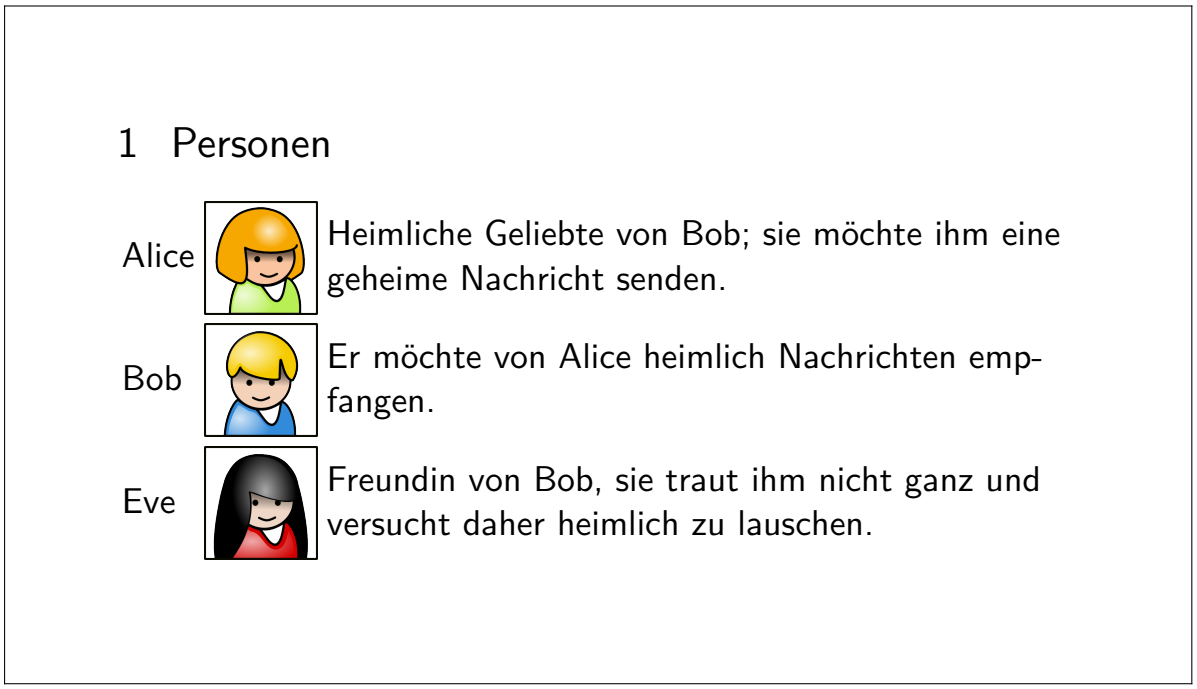


Abbildung 4.1 Ausschnitt aus der ersten Folie

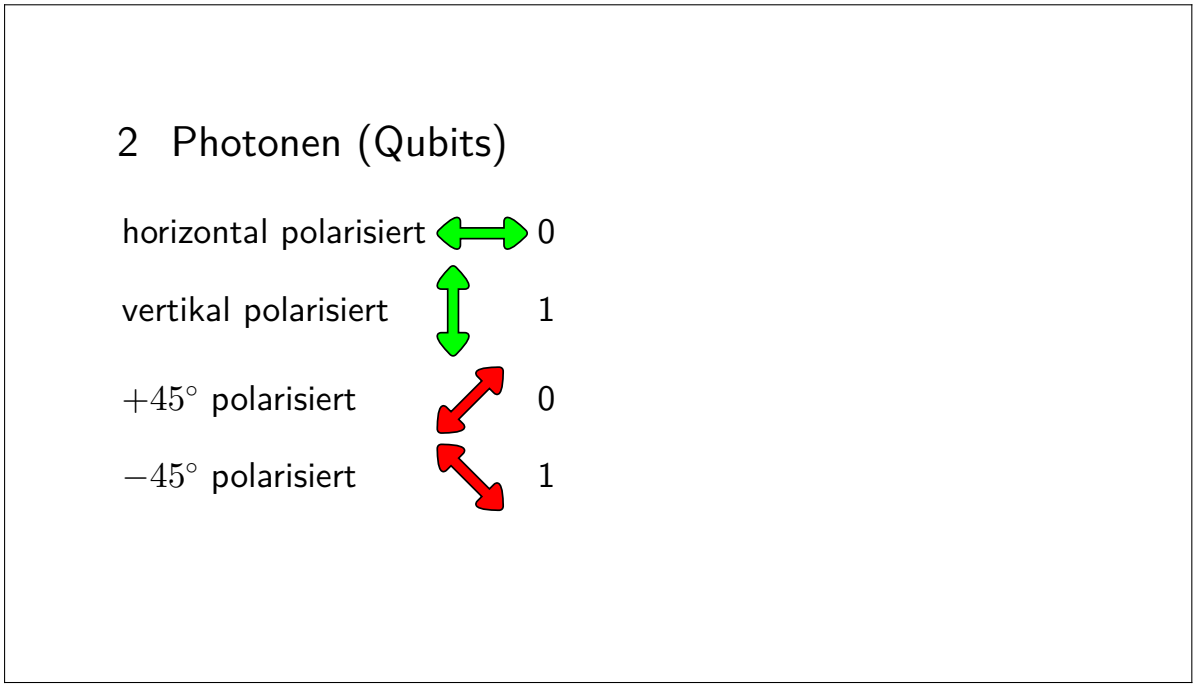


Abbildung 4.2 Ausschnitt aus der ersten Folie

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.

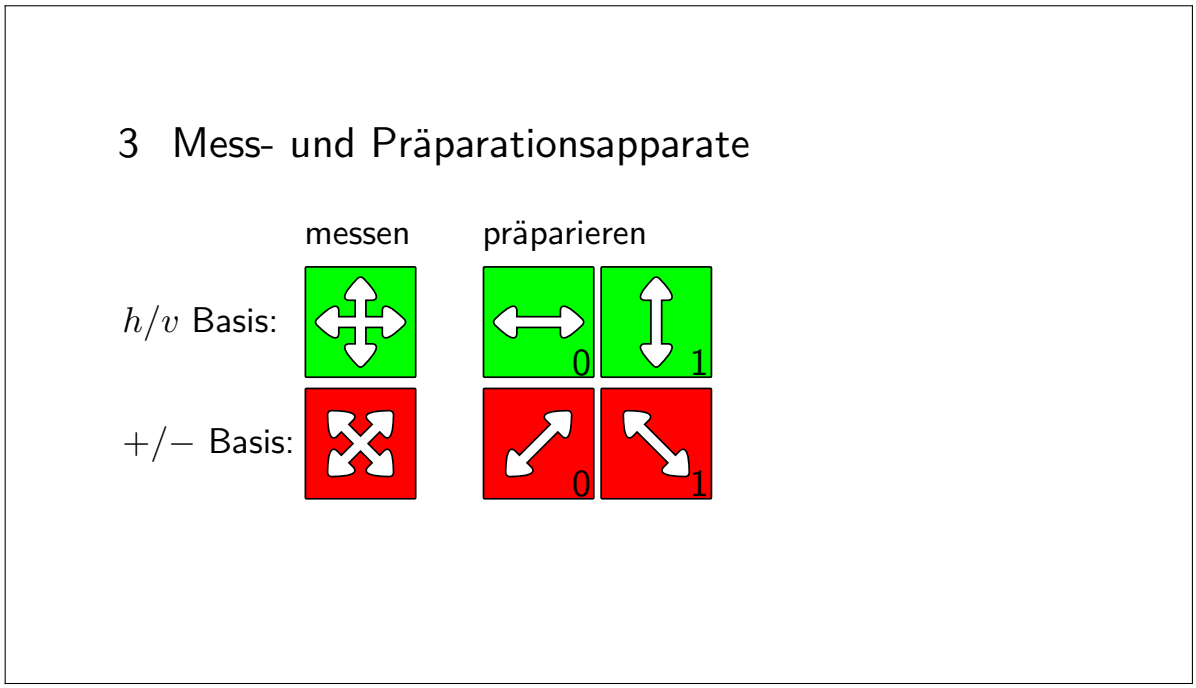


Abbildung 4.3 Ausschnitt aus der ersten Folie

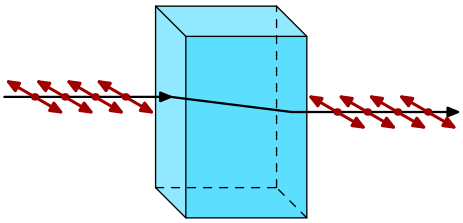
Für die Präparation von Zuständen kann man zum Beispiel Polarisationsfilter verwenden. Diese werden einfach in die gewünschte Richtung gedreht, sodass dann einer dieser vier Zustände herauskommt. Wir bezeichnen eine Präparation eines Photons in horizontaler bzw. vertikaler Richtung als in der Basis h/v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

4.1.2 Zweite Folie: Messung

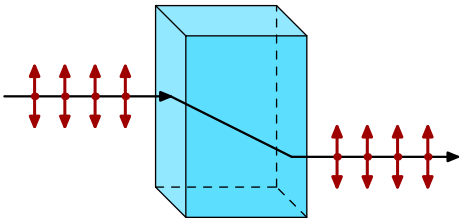
In dieser Folie (siehe Abb. 4.5 und 4.6) spielen die Komponenten nun zusammen. Ein Photon wird zuerst präpariert und anschließend gemessen. Dabei werden verschiedene Fälle untersucht.

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.

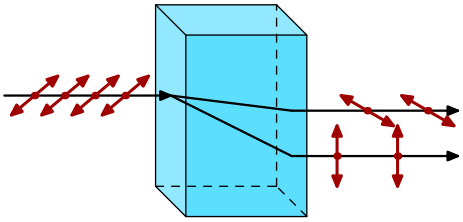
Wie sieht das aber aus, wenn ich ein Photon in einer anderen Basis messe, als ich es präpariert habe? Nehmen wir den Fall, in dem das Photon vertikal präpariert wird, aber in der Basis $+/-$ gemessen wird. Da das Teilchen nicht durch den Messapparat durchgehen kann, ohne verändert zu werden, geht es 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:

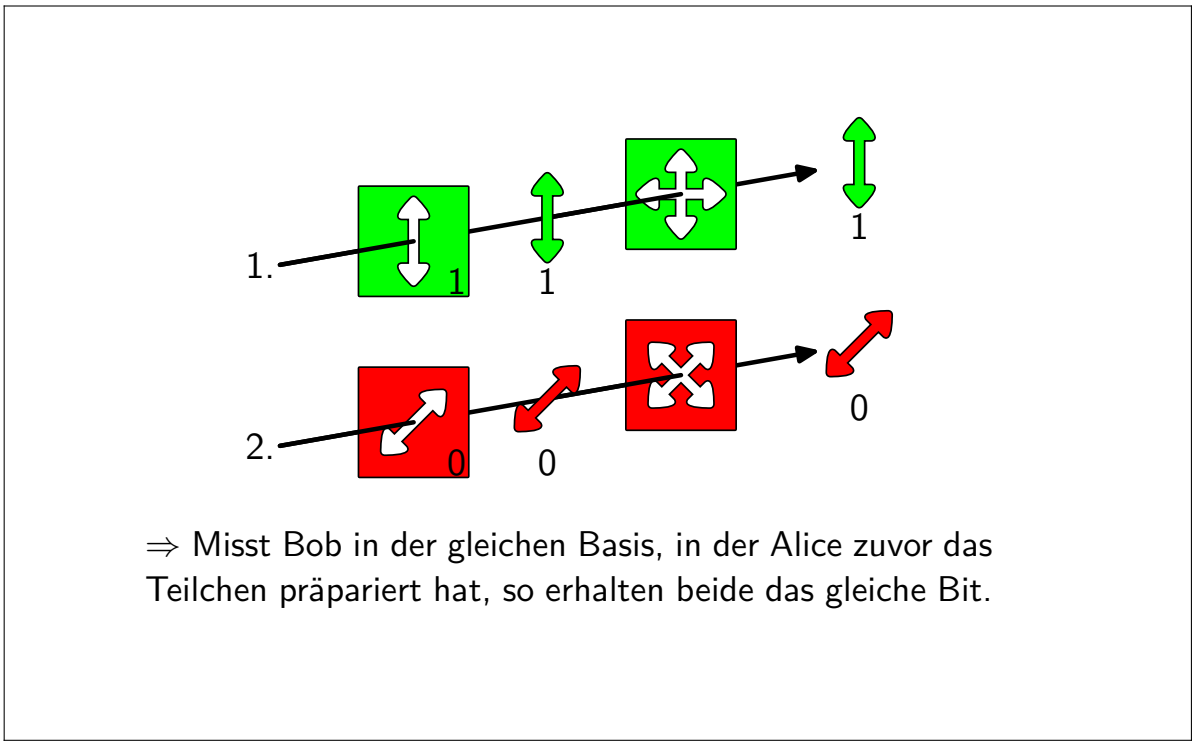


Abbildung 4.5 Ausschnitt aus der zweiten Folie

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

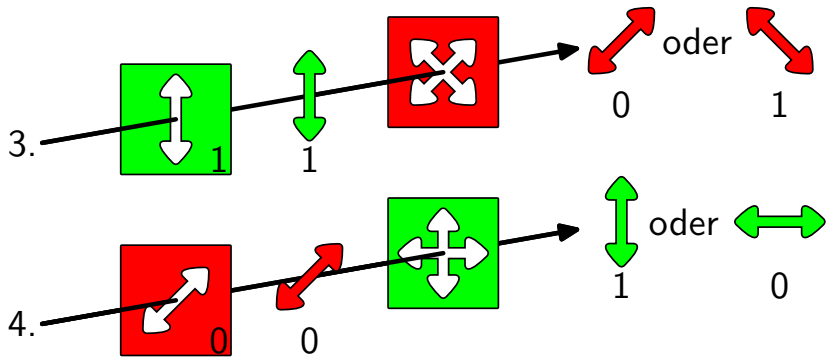
Auf diese Weise erhält man mathematisch das intuitive Ergebnis von oben.

4.2 Klassische Kryptographie

Dieses Kapitel würde sich gut für »Minireferate« eignen. Dazu bekommen die SchülerInnen kurze Texte zugeordnet, die sie sich in ca. 5-10 Minuten durchlesen sollen. Da es weniger Themen als SchülerInnen gibt, haben mehrere den gleichen Text. Anschließend soll immer einer aus der Themengruppe (vom Lehrer/von der Lehrerin bestimmt oder auf freiwilliger Basis) das Gelesene kurz vortragen. Dies ist, glaube ich, eine nette Methode, weil die SchülerInnen dadurch lernen, spontan etwas vor der Klasse vorzutragen. Außerdem eignet es sich gut für einen leistungsdifferenzierten Unterricht, da die Themen einen leicht unterschiedlichen Schwierigkeitsgrad aufweisen.

Die Minireferatsthemen (die Texte zum Kopieren finden sich auf der CD) behandeln folgende Punkte und sollten auch in dieser Reihenfolge vorgetragen werden:

1. Was ist Kryptographie?
2. Verschlüsselung um 400 v.Chr.
3. Cäsar Verschlüsselung
4. Wie man einfache Verschlüsselung knacken kann
5. Vernam-Code



⇒ Misst Bob in der anderen Basis, so kann er entweder das gleiche Bit wie Alice erhalten oder nicht. Die Wahrscheinlichkeiten dafür sind jeweils $\frac{1}{2}$.

Abbildung 4.6 Ausschnitt aus der zweiten Folie

4.2.1 Was ist Kryptographie?

Das erste Thema bildet den Einstieg in die Kryptographie. Es ist eins der leichteren Themen.

Was ist Kryptographie?

Das Wort Kryptographie kommt aus dem griechischen:

kryptós = verborgen

gráphein = schreiben

Zusammengesetzt bedeutet es etwas verborgenes schreiben. Kryptographie ist also die Wissenschaft vom Verschlüsseln und Entschlüsseln von Informationen. Ihre Anwendung findet sie heutzutage bei Bankgeschäften, bei den Geheimdiensten, bei der privaten Nachrichtenübertragung (z.B. e-mails) und vieles mehr.

Kryptographische Verfahren wurden nachweislich schon vor fast 4000 Jahren von den Äqyptern eingesetzt. Auch im alten Griechenland wurden Verschlüsselungsverfahren für militärische Geheimnisse verwendet.

In der Kryptographie geht man stets davon aus, dass das verwendete Verschlüsselungsverfahren dem Lauscher bekannt ist. Dieses Prinzip ist auch unter dem Namen Kerkhoffsches Prinzip (nach Auguste Kerckhoffs von Nieuwenhof; 1835-1903) bekannt.

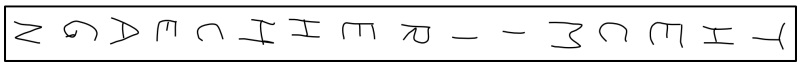
Abbildung 4.7 Erstes Minireferat

4.2.2 Verschlüsselung um 400 v.Chr.

Bei diesem Thema sollte man dem oder der Vortragenden zwei Rollen mit einem Streifen Papier (schon beschriftet) zur Verfügung stellen, sodass er oder sie die Verschlüsselungsmethode anschaulich den anderen KlassenkollegInnen vorführen und zum ausprobieren für alle auch durchgeben kann. Die beiden Rollen sollten einen unterschiedlichen Durchmesser haben, damit der Text, bei der richtigen Rolle herumgewickelt, einen Sinn ergibt und bei der falschen nicht. Dadurch kann vorgezeigt werden, was passiert, wenn jemand den Text abfängt, aber eine Rolle mit falschem Durchmesser hat.

Verschlüsselung um 400 v.Chr.

In Sparta verwendete man 400 v.Chr einen einfachen Holzstab (eine sogenannte Skytale) zur Verschlüsselung von geheimen Botschaften. Diesen umwickelten sie mit einem Leder- oder Pergamentstreifen und schrieben quer dazu die Nachricht darauf. Den Streifen schickten sie dann an die Person, für die die Nachricht gedacht ist. Jemand, der die Botschaft abfing, konnte diese nicht entziffern, wenn er nicht zufällig einen Holzstab mit gleichem Durchmesser hatte.



Natürlich war der richtige Stab nicht im Besitz des Boten. Heutzutage sind diese Methoden leicht entschlüsselbar. Damals kam aber noch die Hürde dazu, dass nur wenige schreiben und lesen konnten.

Abbildung 4.8 Zweites Minireferat

4.2.3 Cäsar Verschlüsselung

Für dieses Referatsthema sollte man eine Chiffrierscheibe zur Demonstration zur Verfügung stellen. Ein Modell zum Ausschneiden findet sich im Anhang bzw. auf der CD. Es würde aber auch eine gute Darstellung auf der Tafel reichen. Für die Klasse wäre es auch interessant, ihnen einen verschlüsselten Text auf die Tafel zu schreiben, den Sie dann mit Hilfe der Scheibe entschlüsseln können. Dazu sollte die Scheibe im Anschluss an das Referat durchgegeben werden oder jeder Schüler/ jede Schülerin bastelt sich eine eigenen Scheibe.

Cäsar-Verschlüsselung

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.

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

Cäsar kannte allerdings die Chiffrierscheibe noch nicht. Mit ihr kann man ganz leicht einen Geheimtext entschlüsseln, indem man alle 26 Möglichkeiten ausprobiert. Dazu muss man den inneren Teil der Scheibe solange verdrehen, bis der damit entschlüsselte Text einen Sinn ergibt.

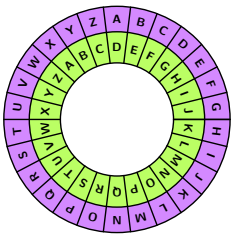


Abbildung 4.9 Drittes Minireferat

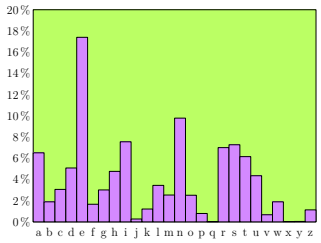
4.2.4 Wie man einfache Verschlüsselung knacken kann

Hier wäre es praktisch, die Häufigkeitstabelle der Buchstaben auf eine Overheadfolie (oder Folie für Beamer) zu kopieren und zur Verfügung zu stellen. Aber auch hier würde eine schematische Zeichnung auf der Tafel ausreichen.

Wie man einfache Verschlüsselung knacken kann

Eine Möglichkeit einen Text zu verschlüsseln besteht darin, die Buchstaben des Alphabets beliebig zu vertauschen. So schreibt man zum Beispiel statt einem A ein R, statt einem B ein E und so weiter. Man kann sich überlegen, dass es $26! \approx 4 \cdot 10^{26}$ Möglichkeiten für diese Art der Vertauschung gibt. Selbst wenn ein Lauscher also jede durchprobieren würde und dafür nur je eine Sekunde bräuchte, würde das die Lebensdauer des Universums um einiges übertreffen.

Trotzdem ist diese Verschlüsselung leicht zu entziffern: Da die Buchstaben in einem Text nicht alle gleich häufig vorkommen, kann man mit Hilfe einer Häufigkeitstabelle den Geheimtext entschlüsseln.



So sieht man zum Beispiel, dass das E in der deutschen Sprache um einiges häufiger als alle anderen Buchstaben vorkommt. Zum Entschlüsseln einer geheimen Nachricht braucht man also im ersten Schritt nur den häufigsten Buchstaben herauszufinden. Ist dies zum Beispiel ein R, so wurden wahrscheinlich alle E durch ein R ersetzt. Das gleiche macht man mit dem zweithäufigsten Buchstaben dem N und so weiter. Natürlich kann es sein, dass am Schluss ein paar Fehler passiert sind, aber das menschliche Gehirn ist dazu fähig, auch Texte, in denen einige Buchstaben vertauscht sind, durchaus leicht lesen zu können. In anderen Sprachen sieht die Häufigkeitstabelle etwas anders aus.

Abbildung 4.10 Viertes Minireferat

4.2.5 Vernam-Code

Das wichtigste, längste und auch anspruchsvollste (aber trotzdem nicht schwere) Thema ist der Vernam-Code. Diese Verschlüsselungsmethode sollten sich die SchülerInnen unbedingt merken, da sie diese Methode später im Simulationsprogramm benötigen. Vielleicht ist es gut, die SchülerInnen darauf hinzuweisen sich das eine oder andere zu notieren, oder man fasst als Lehrer/ Lehrerin im Anschluss an die Referate selbst noch einmal das wichtigste an der Tafel zusammen.

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 nächsthöhere Zweierpotenz 32 (= 2^5) 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.

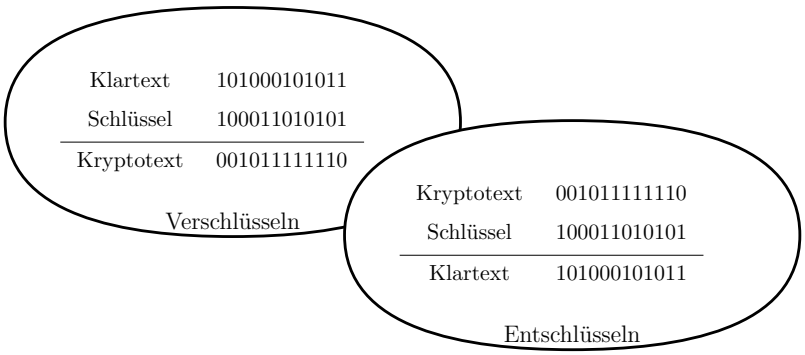


Abbildung 4.11 Fünftes Minireferat

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).

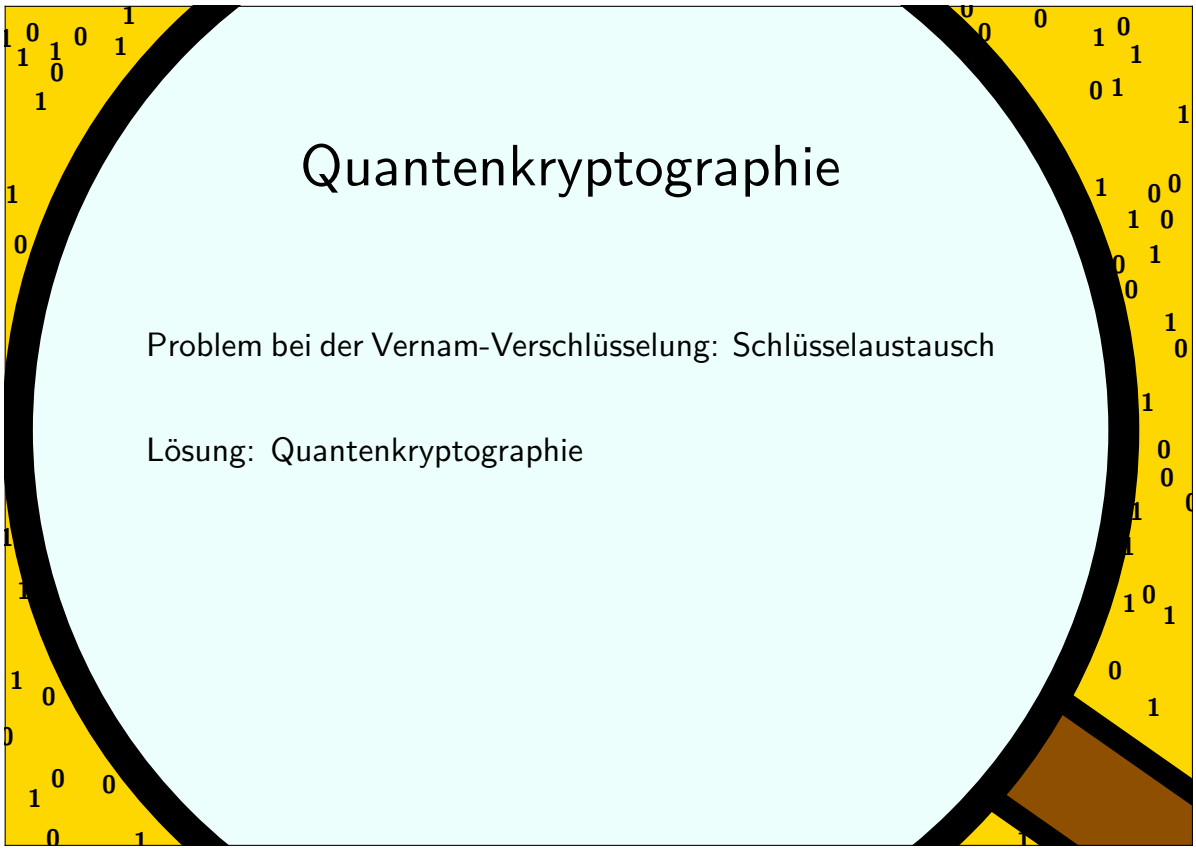


Abbildung 4.12 Dritte Folie

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.

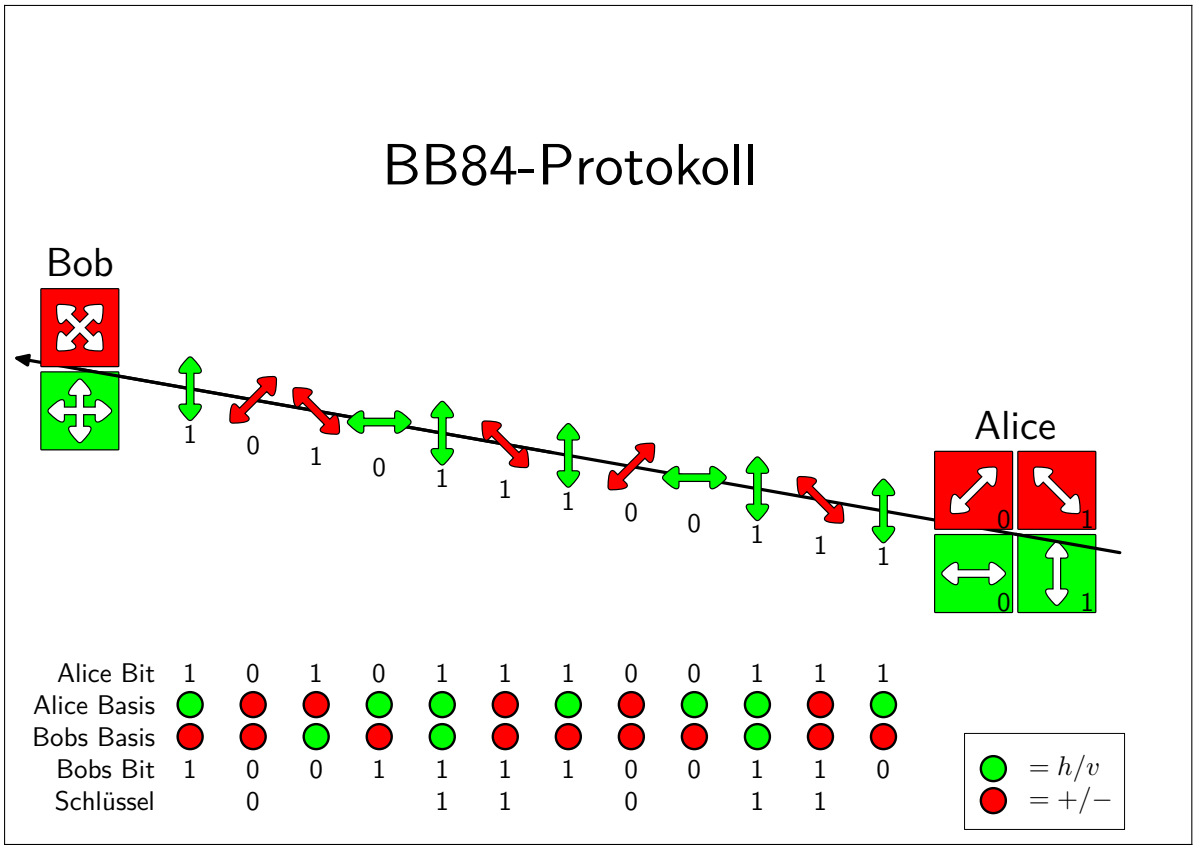


Abbildung 4.13 Vierte Folie

4.3.3 Bell-Ungleichung und Verschränkung

Was Verschränkung ist, könnte man folgendermaßen erklären: Man stelle sich zwei voneinander getrennte Teilchen vor. Führt man die gleiche Messung an beiden Teilchen unabhängig voneinander durch, so liefern sie stets gegengleiche Ergebnisse. Bekommt man also bei einem Teilchen das Ergebnis 0, so erhält man bei dem anderen das Ergebnis 1 und umgekehrt. Die Teilchen scheinen gegenseitig zu wissen, wie sich der jeweils andere während der Messung verhält. Die Messergebnisse waren aber vor der Messung unbestimmt. Diesen Zustand, bei dem das Messergebnis des einen Teilchens, egal in welcher Richtung gemessen wird, vom anderen abhängt, nennt man Verschränkung. Wie kann man das nun erklären?

In der Physik gibt es Experimente, wo solche Teilchen mit dieser Eigenschaft erzeugt wurden. Ein Beispiel ist das Bell-Experiment. Dabei emitiert eine Quelle zwei verschränkte Teilchen, die immer antikorrelierte (= gegengleiche) Ergebnisse liefern.

Wie kann man dieses seltsame Verhalten aber erklären? Um mögliche Erklärungsversuche gemeinsam mit den SchülerInnen zu überlegen, kann man mit ihnen ein anschauliches »Experiment« (nach der Idee von Univ. Doz. Mag. Dr. Beatrix Hiesmayr) durchführen. Dazu sollen vier SchülerInnen freiwillig herauskommen. Zwei davon spielen die Teilchen (Teilchen A und Teilchen B), die anderen zwei die PhysikerInnen (Alice und Bob), die diese messen wollen. Nun sollen sich Teilchen A und Teilchen B mit dem Rücken zueinander aufstellen. Dies soll eine Quelle darstellen, die verschränkte Photonen erzeugt. Anschließend werden die beiden SchülerInnen getrennt. Die beiden sollen nun miteinander verschränkt sein. Im getrennten Zustand (sie dürfen sich nicht ansehen) wird Teilchen A von Alice und Teilchen B von Bob nach einer Richtung gefragt (also oben-unten oder links-rechts) und die Teilchen müssen sich entscheiden, ob sie z.B. nach oben oder nach unten zeigen (nicht sagen, nur mit der Hand deuten). Sie werden so lange gefragt, bis sie bei der Frage nach der gleichen Richtung gleiche Ergebnisse zeigen (also beide zeigen z.B. hinauf). Da die beiden SchülerInnen ja verschränkt sein sollten und daher immer gegengleiche Ergebnisse liefern müssten, kann dies also nicht stimmen und sie müssen sich eine neue Strategie überlegen.

Nun sollte die Klasse überlegen, wie man das Verhalten der Teilchen besser nachvollziehen könnte. Eine Möglichkeit dabei wäre, dass Teilchen A dem Teilchen B nach der Messung mitteilt, wie es sich entschieden hat (also z.B. oben oder unten). Da aber nichts schneller als Licht ist, könnten die Teilchen bei großer Entfernung nicht simultan reagieren. Also ist auch dieser Erklärungsversuch für die Verschränkung hinfällig.

Die Klasse muss sich also eine neue Strategie überlegen. Die letzte Möglichkeit wäre, dass sich Teilchen A und B bei der Quelle ausmachen, bei welcher Richtung sie wohin zeigen. Dies entspricht der Theorie der verborgenen Parameter. Werden sie nun von Alice und Bob gemessen, so liefern sie stets das richtige (gegengleiche) Ergebnis. Dies mag ja für zwei Richtungen funktionieren. Aber wie sieht es aus für 50 oder gar für unendlich viele Richtungen? So wirkt diese Theorie wieder nicht so logisch und tatsächlich hat John Bell (1928-1990) eine Ungleichung gefunden, die ein System mit verborgenen Parametern erfüllen muss. Erst Jahre später konnte diese Ungleichung durch Experimente überprüft werden und es zeigt sich, dass die Quantentheorie die Ungleichung verletzt, dass es also keine verborgenen Parameter geben kann. So musste die Idee, dass ein Objekt ein anders Objekt an einem entfernten Ort nicht beeinflussen kann, aufgegeben werden. Einstein nannte dies »Spukhafte Fernwirkung«. Heute spricht man von Verschränkung. Verschränkte Teilchen können sich also auch über weite Strecken hinweg

gegenseitig beeinflussen. Man sollte sie eher als ein zusammenhängendes System sehen, als zwei getrennte Teilchen.

Wenn man möchte, kann man mit den SchülerInnen (z.B.: Wahlpflichtfach oder Naturwissenschaftlicher Zweig) durchaus auch die mathematische Herleitung der Bell-Ungleichung durchgehen. Siehe dazu Abschnitt 1.7.

4.3.4 Fünfte Folie: Ekert-Protokoll

Das Ekert-Protokoll (siehe Abb. 4.14) wird in zwei Folien erklärt. Als erstes werden an einer Quelle verschränkte Photonenpaare erzeugt. Jeweils eins davon bekommt Alice und das andere Bob. Beide messen ihre Teilchen unabhängig mit einer zufällig gewählten Messbasis. Die Basen und die Ergebnisse wurden in je einer Tabelle auf der Folie dargestellt. Da die Teilchen verschränkt waren, bekommen Alice und Bob immer gegengleiche Ergebnisse, falls sie in der gleichen Basis gemessen haben. Um also einen identischen Schlüssel zu erhalten, müssen sie, wie im BB84-Protokoll, zuerst die Basen vergleichen. Auf der nächsten Folie sind genau diese gelb markiert. Die dazugehörigen Bits müssen entweder von Alice oder von Bob noch invertiert werden. Dann haben sie identische Schlüssel, mit denen sie dann ihre Nachricht geheim verschicken können.

In der folgenden Computersimulation wurde das Invertieren der Bits schon vom Computer automatisch gemacht. Das heißt, dass Alice und Bob bei der Messung in gleichen Basen schon das gleiche Ergebnis erhalten.

Die anderen Schlüsselbits, bei denen sie in unterschiedlichen Basen gemessen haben, verwerfen sie hier im Gegensatz zu BB84 nicht. Im Gegenteil: Alice und Bob tauschen diese (durchaus öffentlich) aus. Die Häufigkeiten davon setzen sie dann in die CHSH-Ungleichung ein und können dadurch feststellen, ob gelauscht wurde. Denn falls sie verletzt wird, kann es keine Eve geben (bzw. sie konnte kaum etwas über den Schlüssel herausgefunden haben). Darum ist das Ekert-Protokoll von der Theorie her besser geeignet, da es gleich einen Test für Lauschattacken mitliefert. Genaueres findet sich im Abschnitt 6.3. Auch technisch ist es leichter umsetzbar.

5 Ein Programm zur Demonstration der Quantenkryptographie

Um den SchülerInnen das Konzept der Quantenkryptographie näher zu bringen, habe ich ein Lernprogramm entwickelt, in dem die SchülerInnen ein Verschlüsselungsschema dazu selbst ausprobieren können.

Umgesetzt habe ich das Programm – namens Geheime Quanten – in der Programmiersprache C# mit dem Framework Mono (Version 2.0) und dem Benutzerinterface GTK unter Linux. Es läuft sowohl in Linux als auch in Windows und auf Mac OS X. Von dem Programm selbst gibt es zwei Versionen: Die erste (Basisversion) kann auf je einem Computer gespielt werden, die zweite (Netzwerkversion) funktioniert über ein Netzwerk, in dem die Computer miteinander verbunden sind. Allerdings ist die Netzwerkversion noch nicht für den Unterricht tauglich, da es noch hin und wieder zu Abstürzen kommt. Sobald das Problem gelöst wird, wird es eine aktuellere Version auf http://homepage.univie.ac.at/heidemarie.knobloch zum Download geben.

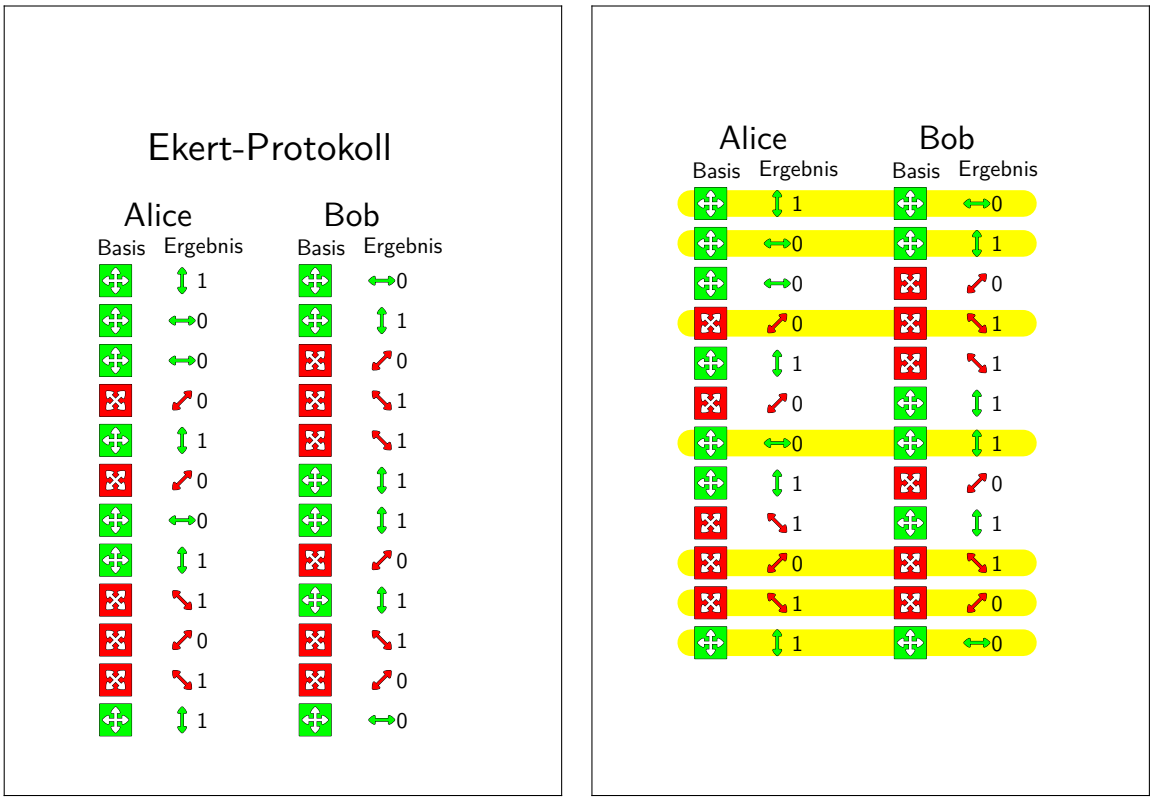


Abbildung 4.14 Fünfter Foliensatz

In der Basisversion kann man auswählen, welches Protokoll (BB84- oder Ekert-Protokoll) simuliert werden soll. Die Netzwerkversion gibt es derzeit nur mit dem BB84-Protokoll. Da ich auch den Quelltext des Programms auf der beigelegten CD und auf der Homepage veröffentlicht habe, kann jeder, der sich damit auskennt, das Programm nach Belieben verändern.

Die Hilfedatei (siehe Anhang D und E) ist unter GNOME in Linux in die Systemhilfe eingebunden und bei allen anderen Betriebssystemen als HTML-Datei vorhanden.

5.1 Basisversion

Im Laufe des Lernprogramms soll Alice an Bob eine mit Hilfe der Quantenkryptographie verschlüsselte Nachricht senden. Bob soll diese dann wieder entschlüsseln. Das Programm ist in vier Abschnitte gegliedert:

Schlüssel erzeugen Im ersten Abschnitt geht es um die Messung bzw. Präparation der Teilchen (je nachdem welches Protokoll verwendet wird). Dabei sollen die SchülerInnen sehen, was passiert, wenn Alice und Bob die Teilchen in der gleichen oder in unterschiedlichen Basen präpariert bzw. gemessen haben.

Basisvergleich Hier sollen die SchülerInnen die Messbasen miteinander vergleichen. Sie erhalten jedenfalls dann den gleichen Schlüssel, wenn sie nur die Messungen auswählen, bei denen in der gleichen Basis gemessen wurde. Natürlich kann es auch vorkommen, das die Ergebnisse bei einer Messung in unterschiedlichen Basen trotzdem zufällig gleich sind.

Nachricht verschlüsseln Im dritten Abschnitt können die SchülerInnen ausprobieren, wie man eine (selbst gewählte) Nachricht, die vom Computer in Nullen und Einsen übersetzt wurde, mit einem Schlüssel verschlüsselt.

Nachricht entschlüsseln Zuletzt können die SchülerInnen sehen, ob sie alles richtig gemacht haben. Nachdem sie die verschlüsselte Nachricht wieder entschlüsselt haben, kommt, wenn alle Schritte richtig durchgeführt wurden, wieder die ursprüngliche Nachricht heraus. Dieser Abschnitt dient quasi zur Selbstüberprüfung.

Eine genauere Beschreibung der einzelnen Schritte findet sich nun im folgenden Unterabschnitt.

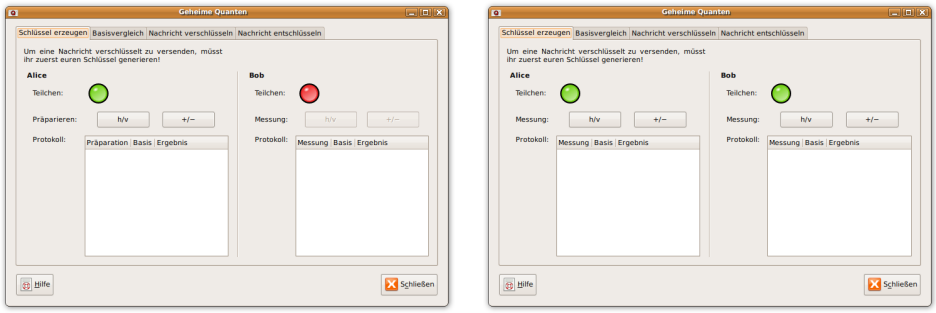
5.1.1 Wie funktioniert das Programm?

Nachdem das Programm Geheime Quanten gestartet wurde, erscheint zuerst ein Fenster (siehe Abb. 5.1), in dem man sich entscheiden muss, ob man das BB84- oder das Ekert-Protokoll verwenden möchte. Beim Ekert-Schema handelt es sich allerdings um eine vereinfachte Version, da hier im Gegensatz zum echten Protokoll nur zwei anstelle von drei Messbasen verwendet werden. Die Anzahl ist aber für die prinzipielle Funktionsweise der Generierung eines Schlüssels mittels Quantenkryptographie nicht entscheidend, so lange es mindestens 2 verschiedene Basen gibt. Wählen Alice und Bob jedoch 3 Basen könnten sie die Messergebnisse, die sie bei unterschiedlichen Basen erhalten haben und daher nicht für den Schlüssel verwenden können, dazu benützen, eine Bell Ungleichung (CHSH-Ungleichung) zu testen. Dazu geben beide diese Messergebnisse (durchaus öffentlich) bekannt und berechnen, daraus die quantenmechanischen Wahrscheinlichkeiten und setzen diese in die CHSH-Ungleichung ein. Diese wird aber nur dann von den quantenmechanischen Wahrscheinlichkeiten (maximal) verletzt, falls Alice und Bob aus 3 bestimmten Basen (nicht orthogonal) wählen können. Dieses Detail habe ich fürs Computerprogramm jedoch nicht berücksichtigt (daher heißt es Ekert Protokoll vereinfacht).

Abbildung 5.1
Protokollauswahl

Anschließend erscheint, je nachdem was man gewählt hat, eines der beiden Hauptfenster (siehe Abb. 5.2). Beide Fenster unterscheiden sich nur im ersten Reiter. Während beim Ekert-Protokoll bei Alice und Bob die Basisauswahl mit **Messung** beschriftet ist, findet sich beim BB84-Protokoll auf Alices Seite stattdessen die Beschriftung **Präparieren**.

Außerdem leuchtet beim BB84-Protokoll zuerst nur Alices Lämpchen (sie muss ja erst das Teilchen präparieren, bevor es Bob messen kann).



BB84 – Protokoll Ekert – Protokoll

Abbildung 5.2 Startfenster

Wenn man versucht das Programm zu schließen, erscheint sicherheitshalber noch ein Fenster, in dem man das Schließen des Programms noch bestätigen muss (siehe Abb. 5.3).

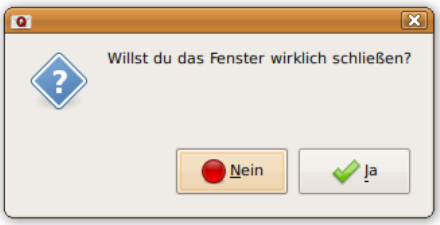


Abbildung 5.3
Programm schließen

Im Hauptfenster befindet sich im unteren Teil des Programms außer dem **Schließen**-Knopf auch noch ein **Hilfe**-Knopf. Dieser ruft das Handbuch (siehe Abb. 5.4) von Geheime Quanten auf, in dem vom Starten des Programms bis hin zu den einzelnen Schritten alles genau erklärt ist.

Ein Ausschnitt aus der Hilfe, in dem die vier Abschnitte behandelt werden, folgt nun. Die komplette Hilfe findet man im Anhang D.

5.1.1.1 Erster Reiter

Dieser Reiter sieht, je nachdem welches Protokoll (BB84 oder Ekert) man eingestellt hat, etwas unterschiedlich aus. Er ist in zwei Hälften aufgeteilt (siehe Abb. 5.5). Die linke ist für Alice, die rechte für Bob bestimmt. Zu Beginn des Spiels haben bei der Ekert-Version beide SpielerInnen ein Teilchen zur Verfügung (Lämpchen leuchtet grün). Bei der BB84-Version leuchtet zuerst nur das Lämpchen von Alice grün. Erst wenn sie ihr Teilchen präpariert hat, wird Bobs Lämpchen leuchten.

Die Teilchen können nun gemessen bzw. präpariert werden, indem man sich für eine Basis (**h/v** oder **+/−**) entscheidet und auf diese klickt. Dabei ist es beim Ekert-Protokoll egal, ob Alice oder Bob beginnt. Hat zum Beispiel Alice begonnen, so schaltet ihr Lämpchen von grün auf rot um und Bob ist an der Reihe. Hat er gemessen, so leuchten beide Lämpchen wieder grün (das bedeutet, dass wieder Teilchen zum Messen vorhanden sind) und das ganze kann von vorne beginnen.

Abbildung 5.4 Hilfe

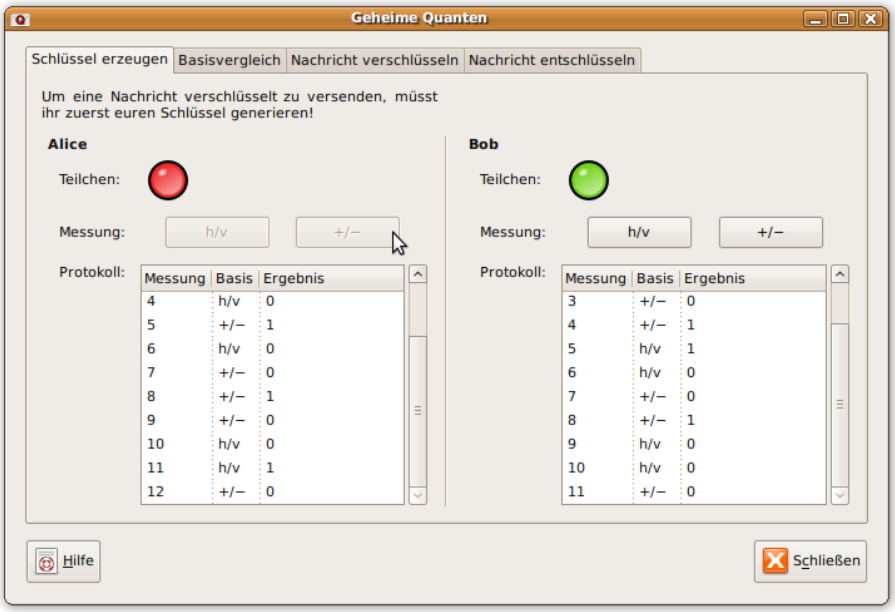


Abbildung 5.5 erster Reiter – Screenshot

Beim BB84-Protokoll muss Alice beginnen. Erst danach kann Bob sein Teilchen (leuchtet nun grün) messen was bewirkt, dass sein Lämpchen wieder auf rot umschaltet. Gleichzeitig wird Alices Lämpchen wieder grün, und so weiter.

Im Feld **Protokoll** finden sich drei Spalten, die während den Messungen gefüllt werden. Diese sind bei beiden Versionen gleich.

Messung Gibt die Nummer der Messung an

Basis Zeigt an, in welcher Basis gemessen wurde

Ergebnis Hier findet man das Ergebnis der Messung

Beim Ekert-Protokoll werden allerdings nicht die antikorrelierten (= gegengleichen) Ergebnisse sondern gleiche in die Tabelle eingetragen. Eine Spalte wurde also vom Computer schon automatisch invertiert, sodass gleiche Ergebnisse angezeigt werden.

5.1.1.2 Zweiter Reiter

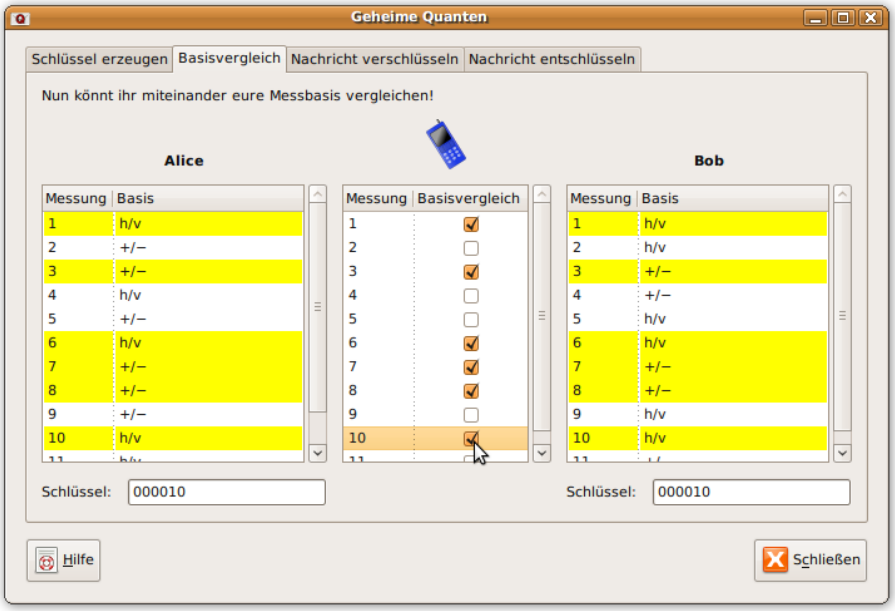


Abbildung 5.6 zweiter Reiter – Screenshot

Nun müssen die Basen, in denen gemessen wurde, verglichen werden. Dazu wurden hier die Protokolle aus dem ersten Reiter übernommen (siehe Abb. 5.6). Die Spalte mit den Messergebnissen wurde allerdings bewusst weggelassen, da einerseits diese keinesfalls öffentlich ausgetauscht werden dürfen und andererseits so verhindert wird, dass die SchülerInnen anstatt der Basen die Messergebnisse vergleichen. Dies würde ja auch dazu führen, dass die Schlüssel die gleichen wären und daher am Ende alles richtig herauskommt, was aber nicht Sinn und Zweck des Lernprogramms ist.

Sind also die Basen, in denen gemessen wurde, gleich, so wählt man sie in der mittleren Tabelle in der Spalte **Basisvergleich** aus. Die dazugehörigen Messungen im Protokoll werden dabei gelb gefärbt. Hat man irrtümlich eine falsche Zeile ausgewählt, so kann diese durch nochmaliges Klicken wieder abgewählt werden.

Während die richtigen Zeilen ausgewählt werden erscheint im unteren Teil des Fensters der dazugehörige Schlüssel für Alice bzw. für Bob. Hat man alles richtig gemacht, so sollten diese gleich sein.

Der Schlüssel muss auf jeden Fall mindestens die Länge von fünf Bits haben, da man für die Übersetzung eines Buchstabens in Nullen und Einsen mindestens fünf Bits braucht. Falls der Schlüssel zu kurz sein sollte, muss man im ersten Reiter gegebenenfalls noch Messungen nachholen.

5.1.1.3 Dritter Reiter

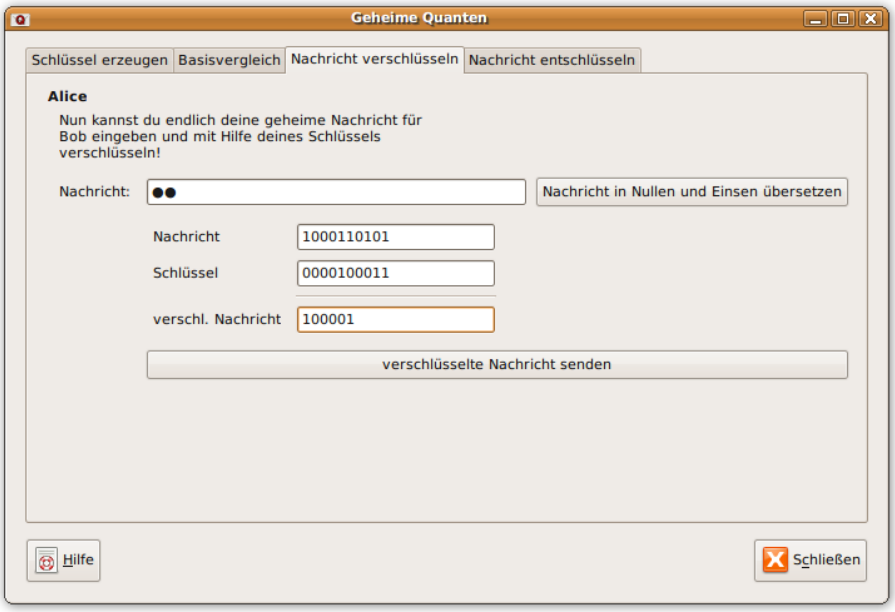


Abbildung 5.7 dritter Reiter – Screenshot

Der dritte Reiter (siehe Abb. 5.7) ist nur für Alice gedacht. Sie kann nun ihre Nachricht für Bob eingeben. Damit Bob die Nachricht nicht gleich sehen kann, erscheinen statt dem Text nur Punkte. Im Eingabefeld werden nur folgende Zeichen akzeptiert: ›a‹, ›b‹, ... ›z‹, ›ä‹, ›ö‹, ›ü‹, ›ß‹, ›!‹ und das Leerzeichen. Dies sind genau $32 = 2^5$, da fünf die minimale Anzahl an Bits ist, die man benötigt um das ganze Alphabet zu kodieren. Daher wurde das Programm so geschrieben, dass eine Nachricht, deren Länge, multipliziert mit fünf, länger ist als der Schlüssel, nicht eingetippt werden kann, da dies sonst zu keinem vernünftigen Ergebnis führen würde.

Durch klicken auf den Knopf **Nachricht in Nullen und Einsen übersetzen** wird der Text, den Alice eingegeben hat, folgendermaßen übersetzt:

Alle Buchstaben werden durchnummeriert und anschließend in Binärschreibweise (5 Bits stehen zur Verfügung) konvertiert (siehe Tabelle 5.1). Zum Beispiel ist »h« der 8. Buchstabe im Alphabet, also 01000 in Binärschreibweise.

a = 00001	b = 00010	c = 00011	d = 00100
e = 00101	f = 00110	g = 00111	h = 01000
i = 01001	j = 01010	k = 01011	l = 01100
m = 01101	n = 01110	o = 01111	p = 10000
q = 10001	r = 10010	s = 10011	t = 10100
u = 10101	v = 10110	w = 10111	x = 11000
y = 11001	z = 11010	ä = 11011	ö = 11100
ü = 11101	ß = 11110	! = 11111	␣ = 00000

Tabelle 5.1

Anschließend erscheint die Übersetzung im darunter liegenden Feld **Nachricht**. Der Schlüssel, der im vorigen Reiter erstellt wurde, ist ebenfalls schon eingetragen.

Die verschlüsselte Nachricht kann jetzt im dafür vorgesehenen Feld **verschl. Nachricht** berechnet werden. Als Eingabe werden nur Nullen und Einsen erlaubt. Weiters existiert eine Sperre, die verhindert, dass man beliebig viele Bits eingeben kann und zwar ist die Grenze das Maximum von Schlüssel- und Nachrichtenlänge.

Die Berechnung erfolgt indem man die Nachricht und den Schlüssel addiert, wobei gilt:

$$0+0=0 \qquad 0+1=1$$
$$1+1=0 \qquad 1+0=1$$

Ist der Schlüssel länger als die Nachricht, so kann man entweder bis zum letzten Bit der Nachricht rechnen und den Rest des Schlüssels ignorieren oder der Nachricht gedanklich Nullen anhängen, je nachdem was einem lieber ist. Das Programm liefert in beiden Fällen das richtige Ergebnis, vorausgesetzt Alice und Bob haben die gleiche Methode verwendet.

Schließlich kann die Nachricht von Alice durch klicken auf den Knopf **verschlüsselte Nachricht senden** ab Bob übermittelt werden. Das Programm springt automatisch auf den letzten Reiter.

5.1.1.4 Vierter Reiter

Dieser Reiter (siehe Abb. 5.8) ist nur für Bob gedacht. Die verschlüsselte Nachricht von Alice sowie Bobs Schlüssel erscheinen automatisch in den dafür vorgesehenen Feldern.

Die Nachricht kann genauso berechnet werden, wie es Alice zuvor getan hat. Wiederum ist die Eingabe sowohl längenmäßig als auch auf die Zeichen 0 und 1 beschränkt. Klickt man auf den Knopf **Nachricht in Buchstaben übersetzen**, so wird die von Bob berechnete Nachricht übersetzt. Es sollte nun die Nachricht, die Alice am Anfang geheim eingetippt hat, im Feld **Nachricht** erscheinen.

Falls doch eine falsche Nachricht herauskommen sollte, empfiehlt es sich sowohl zu überprüfen, ob Alice und Bob den gleichen Schlüssel haben, als auch, ob man sich bei den Rechnungen nicht vertan hat.

5.1.2 Einsatz im Unterricht

Um das Programm sinnvoll im Unterricht einsetzen zu können, sollten die SchülerInnen ein paar wichtige Dinge bereits gehört haben. Je nachdem, ob das BB84- oder das Ekert-Protokoll

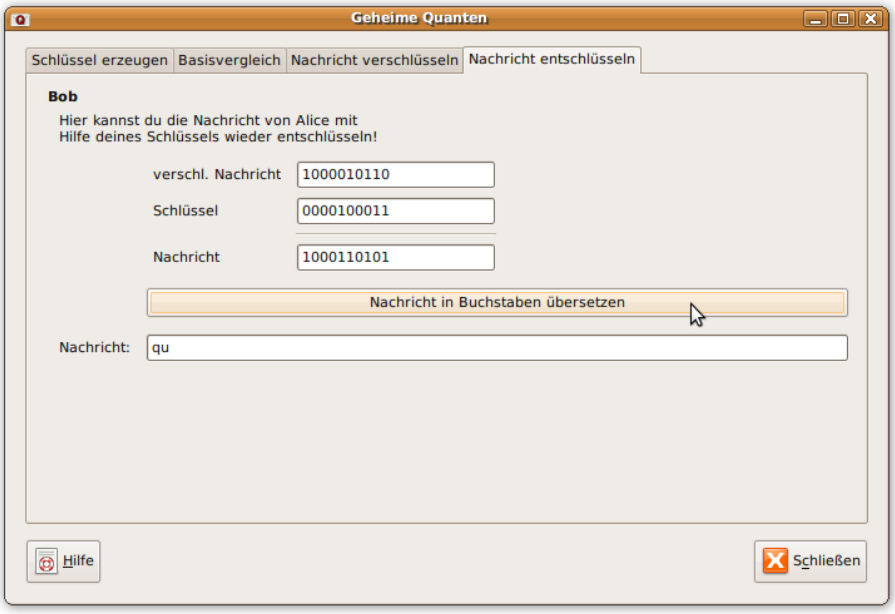


Abbildung 5.8 vierter Reiter – Screenshot

verwendet wird, sind die nötigen Vorkenntnisse etwas unterschiedlich. Im folgenden werden die wichtigsten Punkte für beide Protokolle aufgelistet:

- beide Protokolle
  - Grundlagen der Quantenphysik
  - Polarisation
  - Messung verändert den Zustand
  - Allgemeines über Kryptographie
  - Warum ist Kryptographie so wichtig?
  - Sicherheit
  - Regeln, wie man Schlüssel und Nachricht bzw. Schlüssel und verschlüsselte Nachricht addiert
- BB84-Protokoll
  - Kenntniss des Protokolls
- Ekert-Protokoll
  - Kenntniss des Protokolls
  - Was ist Verschränkung?

Das Lernprogramm ist für jeweils zwei SpielerInnen gedacht, wovon eine/einer die Rolle von Alice und eine/einer die Rolle von Bob übernimmt. Falls die SchülerInnenzahl ungerade sein sollte, ist es auch möglich alleine zu spielen, indem man sowohl Alice als auch Bob gleichzeitig bedient. Nach einem Spiel kann es auch interessant sein, die Rollen zu tauschen.

Der Lehrer/die Lehrerin sollte vor Beginn des Spiels genau erklären, wie es funktioniert und was die SchülerInnen machen sollen.

Zusätzlich gibt es zu dem Programm zwei Arbeitsblätter (siehe Anhang A). Das eine Arbeitsblatt ist für das BB84-Protokoll, das andere für das Ekert-Protokoll gedacht. Sie unterscheiden sich nur in ein paar Formulierungen, die Arbeitsaufträge sind identisch. Die SchülerInnen sollen darin alle wichtigen Schritte protokollieren. Anschließend können die Arbeitsblätter von

den SchülerInnen im Heft oder in einer Mappe (je nachdem wie es im Unterricht üblich ist) aufgehoben werden. Wenn der Lehrer/die Lehrerin möchte, sollte er/sie im Anschluss auch kontrollieren, was genau von den SchülerInnen durchgeführt wurde und ob die Nachricht richtig angekommen ist.

Der Vorteil dieser Basisversion ist, dass die SchülerInnen erkennen können, wie die Ergebnisse von der Wahl der Messbasen abhängen (bei Messung in gleicher Basis kommt immer das gleiche Ergebnis, bei Messung in unterschiedlichen Basen können auch verschiedene Ergebnisse kommen, dies muss aber nicht der Fall sein). Der Nachteil davon ist allerdings, dass dies weniger der Realität entspricht, da ja Alice und Bob normalerweise an unterschiedlichen Orten sind (ansonsten könnten sie sich die Nachricht gleich direkt mitteilen und die Verschlüsselung wäre damit mehr oder weniger sinnlos). In Realität würden sie nie das komplette Protokoll mit den Messergebnissen des jeweils anderen zu Gesicht bekommen.

5.2 Netzwerkversion

Die Netzwerkversion funktioniert ähnlich wie die Basisversion. Der Spielablauf ist im Wesentlichen der gleiche. Der Unterschied zur Basisversion ist, dass hier jeweils zwei SpielerInnen über ein Netzwerk verbunden sind, das heißt Alice und Bob sitzen an verschiedenen Computern. Außerdem kann man diese Version im Moment nur mit dem BB84-Protokoll spielen.

5.2.1 Wie funktioniert das Programm?

Der Lehrer/die Lehrerin hat eine eigene Benutzeroberfläche – das Serverprogramm (siehe Abb. 5.9) –, in der er sehen kann, wer mit wem verbunden ist. Dieses muss als erstes laufen, dann können sich die Programme der SchülerInnen verbinden.

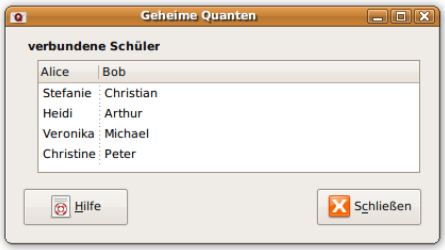


Abbildung 5.9 Serverprogramm

Wenn die SchülerInnen dann das Programm geöffnet haben, erscheint zuerst ein Fenster (siehe Abb. 5.10), in dem sie ihren Namen eingeben müssen. Erst dann öffnet sich das Hauptfenster. Nun kann der Lehrer/die Lehrerin sehen, wer sich schon angemeldet hat und wer jeweils Alice und den dazugehörigen Bob spielt. Letztere Information besitzt nur der Lehrer/die Lehrerin. Die SchülerInnen können sofort mit dem Lernspiel beginnen, sobald ihnen vom Computer ein zweiter Spieler/eine zweite Spielerin zugeteilt wurde. Die Zuteilung erfolgt nach der Anmeldezeit.

Beim Server-Programm sollte man aufpassen, dass man es nicht versehentlich schließt, da sonst alle Geheime Quanten Programme, die mit dem Server verbunden waren, ebenfalls geschlossen werden. Als Sicherheitsmaßnahme erscheint zuvor aber noch ein Fenster, indem man nochmals gefragt wird, ob man das Programm tatsächlich beenden will.

Abbildung 5.10 Namenseingabe

Die Benutzeroberfläche des Programms ist fast identisch mit der Basisversion (BB84-Protokoll). Der Unterschied besteht darin, dass die Fenster von Alice und Bob nun getrennt sind. Da in der vorigen Version der dritte Reiter nur für Alice und der vierte nur für Bob bestimmt war, hat diese Version insgesamt nur jeweils drei Reiter. Diese werden nun kurz beschrieben und die Unterschiede zur Basisversion erklärt.

5.2.1.1 Erster Reiter

Dieser Reiter (siehe Abb. 5.11) ist fast identisch mit der Basisversion, außer, dass das Benutzerinterface von Alice und Bob getrennt wurde.

Reiter 1 – Alice Reiter 1 – Bob

Abbildung 5.11 Netzwerkversion: erster Reiter

5.2.1.2 Zweiter Reiter

Im zweiten Reiter (siehe Abb. 5.12) besteht der einzige Unterschied darin, dass es nur eine Tabelle in der Mitte gibt. In der zweiten Spalte ist die Messbasis des jeweiligen Spielers eingetragen, in der Spalte rechts daneben die des Spielpartners. In der dritten Spalte befindet sich wieder der Basisvergleich. Außerdem ist hier klarerweise nur ein Feld für den Schlüssel vorhanden. Die Basen, die im Feld **Basisvergleich** angehakt wurden, werden hier aus technischen Gründen bzw. der Schönheit halber im Unterschied zur Basisversion nicht gelb gefärbt. Man kann allerdings auf den ersten Reiter zurückspringen und wird entdecken, dass dort die richtigen Basen markiert sind.

Reiter 2 – Alice Reiter 2 – Bob

Abbildung 5.12 Netzwerkversion: zweiter Reiter

5.2.1.3 Dritter Reiter

Im dritten Teil (siehe Abb. 5.14) kann Bob erst etwas machen, wenn Alice ihm eine Nachricht geschickt hat. Das verschlüsseln der Nachricht funktioniert wieder gleich wie vorher. Der einzige Unterschied ist, dass hier die Nachricht bei Alice nicht durch Punkte ersetzt wird, wie in der Basisversion, denn hier sitzt Bob ja sowieso auf einem anderen Computer. Wenn Alice auf den Knopf **Nachricht senden** klickt, erscheint zuerst bei Bob eine Meldung, dass er eine Nachricht bekommen hat (siehe Abb. 5.13). Diese Information kann er mit **OK** bestätigen. Nun kann er seine Nachricht entschlüsseln.

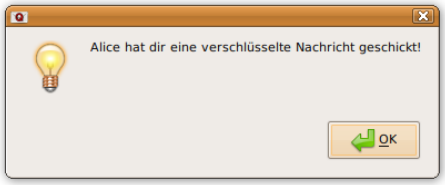


Abbildung 5.13 Information, die Bob erhält, wenn Alice ihm eine Nachricht geschickt hat

Ist das Spiel beendet und schließt einer das Programm, so erhält der jeweils andere automatisch eine Nachricht, dass Alice oder Bob das Fenster geschlossen hat (siehe Abb. 5.15). Zusätzlich wird man sicherheitshalber immer nochmals gefragt, ob man das Programm wirklich schließen möchte.

Schließt auch der Partner/die Partnerin das Fenster, so wird das Programm für diese beiden Spieler beendet. Im Serverprogramm werden die Namen dieser beiden Spieler dann grau gefärbt.

Reiter 3 – Alice Reiter 3 – Bob

Abbildung 5.14 Netzwerkversion: dritter Reiter

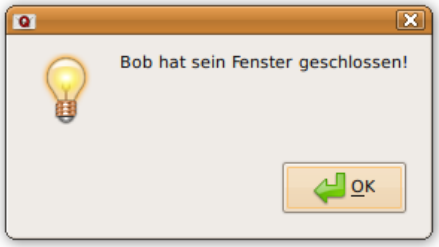


Abbildung 5.15 Nachricht an Alice, wenn Bob sein Fenster geschlossen hat

5.2.2 Einsatz im Unterricht

Ziel des Spieles könnte hier sein, dass die SchülerInnen herausfinden müssen, mit wem sie über Netzwerk verbunden sind, indem sie als Nachricht beispielsweise die ersten drei Buchstaben ihres Namens verschlüsselt verschicken.

Sind alle fertig, so sollen die, die Bob gespielt haben bekannt geben, mit wem sie verbunden waren. Der Lehrer kann nun nachprüfen, ob dies stimmt oder ob den SchülerInnen Fehler unterlaufen sind.

Auch für diese Version können die gleichen Arbeitsblätter (siehe Anhang) wie in der Basisversion verwendet werden. Hier sollten die SchülerInnen vorerst nur ihre eigenen Daten ausfüllen. Den restlichen Teil können sie erst nach dem Spiel behandeln. Haben sie herausgefunden, mit wem sie verbunden waren, so sollten sie sich zusammensetzen, um die Daten zu vergleichen und das Arbeitsblatt zu vervollständigen.

Ist etwas schief gelaufen, haben etwa manche SchülerInnen nicht herausgefunden welcher Partner/welche Partnerin zu ihnen gehört, so müssen diese den Lehrer/die Lehrerin danach fragen. Danach können sie mit ihren Arbeitsblättern (siehe Anhang A) herausfinden, wo die Fehler liegen.

Die Vorteile von der Netzwerkversion gegenüber der Basisversion sind, dass die SchülerInnen hier nicht schummeln können, indem sie bei der Messung immer auf die gleichen Basen klicken

um schneller den Schlüssel zu erhalten, da sie ja nicht sehen können, was der jeweils andere Spieler macht.

Der Nachteil dieser Version besteht allerdings darin, dass die SchülerInnen nun bei der Messung der Teilchen nur das eigene Ergebnis sehen können. Dies entspricht zwar eher der Realität, jedoch kann man nicht erkennen, dass bei Messung in gleicher Basis immer das gleiche Ergebnis herauskommt, bei Messung in unterschiedlichen Basen allerdings beide Fälle auftreten können. Dies könnte allerdings mit dem Arbeitsblatt wett gemacht werden. Denn dazu sollen sich die SchülerInnen nachher zusammensetzen, um die Ergebnisse zu vergleichen.

5.2.3 Erweiterungsmöglichkeiten

Da das Programm Open-Source ist, kann es auch jederzeit von jemandem, der sich auskennt, nach Belieben selbst umgeschrieben oder ergänzt werden. Im folgenden werden ein paar interessante Erweiterungsmöglichkeiten vorgestellt.

5.2.3.1 Ekert-Protokoll

Wie in der Basisversion wäre es natürlich auch hier schön, wenn man zwischen beiden Protokollen auswählen könnte. Bei der Umsetzung des Ekert-Protokolls stieß ich allerdings auf ein paar technische Schwierigkeiten. Das Problem liegt darin, dass Alice und Bob gleichzeitig messen könnten. Nun ist die Frage, wie man die Messergebnisse passend in die Protokolle einträgt. In der Basisversion hat einfach der, der als zweites gemessen hat, »nachgesehen«, was das Messergebnis des Ersten war. Dies ist kein Problem, da beide Benutzer in einem Programm arbeiten (und es ja nur eine Maus gibt). Sind die Benutzerinterfaces allerdings getrennt (also auf unterschiedlichen Computern), so kann es passieren, wenn beide gleichzeitig messen, dass das Programm einfach abstürzen würde oder dass in den Protokollen falsche Einträge (also bei gleicher Basis unterschiedliche Ergebnisse) auftreten könnten.

Eine mögliche Lösung des Problems könnte sein, dass Alice und Bob beim Server jeweils Teilchen anfordern. Dieser verschickt immer jeweils zwei gleiche (eins an Alice und eins an Bob), die aber schon ihre Messergebnisse (bei h/v oder $+/-$ Messung) kennen.

Diese Möglichkeit gefällt mir allerdings nicht so gut, da es dem quantenphysikalischen Prinzip, dass es keine »verborgenen Parameter« gibt, widerspricht. Dies ist zwar ohnehin nur eine Simulation, jedoch finde ich es schöner, wenn der Programmcode größtenteils auch der Realität entspricht und nicht zu sehr verfälscht ist. Andererseits muss man bei diesem Punkt sowieso schummeln, da wir ja für das Programm (leider) keine echten verschränkten Teilchen haben.

5.2.3.2 Alice, Bob und Eve

Noch eine Erweiterungsmöglichkeit, die interessant sein könnte, wäre *Alice, Bob und Eve*. Diese Möglichkeit würde dann ebenfalls am Startbildschirm (wo man die Protokolle auswählen kann) erscheinen. Diese Version wäre insofern gut, da hier auch ein Lauscher/eine Lauscherin ins Spiel gebracht werden kann.

Man könnte es so programmieren, dass etwa nur einem sechstel der Klasse Eve zugeteilt wird. Die anderen SchülerInnen würden wieder Alice und Bob Rollen erhalten. Das bedeutet, dass die Chance, einen Lauscher/ eine Lauscherin dabei zu haben genau 50% ist. Nun könnte es

Ziel des Spieles für Alice und Bob sein, herauszufinden, ob eine Eve mithört oder nicht. Das Ziel für Eve würde natürlich darin bestehen, möglichst viel vom Schlüssel herauszufinden und trotzdem unerkannt zu bleiben.

Hier sollten aber im Gegensatz zur vorigen Netzwerkversion Alice und Bob ihre Namen gegenseitig wissen. Dies könnte z.B. wieder über die Namenseingabe funktionieren. Die Information müsste auch Eve bekommen. Es reicht aber auch, wenn nur der Lehrer/ die Lehrerin die zusammengehörenden Namen kennt, um im anschließenden Gespräch die jeweiligen SchülerInnen fragen zu könne, ob sie Eve richtig entdeckt haben.

Die tatsächliche Ausführung dieser Version könnte folgendermaßen aussehen: Eine Möglichkeit, wie die Benutzeroberflächen für Alice, Bob und Eve aussehen könnten, findet sich in den Abbildungen 5.16, 5.17 und 5.18. Damit Eve sinnvoll lauschen kann, würde sich das BB84-Protokoll eignen. Alice würde hier also wie in den vorigen Versionen ihr Teilchen präparieren und an Bob weiter schicken. Allerdings bekommt es Bob nicht direkt, wenn es eine Eve dazwischen gibt. Diese sollte die Möglichkeiten haben entweder das Teilchen zu messen oder es zu ignorieren (um unerkannt zu bleiben). Anschließend wird es an Bob weiter gesandt, der es nun endlich messen kann. Jetzt ist wieder Alice am Zug, die das nächste Teilchen präpariert. Das Spiel würde so weiterlaufen, bis die Protokollliste genügend lange ist.

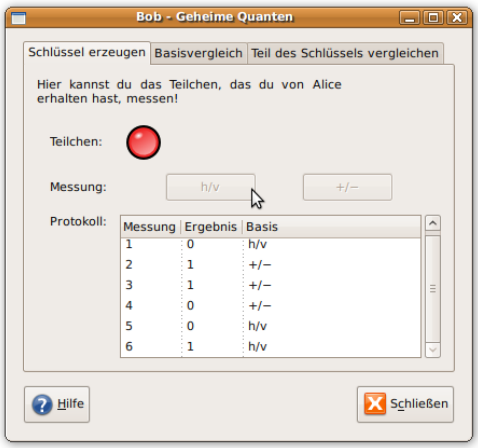
Nun würde es für Alice und Bob ans Vergleichen der Basen gehen. Diesen Schritt kann Eve ebenfalls belauschen (siehe Abb. 5.17). An den Stellen, an denen sie das Teilchen allerdings ignoriert hat, erscheint nur ein »X«. Haben Alice und Bob in den gleichen Basen gemessen und Eve in einer anderen, so konnte sie nichts herausfinden. In ihrem Schlüssel erscheint daher ein Fragezeichen.

Haben Alice und Bob nun einen Schlüssel, so können sie, um herauszufinden, ob sie belauscht wurden oder nicht, zum Beispiel die ersten zehn Bits miteinander vergleichen. Dies kann man entweder so machen, dass die ersten (oder hier sogar alle) Bits von Alice und Bob automatisch eingetragen werden oder an der dafür vorgesehenen Stelle selbst eingetippt werden müssen. Sind die Schlüssel gleich, so gab es mit hoher Wahrscheinlichkeit keine Eve oder sie hat nichts (oder nur sehr wenig) über den Schlüssel herausgefunden. Nun sollten Alice und Bob die Möglichkeit haben, Eve mitzuteilen, dass sie entdeckt wurde. Die Benutzeroberflächen für den Schlüsselaustausch und der Mitteilung könnte zum Beispiel wie in der Abbildung 5.18 aussehen.

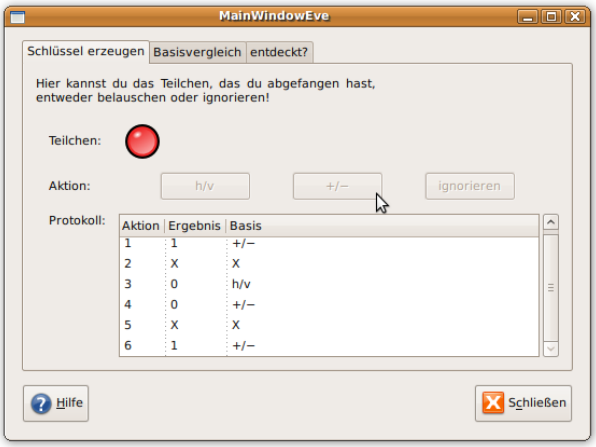
Natürlich kann es beim Austausch bei nur zehn Bits durch Zufall tatsächlich passieren, dass Eve unentdeckt bleibt. Die Wahrscheinlichkeit, dass Alice und Bob einen Lauschangriff bei einem Bit entdecken, ist $\frac{1}{4}$. Folglich bleibt Eve statistisch in drei von vier Fällen unerkannt. Bei zehn Bits hat sie also eine Chance von ungefähr 5.63%. Um diese Wahrscheinlichkeit möglichst gering zu halten, müsste man einen sehr langen Schlüssel austauschen. Jedoch würde es sehr schnell langweilig werden, so viele Messungen durchzuführen, um einen großen Schlüssel zu bekommen. Man könnte aber, nachdem die SchülerInnen bei den andern Simulationsprogrammen verstanden haben, wie man einen Schlüssel generiert, diesen Schritt auch automatisieren.

Man kann auch in dieser Version anschließend eine Nachricht verschlüsselt versenden. Hat man jedoch Eve entdeckt, so hat dies wenig Sinn, da man ja in diesem Fall den Schlüssel ohnehin verwerfen würde. Es wäre höchstens interessant zu sehen, welche Nachricht dann am Ende wieder herauskommt oder welche Nachricht (bzw. welche Teile davon) Eve erhält.

Reiter 1 – Alice



Reiter 1 – Bob



Reiter 1 – Eve

Abbildung 5.16 Alice, Bob und Eve: erster Reiter

Ich würde jedoch fast vorschlagen, diese Teile (Nachricht ver- und entschlüsseln) wegzulassen. Hier sollte der Hauptpunkt eher das Schlüsselerzeugen und Erkennen, ob dieser Schlüssel auch sicher ist, sein. Den restlichen Teil kann man ja in den anderen Versionen ohnehin ausprobieren.

Der Vorteil dieser Version wäre, dass die SchülerInnen schön sehen könnten, was die *Probleme* von Eve sind: Sie kann einerseits versuchen viel über den Schlüssel herauszufinden, dann wird sie aber mit ziemlicher Sicherheit auch erkannt werden. Andererseits kann sie versuchen möglichst unentdeckt zu bleiben, wobei sie allerdings kaum etwas über den Schlüssel herausfinden wird.

6 Diskussion

In diesem Abschnitt werden einige Punkte erwähnt, für die es sich durchaus lohnen würde, im Unterricht behandelt zu werden. Es geht hier unter anderem um die Umsetzung der Kryptographie in der Realität, um Messfehler und wie mögliche Lauschangriffe verhindert werden können.

Reiter 2 – Alice

Reiter 2 – Bob

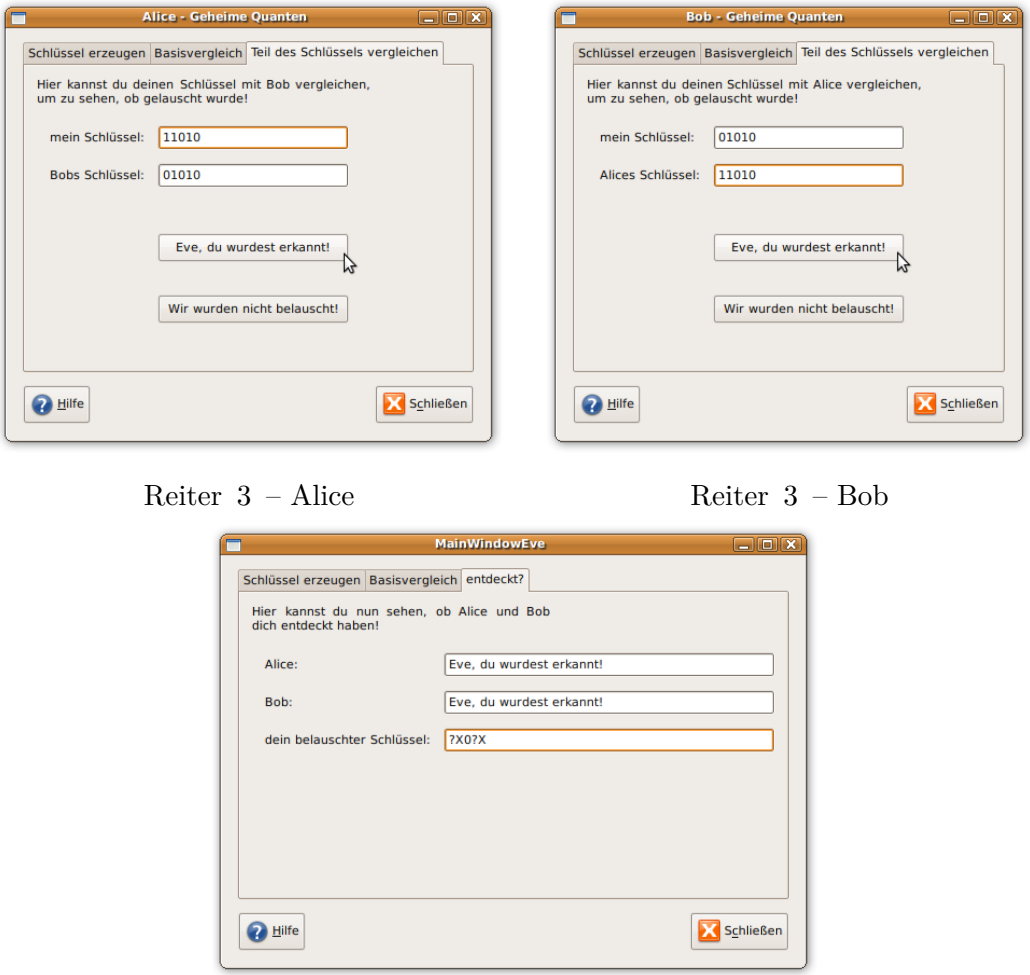
Reiter 2 – Eve

Abbildung 5.17 Alice, Bob und Eve: zweiter Reiter

Zuallererst sollte man den SchülerInnen aber klar machen, dass das zuvor behandelte Lernprogramm nur eine Simulation darstellt. Ich kann mir durchaus vorstellen, dass es SchülerInnen geben wird, die sich anschließend fragen, warum man zur Durchführung dieser Art von Kryptographie die Quantenmechanik überhaupt braucht, wenn es doch auf einem klassischen Computer funktioniert.

Daher sollte man den SchülerInnen klar machen, dass bei dem Programm »getrickst« wurde, denn der Computer kennt die Messbasen von Alice und Bob und teilt ihnen dazu passende Ergebnisse zu. Wenn zum Beispiel Alice zuerst misst, speichert der Computer ihre Basis und das zugehörige Messergebnis ab. Wenn dann anschließend Bob misst, vergleicht der Computer die Basen. Waren die Messbasen gleich, so erhält Bob dasjenige Ergebnis, das der Computer zuvor bei Alice gespeichert hat. Wurde in der anderen Basis gemessen, so bekommt Bob als Ergebnis eine Zufallszahl.

In der Realität wäre das also überhaupt nicht sicher, da nur jemand in den Computer einbrechen müsste, um den Schlüssel zu bekommen. Wenn dieser es auch geschickt anstellen würde, könnte er sogar unentdeckt bleiben.



Reiter 3 – Alice

Reiter 3 – Bob

Reiter 3 – Eve

Abbildung 5.18 Alice, Bob und Eve: dritter Reiter

Der große Unterschied zur Realität besteht also in folgenden zwei wichtigen Punkten. Erstens können am Computer die Bits ohne weiteres kopiert werden (was in der Quantenmechanik eben nicht möglich ist) und zweitens wird ein Bit am Computer durch Messungen nicht verändert.

6.1 Umsetzung in der Realität

Natürlich wäre es auch gut im Unterricht zu erwähnen, wie es eigentlich in der Realität mit der Quantenkryptographie aussieht. Handelt es sich dabei nur um ein Gedankenkonstrukt oder wurde diese Art der Verschlüsselung tatsächlich schon realisiert? Es kann durchaus sein, dass ein paar SchülerInnen zu diesem Thema etwas in den Medien gehört haben, was umso besser für den Unterricht ist, da dann eventuell mehr Interesse dafür vorhanden sein könnte. Außerdem kann man das SchülerInnenwissen auch gleich als Diskussionsgrundlage bzw. für einen Diskussionsbeginn verwenden.

Im Folgenden werde ich den derzeitigen Stand der Technik sowie diverse Rekorde anführen. Bevor man dies allerdings im Unterricht mit den SchülerInnen bespricht, sollte man unbedingt

selbst nachrecherchieren, da diese Daten möglicherweise schon wieder veraltet sind. Bei den Rekorden könnte man die SchülerInnen raten lassen, über welche Strecke hinweg Quantenkryptographie schon durchgeführt wurde.

6.1.1 Stand der Technik

Es gibt schon einige Umsetzungen dieser Ideen in der Praxis. Im Unterabschnitt »Rekorde« finden sich einige Experimente, in denen die Quantenkryptographie erfolgreich umgesetzt wurde. Es sind sogar schon erste kommerzielle Produkte am Markt zu finden, wie zum Beispiel bei IDQUANTIQUE[3] in Genf oder MAGIQ TECHNOLOGIES[4] in den USA oder NEC[5] in Tokyo. Allerdings wurden bei kommerziellen Systemen bisher noch keine verschränkten Photonen verwendet.

Für die tatsächliche Umsetzung werden meist Photonen verwendet, die mittels eines Zweikanalanalysators (z.B. Kalkspat) präpariert bzw. gemessen werden. Um den Analysator bzw. Polarisator zu steuern verwendet man elektronisch gesteuerte Pockelszellen (quasi ein sehr schneller Schalter).

Um verschränkte Photonen zu erzeugen, lässt man die Photonen einen speziellen Kristall durchqueren (z.B. Beta-Bariumborat). Dabei kann es passieren, dass das Photon in zwei Photonen mit halbiertem Energiegehalt übergeht. Dies tritt allerdings nur mit geringer Wahrscheinlichkeit auf. Treten diese anschließend in einem bestimmten Bereich aus dem Kristall aus, so sind sie maximal verschränkt und zwar antikorreliert. Das heißt, der Bellzustand

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$$

entsteht. Das bedeutet, dass entweder Alice oder Bob die Ergebnisse nach der Messung invertieren muss, damit beide die gleichen Resultate erhalten.

Die Übertragung der Photonen geschieht entweder über Glasfaserkabel oder bei direkter Sichtverbindung über Teleskope. Mehr zur technischen Umsetzung findet man unter [3].

6.1.2 Messfehler und wie mit ihnen umgegangen wird

In der Realität sind die Kanäle, über die die Bits übertragen werden, natürlich nicht perfekt. Man sagt, die Kanäle sind verrauscht. In der Praxis entstehen Fehlerraten um die 3%. Diese lassen sich aber durch Fehlerkorrekturen erheblich verringern. Dazu werden beispielsweise die ausgetauschten Bits in Blöcken von je n Bits zusammengefasst. Die Zahl n wird je nach Versuchsanordnung möglichst optimal gewählt. Nun wird von diesen Blöcken die Parität bestimmt. Diese gibt bei Addition aller Bits in einem Block an, ob die erhaltene Zahl (also die Anzahl der 1er) gerade oder ungerade ist. Die Paritäten der einzelnen Blöcke werden anschließend öffentlich ausgetauscht. Sind sie für entsprechende Blöcke verschieden, so werden diese Blöcke verworfen, da sich darin ein fehlerhaftes Bit befinden muss. Sind sie gleich, so wird zur Sicherheit ein Bit aus dem Block entfernt und der Rest dem Schlüssel hinzugefügt. Das Entfernen eines Bits hat den Sinn, dass ein Lauscher nicht einmal Information über die Parität

[3] www.idquantique.com
[4] www.magiqtech.com
[5] www.nec.com

des Blockes erhalten kann, da sich diese ja durch Löschen eines Bits ändern kann oder auch nicht.

Auf diese Art kann der Fehler beispielsweise von $2,5\%$ auf $0,4\%$ gesenkt werden [5].

Entsteht bei der Übertragung allerdings ein erheblich größerer Fehler (bis zu 25%), so wird der Schlüssel gänzlich verworfen, da dann die verursachten Fehler höchst wahrscheinlich von einem Lauscher und nicht vom natürlichen Rauschen stammen (außer der Messaufbau war fehlerhaft).

Natürlich kann es auch vorkommen, dass Bob einmal das Bit von Alice überhaupt nicht erhält. Diese Fälle werden aber einfach aus dem Protokoll entfernt. Dazu werden nicht nur das Messergebnis und die Basis registriert, sondern auch die dazugehörige Zeit.

Ein weiterer Fehler, der in realen Experimenten auftritt ist, dass bei der Erzeugung der Photonen nicht nur ein einzelnes sondern gleich mehrere entstehen. Dadurch bekommt Eve durch den sogenannten »beam splitter attack« eine Möglichkeit den Schlüssel abzuhören. Dabei blockiert sie alle einzelnen Photonen, sodass sie nicht zu Bob gelangen können und somit im Protokoll gestrichen werden müssen. Von den Multiphotonen, die ja alle gleich polarisiert sind, behält sie sich welche, um sie zu messen [6]. Um dies zu verhindern wird in den Experimenten möglichst versucht, sicher zu gehen, nur ein einzelnes Photon zu erzeugen. Benutzt man allerdings verschränkte Photonen, so ist die Wahrscheinlichkeit gleich mehrere zu erzeugen wesentlich geringer als bei einzelnen Photonen [5].

6.1.3 Rekorde

Es wurden seit 1991 in der Quantenkryptographie bereits Schlüssel über verschiedenste Entfernung übermittelt. Der aktuelle Rekord liegt bei einer Freiluftübertragung im Jahr 2007 bei 144 km. Bei der Übertragung mittels Glasfaserkabeln wurde 2009 eine Distanz von 250 km überwunden.

Nun möchte ich die wichtigsten Quantenkryptographieexperimente chronologisch kurz zusammenfassen. Die erste Demonstration fand im Jahr 1991 statt [7]. Dabei wurde der Schlüssel über eine Strecke von 30 cm übertragen.

Das erste Experiment, das verschränkte Photonen verwendete, wurde 1998 durchgeführt [5]. Dabei wurde einerseits eine Variante des Ekert-Protokolls[6] und andererseits eine Variante des BB84-Protokolls, das ebenfalls Verschränkung nutzt, in der Realität getestet. Übertragen wurde ein Bild von der Venus von Willendorf über 360 m.

2002 fand im Süden von Deutschland eine Freiluftübertragung mittels Teleskopen zwischen den Bergen Zug- und Karwendelspitze statt [8]. Die Distanz die dabei überwunden wurde betrug 23,4 km.

Ein weiteres sehr praxisnahes Experiment mit verschränkten Photonen wurde 2004 durchgeführt: Eine Banküberweisung [9]. Die Übermittlung fand zwischen dem Hauptquartier der Bank-Austria Creditanstalt und der Stadthalle in Wien statt. Der Abstand der beiden Gebäude beträgt 650 m. Übertragen wurden die Photonenpaare über Glasfaserkabel, die im Wiener Kanalsystem installiert wurden. Dieses Experiment zeigt unter anderem auch, dass

[6] Anstatt der CHSH-Ungleichung wurde die Wigner-Ungleichung verwendet. Diese erlaubt es, dass Alice und Bob nur zwei Polarisationseinstellungen benötigen. Alice verwendet $-30°$ und $0°$, Bob hat $0°$ und $30°$ zur Verfügung.

diese Systeme nicht nur unter Laborbedingungen funktionieren, sondern auch in realistischen Quantenkryptographieszenarien.

Im Jahr 2007 wurde eine Distanz von 107 km [6] über Glasfaserkabel überwunden. Verwendet wurde dabei das BB84-Protokoll. Die Forscher haben es hier geschafft, auch ohne Verschränkung, immun gegen die »beam-splitting-attack« zu sein.

Ebenfalls im Jahr 2007 wurde der Rekord der Freiluftschlüsselübertragung auf 144 km angehoben [10]. Auch hier wurde das BB84-Protokoll verwendet. Die Übertragung fand mittels Teleskopen zwischen den beiden Inseln La Palma und Teneriffa statt.

Durch diese Experimente rückt die Schlüsselübertragung via Satelliten immer näher.

Der heutige Rekord bezüglich Glasfaserübertragung liegt bei 250 km [11]. Dieser wurde 2009 erreicht. Zur Übertragung wurde ein spezielles sehr verlustfreies Glasfaserkabel verwendet.

6.2 SchülerInnen versus LehrerIn – wie könnte Eve doch noch lauschen?

Interessant wäre nun ein Zwiegespräch zwischen den SchülerInnen und dem Lehrer/der Lehrerin über mögliche Lauschstrategien. Als Grundlage dient hier das BB84-Protokoll, da es dabei mehr (bzw. einfachere) Ideen gibt, wie man lauschen könnte.

Wenn sich die Diskussion nicht ohnehin automatisch ergibt, so könnte man die SchülerInnen auffordern, Ideen zu finden, wie Eve doch lauschen könnte. Der Lehrer/die Lehrerin hat dann die Aufgabe, zu kontern und den SchülerInnen klar zu machen, warum dies oder jenes nicht funktionieren kann.

Ich glaube, dass dadurch das Verständnis des ganzen Prinzips erhöht wird, da sich die SchülerInnen dadurch intensiv mit dem Thema auseinandersetzen. Natürlich kann oder wird es auch passieren, dass einige SchülerInnen der Diskussion nicht folgen werden. Dies ist aber das Risiko aller Diskussionen, trotzdem sollte man aber meiner Meinung nach nicht darauf verzichten. Man könnte den SchülerInnen den Auftrag geben im Anschluss die wichtigsten Punkte zusammenzufassen (eventuell aber mit der Hilfe des Lehrers/der Lehrerin).

Im Folgenden werden mögliche Ideen für Lauschattacken der SchülerInnen vorgestellt. Nach jeder Idee wird die Theorie angeführt, warum Eve so nicht lauschen kann. Danach wird eine Möglichkeit vorgestellt, wie man dieses Wissen auch den SchülerInnen nahebringen könnte.

6.2.1 Idee

Eve könnte doch einfach das Teilchen abfangen, messen und an Bob weiter schicken.

6.2.2 Theorie

Messung verändert den Zustand. Sei $\oplus$ die Basis $\{|0\rangle, |1\rangle\}$ und $\otimes$ die Basis $\{|+\rangle, |-\rangle\}$. Angenommen Alice präpariert ihr Teilchen mit der Polarisation $+45°$, also $|+\rangle$.

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Misst Eve nun in der Basis $\otimes$, so bekommt sie klarerweise das Ergebnis $|+\rangle$. In diesem Fall hat sie also in der richtigen Basis gemessen. Sie erfährt das Schlüsselbit und das Teilchen kommt auch unverändert bei Bob an. Das bedeutet, dass hier die Wahrscheinlichkeit, dass Eve erkannt wird, Null ist.

Misst sie allerdings in der Basis $\oplus$, so erhält sie mit je 50% Wahrscheinlichkeit das Ergebnis $|0\rangle$ oder $|1\rangle$. Dabei wird aber der Zustand des Teilchens auch dementsprechend verändert. Misst nun Bob wieder in der Basis $\otimes$ (der andere Fall ist uninteressant, da dann das Teilchen sowieso nicht Teil des Schlüssels wäre), so bekommt er mit je 50% Wahrscheinlichkeit das Ergebnis $|+\rangle$ oder $|-\rangle$. Angenommen die Messung von Eve hätte das Teilchen in den Zustand $|0\rangle$ versetzt. Schreibt man $|0\rangle$ in der Basis $\otimes$ auf, so kann man schön sehen, dass Bob nur mit Wahrscheinlichkeit $\frac{1}{2}$ den von Alice präparierten Zustand $|+\rangle$ erhält.

$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$$

Die Wahrscheinlichkeit, Eve zu entdecken, beträgt hier also 50%.

Die Fälle, in denen Alice den Zustand $|-\rangle$ verschickt laufen analog. Insgesamt wird also beim Verschicken eines Qubits Eve in einem Viertel der Fälle überführt. Nun tauscht man aber in der Realität nicht nur ein Bit des Schlüssels aus, sondern gleich mehrere. Die Wahrscheinlichkeit Eve bei k Bits zu entdecken ist also

$$1 - \left(\frac{3}{4}\right)^k$$

Da diese Funktion gegen 1 konvergiert, wird Eve bei genügend großer Anzahl ausgetauschter Bits mit ziemlicher Sicherheit erkannt werden. Dieser Zusammenhang wird im Diagramm 6.1 gezeigt. Auf der x-Achse ist die Anzahl der verglichenen Bits und auf der y-Achse die dazugehörige Wahrscheinlichkeit dargestellt.

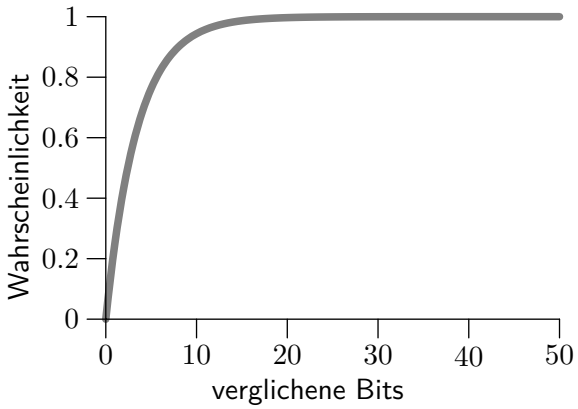


Abbildung 6.1 Wahrscheinlichkeit einen Lauschangriff zu entdecken

Dieser Teil des Schlüssels wird natürlich anschließend verworfen und keinesfalls für die Übertragung der geheimen Daten verwendet!

Natürlich kann man sich mögliche Angriffe von Eve auch noch allgemeiner überlegen. Das Hauptziel von Eve ist auf jeden Fall unerkannt zu bleiben. Daneben wäre es aber günstig für Eve unterscheiden zu können, ob das abgefangene Teilchen im Zustand $|0\rangle$ oder $|+\rangle$ ist.

Wüsste sie das, dann könnte sie die Messbasis demnach wählen und das Bit, das sie an Bob weiterschickt würde nicht verändert werden. So könnte also Eve unentdeckt bleiben und trotzdem lauschen. Dazu kann sie eine unitäre Transformation U auf das abgefangene Bit und ein Bit von ihr anwenden. Danach sollte ihr Bit die nötige Information tragen und sie kann das abgefangene Teilchen ohne Probleme in der richtigen Basis messen. Betrachten wir nun den Fall, in dem Eve völlig unbemerkt bleiben möchte. Sei $|\Phi_a\rangle$ der Anfangszustand (normiert) von Eves Bit. Dazu gibt es zwei Einheitsvektoren $|\Phi_0\rangle$ und $|\Phi_+\rangle$, sodass

$$U(|0\rangle \otimes |\Phi_a\rangle) = |0\rangle \otimes |\Phi_0\rangle$$
$$U(|+\rangle \otimes |\Phi_a\rangle) = |+\rangle \otimes |\Phi_+\rangle$$

gilt.

Eve bekommt also anschließend die Information $|\Phi_0\rangle$ oder $|\Phi_+\rangle$. Das ist auch gleichzeitig die einzige Information die sie dadurch erhält. Da unitäre Transformationen winkelerhaltend sind, also

$$\langle Ua|Ub\rangle = \langle a|b\rangle$$

gilt, muss das Skalarprodukt der Bilder und der Urbilder von U übereinstimmen. Es gilt also

$$\langle 0|+\rangle\langle\Phi_a|\Phi_a\rangle = \langle 0|+\rangle\langle\Phi_0|\Phi_+\rangle$$

Da $|0\rangle$ und $|+\rangle$ nicht orthogonal aufeinander stehen (also $\langle 0|+\rangle \neq 0$ gilt), kann man durch ihr Skalarprodukt auf beiden Seiten dividieren. $\langle\Phi_a|\Phi_a\rangle$ ergibt natürlich 1, da $|\Phi_a\rangle$ normiert ist. Somit erhält man

$$1 = \langle\Phi_0|\Phi_+\rangle.$$

Da es sich bei $|\Phi_0\rangle$ und $|\Phi_+\rangle$ um zwei Einheitsvektoren handelt folgt

$$|\Phi_0\rangle = |\Phi_+\rangle$$

Dies bedeutet aber für Eve, dass sie, wenn sie gänzlich unerkannt bleiben möchte, nichts darüber herausfinden kann, in welcher Basis das Teilchen präpariert wurde und folglich wird sie auch nicht unbemerkt das Bit messen können.

Nun kann man sich aber weiter überlegen, wie die Situation aussieht, wenn Eve doch nicht ganz unauffällig in das System eingreift. Hat sie nun die Chance mehr über den Schlüssel zu erfahren?

Eve verwendet wieder eine unitäre Transformation U. Diese verändert allerdings den Zustand des abgefangenen Teilchens ein wenig. Im folgenden bezeichne ich die durch Eve etwas veränderten Bits mit $|\tilde{0}\rangle$ und $|\tilde{+}\rangle$. Die Transformation würde dann folgendermaßen aussehen:

$$U(|0\rangle \otimes |\Phi_a\rangle) = |\tilde{0}\rangle \otimes |\Phi_0\rangle$$
$$U(|+\rangle \otimes |\Phi_a\rangle) = |\tilde{+}\rangle \otimes |\Phi_+\rangle$$

Wie oben erhält man daraus wieder

$$\langle 0|+\rangle = \langle\tilde{0}|\tilde{+}\rangle\langle\Phi_0|\Phi_+\rangle$$

Da

$$\langle 0|+\rangle = \frac{1}{\sqrt{2}}$$

gilt, kann man die Formel auch vereinfacht schreiben als

$$\frac{1}{\sqrt{2}} = \langle \tilde{0}|\tilde{+}\rangle\langle\Phi_0|\Phi_+\rangle$$

Die Zustände $|\Phi_0\rangle$ und $|\Phi_+\rangle$ kann man umso besser unterscheiden, je kleiner ihr Skalarprodukt wird. Das bedeutet aber wiederum, dass $\langle\tilde{0}|\tilde{+}\rangle$ umso größer werden muss. Dadurch wird Eve aber eher von Alice und Bob entdeckt. Hier kann man schön den Konflikt von Eve – einerseits unerkannt zu bleiben und andererseits möglichst viel Information zu bekommen – erkennen. Die Funktion ist in Abb. 6.2 dargestellt.

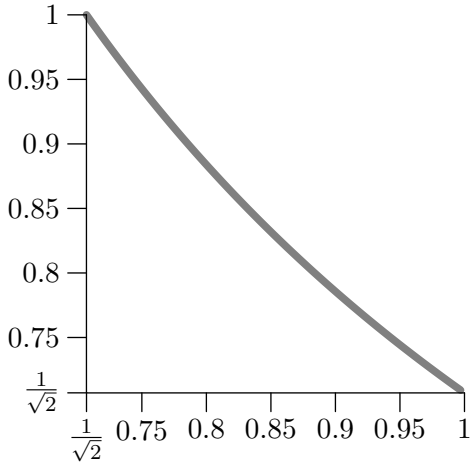


Abbildung 6.2 Konflikt zwischen unerkannt bleiben und trotzdem viel Information erhalten

6.2.3 Erklärung für SchülerInnen

Dies ist der Fall, der in der Programmerweiterung »Alice, Bob und Eve« behandelt werden würde. Man könnte es folgendermaßen den SchülerInnen erklären.

Alice schickt zum Beispiel ein horizontal polarisiertes Teilchen an Bob. Eve fängt es aber ab und misst es in der +/− Basis. Angenommen das Ergebnis ist + (also +45°). Sie schickt ihr Teilchen anschließend zu Bob, der es wieder in der Basis h/v misst. Nun kann Bob das Ergebnis horizontal aber auch vertikal erhalten, da ja das Teilchen nun +45° polarisiert war. Die Wahrscheinlichkeiten dafür sind je 50%.

Das bedeutet, dass Alice und Bob in diesem Fall Eve in der Hälfte der Fälle entdecken. Außerdem konnte sie in diesem Fall vom Schlüssel nichts herausfinden, da sie ja in der falschen Basis gemessen hatte.

Misst Eve allerdings auch in der Basis h/v, so würde sie den Zustand des Teilchens nicht verändern, da es ja schon von Alice horizontal polarisiert wurde. Bob würde also das richtige Ergebnis erhalten und Eve könnte unentdeckt bleiben.

Die Fälle, in denen Alice ihr Teilchen in der Basis +/− polarisiert, sind analog (siehe Tabelle 6.1). Insgesamt ergibt sich also für Eve bei einem einzigen Qubit eine Wahrscheinlichkeit von 25% das richtige Schlüsselbit zu belauschen und dabei unerkannt zu bleiben.

Es wird allerdings nicht nur ein Bit verglichen, sondern viele. Das bedeutet, dass die Wahrscheinlichkeit für Eve entdeckt zu werden immer kleiner wird und sogar gegen Null geht, da sich ja die Wahrscheinlichkeiten multiplizieren. In der Formel (1.1) wurden sie für den Austausch von fünf, zehn und fünfundzwanzig Bits ausgerechnet.

$$\begin{aligned} \text{5 Bits:} \quad & \left(\frac{3}{4}\right)^{5} \approx 0.237 \\ \text{10 Bits:} \quad & \left(\frac{3}{4}\right)^{10} \approx 0.056 \\ \text{25 Bits:} \quad & \left(\frac{3}{4}\right)^{25} \approx 0.001 \end{aligned} \tag{6.1}$$

In der Tabelle 6.1 sind alle möglichen Kombinationen und ihre Folgen für Eve eingetragen. Interessant für die Wahrscheinlichkeiten sind aber nur jene, in denen Alice und Bob in gleicher Basis gemessen haben, denn nur diese sind auch Teil des Schlüssels. In der Tabelle sind sie mit einem Häkchen gekennzeichnet.

Basis Alice	Basis Bob	Basis Eve	Teil des Schlüssels	Konsequenzen für Eve
h/v	h/v	h/v	✓	Eve konnte in diesem Fall erfolgreich lauschen
h/v	h/v	+/−	✓	Eve konnte nicht lauschen; die Wahrscheinlichkeit, dass sie entdeckt wurde beträgt 50%
h/v	+/−	h/v		
h/v	+/−	+/−		
+/−	h/v	h/v		
+/−	h/v	+/−		
+/−	+/−	h/v	✓	Eve konnte nicht lauschen; die Wahrscheinlichkeit, dass sie entdeckt wurde beträgt 50%
+/−	+/−	+/−	✓	Eve konnte in diesem Fall erfolgreich lauschen

Tabelle 6.1

6.2.4 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.

6.2.5 Theorie

Nach dem sogenannten »No-Cloning-Theorem« ist es nicht möglich eine Kopie eines unbekannten Quantenzustandes zu machen.

6.1 No Cloning Theorem Sei $|\psi\rangle \otimes |x\rangle$ ein Quantensystem mit $|\psi\rangle$ und $|x\rangle$ beliebig. Dann gibt es keine unitäre Transformation, die dieses System für alle $|\psi\rangle$ in den Zustand

$$|\psi\rangle \otimes |\psi\rangle$$

überführt.

Beweis Angenommen man hat einen Quantenzustand $|\psi\rangle$. Diesen möchte man kopieren, also den Zustand auf ein anderes Teilchen übertragen. Der Ausgangszustand dieses Teilchens soll ein reiner Zustand $|x\rangle$ sein. Die Ausgangslage ist also

$$|\psi\rangle \otimes |x\rangle.$$

Für den Prozess des Kopierens wird nun die unitäre Transformation U auf unseren Ausgangszustand angewendet.

$$U(|\psi\rangle \otimes |x\rangle) = |\psi\rangle \otimes |\psi\rangle$$

Angenommen wir wenden die Transformation auf zwei reine Zustände $|\psi\rangle$ und $|\varphi\rangle$ an. Dann erhalten wir

$$U(|\psi\rangle \otimes |x\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$U(|\varphi\rangle \otimes |x\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

Da unitäre Transformationen winkelerhaltend sind, muss das Skalarprodukt der Bilder und der Urbilder von U übereinstimmen. Es gilt also

$$\langle \psi \otimes x | \varphi \otimes x \rangle = \langle \psi \otimes \psi | \varphi \otimes \varphi \rangle$$

und folglich

$$\langle \psi | \varphi \rangle \langle x | x \rangle = \langle \psi | \varphi \rangle \langle \psi | \varphi \rangle.$$

Da für jeden Einheitsvektor $\langle a | a \rangle = 1$ gilt, folgt

$$\langle \psi | \varphi \rangle = (\langle \psi | \varphi \rangle)^2$$

Weil aber die Gleichung $x = x^2$ die beiden einzigen Lösungen 0 und 1 hat, folgt, dass $|\psi\rangle = |\varphi\rangle$ für $\langle \psi | \varphi \rangle = 1$ oder $|\psi\rangle$ und $|\varphi\rangle$ für $\langle \psi | \varphi \rangle = 0$ orthogonal sind. Das bedeutet aber, dass zwei Zustände nur dann mit der gleichen Transformation kopiert werden können, wenn sie

entweder gleich sind oder aufeinander orthogonal stehen. Daraus folgt wiederum, dass man für jede solche Zustandsklasse eine eigene »Kopiermaschine« bräuchte. Das heißt, dass ich den Zustand schon kennen muss und daher keine unbekannten Zustände kopieren kann. (Siehe [12] und [3].) □

6.2.6 Erklärung für SchülerInnen

Unbekannte Quantenzustände kann man nicht kopieren. Dies könnte man mit Schrödingers Katze erklären.

Hat man die Katze in der Box und weiß nicht, ob sie noch lebt oder nicht, so kann man die Katze nicht klonen ohne in die Box zu sehen. Würde man hineinsehen, so zerstört man den Zustand des Systems. Im Falle eines Quantenzustandes entspräche das einer Messung. Man möchte aber den Zustand des Teilchens kopieren ohne es zu messen. Der Fall in dem man das Teilchen misst und dann weiter schickt wurde ja schon behandelt.

Wenn man die Box aber nicht öffnet, also das System nicht stört, so kann man die Katze nicht klonen, weil man nicht weiß, ob sie tot oder lebendig ist. Angenommen ich kenne alle Daten der Katze bevor sie in die Box kam (wo sie sicher noch am Leben war) und klone sie nun. Die andere Katze bleibt in der Box. Wenn Eve nun ihre Katze misst, so wird sie immer den Zustand lebend erhalten. Die Katze in der Box könnte aber schon längst tot sein. Das heißt Eve kann mit ihrer Information nichts über die Katze in der Box herausfinden ohne die Box zu öffnen.

Fazit ist, Eve kann den Zustand des Teilchens nicht kopieren ohne es zu kennen. Führt sie aber eine Messung durch, um das Qubit dann zu kopieren, so hat sie das System bereits gestört und die Informationen vernichtet.

6.2.7 Idee

Eve könnte das Teilchen abfangen und mit einem Teilchen von ihr verschränken und das Original an Bob weiter schicken. Danach wartet sie, bis Alice und Bob die Basen miteinander verglichen haben und misst erst dann ihre Teilchen (in der richtigen Basis).

6.2.8 Theorie

Eve möchte also einen verschränkten Zustand zwischen einem ihrer Teilchen und dem abgefangenen Teilchen erzeugen. Angenommen sie besitzt das Bit $|0\rangle$[7]. Mit einem CNOT-Gatter kann sie nun den gewünschten Zweiteilchenzustand erzeugen. Der vierdimensionale Operator

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

verändert das zweite Bit, wenn das erste $|1\rangle$ war. Andernfalls bleibt es gleich.

[7] Würde Eve das Anfangsbit $|1\rangle$ wählen, so würde sie als Messergebnis immer den entgegengesetzten Zustand von Bobs Teilchen erhalten. Sie müsste demnach das Schlüsselbit 1 notieren, wenn sie 0 gemessen hat und umgekehrt.

Betrachten wir nun den Fall, wo Alice den Zustand $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ sendet. Eve wendet nun CNOT darauf an und erhält den Folgezustand

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Ein Teilchen behält sie sich, das zweite schickt sie an Bob. Nun sind die Photonen von Eve und Bob miteinander verschränkt. Angenommen Bob misst es in der Basis $\otimes$. Im anderen Fall wird das Ergebnis ohnehin verworfen und ist daher für uns uninteressant. Um leichter erkennen zu können, wie die Ergebnisse einer Messung in der Basis $\otimes$ aussehen, schreiben wir den Zustand in den Basiselementen $|+\rangle$ und $|-\rangle$ auf. Es gilt

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle),$$

was man leicht nachrechnen kann. Hier kann Bob also sowohl das Ergebnis $|+\rangle$ als auch $|-\rangle$ mit Wahrscheinlichkeiten von jeweils $\frac{1}{2}$ erhalten. Eve bekommt dann zwar immer das gleiche Resultat wie Bob, allerdings stimmen ihre Ergebnisse in der Hälfte der Fälle nicht mit Alice Teilchen überein.

Schickt Alice aber zum Beispiel den Zustand $|0\rangle$, so überführt das CNOT-Gatter es in den Zustand

$$|00\rangle.$$

Dies ist aber nach Definition kein verschränkter Zustand, da man ihn als Tensorprodukt aufspalten kann. Trotzdem ist der Zustand für Eve interessant. Denn misst Bob hier in der richtigen Basis $\oplus$, so erhält er mit Sicherheit den Zustand $|0\rangle$, den Alice verschickt hat. Auch Eve wird, vorausgesetzt sie misst in der richtigen Basis, den gleichen Zustand erhalten. Das heißt, sie würde das Schlüsselbit ohne weiters erfahren und dabei sogar unentdeckt bleiben.

In der Tabelle 6.2 sind alle möglichen Fälle eingetragen. Daraus kann man erkennen, dass Eve hier wiederum in einem viertel der Fälle entlarvt wird.

Alice	Eve und Bob
$\|0\rangle$	$\|00\rangle$
$\|1\rangle$	$\|11\rangle$
$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$

Tabelle 6.2

Man sieht auch, dass der nach Definition eigentlich nicht verschränkte Zustand $|00\rangle$ für Eve besser ist. Wie wir aber beim No-Cloning-Theorem bereits gesehen haben, gibt es keinen Operator, der $|0\rangle$, $|1\rangle$, $|+\rangle$ und $|-\rangle$ in die Folgezustände $|00\rangle$, $|11\rangle$, $|++\rangle$ oder $|--\rangle$ überführt.

6.2.9 Erklärung für SchülerInnen

Auch Verschränkung ändert gewissermaßen den Zustand. Hatte man vorher zwei getrennte Teilchen, so kann man nach der Verschränkung nicht mehr von einzelnen unabhängigen Teilchen sprechen. Das bedeutet, dass Bob einen etwas anderen Zustand erhält, als Alice gesendet

hat. Diese Veränderung bewirkt ähnlich wie bei einer Messung, dass Eve wieder in einem viertel der Fälle entdeckt wird.

Eve hat zwar immer das gleiche Ergebnis wie Bob erhalten, jedoch haben die beiden nicht immer das selbe Resultat wie Alice, was Eve schlussendlich verrät.

6.2.10 Idee

Eve könnte bei Alice oder Bob im Büro die Messergebnisse direkt belauschen.

6.2.11 Erklärung für SchülerInnen

Diese Möglichkeit ist sowohl klassisch als auch quantenmechanisch nicht auszuschließen. Dabei liegt es an Alice und Bob ihr direktes Umfeld möglichst sicher vor Lauschattacken zu gestalten.

6.2.12 Idee

Eve könnte sich bei Alice als Bob ausgeben und bei Bob als Alice (sogenannter »Man in the middle attack«)

6.2.13 Erklärung für SchülerInnen

Auch dieses Problem ist sowohl klassisch als auch in der Quantenkryptographie vorhanden. Eine Möglichkeit dies zu verhindern bieten die sogenannten »digitalen Signaturen« [13].

Durch eine digitale Signatur kann verifiziert werden, dass die erhaltene Nachricht (zum Beispiel eine e-mail) tatsächlich von dem richtigen Absender und nicht von einer anderen Person kommt. Im Prinzip ist die Verwendung wie eine echte Unterschrift am Papier mit dem Zusatz, dass auch festgestellt werden kann, ob die Nachricht während dem versenden von einer dritten Person manipuliert wurde.

Das Prinzip auf dem digitale Unterschriften (vgl. Abb. 6.3) basieren, ist das gleiche das bei den klassischen asymmetrischen Verschlüsselungsmethoden verwendet wird. Dabei hat der Sender der Nachricht einen privaten Schlüssel. Dazu gibt es einen passenden öffentlichen Schlüssel.

Als zusätzliche Sicherheit ist auf Seiten des Versenders eine sogenannte »HASH-Funktion« eingebaut. Eine »HASH-Funktion« ist eine Einwegfunktion, die aus viel Information wenig macht. Diese Funktion ist nicht umkehrbar. Damit erstellt man aus der zu versendenden Nachricht eine Zahl, aus der man nicht auf die ursprüngliche Nachricht schließen kann. Im zweiten Schritt wird die digitale Signatur aus dieser Zahl und aus dem geheimen Schlüssel erstellt.

Nachdem die Nachricht versendet wurde, kann der Empfänger mit dem öffentlichen Schlüssel feststellen, von wem die Unterschrift stammt. Um zu wissen, ob der öffentliche Schlüssel auch tatsächlich von dieser Person ist, hat man zwei Möglichkeiten: Entweder er hat den Sender der Nachricht schon einmal in Realität gesehen und von ihm den öffentlichen Schlüssel persönlich erhalten, oder man nutzt ein sogenanntes »Web of Trust« (Netz des Vertrauens). Dabei kann man die Echtheit von den öffentlichen Schlüsseln »unterschreiben«, wenn man die Person auch wirklich in Realität kennt. So entstehen Vertrauensnetze, was bedeutet, dass ich einer Person A vertraue, wenn eine andere Person B, der ich vertraue, dieser Person A auch vertraut und so weiter.

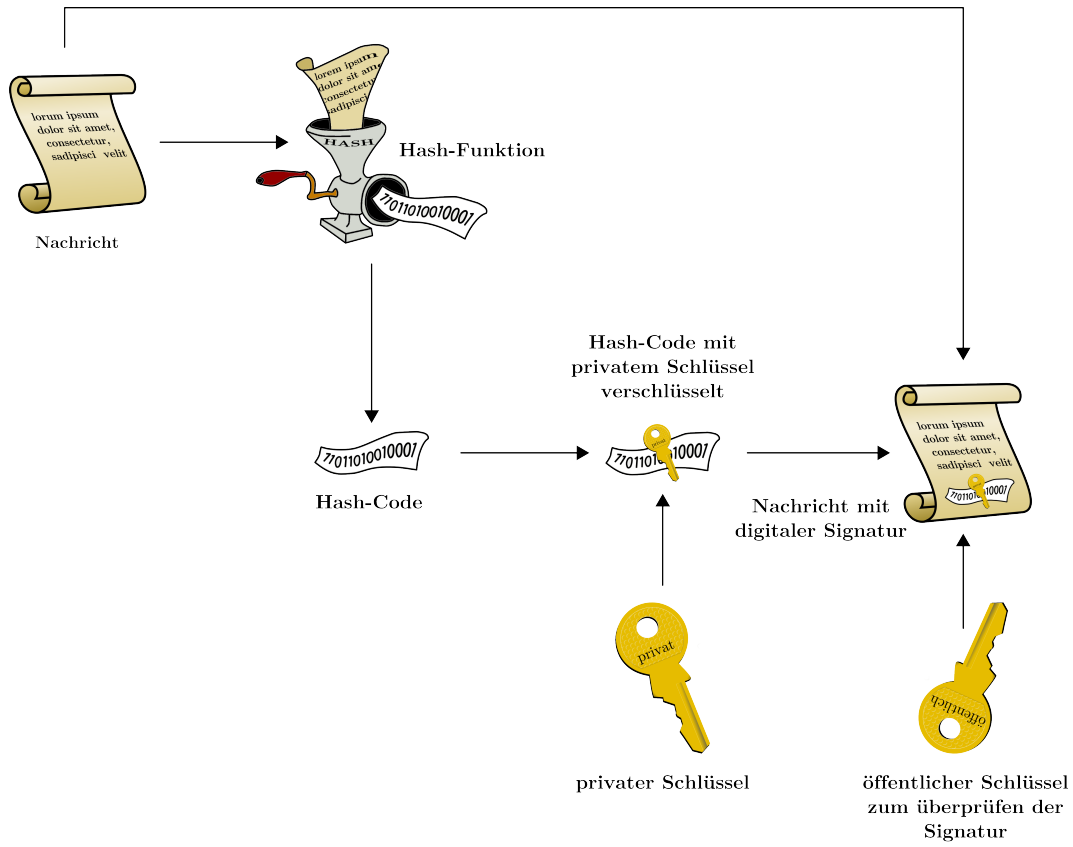


Abbildung 6.3 Prinzip der digitalen Signatur (nach [13])

Eine kurze Anmerkung möchte ich noch hinzufügen: Da die digitale Signatur auf den gleichen Prinzipien wie die klassische asymmetrische Verschlüsselung basiert, könnte das System durch den Einsatz von Quantencomputern genauso wie die klassischen Kryptographiesysteme zunichte gemacht werden. Allerdings gibt es auch hier Ansätze von der Quantentheorie, die die klassische digitale Signatur ersetzt [14].

6.3 Wie könnte Eve beim Ekert Protokoll lauschen?

Da beim Ekert-Protokoll das Abfangen des Teilchens auf dem Weg von Alice zu Bob wegfällt, ist es hier noch schwerer für Eve zu lauschen. Natürlich bleibt ihr aber noch der »Man in the middle attack« und das direkte Mitlauschen der Messergebnisse im Büro. Eine Möglichkeit, die sie allerdings noch ausprobieren könnte, ist das Eingreifen direkt an der Quelle. So kann sie zum Beispiel ein Teilchen, das gerade von der Quelle kam und am Weg zu Bob ist, abfangen. Eine andere Möglichkeit wäre ein Qubit von ihr mit den anderen beiden Teilchen zu verschränken. Nun wären drei Teilchen miteinander verschränkt, wovon eins Alice, eins Bob und das dritte Eve erhält. Dadurch würde sie doch perfekt lauschen können, oder?

6.3.1 Theorie

Angenommen Eve versucht eine Attacke mittels Verschränkung. Den anderen Fall, bei dem Alice ein Teilchen am Weg zu Bob abfängt, haben wir schon genügend beim BB84-Protokoll

diskutiert. Da so ein Eingriff immer den Zustand des Teilchens verändert, wird Eve dies nicht unbemerkt durchführen können. Trotzdem liefert aber die CHSH-Ungleichung, die wir nun behandeln werden, auch einen Test für diese Art von Lauschattacken.

Alice und Bob haben beim Ekert-Protokoll drei verschiedene Richtungen in denen sie die Polarisation des Teilchens messen können, wobei α_1 bis α_3 die Winkel der Messbasen von Alice und β_1 bis β_3 die von Bob sind.

$$\begin{aligned} \alpha_1 &= 0 & \beta_1 &= \frac{\pi}{8} \\ \alpha_2 &= \frac{\pi}{8} & \beta_2 &= \frac{\pi}{4} \\ \alpha_3 &= \frac{\pi}{4} & \beta_3 &= \frac{3\pi}{8} \end{aligned}$$

Messen Alice und Bob nun in der gleichen Basis, so wird das gemessene Teilchen zum Schlüssel hinzugefügt. Hat Eve ihr Teilchen mit den anderen beiden verschränkt, so würde sie auf diese Art ebenfalls den Schlüssel erfahren, vorausgesetzt sie wartet mit ihrer Messung bis sich Alice und Bob über den öffentlichen Kanal ausgetauscht haben, in welcher Basis sie jeweils gemessen haben.

Dies wollen aber Alice und Bob verhindern. Dazu verwenden sie in diesem Protokoll auch die Messergebnisse, in denen sie in unterschiedlichen Basen gemessen haben. Damit überprüfen sie die sogenannte CHSH-Ungleichung. Sie ist benannt nach John Clauser, Mike Horne, Abner Shimony und Richard Holt und stellt eine Variante der Bell-Ungleichung dar, die allerdings in der Realität leichter zu überprüfen ist. Sie lautet

$$|S| = |E(\alpha_1, \beta_1) - E(\alpha_1, \beta_3) + E(\alpha_3, \beta_1) + E(\alpha_3, \beta_3)| \leq 2,$$

wobei E der Korrelationskoeffizient ist. Für unser S gilt also

$$-2 \leq S \leq 2.$$

Sehen wir uns nun die quantenmechanischen Wahrscheinlichkeiten an. Der Korrelationskoeffizient ist dort gegeben durch

$$E(a, b) = -\cos 2(a - b).$$

Einsetzen ergibt nun

$$\begin{aligned} S = & -\cos 2(0 - \frac{\pi}{8}) + \cos 2(0 - \frac{3\pi}{8}) - \cos 2(\frac{\pi}{4} - \frac{\pi}{8}) - \cos 2(\frac{\pi}{4} - \frac{3\pi}{8}) \\ = & -\cos(-\frac{\pi}{4}) + \cos(-\frac{3\pi}{4}) - \cos(\frac{\pi}{4}) - \cos(-\frac{\pi}{4}) \\ = & -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}} \\ = & -2\sqrt{2} \end{aligned}$$

Der erhaltene Wert ist aber kleiner als -2. Das bedeutet, dass maximal verschränkte Teilchen diese Ungleichung verletzen und weiters, dass man durch die Überprüfung dieser Bedingung feststellen kann, ob gelauscht wurde. Da bei der Zugabe eines dritten Teilchens zu zwei verschränkten Teilchen der Verschränkungsgrad geringer wird, wird durch den Eingriff von Eve

diese Ungleichung experimentell nicht so stark verletzt wie bei zwei maximal verschränkten Teilchen. Gleiches gilt für jeden anderen Eingriff von Eve, wie zum Beispiel das Abfangen des Photons am Weg von der Quelle zu Bob. Ist dies der Fall, so werden die bisher erstellten Schlüsselbits verworfen.

Zusammenfassend beeinflusst Eves Lauschattacke die Messergebnisse von Alice und Bob bei der Messung in unterschiedlichen Basen. Der Eingriff ist ähnlich, als würde Eve beim BB84-Protokoll das übermittelte Bit einfach messen.

6.3.2 Erklärung für SchülerInnen

Es gibt nicht nur maximale sondern auch teilweise verschränkte Zustände.

Nun ist es aber so, dass die Verschränkung bei der Zugabe eines dritten Teilchens vermindert wird. Anschaulich ist die Information, die sich zuvor zwei Teilchen teilten, nun auf drei Teilchen verteilt. Diese Tatsache können nun Alice und Bob ausnützen. Sie testen mit Hilfe der sogenannten CHSH-Ungleichung, ob die Messergebnisse ihrer Teilchenpaare klassisch erklärbar sind. Ist dies der Fall, so wissen sie, dass vermutlich jemand gelauscht hat.

Auch eine einfache Lauschattacke, wo Eve das Teilchen gleich nach der Quelle abfängt und anschließend weiter an Bob schickt wird mit dieser Ungleichung aufgedeckt.

6.4 Abschließende Bemerkungen

Wie sich Eve auch bemüht den Schlüssel herauszufinden, steht sie immer vor dem gleichen Problem. Möchte sie möglichst viel Information herausfinden wird sie umso leichter durch Alice und Bob entdeckt. Versucht sie aber möglichst unentdeckt zu bleiben, so kann sie kaum nützliche Information erlauschen.

Zusätzlich können Alice und Bob die Sicherheit mit der sogenannten »privacy amplification« noch um einiges erhöhen. Dabei geht es darum, aus mehreren Bits ein Schlüsselbit zu machen. Zum Beispiel kann man immer jeweils zwei benachbarte Bits addieren. Angenommen Eve kennt ein Bit davon, das andere allerdings nicht. Durch diese Methode bleibt ihr dann das neue Schlüsselbit völlig verborgen.

Natürlich waren die gezeigten Angriffsmöglichkeiten nur spezielle Beispiele, jedoch zeigt sich auch bei allgemeinerer Betrachtung der Lauschangriffe, dass Eve nie Erfolg haben kann. Somit ist die Sicherheit der Quantenkryptographie – anders als bei der klassischen Kryptographie – durch physikalische Gesetzmäßigkeiten gewährleistet.

Anhänge

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 Vergleiche nun die Messergebnisse:

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

Erklärung:

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

Erklärung:

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

Schlüssel:

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

5 Welche Nachricht wurde übertragen?

Nachricht, die Alice gesendet hat:

Nachricht, die Bob erhalten hat:

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 Vergleiche nun die Messergebnisse:

Wie sehen die Ergebnisse aus, wenn ihr in der gleichen Basis gemessen habt?

Erklärung:

Wie sehen die Ergebnisse aus, wenn ihr in unterschiedlichen Basen gemessen habt?

Erklärung:

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

Schlüssel:

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

5 Welche Nachricht wurde übertragen?

Nachricht, die Alice gesendet hat:
Nachricht, die Bob erhalten hat:

Was ist Kryptographie?

Das Wort Kryptographie kommt aus dem griechischen:

kryptós = verborgen

gráphein = schreiben

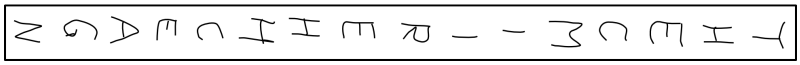
Zusammengesetzt bedeutet es etwas verborgenes schreiben. Kryptographie ist also die Wissenschaft vom Verschlüsseln und Entschlüsseln von Informationen. Ihre Anwendung findet sie heutzutage bei Bankgeschäften, bei den Geheimdiensten, bei der privaten Nachrichtenübertragung (z.B. e-mails) und vieles mehr.

Kryptographische Verfahren wurden nachweislich schon vor fast 4000 Jahren von den Äqyptern eingesetzt. Auch im alten Griechenland wurden Verschlüsselungsverfahren für militärische Geheimnisse verwendet.

In der Kryptographie geht man stets davon aus, dass das verwendete Verschlüsselungsverfahren dem Lauscher bekannt ist. Dieses Prinzip ist auch unter dem Namen Kerkhoffsches Prinzip (nach Auguste Kerckhoffs von Nieuwenhof; 1835-1903) bekannt.

Verschlüsselung um 400 v.Chr.

In Sparta verwendete man 400 v.Chr einen einfachen Holzstab (eine sogenannte Skytale) zur Verschlüsselung von geheimen Botschaften. Diesen umwickelten sie mit einem Leder- oder Pergamentstreifen und schrieben quer dazu die Nachricht darauf. Den Streifen schickten sie dann an die Person, für die die Nachricht gedacht ist. Jemand, der die Botschaft abfing, konnte diese nicht entziffern, wenn er nicht zufällig einen Holzstab mit gleichem Durchmesser hatte.



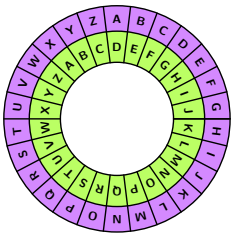
Natürlich war der richtige Stab nicht im Besitz des Boten. Heutzutage sind diese Methoden leicht entschlüsselbar. Damals kam aber noch die Hürde dazu, dass nur wenige schreiben und lesen konnten.

Cäsar-Verschlüsselung

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.

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

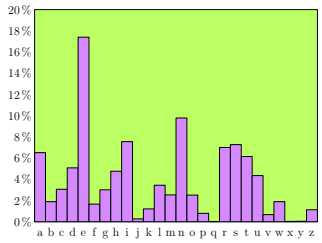
Cäsar kannte allerdings die Chiffrierscheibe noch nicht. Mit ihr kann man ganz leicht einen Geheimtext entschlüsseln, indem man alle 26 Möglichkeiten ausprobiert. Dazu muss man den inneren Teil der Scheibe solange verdrehen, bis der damit entschlüsselte Text einen Sinn ergibt.



Wie man einfache Verschlüsselung knacken kann

Eine Möglichkeit einen Text zu verschlüsseln besteht darin, die Buchstaben des Alphabets beliebig zu vertauschen. So schreibt man zum Beispiel statt einem A ein R, statt einem B ein E und so weiter. Man kann sich überlegen, dass es $26! \approx 4 \cdot 10^{26}$ Möglichkeiten für diese Art der Vertauschung gibt. Selbst wenn ein Lauscher also jede durchprobieren würde und dafür nur je eine Sekunde bräuchte, würde das die Lebensdauer des Universums um einiges übertreffen.

Trotzdem ist diese Verschlüsselung leicht zu entziffern: Da die Buchstaben in einem Text nicht alle gleich häufig vorkommen, kann man mit Hilfe einer Häufigkeitstabelle den Geheimtext entschlüsseln.



So sieht man zum Beispiel, dass das E in der deutschen Sprache um einiges häufiger als alle anderen Buchstaben vorkommt. Zum Entschlüsseln einer geheimen Nachricht braucht man also im ersten Schritt nur den häufigsten Buchstaben herauszufinden. Ist dies zum Beispiel ein R, so wurden wahrscheinlich alle E durch ein R ersetzt. Das gleiche macht man mit dem zweithäufigsten Buchstaben dem N und so weiter. Natürlich kann es sein, dass am Schluss ein paar Fehler passiert sind, aber das menschliche Gehirn ist dazu fähig, auch Texte, in denen einige Buchstaben vertauscht sind, durchaus leicht lesen zu können. In anderen Sprachen sieht die Häufigkeitstabelle etwas anders aus.

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 nächsthöhere Zweierpotenz 32 ($= 2^5$) 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:

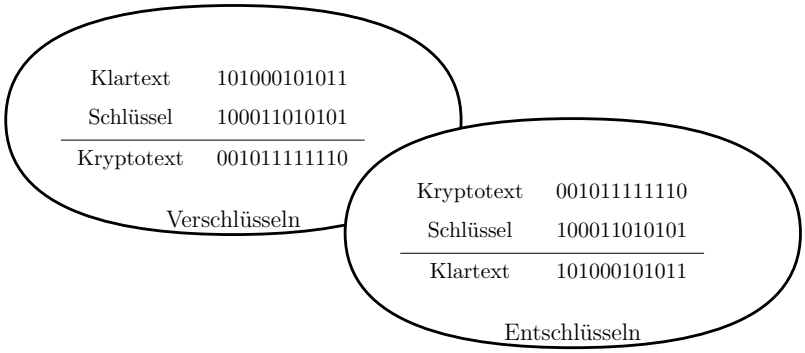
- $0 + 0 = 0$
- $0 + 1 = 1$
- $1 + 0 = 1$
- $1 + 1 = 0$

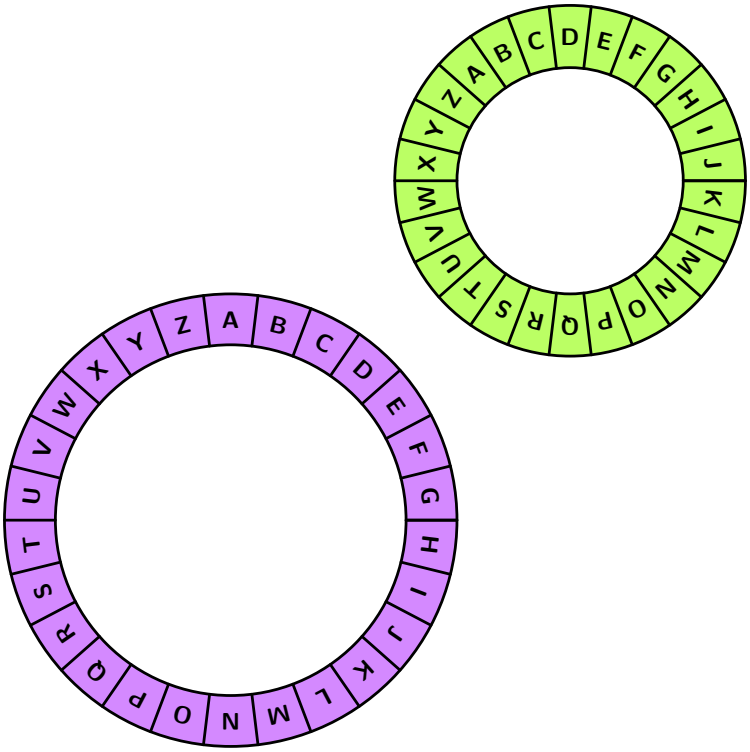
Den nun erhaltenen Kryptotext schickt sie an Bob. Wird die Nachricht am Weg abgefangen, so kann der Lauscher ohne den Schlüssel nichts damit anfangen, da die verschlüsselte Nachricht eine zufällige Folge von Bits ist.

Hat Bob den Kryptotext erhalten, so addiert er nach der gleichen Rechenvorschrift wieder den Schlüssel dazu. Es kommt wieder der Klartext heraus.

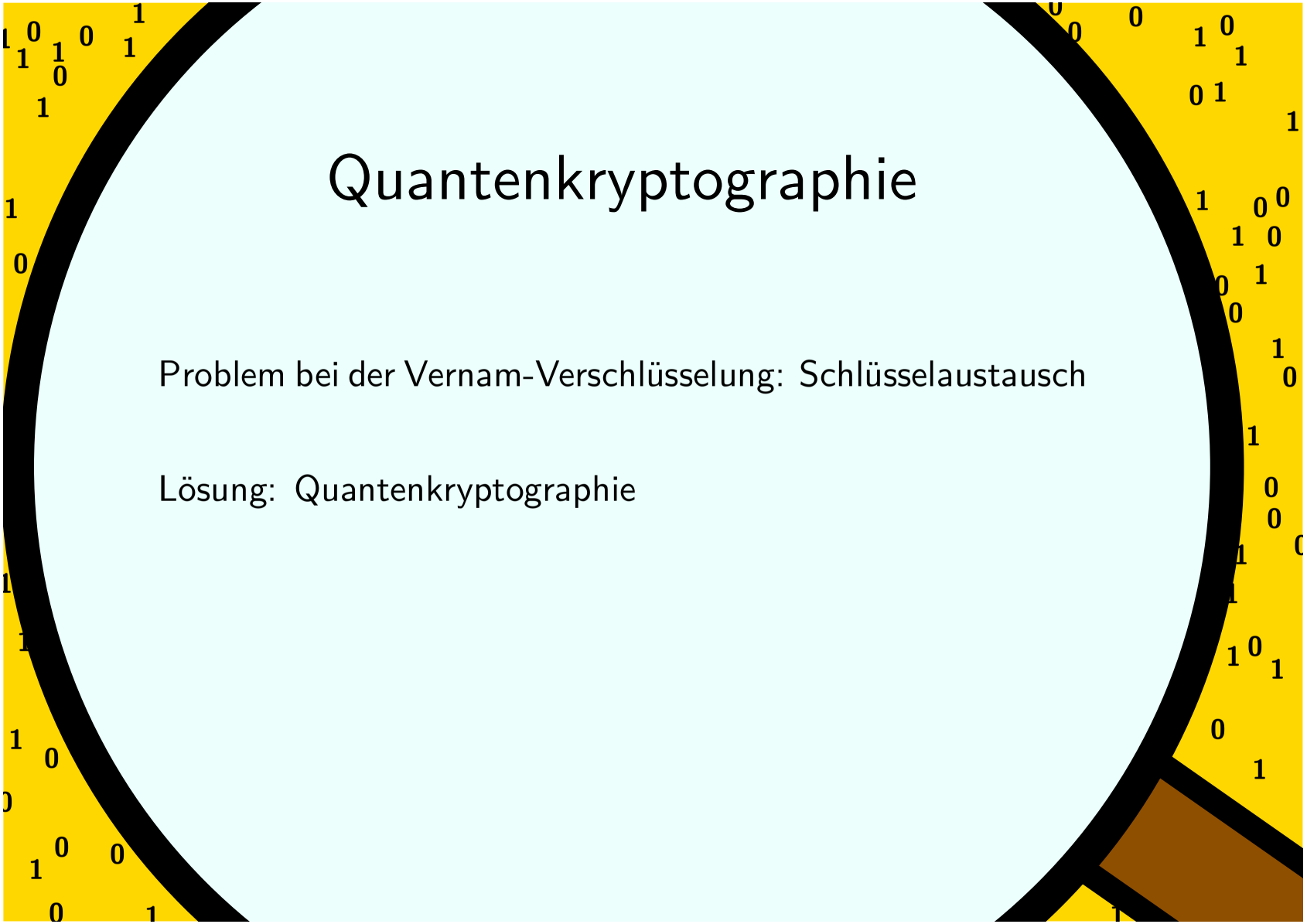
Der Vernam-Code ist absolut sicher, wenn

- 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.





Beide Kreise ausschneiden und auf Karton kleben (eventuell folieren). Anschließend den kleineren Kreis in der Mitte des größeren Kreises so befestigen, dass man den inneren Kreis drehen kann.



Quantenkryptographie

Problem bei der Vernam-Verschlüsselung: Schlüsselaustausch

Lösung: Quantenkryptographie

Akteure

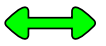
1 Personen

Alice  Heimliche Geliebte von Bob; sie möchte ihm eine geheime Nachricht senden.

Bob  Er möchte von Alice heimlich Nachrichten empfangen.

Eve  Freundin von Bob, sie traut ihm nicht ganz und versucht daher heimlich zu lauschen.

2 Photonen (Qubits)

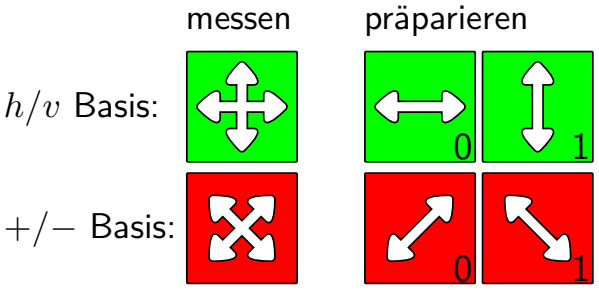
horizontal polarisiert  0

vertikal polarisiert  1

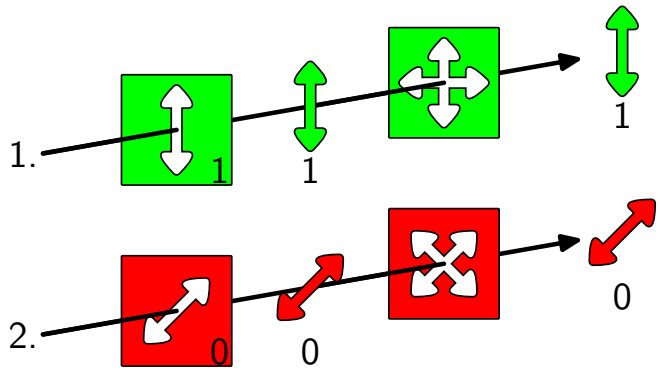
$+45°$ polarisiert  0

$-45°$ polarisiert  1

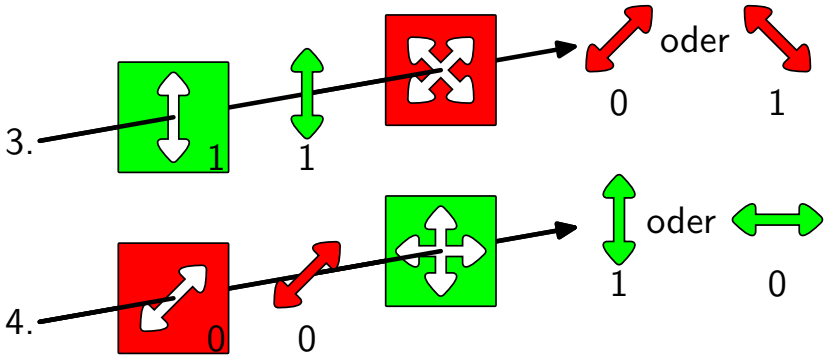
3 Mess- und Präparationsapparate



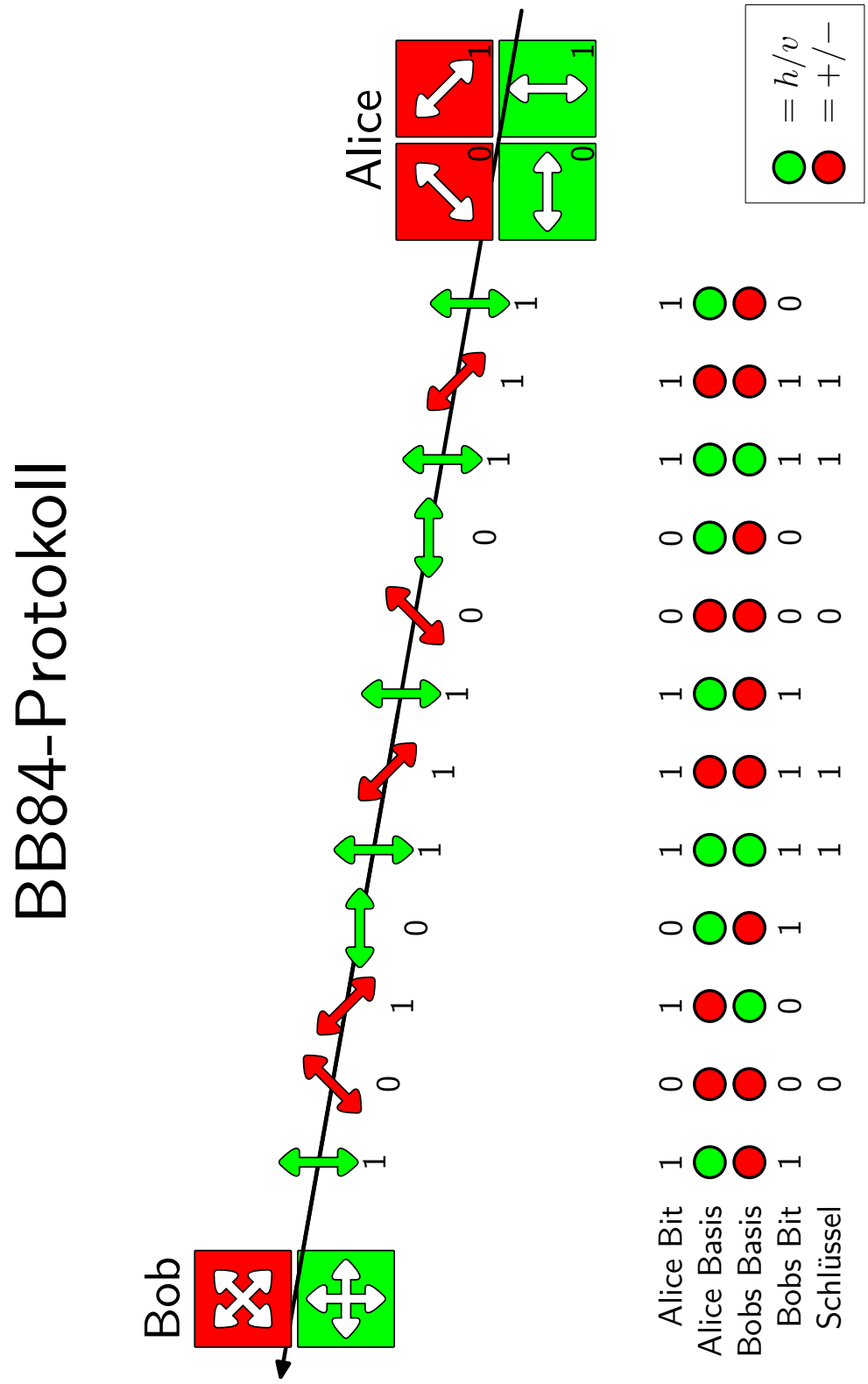
Messung



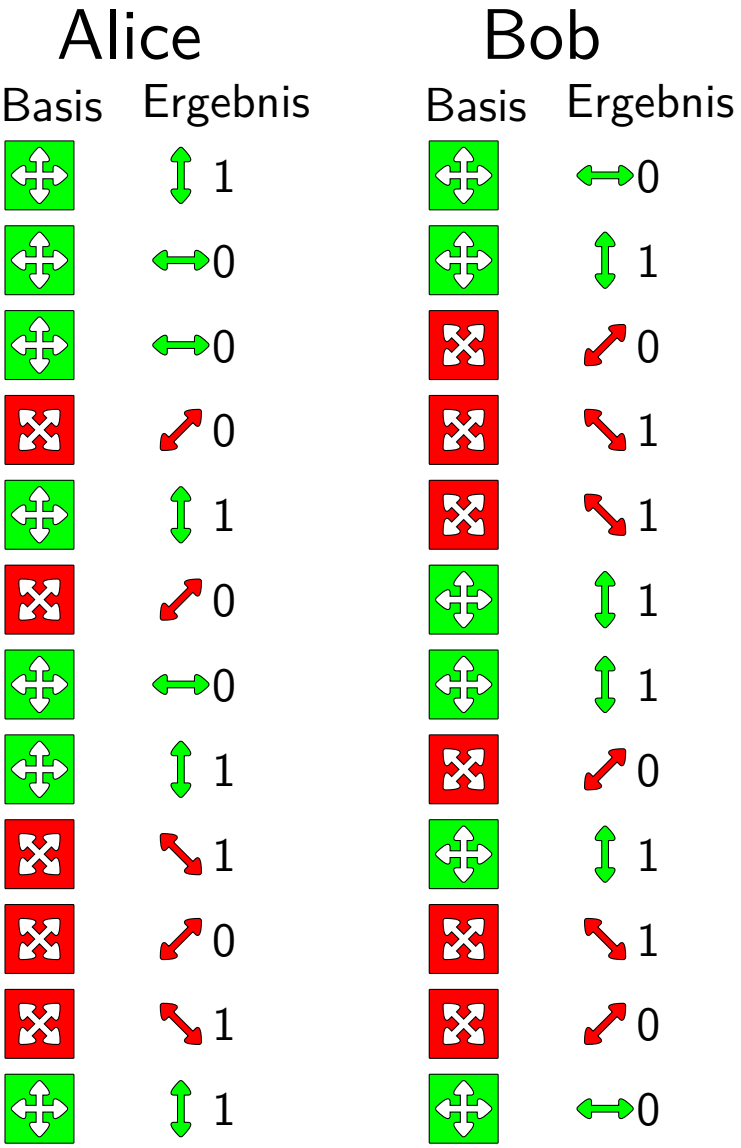
⇒ Misst Bob in der gleichen Basis, in der Alice zuvor das Teilchen präpariert hat, so erhalten beide das gleiche Bit.

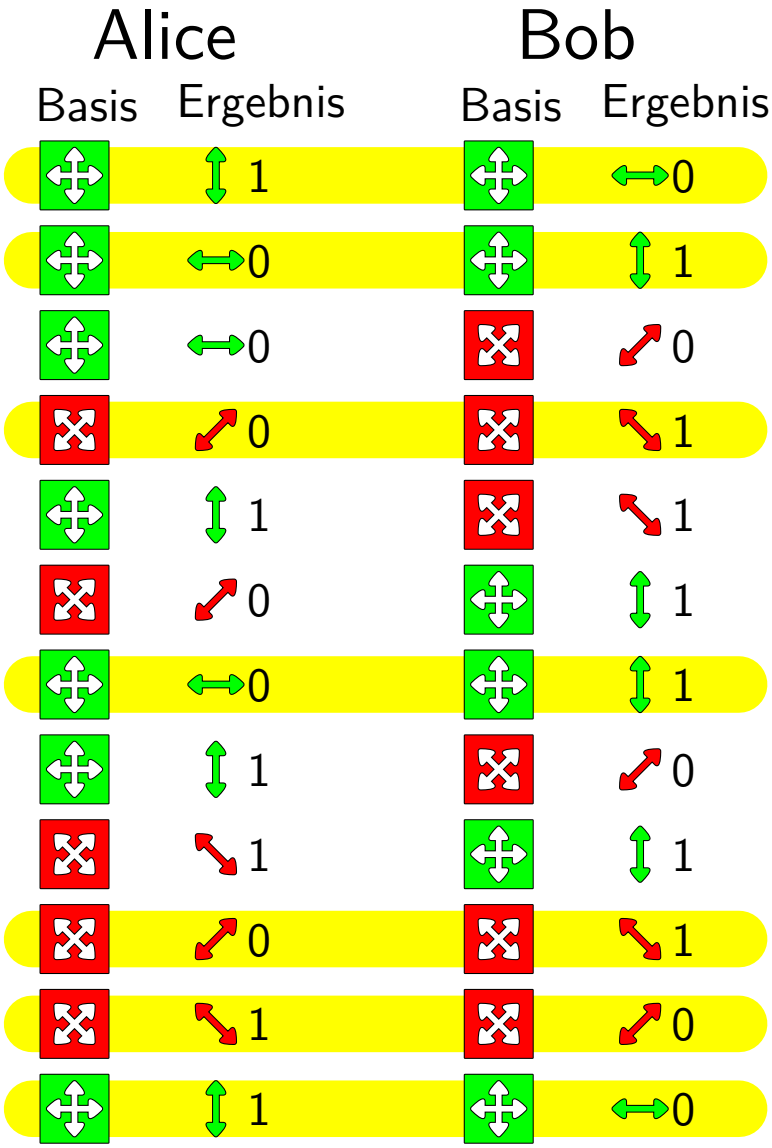


⇒ Misst Bob in der anderen Basis, so kann er entweder das gleiche Bit wie Alice erhalten oder nicht. Die Wahrscheinlichkeiten dafür sind jeweils $\frac{1}{2}$.


BB84-Protokoll
Alice
Bob
Alice Bit 1 0 1 0 1 1 0 1 0 0 1 1
Alice Basis
Bobs Basis
Bobs Bit 1 0 0 1 1 1 0 0 1 0 1 1
Schlüssel 0 1 1 0 1 0 0 1 1
= h/v
= +/−

Ekert-Protokoll




Alice
Bob
Basis
Ergebnis
Basis
Ergebnis
1
0
0
0
1
0
0
1
1
1
0
1
0
1
0
1
1
0
1
1
0
1
1
0
1
0
1
0

Quantenkryptographie

Problem bei der Vernam-Verschlüsselung: Schlüsselaustausch

Lösung: Quantenkryptographie

Akteure

Personen

Alice  Heimliche Geliebte von Bob; sie möchte ihm eine geheime Nachricht senden.

Bob  Er möchte von Alice heimlich Nachrichten empfangen.

Eve  Freundin von Bob, sie traut ihm nicht ganz und versucht daher heimlich zu lauschen.

Photonen (Qubits)

horizontal polarisiert 

vertikal polarisiert 

+45° polarisiert 

−45° polarisiert 

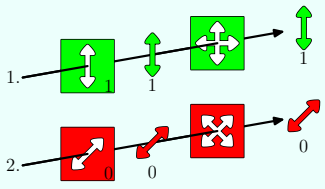
Mess- und Präparationsapparate

Bob misst Alice präpariert

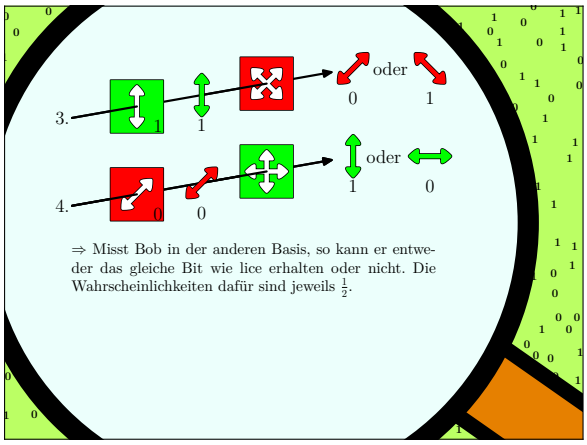
h/v Basis: 

$+/-$ Basis: 

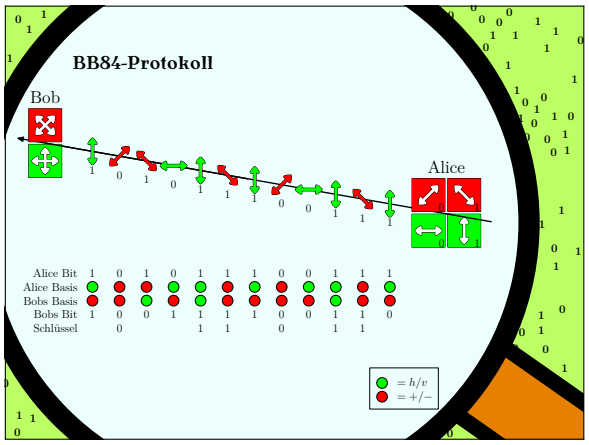
Messung

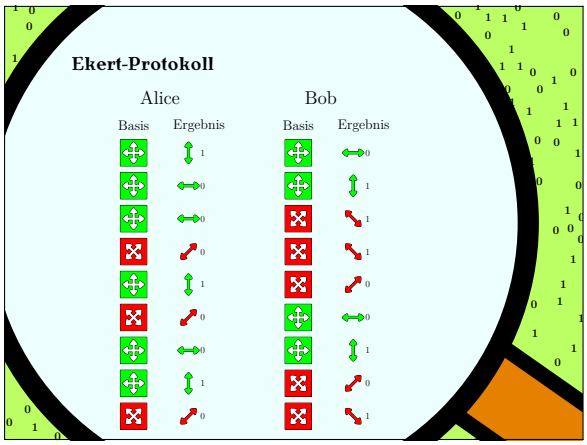


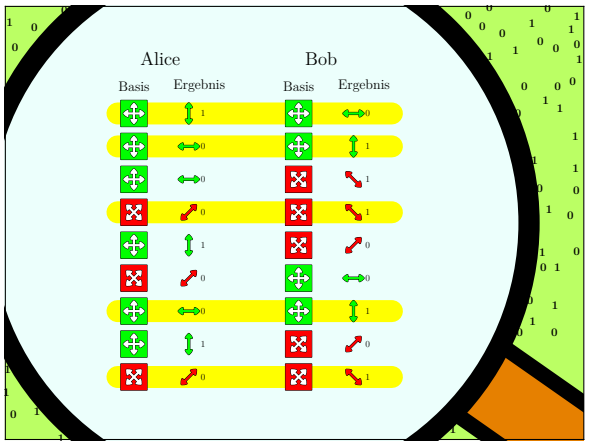
⇒ Misst Bob in der gleichen Basis, in der Alice zuvor das Teilchen räpariert hat, so erhalten beide das gleiche Bit.



⇒ Misst Bob in der anderen Basis, so kann er entweder das gleiche Bit wie lice erhalten oder nicht. Die Wahrscheinlichkeiten dafür sind jeweils $\frac{1}{2}$.







Geheime Quanten Handbuch

1. Einleitung

Geheime Quanten ist ein Quantenkryptographie-Lernprogramm für den Physikunterricht. Das Programm besteht aus folgenden Schritten:

- Schlüssel erzeugen
- Basisvergleich
- Nachricht verschlüsseln
- Nachricht entschlüsseln

Ziel dieses Programms ist es, den SchülerInnen das Prinzip der Quantenkryptographie spielerisch näher zu bringen.

2. Erste Schritte

2.1. Wie man *Geheime Quanten* startet

Sie können *Geheime Quanten* folgendermaßen starten:

Menü **Anwendungen**

Wähle **Bildung** ▸ ***Geheime Quanten***.

Befehlszeile

Um *Geheime Quanten* von der Befehlszeile zu starten, führen Sie folgenden Befehl aus:

`qrypto`

2.2. *Geheime Quanten* starten

Wenn Sie *Geheime Quanten* starten, wird das folgende Fenster erscheinen.

Abbildung 1 ***Geheime Quanten* Protokollauswahl**

In diesem Fenster kann nun das für das Lernprogramm gewünschte Protokoll ausgewählt werden. Danach erscheint, je nachdem was man angeklickt hat, eines der beiden folgenden Fenster.

Abbildung 2 ***Geheime Quanten* BB84-Protokoll**

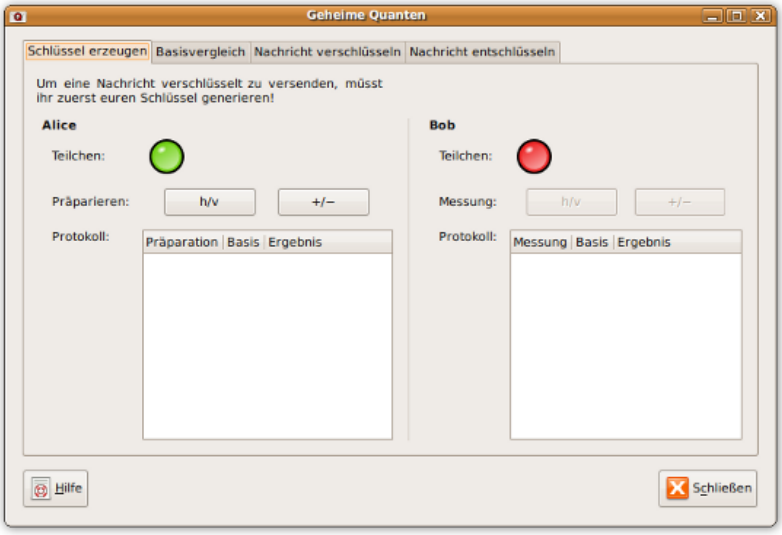
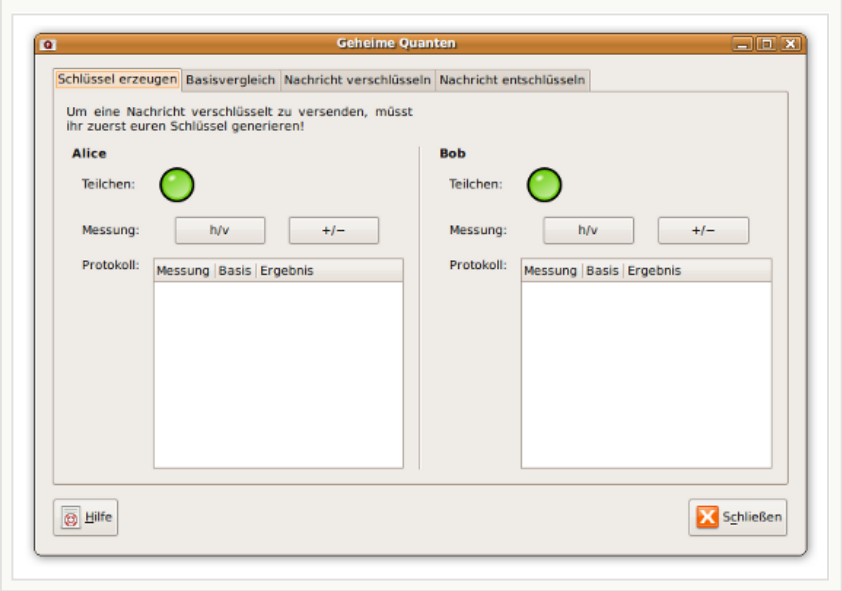


Abbildung 3 ***Geheime Quanten* Ekert-Protokoll**



Die Fenster beinhalten folgende Elemente:

Vier Reiter.

Diese simulieren alle notwendigen Schritte, um eine Nachricht mittels Quantenphysik verschlüsselt zu übermitteln.

Hilfe-Knopf.

Schließen-Knopf.

3. Vorbereitung

3.1. Einsatz im Unterricht

Dieses Lernprogramm ist gedacht für den Einsatz im Physikunterricht. Es sollte erst nach einer Einführung in die Quantenkryptographie verwendet werden, damit die SchülerInnen das Prinzip besser verstehen können.

Bevor das Spiel beginnen kann, sollte man sich überlegt haben, welches Protokoll

das Programm simulieren soll. Dafür gibt es zwei zur Auswahl:

- BB84-Protokoll
- Ekert-Protokoll (vereinfacht)

Das Lernprogramm ist für jeweils zwei SpielerInnen gedacht, wovon eine Alice und einer Bob ist. Falls die SchülerInnenzahl ungerade sein sollte, ist es auch möglich alleine zu spielen, indem man sowohl Alice als auch Bob gleichzeitig bedient. Nach einem Spiel kann es auch interessant sein, die Rollen zu tauschen.

3.2. Ziel des Spiels

Im Laufe des Spiels soll Alice an Bob eine mit Hilfe der Quantenkryptographie verschlüsselte Nachricht senden. Bob soll diese dann wieder entschlüsseln.

4. Schlüssel erzeugen

4.1. Physikalischer Hintergrund

Der erste Reiter sieht, je nachdem welches Protokoll (BB84 oder Ekert) man eingestellt hat, etwas unterschiedlich aus. Alle anderen Reiter sind in beiden Versionen gleich.

Wenn man das Ekert-Protokoll gewählt hat, so erhalten Alice und Bob immer gleichzeitig ihre Teilchen, die miteinander verschränkt sind. Diese können sie in zwei verschiedenen Basen messen:

- h/v = horizontal/vertikal
- +/− = +45°/−45°

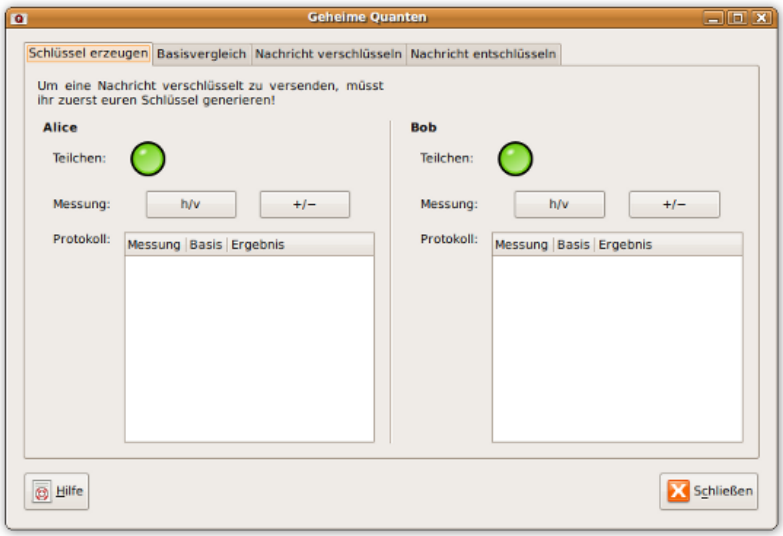
Das Ergebnis einer Messung kann entweder 0 oder 1 sein. Misst man zum Beispiel Polarisation, so bedeutet 0, dass das Teilchen horizontal polarisiert ist und 1 vertikal, falls man in der Basis h/v gemessen hat. Da die Teilchen miteinander verschränkt sind, erhalten beide immer das gleiche Ergebnis, wenn in den gleichen Basen gemessen wurde. Wird in unterschiedlichen Basen gemessen, so können die Ergebnisse zufällig gleich sein oder aber auch verschieden.

Hat man das BB84-Protokoll gewählt, so sind die Teilchen nicht miteinander verschränkt. Alice erhält hier zuerst ein Teilchen. Dieses kann sie in den beiden Basen (h/v oder +/−) präparieren. Das Teilchen erhält anschließend Bob, der es wie in der Ekert-Version messen kann.

4.2. Programmablauf

Der erste Reiter ist in zwei Hälften aufgeteilt. Der linke ist für Alice, der rechte für Bob bestimmt. Zu Beginn des Spieles haben bei der Ekert-Version beide SpielerInnen ein Teilchen zur Verfügung (Lämpchen leuchtet grün).

Abbildung 4 ***Geheime Quanten* erster Reiter**



Bei der BB84-Version leuchtet zuerst nur das Lämpchen von Alice grün. Erst wenn sie ihr Teilchen präpariert, wird Bobs Lämpchen leuchten.

Die Teilchen können nun gemessen bzw. präpariert werden, indem man sich für eine Basis (h/v oder +/−) entscheidet und auf diese klickt. Dabei ist es beim Ekert-Protokoll egal, ob Alice oder Bob beginnt. Hat zum Beispiel Alice begonnen, so schaltet ihr Lämpchen von grün auf rot um und Bob ist an der Reihe. Hat er gemessen, so leuchten beide Lämpchen wieder grün (das bedeutet, dass wieder Teilchen zum Messen vorhanden sind) und das ganze kann von vorne beginnen.

Beim BB84-Protokoll muss Alice beginnen. Erst dann kann Bob sein Teilchen messen und sein Lämpchen schaltet um auf rot. Gleichzeitig wird Alice ihr Lämpchen wieder grün und so weiter.

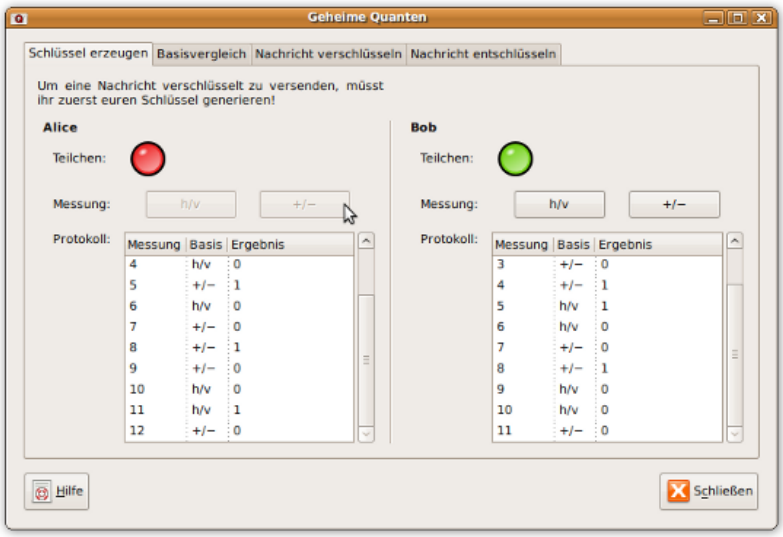
Im Feld Protokoll finden sich drei Spalten, die während den Messungen gefüllt werden. Diese sind bei beiden Versionen für Bob gleich.

- **Messung** — Gibt die Nummer der Messung an

- **Ergebnis** — Hier findet man das Ergebnis der Messung
- **Basis** — Zeigt an, in welcher Basis gemessen wurde

Bei dem BB84-Protokoll ist bei Alice die Beschriftung **Messung** durch **Präparation** ersetzt.

Abbildung 5 ***Geheime Quanten* Protokoll**



Es empfiehlt sich verschiedene Messkombinationen (z.B.: Alice +/− und Bob h/v oder Alice h/v und Bob h/v, ...) auszuprobieren, um herauszufinden, wie die Ergebnisse davon abhängen!

5. Basisvergleich

5.1. Physikalischer Hintergrund

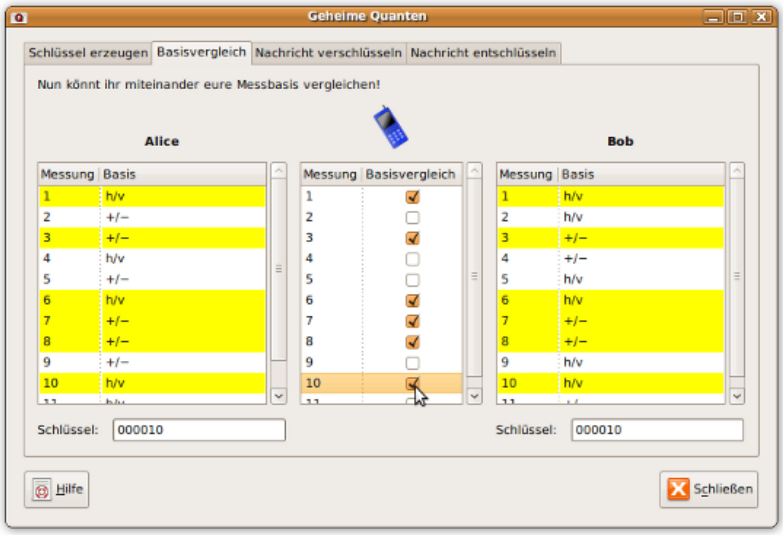
In diesem Reiter geht es um den Vergleich der Basen. Dafür tauschen Alice und Bob Informationen über einen klassischen Kanal (z.B.: Telephon, Internet, ...) aus, wann sie in welcher Basis gemessen haben. Ist die Basis die gleiche, so ist das zugehörige Bit (das hier natürlich nicht angezeigt wird, da die Ergebnisse keinesfalls

öffentlich ausgetauscht werden dürfen) Teil des Schlüssels, da ja die Teilchen verschränkt waren. Haben Alice und Bob keinen Fehler beim Vergleichen gemacht, so erhalten sie den gleichen (geheimen) Schlüssel.

5.2. Programmablauf

Nun müssen die Basen, in denen gemessen wurde, verglichen werden. Dazu wurden hier die Protokolle aus dem ersten Reiter übernommen (ausgenommen der Messergebnisse). Sind sie gleich, so wählt man sie in der mittleren Tabelle in der Spalte **Basisvergleich** aus. Die dazugehörigen Messungen im Protokoll werden dabei gelb gefärbt. Hat man irrtümlich eine falsche Zeile ausgewählt, so kann diese durch nochmaliges Klicken wieder abgewählt werden.

Abbildung 6 ***Geheime Quanten*** **Basisvergleich**



Während die richtigen Zeilen ausgewählt werden, erscheint im unteren Teil des Fensters der dazugehörige Schlüssel für Bob und für Alice. Hat man alles richtig gemacht, so sollten diese gleich sein.

Der Schlüssel sollte auf jeden Fall mindestens die Länge fünf haben, da man für die Übersetzung eines Buchstaben in Nullen und Einsen genau fünf Bits braucht! Falls der Schlüssel zu kurz sein sollte, muss man im ersten Reiter gegebenenfalls noch Messungen nachholen!

6. Nachricht verschlüsseln

6.1. Physikalischer Hintergrund

Hier kann endlich die geheime Nachricht von Alice eingegeben werden. Die Übersetzung in Nullen und Einsen geschieht folgendermaßen: Alle Buchstaben werden durchnummeriert und anschließend in Binärschreibweise (5 Bits stehen zur Verfügung) umgewandelt. Zum Beispiel ist "h" der 8. Buchstabe im Alphabet, in Binärschreibweise wäre das: 01000.

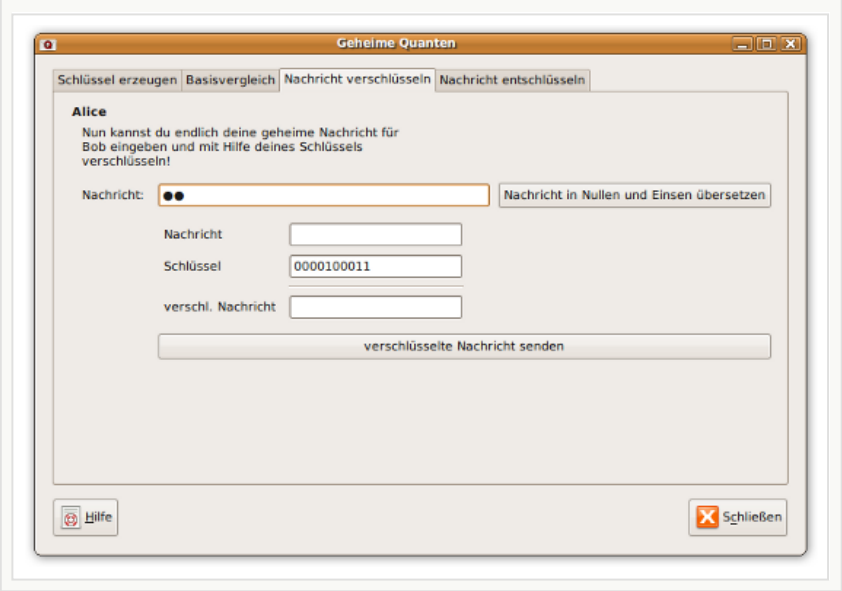
Die verschlüsselte Nachricht erhält man durch addieren, wobei gilt:

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

6.2. Programmablauf

Der dritte Reiter ist nur für Alice gedacht. Sie kann nun ihre Nachricht für Bob eingeben. Damit Bob die Nachricht nicht gleich sehen kann, erscheinen statt dem Text nur Punkte.

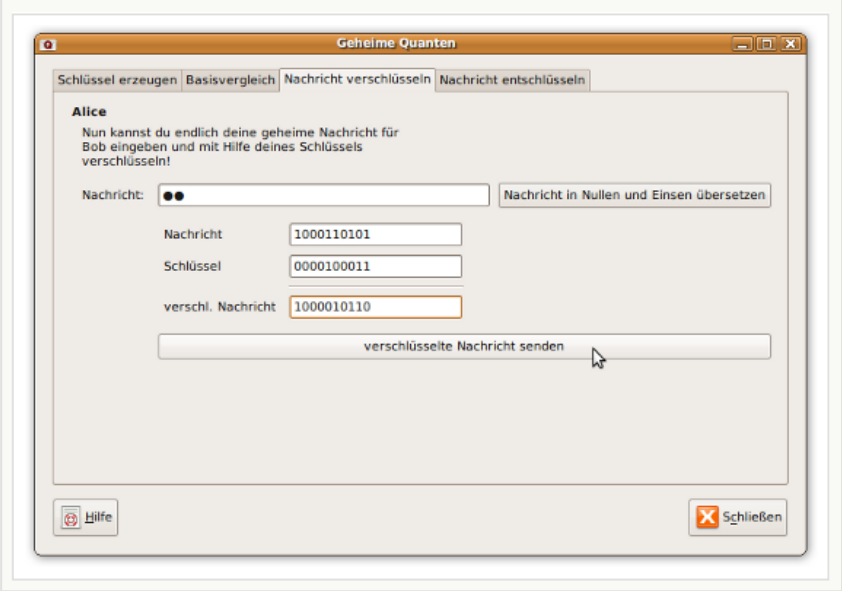
Abbildung 7 ***Geheime Quanten* Nachricht eingeben**



Durch klicken auf den Knopf **Nachricht in Nullen und Einsen übersetzen** wird der Text, den Alice eingegeben hat, dementsprechend übersetzt und erscheint im darunterliegenden Feld **Nachricht**. Der Schlüssel, der im vorigen Reiter erstellt wurde, ist im dazugehörigen Feld schon eingetragen.

Die verschlüsselte Nachricht kann jetzt im vorgesehenen Feld **verschl. Nachricht** berechnet werden. Ist der Schlüssel länger als die Nachricht, so kann man entweder bis zum letzten Bit der Nachricht rechnen und den Rest des Schlüssels ignorieren oder der Nachricht gedanklich eine 0 anhängen, je nachdem was man lieber hat, allerdings müssen Alice und Bob die gleiche Methode verwenden.

Abbildung 8 ***Geheime Quanten* verschlüsselte Nachricht berechnen**



Nun kann die Nachricht von Alice durch klicken auf den Knopf **verschlüsselte Nachricht senden** an Bob übermittelt werden. Das Programm springt automatisch auf den letzten Reiter.

Es können nur der Länge des Schlüssels entsprechend viele Zeichen eingegeben werden. Für jeden Buchstaben benötigt man fünf Bits. Will man also z.B. "qu" verschlüsseln, so braucht man einen Schlüssel der Länge 10. Außerdem werden nur folgende Zeichen akzeptiert: 'a', 'b', ... 'z', 'ä', 'ö', 'ü', 'ß', '!'.

7. Nachricht entschlüsseln

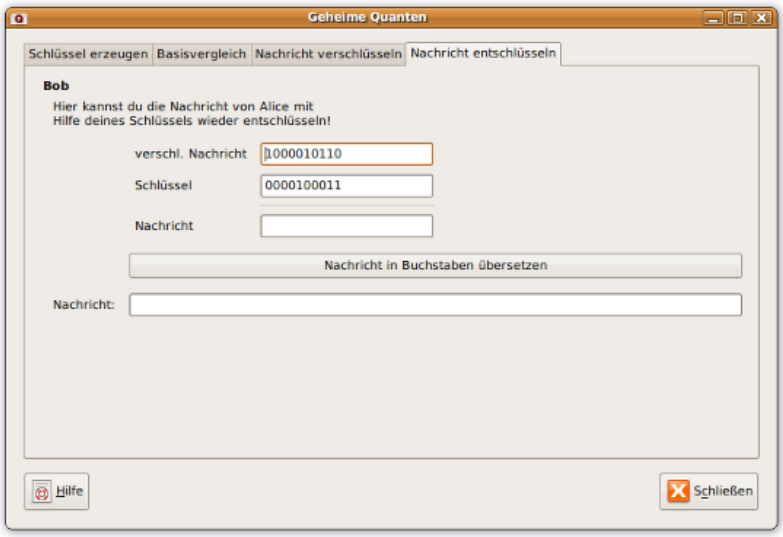
7.1. Physikalischer Hintergrund

Die Nachricht wird genauso wie beim Verschlüsseln mit dem Schlüssel addiert. Auch das Übersetzen der Nachricht in Buchstaben funktioniert nach dem gleichen Schema.

7.2. Programmablauf

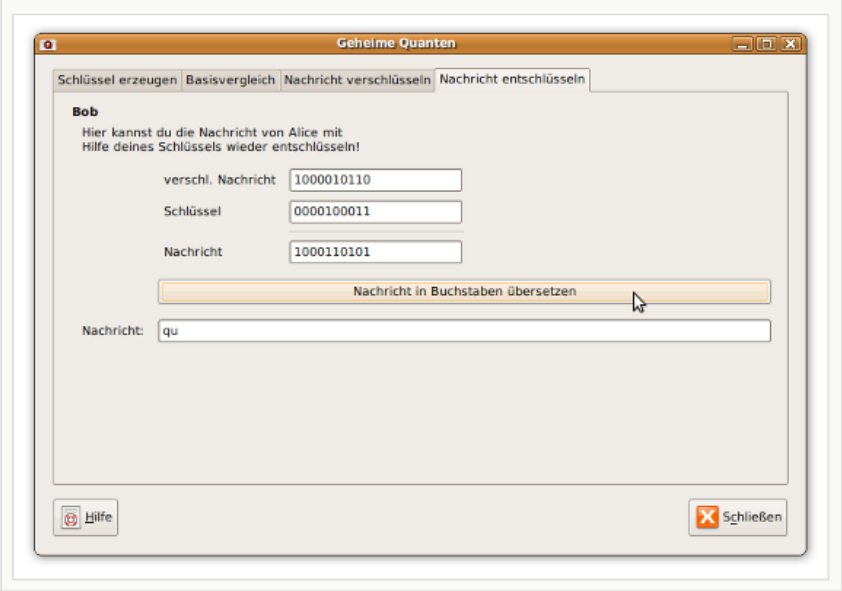
Dieser Reiter ist nur für Bob gedacht. Die verschlüsselte Nachricht von Alice sowie Bobs Schlüssel erscheinen automatisch in den dafür vorgesehenen Feldern.

Abbildung 9 ***Geheime Quanten*** **vierter Reiter**



Die Nachricht kann genauso berechnet werden, wie es Alice zuvor getan hat. Klickt man auf den Knopf **Nachricht in Buchstaben übersetzen**, so wird die von Bob berechnete Nachricht übersetzt. Es sollte nun die Nachricht, die Alice am Anfang geheim eingetippt hat, im Feld **Nachricht** erscheinen.

Abbildung 10 ***Geheime Quanten*** **entschlüsselte Nachricht**



Falls doch eine falsche Nachricht herauskommen sollte, empfiehlt es sich sowohl zu überprüfen, ob Alice und Bob den gleichen Schlüssel haben, als auch, ob man sich bei den Rechnungen nicht vertan hat.

8. Über *Geheime Quanten*

Geheime Quanten wurde von Heidemarie Knobloch im Zuge einer Diplomarbeit bei Univ. Doz. Mag. Dr. Beatrix Hiesmayr mit der Hilfe von Arthur Schuster entwickelt. Um mehr Information darüber zu finden, können Sie in meiner Diplomarbeit nachlesen oder meine Webseite besuchen.

Um Fehler zu melden oder Vorschläge bezüglich *Geheime Quanten* oder diesem Handbuch einzubringen, besuchen Sie die Homepage über das Programm.

Dieses Programm steht unter der GNU General Public license, die bei der Free Software Foundation veröffentlich ist (Version 2 der Lizenz oder, wenn Sie möchten jede spätere Version). Eine Kopie der Lizenz ist in dieser Dokumentation inkludiert; eine weitere kann in der Datei COPYING gefunden werden zusammen mit dem Quelltext von diesem Programm.

Geheime Quanten Handbuch

1. Einleitung

Geheime Quanten ist ein Quantenkryptographie-Lernprogramm für den Physikunterricht. Das Programm besteht aus folgenden Schritten:

- Schlüssel erzeugen
- Basisvergleich
- Nachricht verschlüsseln
- Nachricht entschlüsseln

Ziel dieses Programms ist es, den SchülerInnen das Prinzip der Quantenkryptographie spielerisch näher zu bringen.

2. Erste Schritte

2.1. Wie man *Geheime Quanten* startet

Sie können *Geheime Quanten* folgendermaßen starten:

Menü **Anwendungen**

Wähle **Bildung ▸ *Geheime Quanten* (Server)** für das Serverprogramm,

bzw. **Bildung ▸ *Geheime Quanten* (Client)** für das SchülerInnenprogramm.

Befehlszeile

Um *Geheime Quanten* von der Befehlszeile zu starten, führen Sie folgenden Befehl aus:

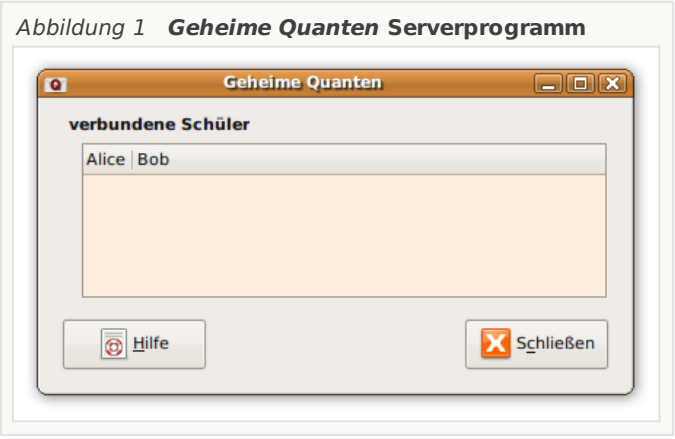
`qrypto-server` für den Server,

`qrypto-client` für die SchülerInnenprogramme.

2.2. *Geheime Quanten* starten

Wenn Sie *Geheime Quanten* (Server) starten wird das folgende Fenster erscheinen.

Abbildung 1 ***Geheime Quanten*** **Serverprogramm**



Wenn Sie *Geheime Quanten* (Client) starten wird zuerst ein Fenster zur Namenseingabe erscheinen.

Abbildung 2 ***Geheime Quanten*** **Namenseingabe**

3. Vorbereitung

3.1. Einsatz im Unterricht

Dieses Lernprogramm ist gedacht für den Einsatz im Physikunterricht. Es sollte erst nach einer Einführung in die Quantenkryptographie verwendet werden, damit die SchülerInnen das Prinzip besser verstehen können.

Das Lernprogramm läuft über Netzwerk und ist für jeweils zwei SpielerInnen gedacht, wovon eine Alice und einer Bob ist. Die Benutzeroberflächen von Alice und Bob sind auf die Rollen abgestimmt. Der Lehrer/ die Lehrerin hat ein eigenes Fenster, indem man sehen kann, wer mit wem über Netzwerk verbunden ist. Die Rollen und welche SchülerInnen verbunden sind, wählt der Computer automatisch aus. Falls die SchülerInnenzahl ungerade sein sollte, sollte der Lehrer/ die Lehrerin ebenfalls mitspielen.

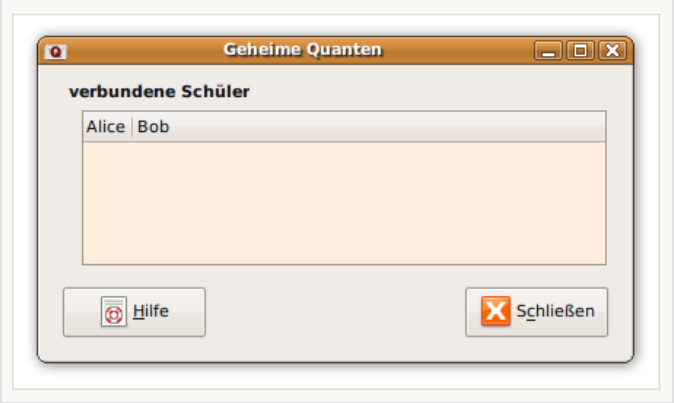
3.2. Ziel des Spiels

Im Laufe des Spiels soll Alice an Bob eine mit Hilfe der Quantenkryptographie verschlüsselte Nachricht senden. Bob soll diese dann wieder entschlüsseln. Die Nachricht könnte zum Beispiel aus den ersten drei Buchstaben der Namen der SchülerInnen bestehen. Dann bestünde die Aufgabe darin, herauszufinden, mit wem man über Netzwerk verbunden ist.

4. Server-Programm

Das Server-Programm ist nur für den Lehrer/ die Lehrerin gedacht. Dieses muss als erstes laufen, denn erst dann können die SchülerInnen ihr Programm starten. Die Benutzeroberfläche sieht folgendermaßen aus:

Abbildung 3 ***Geheime Quanten* Serverprogramm**



Wenn die SchülerInnen nun ihr Programm starten, kann der Lehrer/ die Lehrerin sehen, wer sich schon angemeldet hat und wer mit wem verbunden ist. Letztere Information besitzt nur der Lehrer/ die Lehrerin. Die SchülerInnen können sofort mit dem Lernspiel beginnen, sobald ihnen vom Computer ein zweiter Spieler/ eine zweite Spielerin zugeteilt wurde. Die Zuteilung erfolgt nach der Anmeldezeit.

Abbildung 4 ***Geheime Quanten*** **Serverprogramm: eingeloggte SchülerInnen**

Wenn die SchülerInnen ihr Programm geschlossen haben, so wird ihr Name im Serverprogramm grau hinterlegt.

Abbildung 5 ***Geheime Quanten*** **Serverprogramm: ein paar SchülerInnen haben ihr Programm geschlossen**

Beim Server-Programm sollte man aufpassen, dass man es nicht versehentlich schließt, da sonst alle *Geheime Quanten* Programme, die mit dem Server verbunden sind mit geschlossen werden. Als Sicherheitsmaßnahme kommt allerdings noch ein Fenster, indem man nochmals gefragt wird, ob man das Programm tatsächlich beenden will.

5. Anmeldung

Nachdem das Programm gestartet wurde, erscheint folgendes Anmeldefenster.

Abbildung 6 ***Geheime Quanten*** **SchülerInnenprogramm: Namenseingabe**

Nachdem man den Namen in das vorgesehene Feld eingegeben hat, kommt man über den Knopf **Verbinden** direkt zum Hauptprogramm und das Spiel kann beginnen.

6. Schlüssel erzeugen

6.1. Physikalischer Hintergrund

Im ersten Reiter erhält zuerst Alice ein Teilchen, das sie in zwei verschiedenen Basen präparieren kann:

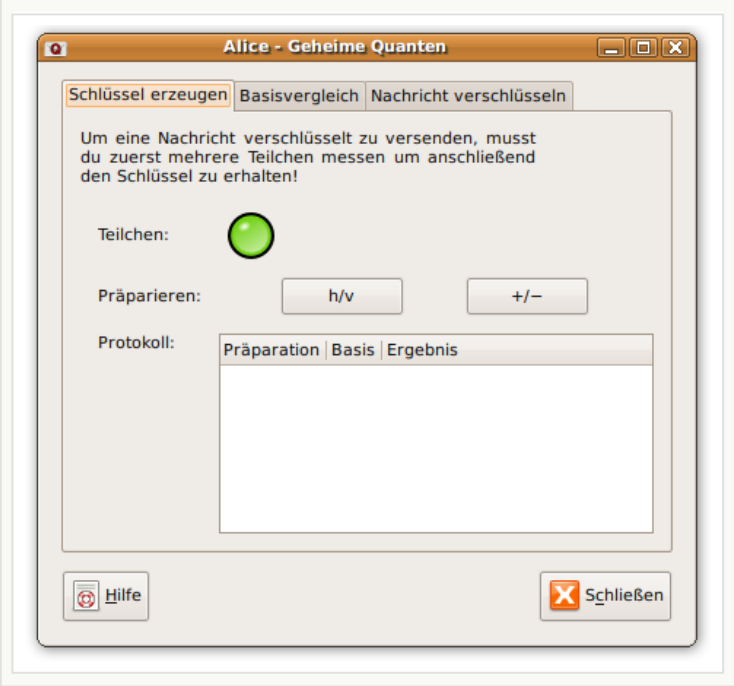
- h/v = horizontal/vertikal
- +/− = +45°/−45°

Das gesendete Teilchen (Ergebnis) kann dabei entweder 0 oder 1 sein. Danach wird es an Bob weitergeschickt, der es in den gleichen zwei Basen messen kann. Das Ergebnis kann ebenfalls entweder 0 oder 1 sein. Misst man zum Beispiel Polarisation, so bedeutet 0, dass das Teilchen horizontal polarisiert ist und 1 vertikal, falls man in der Basis h/v gemessen hat. Wenn Alice in der gleichen Basis präpariert hat, in der Bob anschließend misst, so erhalten beide immer das gleiche Ergebnis. Wird in unterschiedlichen Basen gemessen, so können die Ergebnisse zufällig gleich sein oder aber auch verschieden.

6.2. Programmablauf

Der erste Reiter ist bei Alice und Bob bis auf die Beschriftungen genau gleich. Zu Beginn des Spieles hat Alice ein Teilchen zur Verfügung (Lämpchen leuchtet grün), Bob allerdings noch nicht (Lämpchen leuchtet rot).

Abbildung 7 ***Geheime Quanten* erster Reiter**



Das Teilchen kann nun von Alice präpariert werden, indem sie sich für eine Basis (h/v oder +/−) entscheidet und auf diese klickt. Danach schaltet ihr Lämpchen von grün auf rot um und Bob ist an der Reihe. Hat er gemessen, so leuchtet wieder Alice Lämpchen grün und das ganze kann von vorne beginnen.

Im Feld Protokoll finden sich drei Spalten, die während den Messungen gefüllt werden:

- **Präparation bzw. Messung** — Gibt die Nummer der Präparation bzw. Messung an
- **Ergebnis** — Hier findet man das Ergebnis der Präparation bzw. Messung
- **Basis** — Zeigt an, in welcher Basis präpariert bzw. gemessen wurde

Abbildung 8 ***Geheime Quanten* Protokoll**

7. Basisvergleich

7.1. Physikalischer Hintergrund

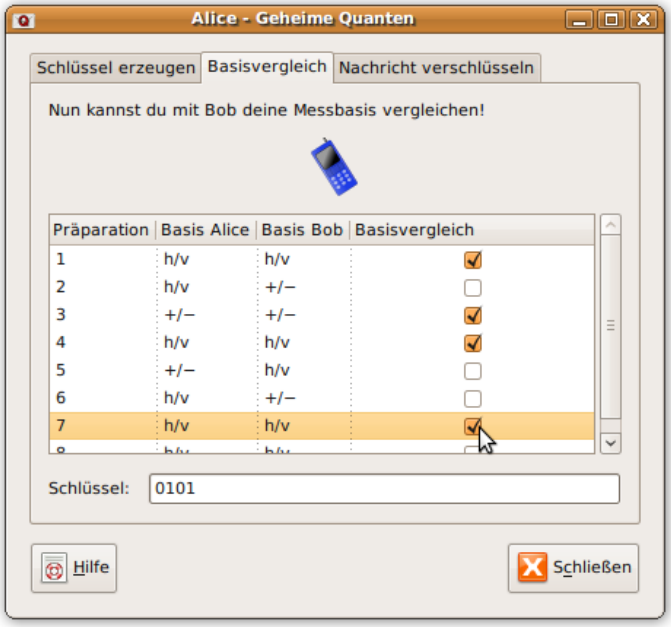
In diesem Reiter geht es um den Vergleich der Basen. Dafür tauschen Alice und Bob Informationen über einen klassischen Kanal (z.B.: Telephon, Internet, ...) aus, wann sie in welcher Basis präpariert bzw. gemessen haben. Ist die Basis die gleiche, so ist das zugehörige Bit (das hier natürlich nicht angezeigt wird, da die Ergebnisse keinesfalls öffentlich ausgetauscht werden dürfen) Teil des Schlüssels, da sie ja auf diesem Wege gleiche Ergebnisse erhalten. Haben Alice und Bob keinen Fehler beim Vergleichen gemacht, so bekommen sie also den gleichen (geheimen) Schlüssel.

7.2. Programmablauf

Nun müssen die Basen, in denen präpariert bzw. gemessen wurde, verglichen

werden. Alice erhält nun die Auskunft, in welcher Basis Bob gemessen hat und umgekehrt. In der ersten Spalte der Tabelle ist die Nummer der Präparation (bzw. Messung) eingetragen, in den weiteren beiden die Basen von Alice und Bob. Sind sie gleich, so wählt man sie in der vierten Spalte **Basisvergleich** aus. Die dazugehörigen Messungen bzw. Präparationen im Protokoll im vorherigen Tab werden dabei gelb gefärbt. Hat man irrtümlich eine falsche Zeile ausgewählt, so kann diese durch nochmaliges Klicken wieder abgewählt werden.

Abbildung 9 ***Geheime Quanten* Basisvergleich**



Während die richtigen Zeilen ausgewählt werden, erscheint im unteren Teil des Fensters der dazugehörige Schlüssel für Bob und für Alice. Haben Alice und Bob jeweils die richtigen Basen ausgewählt, so sollten beide nun den gleichen Schlüssel besitzen. Dabei ist auch wichtig, dass keine Zeilen übersehen werden, sodass wirklich alle übereinstimmenden Basen ausgewählt werden!

Der Schlüssel sollte auf jeden Fall mindestens die Länge fünf haben, da man für die Übersetzung eines Buchstaben in Nullen und Einsen genau fünf Bits braucht! Falls der Schlüssel zu kurz sein sollte, muss man im ersten Reiter gegebenenfalls noch Messungen nachholen!

8. Nachricht verschlüsseln

8.1. Physikalischer Hintergrund

Hier kann endlich die geheime Nachricht von Alice eingegeben werden. Die Übersetzung in Nullen und Einsen geschieht folgendermaßen: Alle Buchstaben werden durchnummeriert und anschließend in Binärschreibweise (5 Bits stehen zur Verfügung) umgewandelt. Zum Beispiel ist "h" der 8. Buchstabe im Alphabet, in Binärschreibweise wäre das: 01000.

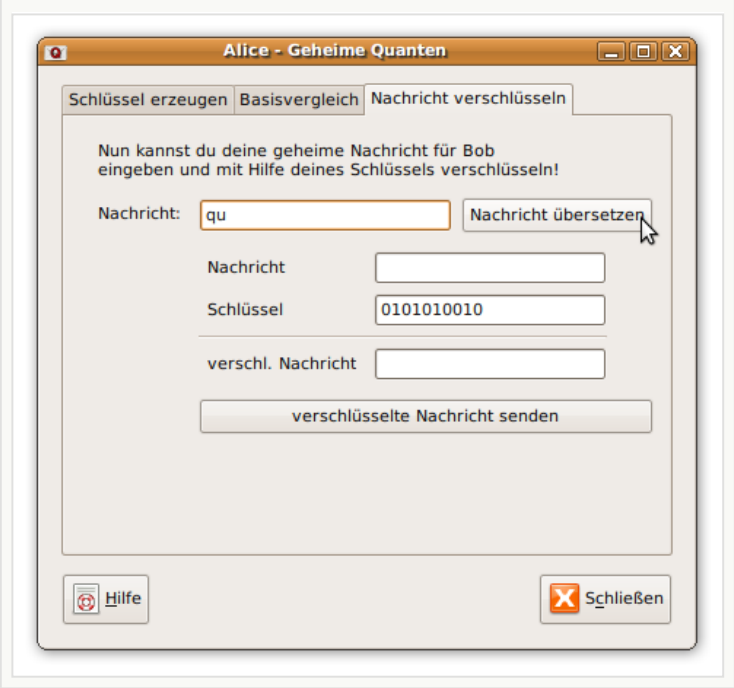
Die verschlüsselte Nachricht erhält man durch addieren, wobei gilt:

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

8.2. Programmablauf

Diesen Reiter besitzt nur Alice. Sie kann nun ihre Nachricht für Bob eingeben.

Abbildung 10 ***Geheime Quanten* Nachricht eingeben**



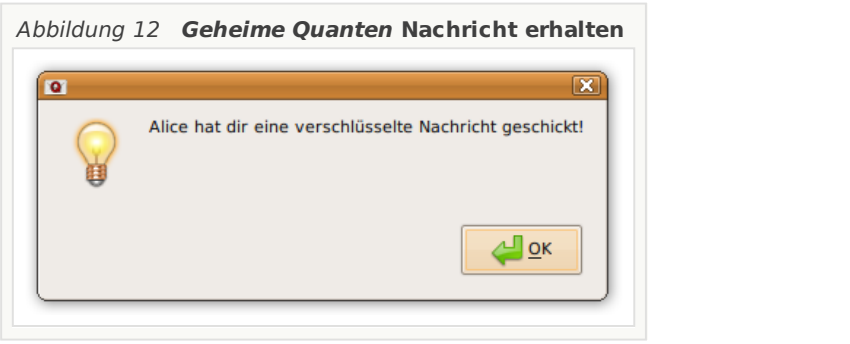
Durch klicken auf den Knopf **Nachricht in Nullen und Einsen übersetzen** wird der Text, den Alice eingegeben hat, dementsprechend übersetzt und erscheint im darunterliegenden Feld **Nachricht**. Der Schlüssel, der im vorigen Reiter erstellt wurde, ist im dazugehörigen Feld schon eingetragen.

Die verschlüsselte Nachricht kann jetzt im vorgesehenen Feld **verschl. Nachricht** berechnet werden. Ist der Schlüssel länger als die Nachricht, so kann man entweder bis zum letzten Bit der Nachricht rechnen und den Rest des Schlüssels ignorieren oder der Nachricht gedanklich eine 0 anhängen, je nachdem was man lieber hat, allerdings müssen Alice und Bob die gleiche Methode verwenden.

Abbildung 11 ***Geheime Quanten* verschlüsselte Nachricht berechnen**

Nun kann die Nachricht von Alice durch klicken auf den Knopf **verschlüsselte Nachricht senden** an Bob übermittelt werden. Bob bekommt nun die Information, dass er eine Nachricht bekommen hat.

Abbildung 12 ***Geheime Quanten*** **Nachricht erhalten**



Es können nur der Länge des Schlüssels entsprechend viele Zeichen eingegeben werden. Für jeden Buchstaben benötigt man fünf Bits.

Will man also z.B. "qu" verschlüsseln, so braucht man einen Schlüssel der Länge 10. Außerdem werden nur folgende Zeichen akzeptiert: 'a', 'b', ... 'z', 'ä', 'ö', 'ü', 'ß', '!'.

9. Nachricht entschlüsseln

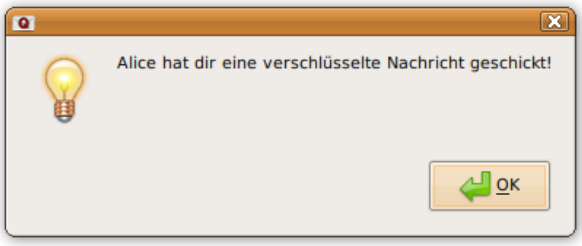
9.1. Physikalischer Hintergrund

Die Nachricht wird genauso wie beim Verschlüsseln mit dem Schlüssel addiert. Auch das Übersetzen der Nachricht in Buchstaben funktioniert nach dem gleichen Schema.

9.2. Programmablauf

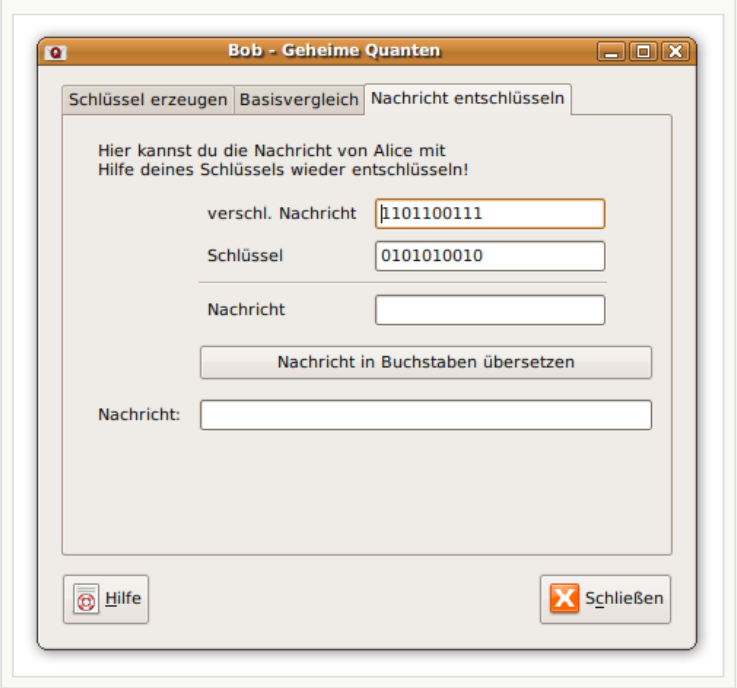
Diesen Reiter besitzt nur Bob. Sobald Alice ihre Nachricht verschickt hat, bekommt Bob die Information, dass er eine Nachricht erhalten hat. Diese kann er nun mit **OK** bestätigen.

Abbildung 13 ***Geheime Quanten*** **Nachricht erhalten**



Die verschlüsselte Nachricht von Alice sowie Bobs Schlüssel erscheinen dann automatisch in diesem Reiter in den dafür vorgesehenen Feldern. Nun kann sich Bob ans entschlüsseln machen.

Abbildung 14 ***Geheime Quanten*** **vierter Reiter**



Die Nachricht kann genauso berechnet werden, wie es Alice zuvor getan hat. Klickt man auf den Knopf **Nachricht in Buchstaben übersetzen**, so wird die von Bob berechnete Nachricht übersetzt. Es sollte nun die Nachricht, die Alice gesendet hat, im Feld **Nachricht** erscheinen.

Abbildung 15 ***Geheime Quanten* entschlüsselte Nachricht**

Falls doch eine falsche Nachricht herauskommen sollte, empfiehlt es sich in einem anschließenden Gespräch sowohl zu überprüfen, ob Alice und Bob den gleichen Schlüssel gehabt haben, als auch, ob man sich bei den Rechnungen nicht vertan hat. Dazu wäre es gut, Schlüssel und Rechnungen auf einem Stück Papier zu notieren.

10. Über *Geheime Quanten*

Geheime Quanten wurde von Heidemarie Knobloch im Zuge einer Diplomarbeit bei Univ. Doz. Mag. Dr. Beatrix Hiesmayr mit der Hilfe von Arthur Schuster entwickelt. Um mehr Information darüber zu finden, können Sie in meiner Diplomarbeit nachlesen oder meine Webseite besuchen.

Um Fehler zu melden oder Vorschläge bezüglich *Geheime Quanten* oder diesem Handbuch einzubringen, besuchen Sie die Homepage über das Programm.

Dieses Programm steht unter der GNU General Public license, die bei der Free Software Foundation veröffentlich ist (Version 2 der Lizenz oder, wenn Sie möchten jede spätere Version). Eine Kopie der Lizenz ist in dieser Dokumentation inkludiert;

eine weitere kann in der Datei COPYING gefunden werden zusammen mit dem Quelltext von diesem Programm.

Literatur

[1] Beatrix C. Hiesmayr. Theoretische Physik fürs Lehramt: L2. 2008

[2] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. , 175, 1984.

[3] Matthias Homeister. *Quantum Computing vestehen*. Vieweg, 2 edition, 2008.

[4] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661-663, 1991.

[5] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter and A. Zeilinger. Quantum cryptography with entangled photons. *Physical Review Letters*, 84(20):4729-4732, 2000.

[6] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett and C. G. Petersonet al.. Long distance decoy state quantum key distribution in optical fiber. *J. Cryptology Phys Rev Lett*, 98:010503, 1992.

[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3-28, 1992.

[8] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter and P. M. Gormanet al.. Quantum cryptography: A step towards global key distribution. *Nature*, 419(6906):450-450, 2002.

[9] A. Poppe, A. Fedrizzi, T. Loruenser, O. Maurhardt and R. Ursinet al.. Practical Quantum Key Distribution with Polarization-Entangled Photons. *Optics Express*, 12:3865, 2004.

[10] T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin and F. Tiefenbacheret al.. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical review letters*, 98(1):10504, 2007.

[11] D. Stucki, N. Walenta, F. Vannel, R. T. Thew and N. Gisinet al.. High rate, long-distance quantum key distribution over 250km of ultra low loss fibres. *Arxiv preprint arXiv:0903.3907*, 2009.

[12] Isaac L. Chuang Michael A. Nielsen. *Quantum Computation and Quantum Information*. cambridge university press , 2000.

[13] PGP Team. PGP Corporation, an Introduction to Cryptography. June-2004, 2004

[14] D. Gottesman and I. Chuang. Quantum digital signatures. *Arxiv preprint quant-ph/0105032*, 2001.

[15] Nicolai Friis Reinhold A. Bertlmann. Theoretical Physics T2, Quantum Mechanics. 2008

[16] Jürgen Audretsch. *Verschränkte Systeme, Die Quantenphysik auf neuen Wegen*. Wiley-vch, 2005.

[17] Mirko Zeppmeisel. Einführung in die Grundlagen der Quantenkryptographie. Master's thesis, Ludwig-Maximilians-Universität, München, 2005/2006.

[18] Beatrix C.Hiesmayr. Zur Idee der Quantenkryptographie. 2004

[19] Gregor Weihs. Ein Experiment zum Test der Bellschen Ungleichung unter Einsteinscher Lokalität. Master's thesis, Universität Wien, Institut für Experimentalphysik , 1999.

[20] Silvia Arroyo Camejo. *Skurille Quantenwelt*. Springer-Verlag, 2006.

[21] Franz Embacher. Quantentheorie. http://homepage.univie.ac.at/franz.embacher/Quantentheorie.

[22] Heidemarie Knobloch. Quantenkryptographie in der Schule. http://homepage.univie.ac.at/heidemarie.knobloch.

[23] LMU München Lehrstuhl für Didaktik der Physik. Münchener Internetprojekt zur Lehrerfortbildung in Quantenmechanik. http://www.cip.physik.uni-muenchen.de/~milq/milq_spezialp01.html.

Abbildungen

Nachwort

Am Ende dieser Arbeit möchte ich mich bei allen bedanken, die mich dabei unterstützt haben, insbesondere bei meiner Diplomarbeitsbetreuerin Univ. Doz. Mag. Dr. Beatrix Hiesmayr für die angenehme Zusammenarbeit, vor allem auch dafür, dass sie mir viel Freiraum für meine eigenen Ideen gegeben hat und mich darin immer wieder bestärkt hat. Mein Dank gilt auch meinen Eltern (Eva und Gerald Knobloch) und Großeltern (Erna Knobloch, Erich und Elfriede Krainz) für die finanzielle Unterstützung im Studium, sowie meinen zukünftigen Schwiegereltern (Dr. Lily Wilmes und Dr. Peter Maria Schuster). Bedanken möchte ich mich auch bei meinen ehemaligen LehrerInnen in der Schulzeit (insbesondere Mag. Margit Thir (†), Mag. Gerhard Theiser und Mag. Alfred Nussbaumer), die mich für Physik und Mathematik so sehr begeistert haben, dass ich es schlussendlich studiert habe. Weiters möchte ich mich auch bei Mag. Robert Pitzl dafür bedanken, dass ich das Lernprogramm in seiner Klasse ausprobieren durfte.

Einen besonderen Dank möchte ich hiermit meinem Verlobten Arthur Schuster aussprechen, dem ich auch diese Arbeit widme. Er hat mir nicht nur beigebracht, wie man objektorientiert programmiert, sondern auch immer wieder bei auftretenden Problemen geduldig weitergeholfen und schließlich war es sein Verdienst, das Programm auch auf Windows und Mac OS X sowie die Netzwerkversion zum Laufen zu bringen.

Lebenslauf

Persönliche Daten

Name:	Heidemarie Elisabeth Knobloch
Geburtsdatum:	23.03.1987
Geburtsort:	Melk
Staatsbürgerschaft:	Österreich

Ausbildung

1993-1997	Volksschule Aggsbach-Dorf
1997-2001	Gymnasium Melk
2001-2005	Oberstufenrealgymnasium Melk mit bildnerischem Schwerpunkt
2005-2009	Lehramtsstudium Mathematik und Physik

Berufliche Tätigkeit

2008	Tutorin am physikalischen Institut
	diverse kleinere Arbeiten (z.B. Kinderführungen bei der Langen Nacht der Forschung)