Referat Quantenkryptographie

(von Frank Kühnlenz und Dennis Reinert)

Inhaltsverzeichnis

1. Einleitung

Bisher haben wir viel über die klassischen Protokolle (bsp. RSA oder DES) in diesem Proseminar gehört. Auch neuere Ansätze, vor allem Zero-Knowledge, wurden bereits genannt. Was aber wird die Zukunft bereithalten?

Der größte Horror des Kryptographen ist, neben dem unwahrscheinlichen P=NP, die reale „Bedrohung“ durch den Quantencomputer. Er ermöglicht einen unvergleichlich schnellen Brute-Force-Angriff, mit dem bekanntlich alle Protokolle zu brechen sind. Das wird erreicht, in dem er einen besonderen Zustand einnimmt (welchen, klärt der folgende Abschnitt), wodurch alle möglichen Lösungen parallel getestet werden und sich die Lösung am Zustandsende fast von Zauberhand offenbart.

1.1. Das Universum der Quantenphysik

Wie genau diese „Magie“ funktioniert, wollen wir hier (ansatzweise) aufklären. Doch zunächst eine Warnung von Niels BOHR, einem der Väter der Quantenmechanik: „*Jeder, der über die Quantenmechanik nachdenken kann, ohne dass ihm schwindelig wird, hat sie nicht verstanden.*“.

1.1.1. Youngs Doppelspaltexperiment

Mit dieser Warnung bedacht, begeben wir uns am besten ganz an den Anfang (nun ja, nicht ganz, jedenfalls nicht bis zum Urknall ☺). Dieser liegt in unserem Fall im Jahre 1799 in Cambridge, als Thomas YOUNG sein Doppelspaltexperiment durchführte. Es diente dazu, die Natur des Lichtes zu ergründen und wird auch heute noch im schulischen Physikunterricht vorgeführt, so dass es jedem hier noch erinnerlich sein sollte (s. Bild 1.1).

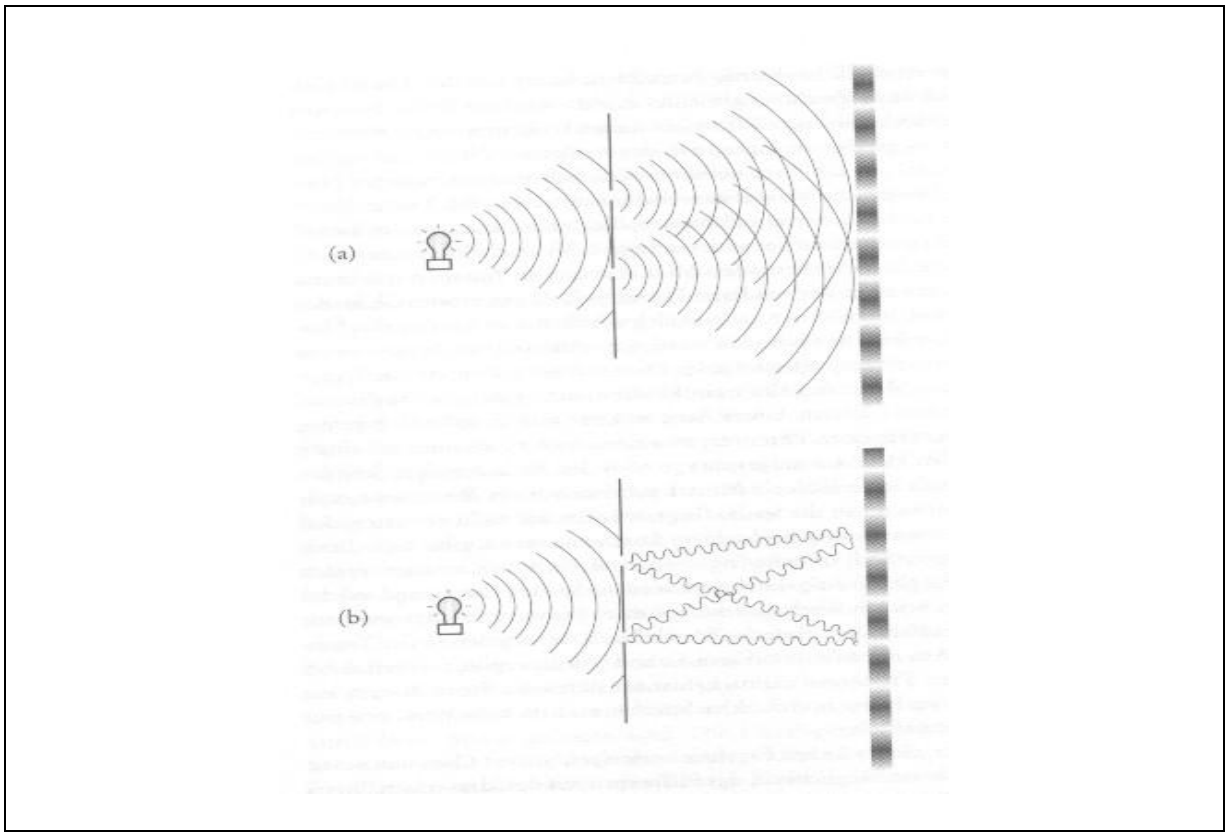

Bild 1.1 Youngs Doppelspaltexperiment

Durch dieses Experiment fand Young zu der Überzeugung, das sich das Licht wellenförmig verhält. Heute wissen wir von seiner Doppelnatur, denn es verhält sich auch so, als bestünde es aus Teilchen und wir sprechen von Lichtphotonen.

1.1.2. Multiversum, Superposition und Verschränkung

In der modernen Physik kann man das Doppelspaltexperiment mit einem Glühfaden wiederholen, der sehr schwach leuchtet und nur ein Photon emittiert. Dabei ist erstaunliches festzustellen: selbst einzelne, nacheinander durch den Spalt fliegende Photonen erzeugen ein Interferenzmuster. Das widerspricht der intuitiven Anschauung, denn ein Photon allein kann mit keinem anderen in Wechselwirkung treten.

Die klassische Physik hat dafür keine Erklärung. Es existieren zwei Theorien, die dieses Ergebnis interpretieren: die des Multiversum und die der Superposition.

Erstere, auch Vielwelten-Deutung genannt, behauptet, das einzelne Photon habe zwei Möglichkeiten: es fliegt durch den linken oder den rechten Spalt. Mit dieser Entscheidung teilt sich das Universum in zwei Universen; in jedem geht es einer der beiden Möglichkeiten nach. Auf „magische“ Weise stehen diese Universen allerdings in Wechselwirkung, die das Streifenmuster bedingt. Generell soll nach dieser Theorie jede unserer Entscheidungen, auch die banalste, ein neues Universum erzeugen. Alle diese Universen werden im Begriff des Multiversum zusammengefasst.

Die alternative Theorie der Superposition verfolgt einen eher philosophischen Ansatz. Demnach wissen wir nur zwei Dinge absolut über das Photon: es verlässt den Glühdraht und trifft auf den Schirm. Dabei ist der genaue Weg, den es zurücklegt, unbekannt. Die erstaunliche Annahme der Überlagerungstheoretiker ist, das es gleichzeitig durch beide Spalte fliegt und somit sehr wohl mit sich selbst in Wechselwirkung treten kann. Zugrunde liegt hierbei die Annahme, das bei Unkenntnis, was das Teilchen tut, es alles gleichzeitig anstellen darf. Seine beiden einzelnen Zustände (linken Spalt oder rechten Spalt durchfliegen) überlagern sich in diesem Moment zur sogenannten Superposition.

1.1.3. Schrödingers Katze und das Qubit

Ein sehr anschauliches Beispiel für eine Superpositionszustand ist das Gedankenexperiment von Erwin SCHRÖDINGER um 1935, genannt „Schrödingers Katze“. In einer geschlossenen Kiste befinden sich eine Katze und ein radioaktives Atom. Wenn dieses Atom zerfällt, setzt es über einen Detektor eine tödliche Substanz frei. Der genaue Zeitpunkt dafür ist unbekannt.

Nach dem Superpositionsprinzip ist die Katze solange „tot“ *und* „lebendig“, bis der Deckel der Kiste geöffnet wird, so dass eine verifizierende Messung den genauen Zustand feststellt. Der offensichtliche Widerspruch zur Realität, wir beobachten schließlich nur tote oder lebendige Katzen, löst sich, indem die Kiste als geschlossenes System definiert wird. Die Realität besteht aber aus vielen geschlossenen Systemen, die in Wechselwirkung stehen, so dass dadurch die Superposition zerstört wird.

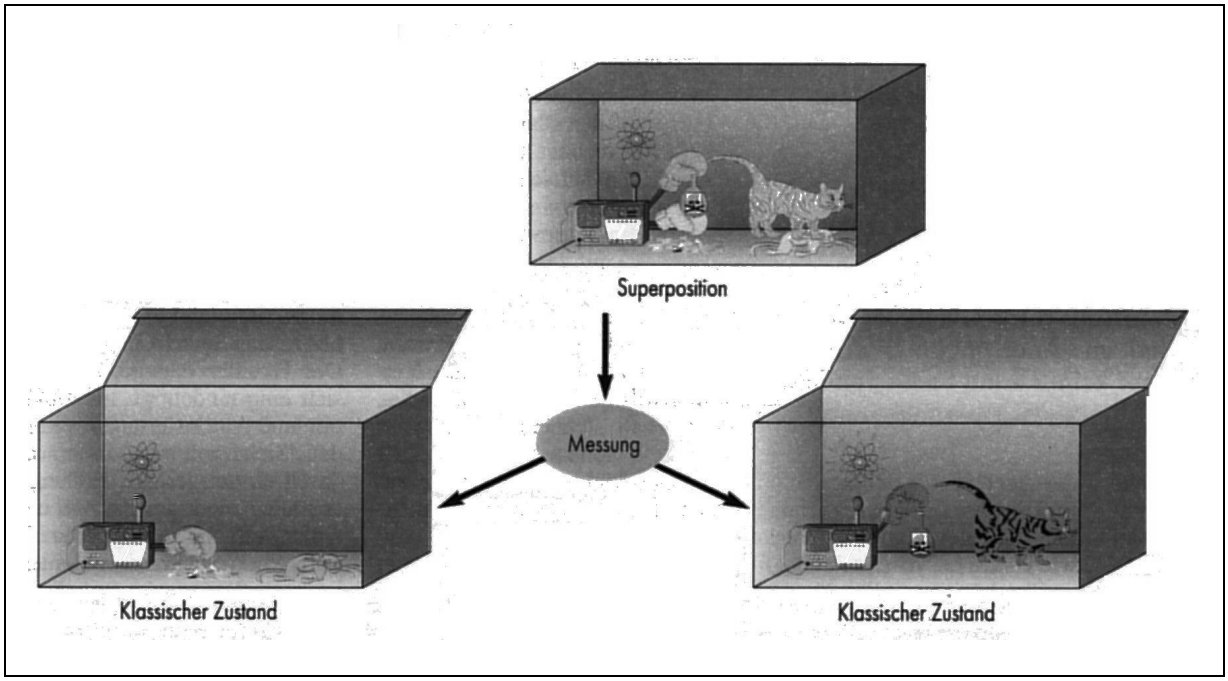

Bild 1.2 Schrödingers Katze

Anton ZEILINGER schlägt folgende Interpretation vor: die Quanten-Realität soll mit Hilfe elementarer Systeme beschrieben werden, die genau ein Bit Information enthalten. Diese Information muss bei Operationen, die auf das System einwirken, erhalten bleiben. Diese Einheit wird als Qubit bezeichnet. Es besitzt die klassischen Zustände 0 und 1, kann aber auch den der Superposition einnehmen.

1.2. Notwendigkeit der Quantenkryptographie

Nachdem wir uns jetzt vom „Horror“ des Kryptographen vor dem Quantencomputer überzeugt haben, stellt sich die Frage, welche System Abhilfe leistet. Diese Frage ist rhetorisch; die Antwort lautet natürlich Quantenkryptographie.

Die Quantenkryptographie schützt nicht nur vor dem übermächtig scheinenden Quantencomputer, sondern erlaubt eine absolut sichere Verschlüsselung auf Grundlage des One – Time – Pad.

Der kritische Leser erinnert sich vermutlich, wie oft in der Geschichte der Kryptographie ähnliches postuliert wurde. Die Vigenère-Chiffre wurde „le chiffre indéchiffrable“ genannt – und von BABBAGE geknackt. Die Enigma galt als uneinnehmbar, bis die Polen ihre Schwächen erkannten und Alan TURING ihr endgültiges Ende einläutete.

Doch bei der Quantenkryptographie ist es nicht so einfach: sie erlaubt, eine dem Klartext angepasste Schlüsselerzeugung und umgeht das Problem der Schlüsselverteilung. Neugierig? Sehr schön, doch zunächst müssen wir noch einige Grundlagen betrachten.

2. Grundlagen und Wiederholung

2.1. One – Time – Pad

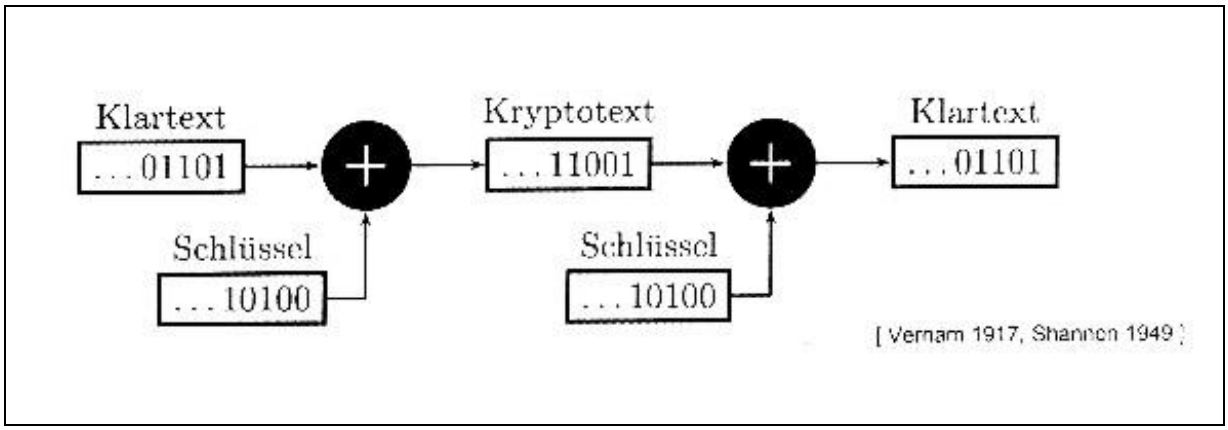

Bild 2.1 One – Time – Pad

Das „One-Time-Pad“ (Einmalblock) ist ein symmetrisches Verschlüsselungssystem, welches sich zufälliger Schlüsselsequenzen bedient, die mindestens so groß sein müssen wie die zu übermittelnde Nachricht. Ein Angriff mittels statistischer Methoden bleibt bei diesem Kryptosystem erfolglos. Die Verschlüsslung der Nachricht wird über die bitweise Addierung des Schlüssels zum Klartext (XOR) erreicht. Um den Geheimtext später wieder zu dekodieren, addiert man wiederholt bitweise den Schlüssel dazu und der Klartext entsteht.

Die Allatagstauglichkeit des „One-Time-Pad“ ist jedoch durch die Verwendung von zufälligen Schlüsseln, welche mindestens die gleiche Größe wie die zu übermittelnden Daten besitzen, und nur einmal verwendet werden sollten, nicht gegeben, da die Kreierung solch großer zufälliger Schlüsselmengen und die sichere Übertragung fraglich ist.

2.2. Heisenbergsche Unschärferelation

Werner Heisenberg zeigte, durch seine 1927 aufgestellte Unschärferelation, die Grenzen der Messung physikalischer Größen im Bereich der Elementarteilchen. Er fasste seine technischen Ausführungen in dem Satz zusammen: „Wir können die Gegenwart in allen Bestimmungstücken prinzipiell nicht kennen lernen“. Damit soll nicht gesagt sein, dass wir nicht alles wissen können, weil wir nicht genug Messgeräte zur Verfügung hätten oder weil unsere Geräte unvollkommen wären. Vielmehr stellte Heisenberg fest, dass es logisch unmöglich ist, jede Eigenschaft eines bestimmten Objektes mit vollkommener Genauigkeit zu messen. Da die präzise Messung der einen Eigenschaft, eine präzise Messung der anderen ausschließt bzw. je genauer man eine Größe feststellt, desto ungenauer kann man die andere feststellen.

2.3. Theorie der Polarisation

Während ein Photon durch den Raum fliegt schwingt es (siehe Bild 2.2 (a)) und die Ausrichtung dieser Schwingung ist von Photon zu Photon jedes Mal verschieden. Man bezeichnet dies als Polarisation der Photonen. Eine Glühbirne erzeugt Photonen, welche in jede Richtung schwingen, also Photonen aller Polarisationen. In diesem Beispiel schwingen Photonen horizontal, vertikal, diagonal oder irgendwo dazwischen auf und ab.

Der Einfachheit nehmen wir an, dass Photonen nur vier verschiedene Polarisationen hätten, welche wir wie folgt bezeichnen:

Mit Hilfe von sogenannten Polarisationsfiltern ist man in der Lage, Photonen derselben Polarisation zu filtern. Wir können uns einen Polarisationsfilter als ein Gitterrost vorstellen, auf das Photonen in Form von Streichhölzern geworfen werden. Es fallen nur die Streichhölzer durchs Gitterrost, welche im selben Winkel ankommen. Für unsere Photonen bedeutet es, sie müssen in die selbe Richtung wie der Filter polarisiert sein, um den Polarisationsfilter zu passieren. Alle anderen Photonen, welche z.B. quer zur Filter Richtung polarisiert sind, werden blockiert.

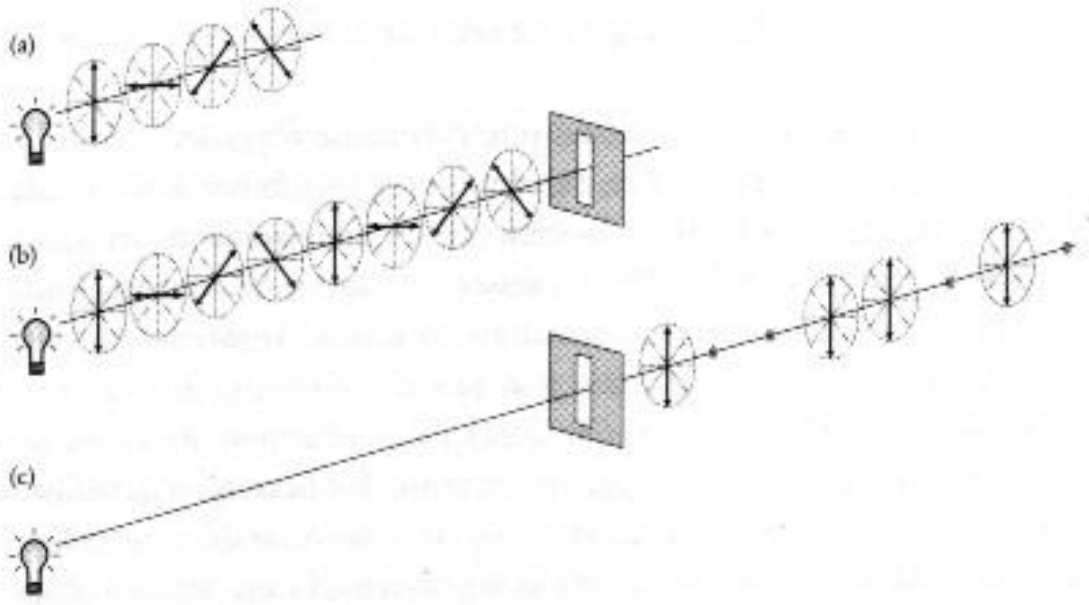

Abbildung 73: (a) Zwar schwingen Lichtphotonen in alle Richtungen, doch der Einfachheit halber nehmen wir an, es seien nur vier verschiedene Richtungen, wie hier gezeigt. (b) Die Lampe hat acht Photonen emittiert, die in verschiedene Richtungen schwingen. Jedes Photon, so heißt es, hat eine Polarisation. Die Photonen fliegen auf einen vertikalen Polarisationsfilter zu. (c) Auf der anderen Seite des Filters ist nur noch die Hälfte der Photonen übrig. Die vertikal polarisierten Photonen sind durchgekommen, die horizontal polarisierten nicht. Doch die Hälfte der diagonal polarisierten Photonen ist ebenfalls durchgekommen und ist danach vertikal polarisiert.

Bild 2.2 Polarisation

Unser Streichholzvergleich führt uns leider nicht weiter, wenn es um diagonal polarisierte Photonen geht, die sich einem vertikalen Polarisationsfilter nähern. Diagonal ausgerichtete Streichhölzer würden durch ein vertikales Gitter blockiert, doch bei diagonal polarisierten Photonen, welche sich einem vertikal polarisierten Filter nähern, wäre dies nicht unbedingt der Fall. Diese Photonen geraten in ein Quanten-Dilemma, wenn sie auf einen solchen Filter

treffen. Die Hälfte aller Photonen wird nämlich blockiert, die andere Hälfte kommt durch, und die durchkommenden Photonen werden vertikal polarisiert. (siehe Bild 2.2 (b) u. (c))

Polaroid-Sonnenbrillen bedienen sich dieser Blockade bestimmter Photonen. Anhand einer eben solchen ist es möglich, die Wirkung eines Polarisationsfilters aufzuzeigen. Einer solchen Sonnenbrille entnehmen wir eine Linse, schließen ein Auge und mit dem anderen schauen wir durch das verbliebene Brillenglas. Wenn wir nun durch die Brille sehen, nehmen wir die Umgebung dunkler war, da die Linse viele Photonen blockiert.

Die Photonen, die unser Auge erreichen, besitzen alle die selbe Polarisation. Wir halten nun die entnommene Linse vor unser verbliebenes Brillenglas und bewegen es im Kreis. In einer bestimmten Position wird die angehaltene Linse auf die Lichtmenge keine Wirkung haben, da in diesem Fall die freie Linse und das Brillenglas die selbe Polarisation besitzen. Bei einer anschließenden Drehung der freien Linse um 90°, wird es völlig dunkel. In dieser Stellung liegt die Polarisation der freien Linse quer zur Polarisation der festen Linse, so dass alle Photonen, die durch die freie Linse gelangen, von der festen Linse blockiert werden. Wenn wir die freie Linse jetzt um weitere fünfundvierzig Grad drehen, erreichen wir eine Zwischenstufe mit nur partieller Blockade, und die Hälfte der Photonen, die durch die freie Linse kommen, schafft es auch durch die feste Linse.

3. Funktionsprinzip

3.1. Der Anfang war das Quantengeld

Die ersten Ideen für eine praktische Anwendung der Quantentheorie stammen aus den 70er Jahren. Stephen WIESNER ersann ein Protokoll für fälschungssicheres Quantengeld. Doch sein Doktorvater und alle Kollegen wiesen sein Idee abwertend zurück.

Erst auf der Konferenz Crypto'82 wurde die Idee aufgegriffen und Charles BENNETT und Gilles BRASSARD stellten das Konzept der Quantenkryptographie einer staunenden Fachwelt vor.

Das erweiterte System nannten sie BB84; es wurde 1984 veröffentlicht. Im Oktober 1989 wurde ein Quantenschlüsselaustausch über einen Freiluft-Quantenkanal von 32cm Länge erreicht.

3.2. Versuchsaufbau

Sehen wir uns diesen Aufbau genauer an. Zunächst in der einfachen Theorie; in der Praxis danach stellt sich wiedereinmal heraus, das alle Theorie grau ist.

3.2.1. Theorie

Im BB84 Schema erzeugt Alice, mit Hilfe einer speziellen (hypothetischen) Quelle, einzelne Photonen mit einer von vier möglichen Polarisationen: 0° und 90° bzw. 45° und 135°. Diese Wahl muss absolut zufällig sein und geheim bleiben.

Bob versucht, die von Alice empfangenen Photonen zu analysieren. Dabei entscheidet er sich zuerst für einen der Polarisationsfilter. Dabei erkennt der eine Detektor nur Teilchen, die um 0° oder 90° Grad ausgerichtet sind, der Andere nur Photonen mit 45° bzw. 135°. Diese werden jeweils in einen von zwei Ausgängen angezeigt (siehe Bild 3.1).

Das Entscheidende ist, wird der falsche Detektor gewählt, wird jeweils mit 50% Wahrscheinlichkeit ein Ausgang benutzt. Während Bobs Messung werden somit nicht nur seine Messergebnisse, sondern auch die Detektor – Einstellung notiert.

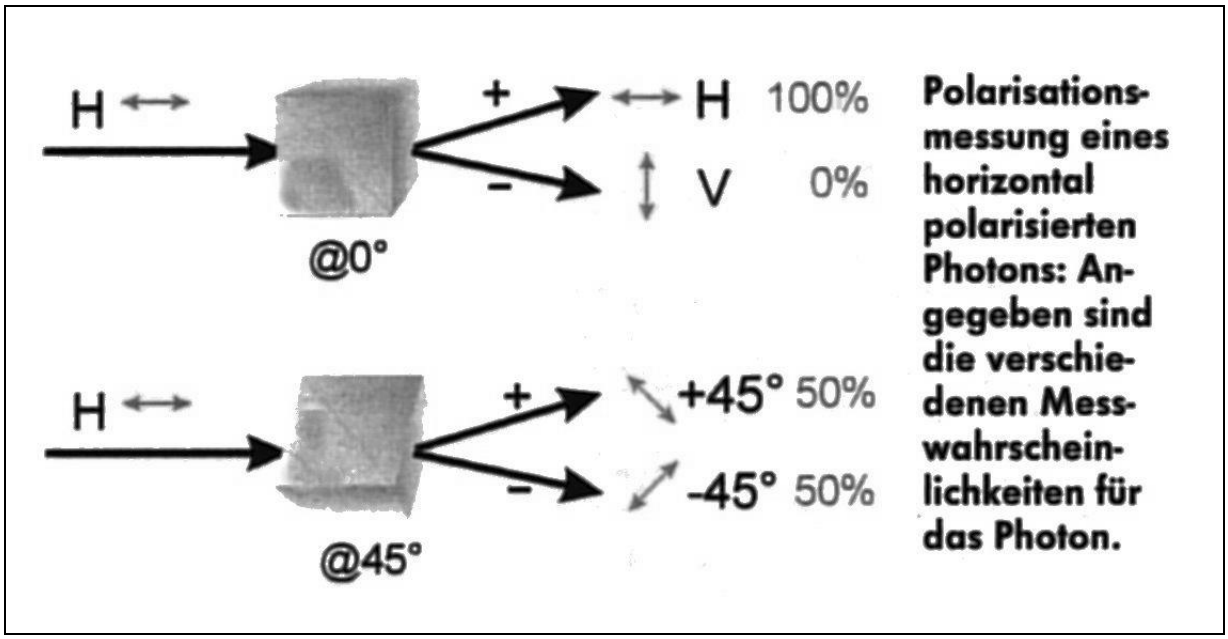

Bild 3.1 Polarisationsmessung

Am Ende des Vorgangs treten Alice und Bob über einen ungesicherten Kanal, der sogar möglichst öffentlich sein sollte, in Verbindung. Bob teilt Alice darüber seine gewählte Detektor-Einstellung mit (natürlich aber nicht das Messergebnis). Alice bestätigt die Qubits, die Bob mit der richtigen Wahl gemessen hat. Nur sie bilden den Quantenschlüssel, indem beispielsweise den Polarisationen 0° und 45° eine binäre 0 bzw. 90° und 135° eine 1 zugewiesen wird.

3.2.2. Praxis

Wie bereits erwähnt, ist bei der praktischen Implementierung streng darauf zu achten, das die Wahl der Polarisation und die Wahl der Analyse absolut zufällig geschieht. Zur Zeit schwieriger zu realisieren ist eine Einzelphotonenquelle.

Die Lösung beider Probleme beschreibt das Magazin „CT“ (s. 5. Literaturliste) in ihrem Report „Quanten-Kryptographie“ (S. 260 – 269). Dabei werden verschränkte Photonenpaare verwendet. Deren wichtigste Eigenschaft ist, das jeweils ein Teilchen zu Alice und eines zu Bob geschickt werden kann, das sich im horizontal – Detektor genau entgegengesetzt verhält. D.h. misst Alice ihr Photon mit dem 0°/90° Detektor und erhält es im + - Ausgang, so findet Bob seines im – - Ausgang (s. Bild 3.2).

Sehr nützlich ist, das die Kombinationen +/- und -/+ rein zufällig, stets gleich häufig sind und nicht gesteuert oder vorherbestimmt werden können. Das zugrundeliegende Prinzip wird als Quanten-Zufall bezeichnet.

Bei den vertikal – Detektoren tritt dieser Effekt nicht auf, so dass auch -/- und +/+ Kombinationen möglich sind, die zufällig und gleich häufig erscheinen.

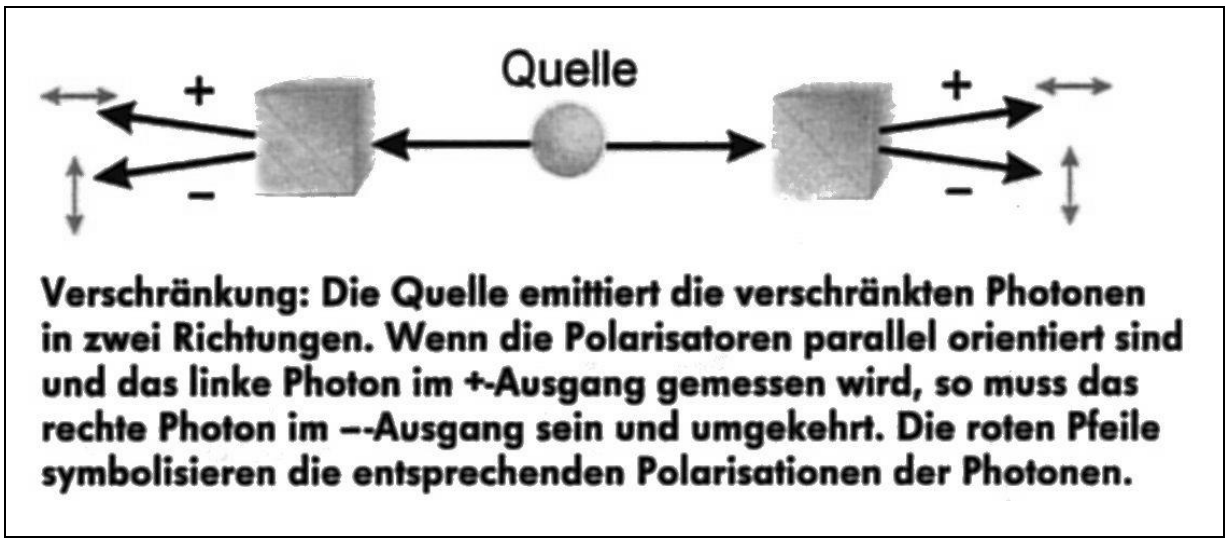

Bild 3.2 Verschränkung von Photonen

Die konkrete Versuchsanordnung auf dem Gelände der Universität Innsbruck überbrückt einen Abstand von Alice und Bob mit 360 Metern, verbunden durch Glasfaserleitungen. Dazwischen befindet sich die Photonenquelle (Argon-Ionen-Laser, der durch ein Beta-Bariumborat-Kristall leuchtet).

Neben dieser Technik wurde auch eine Menge konventioneller Geräte benötigt: Alice und Bob verwenden PCs zur Datenerfassung, die über ein TCP/IP Netzwerk („öffentliche“ Leitung) verbunden sind (s. Bild 3.3).

Zwei Rubidium-Atomuhren synchronisieren das Zeitverhalten, da die Ankunft der Photonen sehr genau (1ns) gemessen werden muss, um die Ergebnisse dem richtigen Teilchen zuordnen zu können. Konkret werden ein 10 Byte großer Zeitstempel (0,1ns Auflösung), das Messresultat und die Detektor-Ausrichtung gespeichert.

Da systembedingt nur 5% der Photonen ein verschränktes Paar darstellen, entsteht ein sehr großer Overhead: pro Bit des Quantenschlüssels ca. 200 Byte.

Im Ergebnis wurde ein Quantenschlüssel mit einer Bit-Rate von 850 Bit/s und einer Bit-Fehlerrate von 2,5% erzeugt. Die Fehlerrate konnte durch einfache Paritätsprüfung auf 0,4% gesenkt werden.

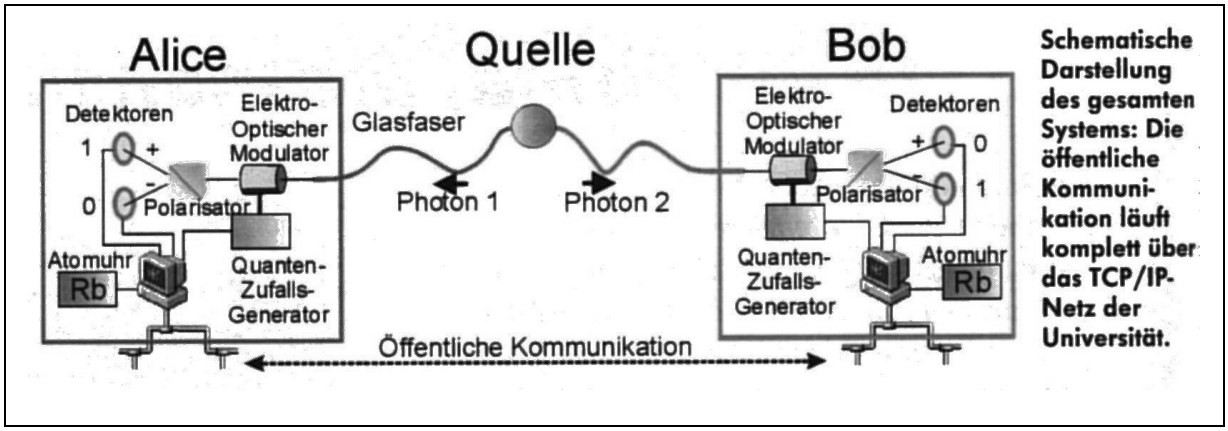

Bild 3.3 Schematische Darstellung des praktischen Versuches

4. Einzigartige Sicherheit

4.1. Abhören unmöglich

Wir betrachten in unserem Modell den Absender, Alice, den Empfänger, Bob und den Lauscher, Eve.

Das Abhören einer Übermittlung zwischen Alice und Bob ist nicht unmöglich, aber in seiner Absicht zwecklos. Wenn Eve versuchen sollte, eine Datenleitung zwischen Alice und Bob anzuzapfen, um die Übertragung aufzuzeichnen oder sogar zu manipulieren, stellt er sich vor das quantenmechanische Problem der Reproduktion von Photonen. Nach den Gesetzen der Quantenmechanik ist ein elementares System wie ein Photon (Qubit) nicht teilbar und kann nicht kopiert werden, ohne eine offensichtliche Veränderung am System zu verursachen.

Im gefährlichsten Fall eines Angriffs würde Eve alle Photonen abfangen, selbst analysieren und dann neue Photonen in der gemessenen Polarität an Bob weiterleiten. Bei der Analyse des Systems passieren Veränderungen zwangsläufig, wenn der Versuch unternommen wird, die Polarität eines Photons zu messen. Der Zustand der Superposition, in dem das Photon vor der Untersuchung steht, stellt Eve vor das Quanten-Dilemma. Seine Unwissenheit über die Polarität des Photons, wird ihm bei der Wahl der Orientierung des Detektors zum Verhängnis, denn ein Fehlgriff verändert die Polarität einiger Photonen unbemerkt. Eve könnte Glück haben und die Orientierung des Polarisators korrekt erraten (50% Chance), aber dürfte im Großen und Ganzen, ohne Zusatzinformationen von Alice, unmöglich feststellen können, welche Messungen richtig sind und welche nicht. Dies bedeutet, dass bei den falsch gemessenen Photonen völlig zufällige Ergebnisse auftreten werden, die Hälfte davon sind zufällig richtig und die andere Hälfte zufällig falsch. Somit hat Eve also für ein Viertel der Photonen die falsche Polarisation gemessen und an Bob weiterversandt. Wenn nun Alice und Bob nach der Schlüsselerzeugung eine Fehlerrate von 25 Prozent feststellen, wissen sie um den Angriff von Eve.

Genaue Analysen der möglichen Angriffsmethoden ergaben eine Mindestfehlerquote von 14 Prozent, die eine sicherheitsbedenkliche Abhörmethode verursachen muss. Eine Fehlerquote unter 14 Prozent kann somit als unbedenklich von Alice und Bob erachtet werden, wobei gilt, je kleiner die Fehlerrate ist, desto sicherer ist das verwandte System.

Wenn Eve nun den Versuch unternehmen würde, mit Hilfe eines Strahlteilers einige Photonen abzuzweigen und diese zu analysieren, so kommen diese Photonen bei Bob einfach nicht an (wegen Unteilbarkeit der Phototonen) und tragen nicht mehr zum Schlüssel bei, der Lauschangriff wäre ebenfalls zwecklos.

Die Quantenkryptographie stellt somit ein Verfahren dar, dass die Sicherheit einer Nachricht gewährleistet, in dem es einem Angreifer nicht erlaubt, die Nachricht überhaupt korrekt aufzuzeichnen. Außerdem ist es den korrespondierenden Partnern möglich, festzustellen, ob eine Angreifer versuchte sie abzuhören. Unter vollkommener Geheimhaltung, ermöglicht die Quantenkryptographie damit Alice und Bob die Vereinbarung eines „One-Time-Pad“ zur Chiffrierung einer Nachricht mit diesem Einmalschlüssel.

4.2. Zukunftsszenario

Im Jahr 2020: Alice muss Bob eine brisante Datei mit Informationen über ihre Finanzgeschäfte übermitteln. Da Alice sehr auf die Sicherheit ihrer Daten bedacht ist, werden ihre Daten mit dem System der Quantenkryptographie verschlüsselt. Zu diesem Zwecke wenden sich Alice und Bob an QTP, einem Quantenkommunikations-Provider. Dort bestellen sie einen Speicher mit verschränkten Atomen. Nachdem sie dann die Schlüsselextraktoren an den Speicher angeschlossen haben, erhalten beide einen 100 Prozent sicheren Kryptoschlüssel. Alice chiffriert

nun ihre Daten und versendet diese als unleserliche Datei an Bob. Über eine beliebige herkömmliche Datenleitung erhält Bob den Geheimtext und dekodiert diesen mit seinem Schlüssel, welcher durch die speziellen Eigenschaften der Quantenkryptographie die Sicherheit garantiert.

5. Literaturverzeichnis

1. Singh, Simon, *Geheime Botschaften – Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*, München: Carl Hanser Verlag, 2000
2. Wrixon, Fred B., *Codes, Chiffren & andere Geheimsprachen,* Köln: Könemann Verlagsgesellschaft mbH, 2000
3. Klein, Artur, *Die faszinierende Welt der Physik,* Basserman'sche Verlagsbuchhandlung, 1990
4. Beutelspacher, Schwenk, Wolfenstetter, *Moderne Verfahren der Kryptographie*, Braunschweig, Vieweg Verlag, 4. Auflage Juni 2001
5. *CT – Magazin für Computertechnik*, Ausgabe 6/2001 (12.3.-25.3.2001)

5.1. Weiterführende URLs zum Stand der Forschung

- QuComm (entwickelt eines quantenkryptographischen Aufbau zur Prototypenreife) *http://www.ele.kth.se/QEO/qucomm/*
- Group of Applied Physics, kurz GAP (hält den Rekord im Abstand von Alice und Bob)
  http://www.gapoptique.unige.ch/
- Gruppe von H. Weinfurter in München (beschäftigt sich in Deutschland experimentell mit Quantenkryptographie) *http://scotty.quantum.physik.uni-muenchen.de/*