Quantenkryptographie

TOBIAS, RAINER
TOBIAS.RAINER@GMAIL.COM

Zusammenfassung

Diese Arbeit beschäftigt sich mit dem äußerst spannenden Thema der Quantenkryptographie, einem Datenverschlüsselungsverfahren, das auf quantenmechanischen Prinzipien beruht und verspricht, absolut sicher zu sein. Im ersten Teil werden einige Grundlagen der Quantenphysik behandelt, die für das Verständnis der Quantenkryptographie wichtig sind. Im Weiteren begeben wir uns auf eine Reise durch die Kryptographie, beginnend bei den Anfängen der Verschlüsselung bis zum mathematisch sicheren Verfahren des One-Time-Pads, das grundlegend für die Quantenkryptographie ist. Abschließend wird ein vielversprechendes Verfahren zum Schlüsselaustausch mit Hilfe der Quantenphysik vorgestellt und Möglichkeiten für eine Einbindung in der Schule angeschnitten.

1 Einleitung

Verschlüsselung von Informationen ist für unser tägliches Leben extrem wichtig, denn viele alltägliche Handlungen wären ohne Geheimhaltung der Daten kaum vorstellbar. Wo Daten verschlüsselt werden, wird jedoch auch immer versucht diese Verschlüsselungen zu knacken. Genau hier bietet die Quantenphysik die Möglichkeit für eine absolut abhörsichere Übertragung von Informationen.

2 Wichtige quantenmechanische Grundlagen

In diesem Kapitel möchte ich einige wichtige Grundlagen der Quantenphysik erläutern. Das Augenmerk liegt dabei auf relevanten Themen für das Verständnis der Quantenkryptographie.

2.1 Superposition

In der Quantenphysik können Teilchen in einem Überlagerungszustand mehrerer Zustände existieren. Dieses Phänomen nennt man Superposition und widerspricht unserer klassischen Weltanschauung. Betrachten wir beispielsweise den Ort, dann können wir guten Gewissens sagen, dass sich eine Person zu jedem Zeitpunkt an genau einem bestimmten Ort aufhält. Bei quantenphysikalischen Teilchen verhält sich das jedoch anders: ein solches Teilchen kann sich an keinem bestimmten Ort befinden. Vielmehr hält sich das Teilchen an mehreren Orten „gleichzeitig“ auf. Sobald aber versucht wird das Teilchen zu messen und somit den Ort zu bestimmen, stellt man fest, dass es sich doch an einem bestimmten Ort aufhält. Ein Teilchen welches ursprünglich also in einem Überlagerungszustand existiert, geht durch die Messung in einen konkreten Zustand über. Genauer erklärt wird dieser Übergang durch zwei unterschiedliche Theorien: der Kopenhagener Deutung, die auf Niels Bohr (1885 – 1962) zurückgeht, und der Dekohärenz Theorie. In dieser Arbeit will ich jedoch nicht genauer auf die beiden Theorien eingehen, es reicht zu wissen, dass quantenmechanische Teilchen in einem Überlagerungszustand existieren, der durch Beobachtung bzw. Messung des Teilchens zerstört werden kann. (vgl. Giancoli 2011, 584-593; Kofler 2011; Steinberger 2011, 37-41)

2.2 Verschränkung

Bei der Verschränkung handelt es sich um ein wichtiges quantenmechanisches Phänomen, das besagt, dass z.B. verschränkte Photonenpaare selbst dann miteinander verbunden bleiben, wenn die einzelnen Teilchen Lichtjahre voneinander entfernt sind. Wird die Eigenschaft eines der Teilchen geändert, indem beispielsweise die Polarisation bestimmt wird, dann reagiert sofort auch das andere Teilchen darauf. Es können sich nur quantenmechanische Objekte in einem Zustand der Verschränkung befinden, aber man kann das Prinzip trotzdem mit makroskopischen Objekten veranschaulichen. Angenommen wir besäßen ein verschränktes Würfelpaar (was natürlich nicht wirklich möglich ist) und positionieren einen Würfel am Nordpol und den anderen am Südpol. Wird nun mit dem Nordpol-Würfel ein Einser gewürfelt, dann würde sofort auch der Würfel am Südpol einen Einser anzeigen. Wichtig hierbei ist das Wort „sofort“, denn die zwei Ereignisse geschehen wirklich zur selben Zeit. Nachdem Informationen nur mit maximal Lichtgeschwindigkeit ausgetauscht werden können, ist eine „Absprache“ zwischen den beiden Teilchen also ausgeschlossen. Sie besitzen eine Art „telepathische“ Verbindung und diese mit dem klassischen physikalischen Weltbild nicht vereinbare Eigenschaft veranlasste Einstein zur

Aussage, dass es sich um eine „spukhafte Fernwirkung“ handelt. (vgl. Steinberger 2011, 41; Zeilinger 2003, 65-72)
In der Quantenkryptographie werden verschränkte Photonenpaare zu Alice und Bob (so nennt man die beiden kommunizierenden Parteien in der Kryptographie) geschickt. Misst z.B. Alice eine Eigenschaft des Photons, dann weiß sie, dass das andere Teilchen auch im selben Zustand sein muss.

2.3 Die Bellsche Ungleichung

Wenn in der Physik von lokalem Realismus gesprochen wird, dann werden zwei Annahmen als sicher angenommen: (vgl. Kofler 2011; Pajic 2013, 15)

- Realismus: Objekte besitzen ihre Eigenschaften unabhängig von der Messung.
- Lokalität: Messungen an einem Ort beeinflussen keine Messungen an einem anderen Ort.

Der Physiker John Bell (1928 – 1990) erstellte eine Ungleichung, die für alle lokal-realistischen Theorien gilt, aber in der Quantenmechanik verletzt wird. Somit zeigte Bell, dass es sich bei der Quantenmechanik nicht um eine Theorie des lokalen Realismus handeln kann.
Kofler zeigt wie wir die Bellsche Ungleichung mit einer einfachen Überlegung herleiten können: Angenommen Alice und Bob sind unsere beiden Experimentatoren. Zufällige Würfelpaare werden nun von einer dritten Person präpariert und jeweils ein Würfel wird zu Alice gebracht und der andere zu Bob. Sie können dann eine von zwei Größen messen, entweder sie messen die Farbe (rot oder schwarz) oder die Parität (gerade oder ungerade). Messen Alice und Bob die Farbe ihres Würfels, dann nennen sie das Ergebnis A_1 bzw. B_1, messen sie die Parität sind die Resultate A_2 bzw. B_2. Wenn eine Messung die Farbe rot ergibt, weisen sie dem Resultat den Wert 1 zu, ansonsten -1. Genauso gehen sie bei der Paritätsmessung vor, bei einem geraden Ergebnis wird der Wert 1 zugewiesen, andernfalls -1. Wir können nun folgende Gleichung aufstellen:

$$A_1(B_1 + B_2) + A_2(B_1 - B_2) = \pm 2$$

Das ist leicht zu überprüfen, entweder B_1 und B_2 nehmen die selben Werte an (also beide $+1$ oder -1), dann wird die Differenz in der rechten Klammer 0 und die Summer der linken Klammer ± 2, oder B_1 und B_2 nehmen unterschiedliche Werte an ($+1$ und -1), dann wird die linke Klammer 0 und die rechte Klammer ± 2. Wird nun jeweils mit dem Wert A_1 bzw. A_2 multipliziert, der nach Voraussetzung entweder $+1$ oder -1 ist, dann lautet das Ergebnis wieder ± 2. Durch Ausmultiplizieren der Klammerausdrücke erhält man:

$$A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2 = \pm 2$$

Werden nun unzählige solcher Würfelpaare von den beiden Experimentatoren gemessen und von all diesen Messungen der Mittelwert gebildet, dann muss das Ergebnis ≤ 2 sein. Das gilt deshalb, da der Mittelwert ja nur aus Werten die entweder $+2$ oder -2 annehmen, gebildet wird.

$$\langle A_1B_1 \rangle + \langle A_1B_2 \rangle + \langle A_2B_1 \rangle - \langle A_2B_2 \rangle \leq 2$$

$\langle A_1B_1 \rangle$ beschreibt hier den Mittelwert der Produkte der Messergebnisse A_1 und B_1. Diese zuletzt notierte Gleichung gilt für alle Theorien des lokalen Realismus und heißt nach ihrem Entdecker Bellsche Ungleichung.
Wird das Experiment aber mit quantenmechanischen Teilchen wie z.B. verschränkten Photonen, die von Alice und Bob gemessen werden, durchgeführt, dann wird die Bellsche Ungleichung verletzt. Die linke Seite der Gleichung nimmt nämlich den Wert $2\sqrt{2} \approx 2{,}83$ an. (vgl. Kofler 2011)
Quantenmechanische Zustände verletzen also die Bellsche Ungleichung und können deswegen auch nicht durch den lokalen Realismus erklärt werden. In der Quantenkryptographie kann man sich diese Bedingung zu Nutze machen um einen Lauscher zu entlarven.

2.4 Polarisation von Photonen

Die Polarisation von Photonen scheint auf den ersten Blick wenig mit den vorhergehenden Kapiteln zusammenzuhängen, ist aber für das Verständnis der Quantenkryptographie wichtig. Wie wir wissen handelt es sich bei Licht um eine elektromagnetische Welle, welche aus einzelnen Quanten, den Photonen, besteht. Elektromagnetische Wellen sind transversale Wellen, d.h. das elektrische Feld der Welle schwingt im rechten Winkel zur Ausbreitungsrichtung. Schwingt das elektrische Feld nur in einer Ebene, dann sagt man das Licht ist linear polarisiert. (vgl. Tipler/Mosca 2012, 1209)
Mit Polarisationsfolien (oft auch Polarisationsfilter oder kurz Polfilter genannt) kann man linear polarisiertes Licht erzeugen. Sie bestehen aus langkettigen Kohlenwasserstoffmolekülen, die vereinfacht betrachtet ein enges Gitter bilden. Schwingen Lichtwellen senkrecht zu den Ketten, dann wird Licht durchgelassen (transmittiert). Deshalb nennt man die senkrecht zu den Molekülketten stehende Achse Transmissionsachse. Etwas vereinfacht gesagt, werden parallel zur Transmissionsachse schwingende Lichtwellen komplett durchgelassen, während orthogonal

schwingende Wellen komplett absorbiert werden. Wird unpolarisiertes Licht auf einen Polarisationsfilter geschickt, dann wird nur jener Teil durchgelassen, der parallele Anteile zur Transmissionsachse hat. Das Licht ist danach in diese Richtung polarisiert. (vgl. Bäker 2013; Giancoli 2011, 510-512; Steinberger 2011, 42-43)

3 Kryptographie

Kryptographie beschäftigt sich mit dem Verschlüsseln von Informationen, sodass diese nicht von einer unbefugten Partei gelesen werden können. Der Name ergibt sich aus den altgriechischen Worten *kryptós* (verborgen, geheim) und *gráphein* (schreiben). (vgl. fremdwort.de 2018)

3.1 Warum brauchen wir Kryptographie?

In vielen Bereichen unserer Gesellschaft ist ein sicherer Austausch von Informationen extrem wichtig. Beispiele für sensitive Übertragung von Daten sind Eingabe des persönlichen PIN Codes am Bankomaten oder Handy, beim E-Banking und bei digitalen Signaturen. Irgendwie müssen die Daten übertragen werden, aber die Übertragungskanäle wie z.B. das Internet oder klassisch per Post sind an sich nicht sicher. Deswegen verschlüsselt man die zu übertragenden Daten. (vgl. Hellekalek 2014, 6)

Kryptographische Vorgänge finden normalerweise unter der Teilnahme mehrerer Personen bzw. Parteien statt. Es gibt eine sendende, eine empfangende und eine (fiktive) angreifende Partei. Üblicherweise werden die beiden miteinander kommunizierenden Partner mit Alice und Bob bezeichnet. Die dritte Person, die versucht den Informationsabtausch zu sabotieren oder zu belauschen, wird Eve genannt. (vgl. Hellekalek 2014, 6; Steinberger 2011, 3)

Nach Hellekalek kann Eve auf drei verschiedene Weisen in die Kommunikation zwischen Alice und Bob eingreifen:

1. Entschlüsseln der geheimen Nachricht, z.B. durch Knacken des Geheimcodes.
2. Abfangen und Verändern der geheimen Nachricht, so dass diese Veränderung unbemerkt bleibt, und anschließendes Weitersenden an Bob.
3. Eve gibt sich als Alice aus, ohne dass Bob dies bemerkt und kommuniziert dann mit Bob.

Ziel der Kryptographie ist es diese drei Möglichkeiten zu verhindern.

3.2 Klassische Kryptographie

Zu der Zeit als die ersten Schriften entwickelt wurden, war das Lesen und Schreiben nur einigen wenigen Privilegierten vorbehalten. Deshalb war es auch noch nicht nötig Nachrichten zu verschlüsseln, da die Schrift an sich von kaum jemanden identifiziert werden konnte. Nach und nach verbreitete sich aber die Fähigkeit des Lesens und Schreibens und so wurde es auch notwendig, Nachrichten so zu verfassen, dass sie nicht von jedem gelesen werden konnten. (vgl. HPs kryptologisches Sammelsurium 2003)

Eines der ersten überlieferten Verschlüsselungsverfahren war die sogenannte Skytale im 5. Jahrhundert v. Chr. im antiken Griechenland. Dabei handelte es sich um ein sehr einfaches Prinzip, bei welchem ein Holzstab die Funktion des Schlüssels übernahm. Es wurde ein Band um eben jenen Holzstab gewickelt und anschließend eine Nachricht darauf geschrieben. Löste man das Band wieder vom Stab stand darauf eine scheinbar zufällige Zeichenfolge. Erst wenn der Empfänger das Band wieder auf einen Stab mit dem selben Durchmesser, wie ihn der Erzeuger der Nachricht zur Verschlüsselung verwendet hatte, aufwickelte ergab sich wieder der ursprüngliche Text. Mit diesem Verfahren sollen bereits im Peloponnesischen Krieg Generäle verständigt worden sein. (vgl. Galan y Martins/Jocic; HPs kryptologisches Sammelsurium 2003)

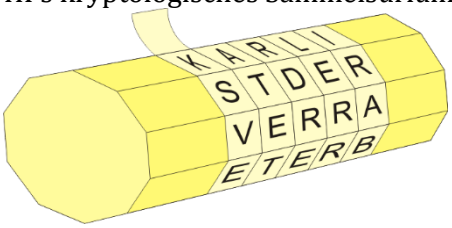

Abb. 1 – schematische Darstellung einer Skytale (wikimedia commons)

3.2.1 Mono- und polyalphabetische Verfahren

Beim Caesar Verfahren handelt es sich um eine allgemein recht bekannte Verschlüsselungsmethode, die ihren Ursprung ebenfalls in der Antike hat. Es wird hierbei einfach das Alphabet um einen bestimmten Wert verschoben. Diese Art zu verschlüsseln nennt man auch monoalphabetische Verschlüsselung. Der Schlüssel besteht aus

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
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
v	e	n	i		v	i	d	i		v	i	c	i												
g	p	y	t		g	t	o	i		g	t	n	t												

Abb. 2 – Caesar Verfahren mit Verschiebung um elf Stellen mit Beispieltext und Geheimtext

Buchstaben, welchen wiederum Zahlen zugeordnet werden können ($A = 1, B = 2, \dots$). Der Schlüssel K beispielsweise bedeutet dann eine Verschiebung um 11 Stellen. Verschlüsselt man mit diesem Schlüssel nun die berühmten Worte *veni, vidi, vici* erhält man den Geheimtext *gpyt, gtoi, gtnt* (siehe Abb. 2). (vgl. Galan y Martins/Jocic; Hellekalek 2014, 9-10; HPs kryptologisches Sammelsurium 2003)

Monoalphabetische Verschlüsselungsverfahren sind sehr einfach und haben den Nachteil, dass sie mit Hilfe einer Häufigkeitsanalyse leicht durchschaut werden können. Es wird dabei geschaut welcher Buchstabe des Alphabets normalerweise am häufigsten verwendet wird. In der deutschen Sprache ist das der Buchstabe E. Wenn also in einem (deutschen) Geheimtext der Buchstabe P am öftesten auftaucht, kann daraus gefolgert werden, dass E einem P entspricht und der Schlüssel in weiterer Folge elf sein muss. (vgl. Galan y Martins/Jocic; Hellekalek 2014, 15-17)

Eine Weiterentwicklung des Caesar Verfahrens stellt die polyalphabetische Verschlüsselung dar. Dabei wird anstatt eines einzelnen Schlüsselbuchstabens ein ganzes Codewort gewählt. Dieses Codewort wird so oft hintereinander gereiht, bis ein Schlüssel mit derselben Länge wie der zu verschlüsselnde Text entsteht. (vgl. Galan y Martins/Jocic)

K	R	Y	P	T	O	G	R	A	P	H	I	E
K	E	Y	K	E	Y	K	E	Y	K	E	Y	K
U	V	W	Z	X	M	Q	V	Y	Z	I	G	O

Tabelle 1 – ein einfaches Beispiel für eine polyalphabetische Verschlüsselung.

In Tabelle 1 sieht man ein simples Beispiel für eine polyalphabetische Verschlüsselung mit dem Codewort Key. In der ersten Zeile befindet sich der Klartext, in der zweiten Zeile der Schlüssel, welcher durch Wiederholung des Codeworts erstellt wird, und in der dritten Zeile der erhaltene Geheimtext. Mit einer Häufigkeitsanalyse kann der Text nun nicht mehr geknackt werden, da derselbe Buchstabe im Geheimtext für verschiedene Buchstaben im Klartext stehen kann. Der Text kann jedoch auf typische Zeichenfolgen untersucht werden und dadurch evtl. geknackt werden. Je länger das verwendete Codewort, desto sicherer ist die Verschlüsselung.

3.2.2 One-Time-Pad

Beim One-Time-Pad handelt es sich um einen polyalphabetischen Algorithmus, welcher 1917 von Gilbert Vernam (1890 – 1960) und Josep Mauborgne (1881 – 1971) entwickelt wurde. Es wird dabei ein zufällig erzeugter Schlüssel, der mindestens so lange ist wie der zu verschlüsselnde Text, verwendet. Solange zwei Bedingungen eingehalten werden ist dieses Verfahren nicht entschlüsselbar: (vgl. Beck; Steinberger 2011, 15-17)

1. Der Schlüssel besteht aus einer zufällig erstellten Abfolge von Zahlen.
2. Der Schlüssel darf nur einmalig verwendet werden.

Erwähnenswert ist hierbei, dass es sich bei softwaregenerierten Zufallszahlen um keine echten Zufallszahlen, sondern um Pseudozufallszahlen handelt. Sie wirken zufällig aber können berechnet werden, da ja ein Algorithmus für die Erstellung der Zahlen verantwortlich ist. Es können mit dem Computer also keine echten Zufallszahlen erzeugt werden. Hier kommt aber die Quantenmechanik ins Spiel, denn mit ihrer Hilfe können echte Zufallszahlen generiert werden. Schickt man ein Photon auf einen Strahlteiler, dann wird es zufällig reflektiert oder transmittiert (siehe Abb. 3). Diese beiden Ereignisse entsprechen dem binären eins und null. (vgl. Quantum Lab 2010)

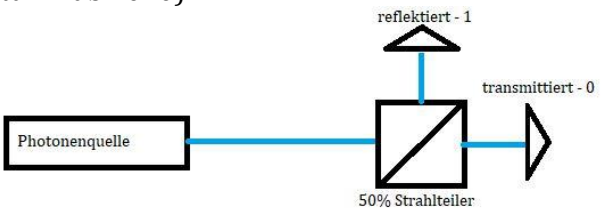

Abb. 3 – schematische Darstellung eines Quantenzufallsgenerators (nach Quantum Lab, 2010)

Die zweite Bedingung scheint bei guter Geheimhaltung auf den ersten Blick nicht so wichtig zu sein, aber schon bei zweimaliger Benutzung eines Schlüssels kann die Nachricht ganz ohne Wissen über den Schlüssel selbst geknackt werden. Jede weitere Verwendung vereinfacht diesen Prozess weiter. (vgl. Beck)

Die Verschlüsselung selbst ist beim One-Time-Pad recht simpel. Informationen werden in der heutigen Zeit meist im Binärsystem verschlüsselt, d.h. das verwendete Alphabet ist {0,1}. Ein Bit a des Klartexts wird mit dem Zufallsbit k des Schlüssels wie folgt verschlüsselt: (vgl. Steinberger 2011,15)

$$a \equiv (a + k)\ mod\ 2 = a\ XOR^{1}\ k = a \oplus k$$

[1] XOR: sind die Bits unterschiedlich, ist das Ergebnis 1, sonst 0.
$(0 \oplus 1 = 1, 0 \oplus 0 = 0, 1 \oplus 1 = 1)$

Beim One-Time-Pad handelt es sich also um eine absolut sichere Methode der Verschlüsselung, vorausgesetzt die beiden oben genannten Bedingungen werden eingehalten. Allerdings muss der Schlüssel geheim sein. Es bietet sich also für einen Angreifer Eve an den Schlüsselaustausch anzugreifen. Die Quantenkryptographie bietet aber eine Möglichkeit für einen abhörsicheren Austausch des Schlüssels.

3.3 Quantenkryptographie

Quantenkryptographie funktioniert mit zwei getrennten Kommunikationskanälen. Einerseits gibt es den öffentlichen, klassischen Kanal (z.B. Internet, Telefon, …), den Alice und Bob zur Kommunikation verwenden. Der öffentliche Kanal kann von Eve abgehört werden ohne dass sie dadurch die Nachricht verstehen kann. Zusätzlich gibt es noch den Quantenkanal, der für den Schlüsselaustausch zwischen Alice und Bob genutzt wird. Dieser ist abhörsicher, da ein Eingreifen eines Angreifers direkt erkannt wird. (vgl. Gänger 2010, 2)

Für den Austausch des Quantenschlüssels gibt es zwei verschiedene Methoden. Es können einzelne Photonen gesendet werden (BB84-Protokoll) oder verschränkte Photonenpaare werden von einer zentralen Quelle aus zu Alice und Bob geschickt (Ekert-Protokoll). Bei beiden Varianten wird mit Hilfe des One-Time-Pads verschlüsselt, einzig in der Schlüsselerzeugung weichen sie voneinander ab. In diesem Paper möchte ich die Methode mit den verschränkten Photonenpaaren genauer unter die Lupe nehmen.

3.3.1 Ekert-Protokoll

Das Ekert-Protokoll wurde 1991 von Artur Ekert (geb. 1961) formuliert. Für den Quantenschlüsselaustausch werden verschränkte Teilchen verwendet. Anders als beim BB84-Protokoll versendet hier aber nicht Alice Teilchen an Bob, sondern es gibt eine zentrale Quelle, die verschränkte Teilchen erzeugt und anschließend zu Alice und Bob schickt. Reale Anwendungen sollten dadurch eher beschrieben werden, da eine zentrale Quelle, wie beispielsweise ein Satellit, besser für längere Distanzen geeignet ist. Es werden also insgesamt drei Parteien benötigt: ein Sender für die verschränkten Teilchen (normalerweise Photonen) und zwei Empfänger (Alice und Bob), welche die Teilchen messen. (vgl. Quantum Lab 2010; Steinberger 2011, 63)

Die Funktionsweise des Protokolls kann auf vier grundsätzliche Schritte reduziert werden. Im ersten Schritt emittiert eine zentrale Quelle Teilchenpaare in einem maximal verschränkten Zustand wie zum Beispiel: (vgl. Pajic 2013, 16)

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$

Hierbei sind $|0\rangle$ und $|1\rangle$ die beiden Basiszustände der Quanten, welche mit dem Index A bzw. B eindeutig zugeordnet werden können.

Alice und Bob wählen danach zufällig zwischen drei Messbasen für jede Messung. Die Basen[2] werden durch Rotation der Horizontal-Vertikal Basis um die z-Achse erhalten: (vgl. Ilic 2007, 2)

$\phi_1^a = 0$	für Alice	$\phi_1^a = \frac{\pi}{4}$	für Bob
$\phi_2^a = \frac{\pi}{4}$		$\phi_1^a = \frac{\pi}{2}$	
$\phi_1^a = \frac{\pi}{2}$		$\phi_1^a = \frac{3\pi}{4}$	

Tab. 2 – mögliche Messbasen

Nach der Übertragung tauschen sich Alice und Bob im öffentlichen Kanal darüber aus welche Basis sie für die jeweiligen Messungen gewählt haben. Die Messungen können somit in drei Gruppen eingeteilt werden: (vgl. Pajic 2013, 16-17)

1. Messungen mit unterschiedlich ausgerichteten Analysatoren.
2. Messungen mit gleich ausgerichteten Analysatoren.
3. Messungen bei denen zumindest einer der beiden Experimentatoren kein Teilchen registriert hat.

Die erste Gruppe an Messungen wird für die Berechnung der Bellschen Ungleichung verwendet, die zweite wird in den Schlüssel aufgenommen und die dritte wird verworfen.

Abschließend veröffentlichen Alice und Bob die Ergebnisse, die in die erste Gruppe fallen. Mit Hilfe der Bellschen Ungleichung können sie überprüfen, ob sich ein Lauscher (Eve) im System befindet. Wird kein Lauscher entdeckt, dann werden die Ergebnisse der zweiten Gruppe in den Schlüssel aufgenommen. So wird eine Abfolge zufälliger Bits erzeugt. (vgl. Pajic 2013, 16)

Mit den gegebenen Basen gibt es genau zwei Möglichkeiten (ϕ_2^a, ϕ_1^b *und* ϕ_3^a, ϕ_2^b), dass Alice und Bob dieselbe Basis verwenden. Es werden also mit einer Wahrscheinlichkeit von 2/9 zueinander kompatible Basen gewählt. Messen beide in der selben Basis, dann weiß beispielsweise Alice beim Messen des Zustandes $|1\rangle_A$, dass Bob den Zustand $|1\rangle_B$ gemessen haben muss. Die beiden besitzen also die selbe Information. Messen

[2] Die Messbasen werden in Radiant angegeben, wobei π gleich 180° ist.

sie aber in unterschiedlichen Basen, dann sind auch die gemessenen Zustände zufällig. Bobs Teilchen muss also irgendwie „wissen“ wie Alices Teilchen gemessen wurde und sich dementsprechend ausrichten. Dieses Phänomen heißt eben Verschränkung. (vgl. Ilic 2007, 2)

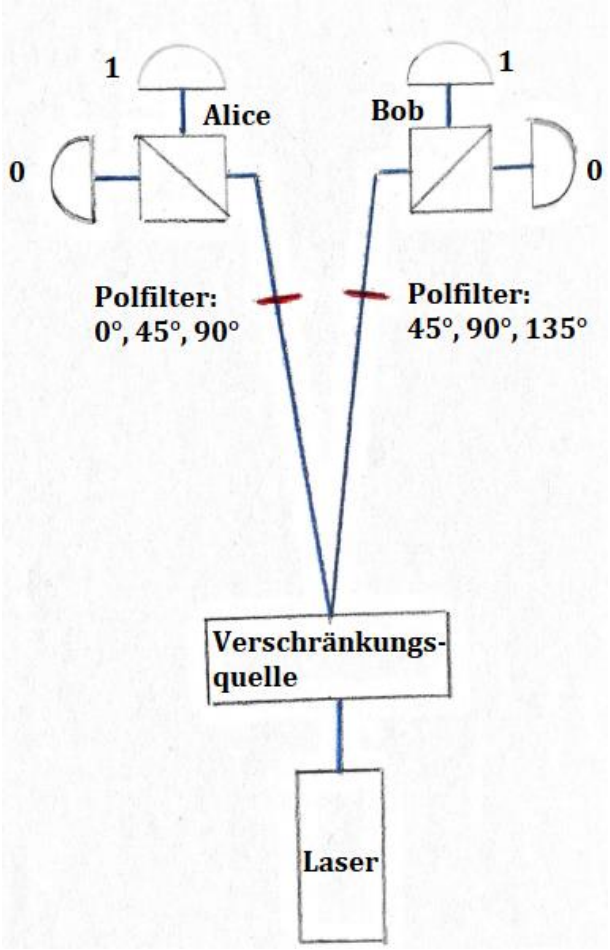

Abb. 3 – schematische Darstellung des Ekert-Protokolls (nach Quantum Lab, 2010)

Um all die zufälligen Messergebnisse streichen zu können, vergleichen Alice und Bob auf einem öffentlichen Kanal ihre gewählten Messbasen. Nur wenn sie die selbe Basis gewählt haben, nehmen sie das Ergebnis in den Schlüssel auf, die restlichen Ergebnisse werden verworfen. Durch dieses Verfahren schrumpft der Schlüssel auf 22% (= 2/9) der Länge zusammen. (vgl. Ilic 2007, 2)

Da verschränkte Zustände verwendet werden, ist es für einen Angreifer schwierig Informationen über den Schlüssel zu erhalten. Messen Alice und Bob ihr Teilchen beispielsweise in der $\pi/4$ Basis, dann erwarten sie auch übereinstimmende Ergebnisse. Sollten sie unterschiedliche Ergebnisse haben, könnte das auf eine Anwesenheit eines Angreifers (Eve) hindeuten. Versucht Eve die von der Quelle versendeten Teilchen zu messen, dann muss sie ebenfalls eine Basis wählen. Bei der Messung zerstört sie aber das Teilchen und außerdem ist ihr Ergebnis zufällig, sofern ihre Basis nicht mit denen von Alice und Bob übereinstimmt. Anschließend muss Eve natürlich wieder ein neues Teilchen erzeugen und an Bob weitersenden. Die Polarisation des Teilchens ist aber nach dem Eingriff durch Eve zufällig. Misst Bob einen Zustand, der nicht mit Alices Messung übereinstimmt, dann erhält er eine Fehlermeldung. (vgl. Ilic 2007, 2-3; Quantum Lab 2010)

Mit den Ergebnissen, die sie bei der Messung mit verschiedenen Basen erhalten haben, berechnen Alice und Bob die Bellsche Ungleichung. Wird die Ungleichung verletzt, bedeutet das, dass sich die Teilchen immer noch in einem verschränkten Zustand befinden und die Anwesenheit eines Angreifers somit ausgeschlossen werden kann. Es wird also ein absolut sicherer Schlüssel erzeugt.

Bei der Verschlüsselung kommt die Methode des One-Time-Pads ins Spiel. Alice verschlüsselt ihre Nachricht mit dem sicheren Schlüssel und kann sie dann ohne Bedenken an Bob senden. Eve hat keinen Schlüssel und kann selbst wenn sie die Nachricht abfängt nichts damit anfangen. Bob entschlüsselt die Nachricht mit dem sicheren Schlüssel, den er ja genauso wie Alice besitzt, und erhält so den Klartext. Wollen weitere Nachrichten verschickt werden, muss jeweils wieder mit dem Ekert-Protokoll ein neuer Schlüssel erzeugt werden, da das One-Time-Pad ansonsten geknackt werden kann. (vgl. Ilic 2007, 3)

4 Quantenkryptographie in der Schule

Das Thema Quantenkryptographie ist normalerweise kein übliches Schulthema, aber ich bin der Meinung, dass die Thematik äußerst interessant für die Schüler und Schülerinnen ist. Denn es handelt sich dabei um eine moderne, aktuelle Anwendung der Physik und aus meiner Erfahrung, bringen Schüler und Schülerinnen ein hohes Interesse für aktuelle Themen mit.

Ich möchte hier ein paar Ideen aufzählen, die ich für die Gestaltung eines Unterrichts zur Quantenkryptographie habe. Zu allererst bietet sich aufgrund der mathematischen Natur der Kryptographie ein fächerübergreifender Unterricht mit dem Fach Mathematik an. So können mathematische Grundlagen wie die Modulo-Rechnung und das Binärsystem, welche den meisten kryptographischen Vorgängen zu Grunde liegen, behandelt werden. Außerdem kann mit Hilfe von statistischen Auswertungen versucht werden verschlüsselte Texte zu knacken oder beispielweise bewiesen werden, dass bereits eine doppelte Verwendung des Schlüssels beim One-Time-Pad

eine Identifizierung des Klartexts erlaubt. Im Physikunterricht kann dann mit Photonen und Polarisation von Licht experimentiert werden. Darauf aufbauend können quantenkryptographische Protokolle wie z.B. das Ekert-Protokoll behandelt werden. Zu guter Letzt kann man nach aktuelle Forschungen und technischen Anwendungen suchen und diese diskutieren.

Eine Begründung der Behandlung von Quantenkryptographie kann auch im AHS-Lehrplan der Oberstufe gefunden werden. (vgl. AHS-LP 2017) Quantenkryptographie im Physikunterricht kann einen Beitrag zu den Bildungsbereichen *Mensch und Gesellschaft* („Physik als angewandte Wissenschaft verstehen“) sowie *Natur und Technik* („Physik als Grundlage der Technik verstehen“) liefern. Vom Lehrstoff könnte ein Unterricht zur Quantenkryptographie am besten im 6. Semester (zweites Semester der 7. Klasse) oder im 8. Semester (zweites Semester der 8. Klasse) durchgeführt werden. So sollen im 6. Semester die Quantenphysik und speziell die „Besonderheiten der Quantenwelt“ behandelt werden. Im 8. Semester soll hingegen ein „Einblick in aktuelle physikalische Forschung“ gegeben werden, hier kann auf aktuelle Entwicklungen eingegangen werden. Besonders erwähnenswert ist hierbei, dass sich mit dem Team unter der Leitung von Anton Zeilinger auch österreichische Physiker und Physikerinnen intensiv mit Quantenphänomenen und ihrer Anwendung beschäftigen. (vgl. Taschwer 2017)

5 Fazit

Die Welt der Quantenphysik ist nur schwer durchschaubar, aber trotzdem äußerst interessant und vor allem hochrelevant. Ein gewisses Grundverständnis der Quantenmechanik ist Voraussetzung um sich mit Quantenkryptographie auseinandersetzen zu können, aber durch Einbindung des kryptographischen Aspekts und mit der einhergehenden realen Anwendungsmöglichkeit, ergeben sich für Lehrpersonen neue, interessante Möglichkeiten einen Unterricht über Quantenphysik zu gestalten.

6 Literatur

AHS-LP (2018) Lehrplan der AHS Oberstufe. Online unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008568&FassungVom=2017-09-01 (06.05.2018)

Bäker, M. (2013) Quantenmechanik verstehen III – Verschränkung. Online unter: http://scienceblogs.de/hier-wohnen-drachen/2013/01/27/quantenmechanik-verstehen-iii-verschrankung/ (25.02.2018)

Beck, A. Vernam-Code. Online unter: http://www.pruefzifferberechnung.de/V/Vernam.shtml (25.02.2018)

Fremdwort.de (2018) Kryptographie. Online unter: www.fremdwort.de/suchen/bedeutung/kryptographie (02.05.2018)

Galan y Martins, S. und Jocic, A. Kryptologie -Sicherheit für alle. Online unter: http://www.mathematik.de/spudema/spudema_beitraege/beitraege/galan/kryptmed.htm (25.02.2018)

Gänger, B. (2010) Quantenkryptographie und Quantenteleportation. Kaiserslautern: Technische Universität Kaiserslautern.

Giancoli, D. C. (2011) Physik: Gymnasiale Oberstufe. Hallbergmoos, Pearson Deutschland GmbH.

Hellekalek, P. (2014) Vorlesung Kryptologie: Kapitel 1: Historische Chriffren [Skriptum]. Salzburg: Universität Salzburg.

HPs kryptologisches Sammelsurium (2003). Online unter: http://www.hp-gramatke.de/crypto/german/page0010.htm (25.02.2018)

Ilic, N. (2007) The Ekert Protocol. Waterloo: University of Waterloo. Online unter: http://www.ux1.eiu.edu/~nilic/Nina's-article.pdf (25.02.2018)

Kofler, J. (2011) Vortrag zu Quantencomputer und Quantenkryptographie. Online unter: https://youtu.be/Cb79hh_Hlsg?t=1s (25.02.2018)

Pajic, P. (2013) Quantum Cryptography [Bachelorarbeit]. Wien: Universität Wien.

Quantum Lab – Quantenkryptographie (2010) Erlangen-Nürnberg, Friedrich-Alexander-Universität. Online unter: http://www.didaktik.physik.uni-erlangen.de/quantumlab/index.html?/quantumlab/Kryptographie (25.02.2018)

Steinberger, M. (2011) Quantenkryptographie: Das BB84-Protokoll [Masterarbeit]. Salzburg: Universität Salzburg.

Tipler, P. A. und Mosca, G. (2012) Physik für Wissenschaftler und Ingenieure. Berlin, Heidelberg: Springer-Verlag.

Taschwer, K. (2017) Durchbruch bei der Quantenkommunikation. Online unter: https://derstandard.at/2000059364211/Durchbruch-bei-der-Quantenkommunikation (06.05.2018)

Zeilinger, A. (2003) Einsteins Schleier. München, Verlag C. H. Beck.