Seminar Quanten-Computing und Quanten-Informationstheorie
Sommersemester 2003 Nielaba

Quantenkryptografie

Moritz Bubek
bubek@gmx.de

PACS numbers:

I. MOTIVATION

Verschlüsselung spielt in der heutigen Welt, aber auch schon seit der Antike eine wichtige Rolle. Zuerst hauptsächlich für militärische und diplomatische Zwecke genutzt, heutzutage aus wirtschaftlichen Interessen. Firmen schützen ihre Daten beim Senden an Partnerunternehmen, an Zweigstellen oder einfach nur beim archivieren vor fremdem Zugriff. Bei elektronischen Zahlungsmitteln, wie EC-Karten, müssen die Daten ebenfalls verschlüsselt übertragen werden.

II. KLASSISCHE KRYPTOGRAFIE

A. Kryptografische Verfahren

Alle verwendeten Verschlüsselungsverfahren basieren darauf, jedes Zeichen des Textes durch ein mit dem Verfahren festgelegten Zeichen zu ersetzen. Dabei gibt es verschieden komplizierte Varianten, die entsprechend schwerer zu knacken sind.

Das einfachste davon ist sicher eine Zuordnungstabelle, die jedem Zeichen des Zeichensatzes (z.B. von A bis Z) jeweils ein anderes zuordnet. Dieses Verfahren wurde schon bei den Ägyptern 1900 v. Chr. verwendet, die nicht Standard-Hiroglyphen verwendeten und dadurch jedes Zeichen ersetzten. Der Empfänger der Nachricht braucht nur die entsprechende Tabelle und kann die Nachricht wieder entschlüsseln.

Ebenso einfach ist der Ceasar-Code, bei dem jedes Zeichen einfach um eine bestimmte Zahl n (z.B. n= 13[1]) weiter gedreht wird (mit n = 3 wird aus $A \rightarrow D$, $B \rightarrow E$, $C \rightarrow F$, usw). Zum entschlüsseln der Nachricht muss nur die Zahl bekannt sein, mit der chiffriert wurde und mit dieser das Verfahren dann rückwärts angewendet werden.

Diese beiden Verfahren sind sehr einfach zu knacken, da jedes Zeichen immer durch das selbe Zeichen ersetzt wird. Dadurch kann man einfach durch statistische Analyse der Sprache (im Deutschen kommt das e am häufigsten vor) die jeweiligen Ersetzungen herausbekommen.

Durch Wahl eines Schlüssels einer bestimmen Länge kann dieses System verbessert werden. Durch periodische Aneinanderreihung des Schlüssels und Addition zum zu verschlüsselnden Textes wird dieser chiffriert.Dieses Verfahren nennt man Vignere-Chiffre.

Orginaltext	Q	U	A	N	T	E	N
Schlüssel (+)	K	E	Y	K	E	Y	K
Verschlüsselter Text	B	Z	Z	Y	Y	D	Y
	↓ öffentlicher Kanal ↓						
Empfangener Text	B	Z	Z	Y	Y	D	Y
Schlüssel (-)	K	E	Y	K	E	Y	K
Entschlüsselter Text	Q	U	A	N	T	E	N

Tabelle I: Anwendungsbeispiel einer Privat-Key-Verschlüsselung

Aber auch dieses Verfahren ist immer noch durch statistische Verfahren knackbar[2].

Das Verfahren wird erst dann sicher, wenn der Schlüssel die selbe Länge wie der zu verschlüsselnde Text hat und auch keine Regelmäßigkeiten mehr vorweist, er also eine völlig zufällige Kombination ist. Diesen Schlüssel nennt man Vernam Chiffre oder auch One-Time-Pad (OTP), da er nur einmal verwendet werden kann, ohne einen Verlust an Sicherheit zu haben. Solange der Schlüssel wirklich geheim bleibt, ist das OTP die einzige informationstheoretisch sichere Verschlüsselungsverfahren, d.h es kann nur durch eine Brute-Force-Attacke[3] geknackt werden.

Orginaltext	Q	U	A	N	T	E	N
Schlüssel (+)	G	U	R	H	W	A	F
Verschlüsselter Text	X	P	S	V	Q	F	T
	↓ öffentlicher Kanal ↓						
Empfangener Text	X	P	S	V	Q	F	T
Schlüssel (-)	G	U	R	H	W	A	F
Entschlüsselter Text	Q	U	A	N	T	E	N

Tabelle II: Anwendungsbeispiel einer Verschlüsselung mit einem OTP

[1] ROT13 ist eine gängige Variante im Usenet, Text gegen zufälliges Lesen zu schützen → Netikette

[2] Auch in Tabelle II A sieht man schon sehr deutlich, dass bei kurzem Schlüssel Wiederholungen vorkommen , die ausgenutzt werden können

[3] welche natürlich je nach Schlüssellänge mehr oder weniger Zeit beansprucht

B. Problem: Schlüsselübertragung

Alle diese Verfahren haben aber ein gemeinsames Problem. Bei allen müssen zuerst die Schlüssel (die Tabelle, die Zahl, das Schlüsselwort) über einen unsicheren Kanal zum Empfänger übertragen werden. Dabei kann dieser so wie ursprünglich die Nachricht abgefangen und abgehört werden. Damit wäre ein Angreifer in der Lage jede auch noch so gut verschlüsselte Nachricht zu entschlüsseln.

Zur Lösung dieses Problems kann man auf asymmetrische Verfahren zurückgreifen, bei dem der Absender und der Empfänger verschiedene Schlüssel haben. Eines dieser Verfahren ist RSA, welches auf der Faktorisierung großer Primzahlprodukte aufbaut und ist dadurch für klassische Computer nur sehr schwer zu knacken. Für einen Quantencomputer allerdings stellt dies bei entsprechender Realisation des Shor-Algorithmus nur ein geringfügiges Problem dar.

Die Lösung des Problems der Schlüsselübertragung ist aber ebenfalls die Quantenmechanik, was in den folgenden Absätzen beschrieben wird.

III. THEORETISCHE VORAUSSETZUNGEN

In den folgenden Abschnitten werden einige physikalische Theorien angesprochen und skizziert. Diese bilden die Grundlage für die Möglichkeiten der darauffolgenden Verfahren der Quantenkryptografie.

Eines der wichtigsten Prinzipien ist gleichzeitig auch eine der Grundaussagen der Quantenmechanik, nämlich dass eine Messung das System beeinflusst, was in allen Verfahren als Grundvoraussetzung benutzt wird.

A. Das Non-Cloning-Theorem

Ist es möglich, einen unbekannten, beliebigen Quantenzustand zu kopieren ?

Nehmen wir an, es gäbe einen Quantenkopierer, eine Quantenmaschine mit zwei Eingängen A und B. A ist in einem unbekannten, aber reinem Zustand $|\psi\rangle$. Dieser Zustand soll auf den Ausgang B, welcher sich am Anfang im Zustand $|s\rangle$ befindet, kopiert werden.

Der Anfangszustand des Kopierers, also der beiden Gates ist

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

Durch eine unitäre Entwicklung U wird der Kopiervorgang durchgeführt

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

Wendet man dieses Kopieren auf zwei unabhängige Zustände $|\psi\rangle$ und $|\varphi\rangle$ an, erhält man

$$\begin{aligned} U(|\psi\rangle \otimes |s\rangle) &= |\psi\rangle \otimes |\psi\rangle = |\psi\psi\rangle \\ U(|\varphi\rangle \otimes |s\rangle) &= |\varphi\rangle \otimes |\varphi\rangle = |\varphi\varphi\rangle \end{aligned}$$

Der Zustand $|\xi\rangle$ setzt sich aus den Zuständen $|\psi\rangle$ und $|\varphi\rangle$ zusammen

$$|\xi\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\varphi\rangle)$$

Da U Qubits klont, muss gelten

$$\begin{aligned} U(|\xi s\rangle) = |\xi\xi\rangle &= \frac{1}{2}\left(|\psi\rangle + |\varphi\rangle\right) \otimes \left(|\psi\rangle + |\varphi\rangle\right) \\ &= \frac{1}{2}\left(|\psi\psi\rangle + |\psi\varphi\rangle + |\varphi\psi\rangle + |\varphi\varphi\rangle\right) \end{aligned}$$

Wegen der Linearität des unitären Operators U gilt aber auch

$$U(|\xi s\rangle) = \frac{1}{\sqrt{2}}\left(U(|\psi s\rangle) + U(|\varphi s\rangle)\right) = \frac{1}{\sqrt{2}}\left(|\psi\psi\rangle + |\varphi\varphi\rangle\right)$$

Im Allgemeinen ist aber

$$\frac{1}{2}\left(|\psi\psi\rangle + |\psi\varphi\rangle + |\varphi\psi\rangle + |\varphi\varphi\rangle\right) \neq \frac{1}{\sqrt{2}}\left(|\psi\psi\rangle + |\varphi\varphi\rangle\right)$$

sodass es diese unitäre Transformation U nicht geben kann, die beliebige Quantenzustände kopiert. Die Kopiermaschine kann nur Zustände kopieren, die orthogonal zueinander sind.

B. Quantenverschränkung

Die Quantentheorie ist eine nichtlokale Theorie, d.h. sie beschreibt Wellenfunktionen mit globalen Eigenschaften. Das bewirkt, dass zwei[4] quantenmechanische Teilchen und ihre Eigenschaften als ein System gesehen werden kann. Auch über größere Entfernungen bleibt dieser Verbund, der gemeinsame Zustand bestehen. Misst man nun eine Eigenschaft, z.B. den Spin eines Teilchens, so ist automatisch der Zustand des anderen festgelegt, was man als Fernwirkung bezeichnet.

C. Bell'sche Ungleichung

1. *Herleitung*

Eine Quelle emittiert verschränkte Paare von Spin-1/2 Teilchen, die an zwei entfernten Orten mit unabhängigen Stern-Gerlach-Apparaten, in den Richtungen a und b, analysiert werden. Es sind in den Richtungen a und b jeweils die Messergebnisse ± 1 möglich, je nach Ablenkungsrichtung. $E(a, b)$ ist das gemittelte Produkt der beiden Messergebnisse.

[4] oder mehrere

Klassisch wird das Ergebnis A (± 1) einer Messung der quantenmechanischen Observablen am Teilchen 1 nur durch a und eventuelle verborgene Parameter bestimmt, ebenso für Teilchen 2 mit b

Es ist also $A(a,\lambda) = \pm 1$ und $B(b,\lambda) = \pm 1$, wobei λ eventuell verborgene Parameter sind. $\rho(\lambda)$ ist eine normierte Wahrscheinlichkeitsverteilung der Messergebnisse. Der klassische Erwartungswert ist dann

$$E(a,b) = \int \rho(\lambda) A(a,\lambda) B(b,\lambda) d\lambda \tag{1}$$

Dieser Ausdruck kann nicht kleiner als -1 werden und wenn -1, dann nur wenn a = b und dann ist $A(a,\lambda) = -B(a,\lambda)$

$$E(a,b) = -\int \rho(\lambda) A(a,\lambda) A(b,\lambda) d\lambda \tag{2}$$

Führt man eine dritte Messrichtung c ein, dann kann man mit $A(b,\lambda)A(b,\lambda) = 1$ folgende Beziehung aufstellen

$$\begin{aligned} & E(a,b) - E(a,c) \\ &= -\int \rho(\lambda)[A(a,\lambda)A(b,\lambda) - A(a,\lambda)A(c,\lambda)]d\lambda \\ &= \int \rho(\lambda) A(a,\lambda)A(b,\lambda)[A(b,\lambda)A(c,\lambda) - 1]d\lambda \end{aligned} \tag{3}$$

Mit den allgemeingültigen Relationen

$$\left|\int f(x)dx\right| \leq \int |f(x)|dx \text{ und } |A(a,\lambda)A(b,\lambda)| = 1$$

kann Gleichung 3 umgewandelt werden.

$$\begin{aligned} & |E(a,b) - E(a,c)| \\ &= \left|\int \rho(\lambda)A(a,\lambda)A(b,\lambda)[A(b,\lambda)A(c,\lambda) - 1]d\lambda\right| \\ &\leq \int |\rho(\lambda)A(a,\lambda)A(b,\lambda)[A(b,\lambda)A(c,\lambda) - 1]|\, d\lambda \\ &= \int \rho(\lambda)\,|[A(b,\lambda)A(c,\lambda) - 1]|\, d\lambda \\ &= \int \rho(\lambda)[1 - A(b,\lambda)A(c,\lambda)]d\lambda \end{aligned} \tag{4}$$

Daraus kann man die Bell'sche Ungleichung (BUG) in der Originalfassung erstellen, welche mathematische Bedingung für lokal realistische Theorien ist.

$$|E(a,b) - E(a,c)| \leq 1 + E(b,c) \tag{5}$$

Wird die Ungleichung verletzt, handelt es sich nicht um eine lokale Theorie.

2. Klassische Überprüfung

Klassisch ist $E^{kl}(a,b) = \pm 1$, es ist also unabhängig von a oder b. Durch einsetzen kann man die BUG überprüfen.

$$\begin{aligned} E^{kl}(a,b) &= 1 \overset{BUG}{\longrightarrow} 0 \leq 2 \ \checkmark \\ E^{kl}(a,b) &= -1 \overset{BUG}{\longrightarrow} 0 \leq 0 \ \checkmark \end{aligned}$$

3. Quantentheoretische Überprüfung

In der Quantentheorie ist die Wahrscheinlichkeit über die Winkel zwischen den entsprechenden Messoperatoren. Sie hängt also im Gegensatz zu klassischen Annahme durchaus von a und b (und c) ab.

In Spezialfällen wird auch quantentheoretisch die BUG erfüllt

1. Grenzfall gleicher Messrichtungen, d.h. $a = b = c$

$$E^{qt}(a,b) = -a.b = -1 \overset{BUG}{\longrightarrow} 0 \leq 0 \ \checkmark \tag{6}$$

2. Grenzfall senkrechter Messungen, d.h. $a = b \perp c$

$$\begin{aligned} & E^{qt}(a,b) = -1 \\ & E^{qt}(a,c) = E^{qt}(b,c) = 0 \overset{BUG}{\longrightarrow} 1 \leq 1 \ \checkmark \end{aligned} \tag{7}$$

   In diesen beiden Fällen geht die Ungleichung auf, im Allgemeinen liegen diese Spezialfälle aber nicht vor.

3. $a.b = b.c = cos(45°) = 1/\sqrt{2}$ und a.c = 0

$$\overset{BUG}{\longrightarrow} \left|-\frac{1}{\sqrt{2}} - 0\right| \leq 1 - \frac{1}{\sqrt{2}} \tag{8}$$

   Diese Ungleichung ist nicht erfüllt, denn $0.707 \leq 0.293$ ist nicht korrekt. Daraus folgt das die Quantentheorie eine nichtlokale Theorie ist.

Die Bell'sche Ungleichung kann in dieser oder mehrerer anderer Varianten auftreten. Je nach Problemstellung muss sie entsprechend angepasst werden, aber die Herleitung verläuft immer nach dem selben Prinzip und die Aussage ist immer dieselbe.

IV. VERSCHIEDENE VERFAHREN

Wie schon gesehen, können mittels Quantencomputer die besten Verschlüsselungsverfahren sehr schnell geknackt werden. Um trotzdem eine sichere Verschlüsselung nutzen zu können, wurden verschiedene Verfahren zu Schlüsselerzeugung bzw -übermittlung erdacht und auch im Experiment durchgeführt.

Das QKD Protokolle, mit dem private Schlüssel über einen öffentlichen Kanal erzeugt werden können, sind nachweislich sicher. Das einzige was dazu benötigt wird,

ist eine Leitung[5] durch die Qubits mit einer geringen Fehlerrate gesendet werden können. Die Qubits können dann zur Erstellung eines Schlüssels für klassische Verschlüsselungsverfahren genutzt werden. Die Sicherheit des Schlüssels hängt nur von der Richtigkeit der Quantenmechanik ab.

Der Grundgedanke des QKD ist die Beobachtung, dass es einem Abhörer[6] Eve nicht gelingt Informationen über den Zustand des zwischen Alice und Bob übertragenen Qubits zu messen, ohne diesen Zustand zu zerstören. Wegen des Non-Cloning-Theorems (III A) kann Eve auch nicht einfach den Zustand klonen um an die Informationen zu gelangen.

A. Das BB84-Protokoll

Mit dem BB84-Protokoll, das 1984 von C. Benett und G. Brassard entwickelt wurde, können Alice und Bob wie folgt einen geheimen Schlüssel generieren, um anschließend eine damit kodierte Nachricht auszutauschen.

Alice hat vier Photonentransmitter mit den Polarisationen[7] 0, 45,90 und 135 Grad, die den Quantenzuständen $|1\rangle$, $|0'\rangle$,$|0\rangle$ und $|1'\rangle$ entsprechen. Bobs Detektor kann so eingestellt werden, dass er entweder zwischen $|0\rangle$ und $|1\rangle$ (Standartbasis) unterscheiden kann oder aber zwischen $|0'\rangle$ und $|1'\rangle$ (Dualbasis), nicht aber zwischen allen vier Möglichkeiten, was durch die Heisenberg'sche Unschärferelation verboten wird.

Damit Alice und Bob einen Schlüssel der Länge n austauschen können, erzeugt Alice zwei Reihen von Zufallsbits der Länge m, wobei m deutlich größer als n sein soll ($m > n$). Bob erzeugt ebenfalls eine solche zufällige Bitfolge. Es kommt darauf an, dass keinerlei Regelmäßigkeit in den Reihen vorliegt, sodass man diese Reihe z.B. durch Quanteneffekte erzeugen muss. Jede Regelmäßigkeit oder Berechenbarkeit stellt eine Schwachstelle dar und kann durch statistische Verfahren als Mittel zu einer Attacke genutzt werden.

Alice sendet nun Bob die erste Reihe Zufallbits. Dabei sendet sie die 0 als $|0\rangle$ oder $|0'\rangle$ und die 1 zufällig als $|1\rangle$ oder $|1'\rangle$, wobei sie ihre zweite Reihe als Auswahlkriterium für die Sendebasis nutzt. Bob entscheidet anhand seiner Zufallsreihe vor jeder Messung ob er eine orthogonale oder diagonale Detektorstellung nutzt, d.h. ob er die Standartobservable $B = \{|0\rangle, |1\rangle\}$ oder die Dualobservable $D = \{|0'\rangle, |1'\rangle\}$ benutzt.

Die diagonalen Zustände lassen sich durch die orthogonalen Zustände ausdrücken. $|0'\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ und $|1'\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. Bei einer Messung dieser Zustände in der Standartbasis entspricht die Wahrscheinlichkeit, dass ein bestimmter Basiszustand gemessen wird, dem Quadrat des jeweiligen Faktors, in diesem Fall also je $\frac{1}{2}$. Analog wenn ein orthogonaler Zustand mit einem diagonal eingestellten Detektor gemessen wird. Entscheidet sich Bob also für die "falsche" Basis, so ist sein Messergebnis rein zufällig.

Anschließend teilt Bob Alice mit, wie er seinen Detektor bei jeder Messung eingestellt hatte, nicht aber die Messergebnisse. Alice teilt nun Bob mit, bei welchen Messungen er den Detektor "richtig" eingestellt hatte, d.h. er die selbe Basis verwendet wie sie selbst. Dieser Informationsaustausch kann über einen öffentlichen Kanal erfolgen, da ein Lauscher ohne eine eigene Messung nichts mit dieser Information anfangen kann. Der gemeinsame Schlüssel von Alice und Bob besteht nun aus den Messergebnissen, die mit den gleichen Einstellungen gemacht wurden. Die "falschen" werden verworfen.

Mit diesem erhaltenen Schlüssel verschlüsselt Alice nun die Nachricht, die sie an Bob senden will und schickt diese über den öffentlichen Kanal zu Bob. Dieser kann ihn dann mit Hilfe seines Schlüssels wieder entschlüsseln. Bei den QKD-Verfahren wird also nicht die Nachricht quantenmechanisch übertragen, sondern immer nur ein Schlüssel.

Alice' 1. Zufallsreihe	1	1	0	0	0	1
Alice' 2. Zufallsreihe	0	1	1	0	0	0
Alice's Polarisierung	$\|1\rangle$	$\|1'\rangle$	$\|0'\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$
Bobs Zufallsreihe	0	0	1	0	0	1
Bobs Basis	B	B	D	B	B	D
Messergebnisse	1	Z	0	0	0	Z
→ Schlüssel 1 0 0 0						

Tabelle III: Anwendungsbeispiel des BB84-Protokolls ohne Abhörer und ohne Rauschen, Z ist dabei ein zufälliges Messergebnis

Das Anwendungsbeispiel (Tabelle IV A) zeigt zwar das Verfahren, allerdings wird erst bei wesentlich mehr übertragener Qubits richtig sichtbar, wie die Statistik angewendet werden kann. Sobald ein Abhörer und Rauchen hinzukommt, sieht man erst ab einer viel größeren Anzahl wie das Verfahren sich verhält. (→ Abb.1)

1. *Entdeckung eines Abhörers*

Bisher wurde kein Abhörer Eve in der Leitung angenommen. Dieser ist aber anzunehmen[8] und Eve versucht den übertragenen Schlüssel abzufangen.

Eve kann den öffentlichen Kanal belauschen, über den Alice und Bob ihre Einstellungen austauschen. Da Eve zusätzlich zu den Informationen über die Stellungen der

[5] Glasfaser, Luft, ...

[6] im nachfolgenden Eve genannt

[7] Die Messungen müssen nicht zwingend mit Polarisationen durchgeführt werden, es erweist sich aber im Experiment als praktisch

[8] ansonsten ist das ganze Verfahren überflüssig

```
Alices Basis: +++++XX++XX+++XXX+++X+++XX+X+XXX+X+X+XX+XX+++XXXX+X++XX+++X+XXX+
Alice sendet: |--||\/|-\\|--///-||\-|-\/-/-\\\-\-\-//|\\--|\\/\|/|-//||-/-//\-
Bobs Basis  : X+XX++XXX+++XX++X++XXX+++X++XXXX+X++X++X++XXX+XXXX+XXXXXX++++++X
Bob misst   : /-/\||///--|\/-|/-|/\\|--/-|/\\\-\--\|-/|-///|\/\/|\\//\/-|-||-\

Bob         : X+XX++XXX+++XX++X++XXX+++X++XXXX+X++X++X++XXX+XXXX+XXXXXX++++++X
Alice       :  .  . .    .    ... . .. ..  ......          ...    ..  . .
Schluessel  :  0  1 1    1    101 0 10 00  111010          101    00  0 0
```

Abbildung 1: Das BB84-Protokoll ohne Abhörer und ohne Rauschen mit 64 übertragenen Qubits

Detektoren auch die entsprechenden Messwerte braucht, muss sie diese messen. Anders als bei der klassischen Schlüsselübermittlung kann Eve die ausgetauschten Informationen aber nicht nur passiv abhören, da jede Messung den Zustand verändert und sich die Zustände auch nicht klonen lassen (III A).

Sie fängt die von Alice zu Bob gesandten Quantenzustände ab, misst sie und leitet sie dann zu Bob weiter. Da sie aber nicht wissen kann, mit welcher Polarisation Bob die Messung durchführt, kann sie die Polarisation bei ihrer Messung zufällig wählen. Dadurch erhöht sie aber zwangsläufig die Fehlerrate der Übertragung, wenn sie und Bob verschiedene Polarisationen gewählt haben, also in 50 % der Fälle. Bobs Messung ist dadurch also in 25 % der Fälle falsch, die Wahrscheinlichkeit, dass Eve entdeckt wird ist somit $1 - \left(\frac{1}{4}\right)^n$. Sie geht für eine große Anzahl n ausgesandter Qubits gegen 1.

Alice und Bob schützen sich vor einem Lauschangriff, indem sie die Fehlerrate ermitteln und ab einem Grenzwert an Fehlern ihren ausgetauschten Schlüssel verwerfen. Dazu wählt Bob zufällig eine Menge Qubits, die als Grundlage für die Schlüsselerzeugung dienen aus und veröffentlicht deren Messwerte.

Alice vergleicht diese mit ihren an der selben Position. Ist die Fehlerrate zu groß, verwerfen sie den Schlüssel und beginnen von vorne. Ist die Fehlerrate im Rahmen der Übertragungsfehler, werden die veröffentlichten Bits weggeworfen und aus den restlichen der Schlüssel gebildet.

Da dieses Verfahren erst bei größerer Anzahl von Qubits seine Probleme zeigt, ist in Abbildung 3 ein Beispiel mit 64 Qubits dargestellt.

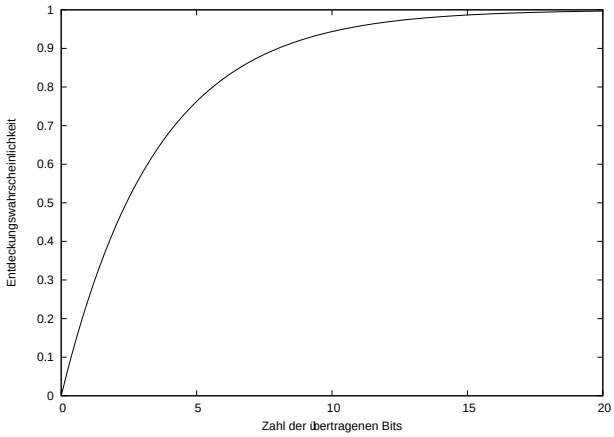
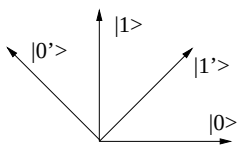


Abbildung 2: Wahrscheinlichkeit in Abhängigkeit von der Zahl der von Bob empfangenen Qubits Eve beim Abhören zu erwischen

B. Das B92-Protokoll



Beim 1992 von C. Benett entwickelten B92-Protokoll werden im Gegensatz zum BB84-Protokoll nur zwei nicht-orthogonale Zustände benötigt. Diese vereinfachte Variante des BB84-Protokolls benutzt nur die Polarisation 90° und 135° bzw $|0\rangle$ und $|1'\rangle$.

Die Zahl 1 wird über den Zustand $|1'\rangle$, die 0 über den Zustand $|0\rangle$ übertragen. Bob verwendet wiederum zum Messen zufällig die Basis B oder D. Misst er $|0\rangle$ oder $|1'\rangle$, kann er das Ergebnis verwerfen, da er sich nicht sicher sein kann, ob Alice tatsächlich diese Observable benutzt und diesen Zustand übertragen hat, oder ob sein Messergebnis rein zufällig ist.

Erhält er aber als Ergebnis den Zustand $|0'\rangle$ oder $|1\rangle$, dann weiß er sicher, dass Alice die andere Basis benutzt hat, da sie niemals die von ihm gemessenen Zustände benutzt. Misst er $|0'\rangle$, hat sie 0 übertragen, misst er $|1\rangle$ hat sie 1 übertragen. Bob teilt dann Alice die Positionen dieser Bits mit und sie bilden damit die Basis für ihren gemeinsamen Schlüssel.

Da hier nur zwei Zustände benutzt werden und auch ein Kommunikationschritt weniger[9] benötigt wird, hat das Verfahren Vorteile gegenüber BB84, allerdings können weniger übertragene Bits verwendet werden.

[9] Alice muss Bob nicht mitteilen mit welcher Observablen sie präpariert hat

```
Senden
Alices Basis: X+XX++++++X++XX++XXXX++++X++++XX++X+X+XXX+XXX+X+XXX++XXX+++X+XXX
Alice sendet: /-/\-|---|/||/\||\//\-|--/-|||/\-|\|/-\/\|//\|/|\\\-|\//|-|/|/\\
Abhoeren
Eves Basis  : XXX+X+X+X+++XX++X++XX+XX+XX+X++X+++X+X++XX++X+++++XX+X++X+XXX+X+
Eve misst   : ///|\|\-\|-|\/||\||/\-\/-//|/|-\-|-/-/-|\\|-\|-|-|\/|\-|\-\//|\-
Empfangen
Bobs Basis  : XXXX++++XXX+XXXXXX+++XXXX+X+XX++++X++++XXX+X++X+++X+XX+++X+++X++
Bob misst   : ///\||--\/\|\//\\\||-/\//|/|//---|/----\\\|\-|/|-|\-\\-|-/|-|/|-
Vergleichen der Basis
Bob         : XXXX++++XXX+XXXXXX+++XXXX+X+XX++++X++++XXX+X++X+++X+XX+++X+++X++
Suche nach Fehlern
Alice       : / .\..-.  /| ..  .        |    ..\| - /.  / |/|  .. .  . | |/
Bob         : / .\..-.  \| ..  .        |    ../- - \.  \ |/|  .. .  . | |/
```

Abbildung 3: Das BB84-Protokoll mit Abhörer Eve (ohne Rauschen) mit 64 übertragenen Qubits. Von diesen wird die Hälfte von Alice und Bob zur Ermittlung der Fehlerrate herangezogen. Alle mit Punkt markierten verbleiben um im Nicht-Abhörfall den Schlüssel zu erzeugen. Von diesen 17 getesteten Bits sind hier 5 falsch. Alice und Bob wurden abgehört.

C. Kommunikation über unzuverlässige Medien

Bisher haben wir angenommen, dass Alice und Bob über ein perfektes Medium, also ein verlust- und rauschfreies Medium[10], kommunizieren. Da es ein solches Medium im Allgemeinen nicht gibt, muss man darüber diskutieren, wie man die Fehler die durch das Medium entstehen herausrechnen kann.

Durch das Rauschen bzw die Absorption kann Bob manche Bits nicht oder nur verändert empfangen. Da die Quantenkryptografieverfahren darauf basieren, Eve über die Fehlerrate zu entdecken, muss festgestellt werden, ob ein Fehler von Eve oder durch das Rauschen verursacht wird.

Die Schlüsselerzeugungsverfahren werden genauso durchgeführt wie bisher ohne Rauschen, allerdings wird dann ein Schritt, die Fehlerkorrektur, eingefügt. Sie verläuft analog zu einer klassischen Fehlerkorrektur.

Zuerst ermitteln Alice und Bob, ob es überhaupt Sinn macht, über das Medium zu kommunizieren, indem sie die Fehlerrate an einer extra dafür erzeugten Bitsequenz ermitteln[11]. Ist diese Fehlerrate zu hoch, ist die Kommunikation allgemein nicht möglich oder sinnvoll.

Schätzen sie die Fehlerrate als annehmbar ein, so beginnen sie mit der Schlüsselerzeugung. Den fertigen Schlüssel zerteilen sie nun in kleine Blöcke. Sie überprüfen eine Checksumme eines Blockes, z.B. die Parität, die nur durch vollständige Kenntnis der Daten den selben Wert ergibt. Sie tauschen diese über einen öffentlichen Kanal aus. Ist diese Checksumme gleich entfernen sie das letzte Bit des Blocks, um diesen weiterhin als Schlüssel verwenden zu können.

Schlägt der Vergleich fehl, führen die beiden eine Binärsuche durch, d.h. sie teilen den Block in zwei Teile und vergleichen abermals deren Checksummen. Dies geht solange weiter, bis sie keinen Fehler mehr finden oder die Blöcke zu klein werden, um noch Sicherheit garantieren zu können. In diesem Fall verwerfen sie den entsprechenden Block.

Da Eve's Fehler rein zufällig sind, die Fehler des Mediums aber meist eine Regelmäßigkeit aufweisen, können Eve's Störungen darüber identifiziert werden.

D. Das EPR-Protokoll

Dieses Protokoll zur Schlüsselerzeugung wurde 1991 von Arthur Ekert vorgeschlagen und basiert auf der Verschränkung der Teilchen[12], die dem Austausch dienen. Zwischen Alice und Bob gibt es eine Quelle, die Paare verschränkter Teilchen produziert [13].

1. Präparation des Systems

Die Basis besteht aus einem System von drei Paaren orthogonaler Zustände $|\Omega_1\rangle$, $|\Omega_2\rangle$ und $|\Omega_3\rangle$, aus der die Quelle Teilchen erzeugen kann.

$$
\begin{aligned}
|\Omega_1\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle_1|\frac{3\pi}{6}\rangle_2 - |\frac{3\pi}{6}\rangle_1|0\rangle_2\right)\\
|\Omega_2\rangle &= \frac{1}{\sqrt{2}}\left(|\frac{\pi}{6}\rangle_1|\frac{4\pi}{6}\rangle_2 - |\frac{4\pi}{6}\rangle_1|\frac{\pi}{6}\rangle_2\right)\\
|\Omega_3\rangle &= \frac{1}{\sqrt{2}}\left(|\frac{2\pi}{6}\rangle_1|\frac{5\pi}{6}\rangle_2 - |\frac{5\pi}{6}\rangle_1|\frac{2\pi}{6}\rangle_2\right)
\end{aligned}
$$

Diese entsprechen den Polarisationsrichtungen eines Filters von, z.B. (0°,90°), (30°,120°) und (60°,150°)

[10] z.B. Vakuum oder rauschlose, verlustfreie Glasfasern
[11] oder über die physikalischen Daten des Mediums ermitteln
[12] hauptsächlich Photonen
[13] nichtlineare Kristalle, ...

Die zugehörigen Messoperatoren sind M_1, M_2 und M_3 und es werden folgende Vereinbarungen getroffen

Zustand	Bit	Zustand	Bit	Zustand	Bit
$\|0\rangle$	0	$\|\frac{\pi}{6}\rangle$	0	$\|\frac{2\pi}{6}\rangle$	0
$\|\frac{3\pi}{6}\rangle$	1	$\|\frac{5\pi}{6}\rangle$	1	$\|\frac{6\pi}{6}\rangle$	1

2. *Kommunikation über einen Quantenkanal*

Ein EPR-Paar wird von der Quelle generiert und jeweils teilweise zu Alice bzw Bob gesendet. Beide wählen unabhängig voneinander, zufällig einen der drei Messoperatoren M_1, M_2 oder M_3, also z.B. eine Polarisationsrichtung. Sie messen den Zustand. Alice merkt sich das Messergebnis und Bob das Komplement seines Ergebnisses, da er über die Verschränkung genau den gegensätzlichen Zustand erhält. Dieser Vorgang wird solange wiederholt bis genügend Qubits vorhanden sind.

3. *Kommunikation über einen öffentlichen Kanal*

Alice und Bob vergleichen nun wieder ihre Messeinstellungen über einen öffentlichen Kanal.

Sie extrahieren die Bits, bei denen sie die selben Einstellungen benutzt haben und bilden daraus ihren Schlüssel. Die Ereignisse, bei denen verschiedene Einstellungen benutzt wurden, werden dazu verwendet, einen Abhörer zu entdecken.

Mit der Annahme, dass die Fernwirkung, also die Verschränkung die Bell'sche Ungleichung verletzt, kann Eve entdeckt werden. Sobald die Ungleichung erfüllt wird, liegen keine verschränkte Teilchen mehr vor, der Zustand wurde gestört und man kann den Schluss ziehen, dass Eve in der Leitung mithört.

V. EXPERIMENTELLE UMSETZUNG

A. Allgemein

Gerade in letzter Zeit werden auf dem Gebiet der Quantenkryptografie sehr viele Experimente und Fortschritte gemacht. Obwohl die ersten theoretischen Vorschläge erst Mitte der 80er Jahre gemacht wurden, gab es 1989 das erste Experiment. IBM-Forschern gelang es zum ersten mal über eine Strecke von 30 cm durch Luft im Labor einen Schlüssel über ein QKD-Verfahren zu generieren.

In den darauffolgenden Jahren wurden immer größere Entfernungen mit verschiedenen Verfahren überbrückt, z.B.1995 über 23 km Glasfaser in Genf oder 1997/98 per EPR-Protokoll über ca. 10 km ebenfalls in Genf.

B. Aktuelle Experimente

1. *Übertragung durch Glasfaser*

An der Universität Innsbruck wurden EPR-Übertragungen über 360 m Glasfaser gemacht. Da beim Erzeugen von verschränkten Photonenpaaren nur sehr wenige entstehen, d.h. es entstehen sehr viele Photonen die nicht verschränkt sind, müssen die beiden Messungen mittels einer hochpräzisen Atomuhr aufeinander abgestimmt werden. Nur Paare die innerhalb eines Zeitfensters detektiert werden, gehen in die Auswertung ein. Die Auswahl der Polarisationsrichtung wird über einen quantenmechanischen Prozess geführt. Über diesen wird dann der Polarisationsfilter in 100 ns Intervallen geschaltet. Die öffentliche Kommunikation findet in diesem Fall über das TCP/IP Netz statt.

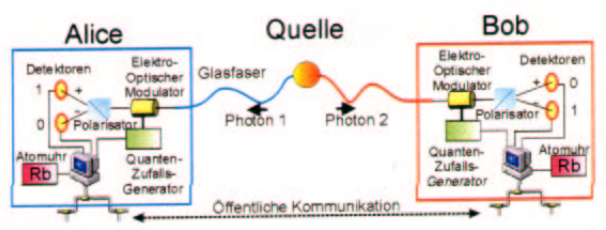


Abbildung 4: Schema des Insbrugger Versuchs, Bildquelle [4]

2. *Übertragung durch Luft*

Letzten Oktober wurde in einem Experiment einer Experimentalgruppe der LMU München eine Entfernung von 23.4 km zwischen der Zugspitze, von wo Alice sendet, zur Karwendelspitze mit Bob als Empfänger, eine Quantenkryptografiestrecke aufgebaut.

Die große Höhe der Berge[14], in der das Experiment bietet ruhige, klare und dünne Luft, die wenig Störungen und Rauschen verursacht. Außerdem ist in diesen abgeschiedenen Regionen das Streulicht der Zivilisation viel geringer, was bei Messungen mit nur wenigen Photonen unabdingbar ist.

Bei dem Versuch wurde das BB84-Protokoll benutzt, das dann Übertragungsraten von ca. 1-2 KBit/s ermöglichte.

Eine Quelle bei Alice, die vier verschiedene Polarisationen über vier Dioden produzieren kann, die über einen Zufallsgenerator ausgewählt werden sendet zu regelmäßigen Zeitmarken über ein Teleskop zu Bob. Dort wird ebenfalls über einen Zufallsgenerator ein Polarisationsanalysator angesteuert und entsprechend danach gemessen. Die ankommenden Signale werden mit den Zeit-

[14] 2950 bzw. 2244 m ü. NN

marken mit den entsprechend von Alice ausgesandten in Zusammenhang gebracht. Die öffentliche Kommunikation erfolgt über eine Telefonleitung.

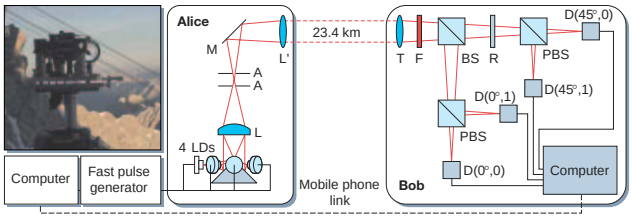


Abbildung 5: Versuchsaufbau des Quantenkryptografieexperiments der LMU München, Bildquelle [8]

C. Experimentelle Probleme

Um Quantenkryptografie wirklich in der Anwendung betreiben zu können, gilt es einige experimentelle aber auch theoretische Probleme zu lösen. Für manche gibt es schon Lösungsansätze oder sogar komplette Verfahren im Experiment, andere sind nachwievor vorhanden.

Zum einen basiert die Quantenkryptografie darauf, dass keine Kopie der Information gemacht werden kann. Dazu darf sich aber im Prinzip nur ein Teilchen, z.B. ein Photon, in dem zu übertragenden Zustand und in der Leitung befinden. Wären es mehrere, könnte man mit einem Strahlteiler eines davon abzweigen, und ohne entdeckt zu werden, ausmessen. Durch starke Abschwächung eines Laser kann so eine Ein-Photon-Quelle gebaut werden. Dadurch fällt aber auch die Übertragungsrate stark ab.

Desweiteren basieren die Verfahren darauf, dass keinerlei Regelmäßigkeit in der Auswahl der Messpolarisation vorliegt, d.h. es muss echt zufällig geschehen, um keinerlei Angriffe mit statistischen Methoden zuzulassen (siehe auch II A).

Störung durch Rauschen können über die genannten Verfahren herausgerechnet werden. Trotzdem benötigt man Medien mit möglichst geringer Fehlerrate, um nachwievor den Abhörer Eve sicher entdecken zu können.

Eines der größten Probleme ist, wie auch in der klassischen Kryptografie, die Authentifizierung der Gegenstelle. Es muss garantiert sein, dass Bob auch tatsächlich Bob ist, und sich nicht nur als dieser ausgibt, was die ganze Sicherheit zunichte macht. Genauso ist bei der EPR-Methode sicherzustellen, dass die Quelle auch tatsächlich verschränkte Teilchen aussendet und nicht in der Hand eines Dritten ist, der sie steuern kann.

VI. AUSBLICK

Die Quantenkryptografie funktioniert prinzipiell. Mit der Anwendung im Produktiveinsatz hapert es zwar noch, aber es gibt hier sogar schon kommerzielle Produkte. Für 70000 € kann man von der Firma “Id Quantique“ aus Genf eine Plug-n-Play Lösung erstehen. Mit dieser kann man über eine Entfernung von 67 km mit 1000 Bit/s über Glasfaser an einem Windowsrechner und USB Quantenkryptografie betreiben.

Abbildung 6: Kommerzielles Produkt von “Id Quantique“ ,Bildquelle: [9]

Um globale Kryptografie betreiben zu können, muss die Reichweite noch gesteigert werden, z.B. auf 200-600 km um Satelliten zu erreichen. Dazu ist aber zur Zeit noch ein wolkenloser Himmel notwendig. Außerdem ist die Übertragungsrate noch zu gering. Desweiteren taucht bei diesem globalen Schlüsselaustausch wieder das Problem der Authentifizierung der Gegenstelle und der Übertragungswege (z.B. Satellit), d.h. wer traut dem Satellit[15].

Im kleinen könnte man das ganze heute sicher schon anwenden, z.B. innerstädtisch als Verbindung zwischen Firmenzweigstellen oder Banken.

Contents

[15] dem Betreiber

---

[1] M.A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press 2000
[2] Jürgen Audretsch, *Verschränkte Welt*, WILEY-VCH 2002
[3] C.Cohen-Tannoudji, B. Diu, F. Laloë, *Quantenmechanik*, de Gruyter 1999
[4] T. Jennewein, G. Weihs, A. Zeilinger, *Schrödingers Geheimnisse*, c't 6/2001, Seite 260ff, Verlag Heinz Heise 2001
[5] http://www.cs.dartmouth.edu/-henle/Quantum/cgi-bin/Q3e.cgi
[6] Christian Kurtsiefer *Experimentelle Quantenkryptografie*, PDF-Document
[7] http://www.arcs.ac.at/quanteninfo/docs/Seminar_Qu_Krypt_Bell
[8] http://scotty.quantum.physik.uni-muenchen.de/publ/419450a_r.pdf
[9] http://www.idquantique.com