Quantenkryptographie

Sebastian Kühn

Wintersemester 2006/2007

Zusammenfassung

Zunächst wird auf die Notwendigkeit der Quantenkryptographie eingegangen, dann das Prinzip der klassischen Kryptographie an Hand von zwei Beispielen (RSA - code und Vernams one - time - pad) erläutert. Des weiteren werden mehrere Protokolle der Quantenkryptographie, insbesondere das BB84 - Protokoll und die dazugehörigen Methoden der Fehlerkorrektur, besprochen. Im Anschluss daran wird gezeigt werden, dass das BB84 - Protokoll ein sicheres Protokoll ist. Zum Schluss wird noch auf die experimentelle Realisierung der Protokolle, sowie die dabei auftretenden Probleme eingegangen.

Inhaltsverzeichnis

1 Quantenkryptographie - Wozu?? 2

2 Allgemeines zur Kryptographie 3
2.1 Prinzip der Kryptographie . . . 3
2.2 asymmetrische Schlüssel . . . 3
2.3 symmetrische Schlüssel . . . 4
2.4 Authentifizierung . . . 4

3 Protokolle 5
3.1 BB84 - Protokoll . . . 5
3.2 Two - State - Protokoll . . . 5
3.3 Six - State - Protokoll . . . 6
3.4 EPR - Protokoll . . . 6

4 Fehlerkorrektur 7
4.1 Shannon's Coding Theorem . . . 7
4.2 Lineare Fehlerkorrektur . . . 7
4.3 Fehlerkorrektur nach Brassard und Salvail . . . 7
4.4 Privacy Amplification . . . 8

5 Sicherheit vor Lauschern 9
5.1 Sicherheitsbeweis für das BB84 - Protokoll . . . 9

6 Experimentelle Umsetzung 11

1 Quantenkryptographie - Wozu??

Durch die starke Verbreitung des Internets und der mobilen Kommunikation ist der Bedarf an Verschlüsselung und der daraus folgenden „sicheren“ Kommunikation stark gestiegen. Bereits die alten Griechen haben erste Verschlüsselungstechniken entwickelt, doch mit der Leitstungsfähigkeit heutiger Computer sind auch die Anforderungen an diese Techniken gestiegen, so dass auch heute noch nach immer neuen Wegen der Kryptographie gesucht wird. Da liegt es nahe sich die Frage zu stellen, ob man Quantenkryptographie betreiben kann. Doch wenn man beginnt sich mit Quantenkryptographie zu beschäftigen, stellt sich auch wieder direkt die Frage: Lässt sich diese tatsächlich zur Verschlüsselung von Daten nutzen oder ist sie „nur“ ein theoretisches Gedankenspiel, das - wenn auch sehr interessant - keinen praktischen Nutzen hat?
Die Antwort auf diese Frage ist eindeutig: Quantenkryptographie ist notwendig!
Denn der momentane kryptographische Standard basiert auf unbewiesenen Annahmen, nämlich hauptsächlich darauf, dass die Faktorisierung von Primzahlen ein Problem aus der Klasse der NP - Probleme ist. Da der Beweis dafür aber noch nicht geführt wurde, ist die klassische Kryptographie also potenziell unsicher. Die Quantenkrypthographie dagegen basiert auf physikalischen Gesetzen, insbesondere auf denen der Quantenmechanik. Die Quantenmechanik wird vor allem durch sogenannte Negativ - Regeln beschrieben, das heißt durch Dinge, die nicht getan werden dürfen, wie z.B.:

1. Impuls und Position eines Teilchens sind nicht gleichzeitig scharf messbar.
2. Die Polarisation kann nicht gleichzeitig in diagonaler und horizontal - vertikaler Basis gemessen werden.
3. An einem System kann nicht, ohne eine Störung auszuführen, gemessen werden.
4. Unbekannte Zustände können nicht dupliziert werden (No - Cloning - Theorem).

Dies kann man sich zu Nutze machen, indem man einen Teil der übertragenen Daten vergleicht, um zu sehen, ob jemand lauscht. Die Logik ist dann folgende: Ist das System des Empfängers ungestört, so wurde keine Messung ausgeführt. Dann kann aber auch niemand gelauscht haben!

2 Allgemeines zur Kryptographie

Bisher wurde lediglich motiviert, sich mit Quantenkryptographie zu beschäftigen. Doch nun werden zunächst einmal das Prinzip der Kryptographie sowie verschiedene Ideen zur Verschlüsselung aufgezeigt.

2.1 Prinzip der Kryptographie

Bei der Kryptographie kommt es darauf an, eine Nachricht vom Sender (im Folgenden Alice genannt) zum Empfänger (Bob) zu übertragen, ohne dass ein Lauscher (Eve) Informationen über die Nachricht erhält.

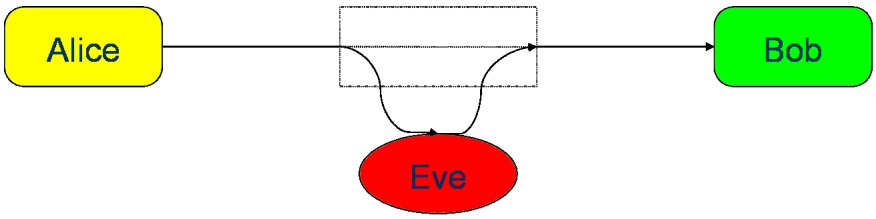

Abbildung 1:

Das Ziel ist es nun, einen effizienten Algorithmus zur Verschlüsselung der Nachricht zu entwickeln. Der Algorithmus kodiert (auf Alice´s Seite) mit Hilfe des sogenannten Schlüssels die Nachricht und liefert das Kryptogramm (die verschlüsselte Nachricht). Das Kryptogramm wird nun in einem Übertragungskanal von Alice an Bob versandt. Bob dekodiert diese nun mit Hilfe des Schlüssels und des Algorithmuses, um die ursprüngliche Nachricht zurückzuerhalten. Es besteht allerdings die Möglichkeit, dass Eve das Kryptogramm abfangen kann, da sie Zugriff auf den Übertragungskanal hat und somit je nach Güte der Verschlüsselung Informationen über die ursprüngliche Nachricht erhalten kann. Die Probleme der Kryptographie sind also eine möglichst gute Verschlüsselung der Nachricht zu erreichen und den Empfänger zu authentifizieren. Das heißt sicherzustellen, dass nicht Eve die gesamte Nachricht zugesandt wird anstatt Bob. Dazu verwendet man einen der folgenden Ansätze:

2.2 asymmetrische Schlüssel

Bei der Verschlüsselungsmethode haben Alice und Bob unterschiedlich viel Informationen über den Schlüssel (daher der Name). Eine erste Anwendung, die auch heute noch teilweise verwendet wird, ist der RSA - code, der 1978 von Ronald Rivest, Adi Shamir und Leonard Adleman entwickelt wurde. Am Beispiel dieses Codes wird hier dargestellt werden, wie das Prinzip eines asymmetrischen Schlüssels funktioniert. Die Idee ist, dass ein Teil des Schlüssels veröffentlicht wird (der sogenannte „public key“). Mit Hilfe des public keys verschlüsselt Alice nun die Nachricht und sendet Bob das Kryptogramm. Der Kanal, über den Alice dabei sendet darf öffentlich zugänglich sein, da nur Bob im Besitz des zweiten Teils des Schlüssels, dem „private key“ ist, der die Dekodierung des Kryptogramms ermöglicht. Dieses Verfahren ist vergleichbar mit der Versendung eines Briefes. Die Adresse des Empfängers (Bob) kann öffentlich zugänglich sein, aber den Schlüssel zum Briefkasten besitzt nur Bob, so dass kein anderer an den Brief herankommt. Dieser Vergleich hinkt etwas, da der Briefträger den Brief öffnen könnte, ohne dass Bob davon erfährt. Aber diese Möglichkeit ist bei dem oben beschriebenen Protokoll ausgeschlossen. Denn der private key besteht aus Primzahlen und der public key aus ihrem Produkt. Das heißt, dass die mathematische Operation zur Erstellung des public keys einfach ist. Aber die Umkehrung, also die Primzahlfaktorisierung, die zur Dekodierung benötigt wird, ist ein NP - Problem. Damit ist die Sicherheit für klassische Systeme gewährleistet. Doch 1994 hat Peter Shor einen Algorithmus entwickelt, der die Primzahlfaktorisierung auf

einem Quantencomputer in polynomieller Zeit durchführt. Daraus folgt also, dass diese Verschlüsselungsmethode nicht mehr sicher ist, sobald ein Quantencomputer realisiert wird. Deshalb betrachten wir jetzt noch symmetrische Schlüssel.

2.3 symmetrische Schlüssel

Bei der Methode der symmetrischen Schlüssel haben Sender und Empfänger je eine Kopie desselben Schlüssels. Bereits 1926 hat Gilbert Vernam für AT&T ein Protokoll entwickelt, das auf der Methode der symmtrischen Schlüssel basiert. Anhand dieses sogenannten „one - time - pads“ wird hier die prinzipielle Funktionsweise eines solchen Protokolls dargestellt werden. Das Kryptogramm wird dabei erzeugt, indem mit der XOR - Operation der binäre Schlüssel mit der ebenfalls in binärer Darstellung vorliegenden Nachricht verknüpft wird. Durch erneute Anwendung der XOR - Operation auf Schlüssel und Kryptogramm erhält man die Nachricht zurück. Im Jahr 1949 gelang es Shannon zu zeigen, dass diese Verschlüsselung sicher ist, wenn folgende Vorraussetzungen erfüllt sind:

1. Der Schlüssel ist absolut zufällig ausgewählt.
2. Der Schlüssel ist ebensolang wie der zu verschlüsselnde Text.
3. Der Schlüssel wird nur ein einziges Mal verwendet.

Der erste Punkt ist hierbei recht einfach zu erfüllen, aber schon der zweite Punkt bringt Schwierigkeiten mit sich. Das momentan am häufigsten verwendete Protokoll, das DES (Data Encryption Standard), dessen Grundlage das one - time - pad ist, verwendet lediglich einen 64 bit Schlüssel. Allerdings wird dabei durch Aufteilung des Textes in kleine Unterblöcke und Umsortierung dieser Unterblöcke mittels nichtlinearer Funktionen noch immer eine Sicherheit von mehr als 90 % erreicht. Das größte Problem des Protokolls verbirgt sich hinter dem dritten Punkt, denn der Sicherheitsverlust bei erneuter Anwendung desselben Schlüssels ist enorm. Das heißt, dass bei jeder Übertragung der Schlüssel neu erstellt werden muss.

2.4 Authentifizierung

Selbst wenn man davon ausgeht, dass ein perfekter Schlüssel zur Verfügung steht, bleibt immer noch das Problem der Authentifizierung. Das heißt, dass Alice sicherstellen muss, dass am Ende der Leitung wirklich Bob sitzt und nicht Eve. Dieses Problem, dass der Lauscher zwischen Alice und Bob sitet heißt „man - in - the - middle“ - Problem. Die Lösung dieses Problems stellt sowohl klassisch als auch quantenmechanisch ein Problem dar, denn die einzig bekannte sichere Methode ist, vor Beginn der Datenübertragung einen Authentifizierungsschlüssel zu übertragen. Dieser muss aber zuvor festgelegt werden sein, was also das Problem nicht löst sondern nur zeitlich verschiebt.
Trotzdem genügt uns die Feststellung, dass sich das Authentifizierungsproblem prinzipiell klassisch lösen lässt. Zusammen mit dem one - time - pad von Vernam sind dann auch alle Möglichkeiten gegeben, auf klassische Weise absolut sichere Kryptographie durchzuführen und es stellt sich erneut die Frage, wozu Quantenkryptographie noch benötigt wird?!
Doch dies kann man nun beantworten: Die Quantenkryptographie wird zur Schlüsselübertragung benötigt, denn diese ist klassisch nicht auf sichere Weise möglich. Nach der Etablierung des Schlüssel wird dann die eigentliche Nachricht klassisch übertragen.

3 Protokolle

Nachdem bisher festgestellt wurde, dass man die Quantenkryptographie „nur“ zur Etablierung eines hinreichend langen Schlüssels benötigt, werden im folgenden Kapitel nun einige Protokolle vorgestellt, die dies ermöglichen. In Kapitel 4 wird dann die Sicherheit der Protokolle bewiesen.

3.1 BB84 - Protokoll

Charles Bennett und Giles Brassard entwickelten 1984 ein Protokoll zur Schlüsselübertragung mittels Spin-$\frac{1}{2}$-Teilchen als qubits. Da dieses Protokoll bereits experimentelle Anwendungen hervorgebracht hat, wird es am ausführlichsten dargestellt werden. Das Protokoll benötigt **zwei** Übertragungskanäle, zum einen den Quantenkanal, zum anderen einen klassischen Kanal (z.B. Telefon oder LAN).

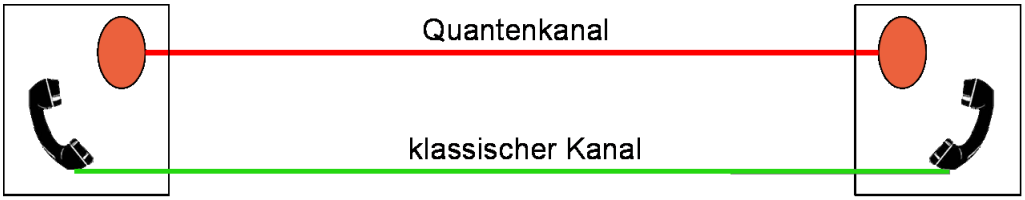

Abbildung 2:

Für die verwendeten Spin - $\frac{1}{2}$ - Teilchen sollen außerdem zwei verschiedene Messbasen zur Verfügung stehen. Alice wählt nun aus den vier möglichen Zuständen zufällig einen Zustand aus und sendet ihn an Bob. Dieser misst nun in einer ebenfalls zufällig ausgewählten Basis. Das Ergebnis seiner Messung ist der sogenannte „raw key“ mit einer Fehlerrate von 25%. Mit klassischen Methoden lässt sich diese Fehlerrate nicht verringern, doch nun lassen sich die quantenmechanischen Eigenschaften des Systems ausnutzen. Denn falls Bob in der Basis gemessen hat, in der Alice das qubit präpariert hat, dann sind die Ergebnisse perfekt korreliert. Andernfalls sind sie vollständig unkorreliert. Deshalb teilt Bob nach der Messung eines jeden qubit Alice über den klassischen Kanal mit, in welcher Basis er das jeweilige qubit gemessen hat. Alice sagt ihm daraufhin, welche qubits in der richtigen Basis gemessen wurden und welche in der falschen Basis. Die qubits, welche in der falschen Basis gemessen wurden, werden verworfen, die restlichen (sie bilden den „sifted key“) werden behalten. Um den endgültigen Schlüssel zu erhalten werden auf den sifted key klassische Fehlerkorrekturverfahren angewandt, die etwaige Übertragungsfehler beseitigen. Diese Korrekturverfahren werden in Kapitel 4 vorgestellt. Die Sicherheit des Protokolls wird durch das No - Cloning - Theorem gewährleistet, das Eve verbietet, den Zustand des qubits zu kopieren.

3.2 Two - State - Protokoll

Das Two - State - Protokoll funktioniert auf die gleiche Art und Weise wie das BB84 - Protokoll, verwendet aber zwei nicht orthogonale Zustände. Diese sind zwar nicht ohne Störung eindeutig unterscheidbar aber unter in Kaufnahme von Verlusten im Quantenkanal ist die Realisierung dennoch möglich. Zur Garantie des Sicherheit müssten Alice und Bob bei diesem Protokoll aber zusätzlich noch die Abschwächung im Quantenkanal überwachen, was nicht so genau möglich ist. Deshalb ist dieses Protokoll zu unsicher und dient nur als theoretischer Beweis dafür, dass bereits zwei unterschiedliche Zustände ausreichend sind, um Quantenkryptographie zu betreiben.

3.3 Six - State - Protokoll

Auch das Six - State - Protokoll verwendet dieselben Ideen wie das BB84 - Protokoll, benutzt aber drei Basen also sechs verschiedene Zustände. Damit respektiert es die Symmetrie des qubit - Zustandsraumes am besten. Allerdings ist es sehr ineffizient, da Alice und Bob nur noch in einem Drittel aller Fälle dieselbe Basis wählen anstatt wie im BB84 - Protokoll in der Hälfte der Fälle. Der Vorteil dieses Protokolls ist dafür aber die vereinfachte Sicherheitsanalyse. Denn um sicherzustellen, dass Eve nicht lauscht, ist nur noch ein qubit - error (QBER) von 33% notwendig (statt 50% beim BB84 - Protokoll).

3.4 EPR - Protokoll

Die Idee zum EPR - Protokoll stammt von Artur Ekert (Oxford, 1991), weshalb es auch Ekert Protokoll genannt wird, und basiert auf dem EPR - Paradoxon (1935). Bei diesem Protokoll sendet nicht Alice qubits an Bob, sondern eine verlässliche Quelle sendet gleichzeitig zwei maximal verschränkte qubits an Alice und Bob. Diese messen dann in einer zufälligen Basis und tauschen die Information über die Messbasis öffentlich aus. Dabei entstehen genug Daten (das sind die, die verworfen werden, da sie in unterschiedlichen Basen gemessen wurden), um die Bell - Ungleichung zu testen. Ist die Bell - Ungleichung verletzt, lag wirklich ein maximal verschränktes qubit - Paar vor und es kann keinen Lauscher gegeben haben. Allerdings ist noch nicht endgültig bewiesen, dass die Verletzung der Bell - Ungleichung wirklich zur Sicherheit des Protokolls führt.

4 Fehlerkorrektur

4.1 Shannon's Coding Theorem

Bei der Übertragung von qubits können immer Fehler entstehen, das heißt, dass Alice und Bob verschiedene Werte erhalten, obwohl sie in der gleichen Basis gemessen haben. Diese Fehler lassen sich physikalisch nicht vermeiden und auch mit Hilfe der Quantenmechanik nicht beheben. Deshalb muss man auf klassische Methoden zurückgreifen, die nun vorgestellt werden.
Sei ϵ die Wahrscheinlichkeit für einen Übertragungsfehler, dann lässt sich die Anzahl der bits abschätzen, die ausgetauscht werden müssen, um alle Fehler zu korrigieren. Diese bits, welche verglichen werden, können dann aber nicht mehr für den eigentlichen Schlüssel verwendet werden und müssen verworfen werden. Da man aber einen möglichst langen Schlüssel erhalten möchte, versucht man die Zahl der zu vergleichenden bits klein zu halten. Nun liefert das aus der Informationstechnologie bekannte Coding Theorem von Shannon eine Abschätzung der minimal auszutauschenden bits r in Abhängigkeit der Gesamtzahl der bits n und der Fehlerwahrscheinlichkeit ϵ :

$$r = n(-\epsilon\, log_2(\epsilon) - (1-\epsilon) log_2(1-\epsilon))$$

Der Beweis dieses Theorems ist leider nicht konstruktiv, weshalb bis jetzt noch kein Algorithmus gefunden wurde, der diese Schranke erreicht. Deshalb betrachten wir zunächst ein einfaches aber ineffizientes Verfahren und dann seine Verbesserung von Brassard und Salvail.

4.2 Lineare Fehlerkorrektur

Die lineare Fehlerkorrektur ist der einfachste Ansatz einen perfekten Schlüssel zu destillieren. Alice wählt hierbei zufällig bit - Paare aus und berechnet deren XOR - Wert. Diesen und um welche bits es sich handelt teilt sie Bob über den öffentlichen Kanal mit. Bob berechnet nun ebenfalls den XOR - Wert seines entsprechenden bit - Paares. Stimmen beide XOR - Werte überein so ersetzen Alice und Bob das erste der beiden bits durch den XOR - Wert und verwerfen das zweite bit, andernfalls werden beide bits verworfen. Man erhält als Ergebnis schließlich einen gekürzten, fehlerfreien Schlüssel.

4.3 Fehlerkorrektur nach Brassard und Salvail

Da die lineare Fehlerkorrektur sehr ineffizient ist, werden immer wieder andere Ansätze vorgestellt, die weniger bits verwerfen. Die Methode, die dabei der Untergrenze aus Shannon's Coding Theorem am nächsten kommt, ist die Fehlerkorrektur nach Brassard und Salvail. Hierbei werden die bits in Blöcke sortiert, von welchen Alice und Bob die Parität bestimmen. Ist sie ungleich, so enthält der betrachtete Block eine ungerade Anzahl Fehler und wird in Unterblöcke aufgeteilt. Dieses Verfahren wird dann rekursiv auf die Unterblöcke angewendet bis nur noch ein einzelner bit verglichen wird. Dieser kann dann direkt verglichen werden. Nach einem einzelnen Durchlauf sind alle Blöcke entweder fehlerfrei oder enthalten eine gerade Anzahl Fehler. Für einen neuen Durchlauf werden die bits umsortiert und größere Blöcke gebildet, auf die das Verfahren angewendet wird. Nach einer hinreichend großen Anzahl an Durchläufen ist der Schlüssel korrekt und dies, ohne ein einziges bit verworfen zu haben!
Das Problem dieser Methode ist, dass der Abgleich der Parität über einen öffentlichen Kanal erfolgt. Eve erhält also während des Reinigungsprozesses Informationen über den Schlüssel. Um diese Informationen wieder zu reduzieren, muss deshalb im Anschluss an die Fehlerkorrektur noch die sogenannte Privacy Amplification durchgeführt werden.

4.4 Privacy Amplification

Die einzige Möglichkeit, Eves Information über den Schlüssel zu verringern, ist den Schlüssel geschickt zu verkleinern. Dies wird bei der Privacy Amplification durch ein ähnliches Verfahren wie der linearen Fehlerkorrektur gewährleistet. Alice wählt nämlich auch hier zufällig ein bit - Paar aus und berechnet den XOR - Wert. Allerdings teilt sie Bob diesmal **nicht** den XOR - Wert mit, sondern nur welche bits sie zur Berechnung verwendet hat. Da Alice und Bob einen identischen Schlüssel besitzen, erhält Bob bei der Berechnung des XOR - Wertes seines bit - Paares den selben Wert wie Alice. Nun ersetzen beide das erste der beiden bits durch den XOR - Wert. Wenn das Verfahren hinreichend lange durchgeführt wird, hat Eve keine Information mehr über den Schlüssel. Das heißt, Alice und Bob haben sich einen gekürzten, fehlerfreien und geheimen Schlüssel erschaffen, den sogenannten „secret key“.

5 Sicherheit vor Lauschern

In den beiden vorangegangenen Kapiteln wurden Protokolle und Methoden zur Fehlerkorrektur vorgestellt. Nun bleibt noch die Frage zu klären, inwieweit diese Verfahren sicher sind gegen einen Angriff (eine sogenannte Attacke) von außen. Bemühen wir dazu noch einmal das Bild aus Kapitel 2 (Abb. 1) und und beweisen, dass Eve auf keinen Fall Informationen erhalten kann.
Zur Erleichterung der Beweisarbeit klassifiziert man die Attacken wie folgt:

1. inkohärente Attacke: Eve untersucht jedes gesendete qubit einzeln und nacheinander (z.B. mit der „receive and resend“ - Strategie)

2. kohärente Attacke: Eve kann mehrere qubits gleichzeitig untersuchen. In diesem Fall kann sie ihre Untersuchung erst nach Ende des Protokolls durchführen.

3. kollektive Attacke: Dies ist eine Zwischenklasse. Eve führt hier nur eine Untersuchung pro qubit durch, kann aber mehrere Untersuchungen gleichzeitig ausführen.

Im Folgenden wird nur die Sicherheit des BB84 - Protokolls gegenüber kohärenten Attacken beweisen, da dieses das Protokoll ist, welches der technischen Realisierung am Nächsten ist.

5.1 Sicherheitsbeweis für das BB84 - Protokoll

In diesem Beweis werden keine Vorraussetzungen an den Kanal gestellt. Das heißt, dass der Kanal verrauscht sein kann, was den Sicherheitsbeweis nicht mehr trivial macht. Denn nun können Fehler in der Übertragung nicht nur Eve angelastet werden, sondern sind unter Umständen durch Rauschen im Kanal entstanden.
Die generelle Beweisidee beruht darauf, dass Alice, Bob und Eve irgendwann Messungen an ihren Quantensystemen durchführen müssen. Als Resultat ihrer Messungen erhalten sie klassische Zufallsvariablen α, β und ϵ mit einer gemeinsamen Wahrscheinlichkeitsverteilung $P(\alpha, \beta, \epsilon)$. Ein Theorem der klassischen Kryptographie (Csizár und Körner, 1978) liefert dann eine notwendige und hinreichende Bedingung für die Erstellung eines „secret keys“:

<u>Theorem 1</u>
Sei $P(\alpha, \beta, \epsilon)$ gegeben. Dann gilt:

$$\begin{gathered}\text{Erstellung eines „secret keys“ ist möglich}\\ \Longleftrightarrow I(\alpha,\beta) \geq I(\alpha,\epsilon) \text{ oder } I(\alpha,\beta) \geq I(\beta,\epsilon)\end{gathered}$$

mit $I(\alpha, \beta) = H(\alpha) - H(\alpha|\beta)$
wobei I die Shannon - Information und H die Shannon - Entropie darstellt.

Aus Theorem 1 folgt nun, dass Bob mehr Information über Alice´ bits haben muss als Eve. Fehlerkorrektur und Privacy Amplification können Einbahnkommunikation umgesetzt werden. Das heißt, dass Bob und Eve jeweils die gleiche Menge an Information erhalten und somit ihren Informationsunterschied δ behalten (Abb. 3 a und b). Nach der Privacy Amplification (Abb. 3 c) hat der Schlüssel noch seine ursprüngliche Länge, aber die enthaltene Information ist gesunken, da Bob alle bits, die ignoriert werden sollen, durch zufällige bits ersetzt hat. Entfernen dieser bits kürzt nun den Schlüssel auf die ursprüngliche Informationsdifferenz δ (Abb. 3 d). Bob hat nun alle Information und Eve keine.

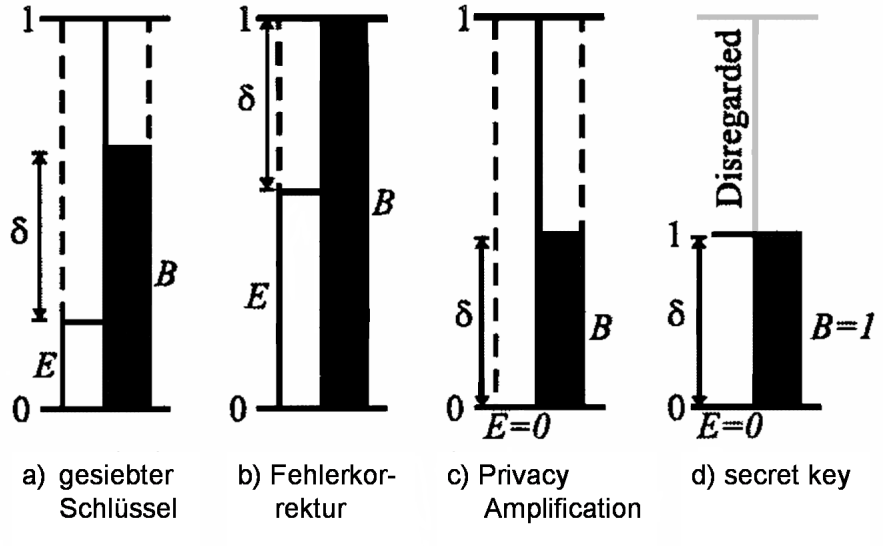

Abbildung 3:

Verwenden eines weiteren Theorems (Hall, 1995), welches die Heisenbergsche Unschärferelation in Termen der verfügbaren Information ausdrückt, liefert nun eine obere Schranke für die Bob und Eve zur Verfügung stehenden Information über Alice´ Schlüssel.

<u>Theorem 2</u>
Seien E, B Observable im N - dimensionalen Hilbertraum, ϵ, β sowie $|\epsilon>$, $|\beta>$ die zugehörigen Eigenwerte und Eigenvektoren und $c = max_{\epsilon,\beta}\{| < \epsilon|\beta > |\}$. Dann gilt:

$$I(\alpha, \beta) + I(\alpha, \epsilon) \leq 2log_2(Nc)$$

mit $I(\alpha, \beta) = H(\alpha) - H(\alpha|\beta)$

Sendet Alice nun n qubits, so ist die Dimension des zu betrachtenden Hilbertraums $N = 2^n$. Des weiteren lässt sich ohne Beschränkung der Allgemeinheit annehmen, dass Alice alle qubits in der x - Basis versendet. Damit ist Bobs Observable das n - fache Tensorprodukt $\sigma_x \otimes \ldots \otimes \sigma_x$. Aus Gründen der Symmetrie ist Eves maximale Information über die korrekten Basen die gleiche wie ihre maximale Information über die falschen. Folglich ist ihre Information beschränkt durch $c = 2^{\frac{n}{2}}$. Theorem 2 liefert nun:

$$I(\alpha, \beta) + I(\alpha, \epsilon) \leq 2log_2(2^n 2^{-\frac{n}{2}}) = n \tag{1}$$

Dieses Resultat ist intuitiv klar, da Bob und Eve zusammen nicht mehr Information erhalten können, als Eve versendet! Aus Theorem 1 folgt nun:

$$I(\alpha, \beta) + I(\alpha, \epsilon) \geq \frac{n}{2} \tag{2}$$

Mit $I(\alpha, \beta) = n[1 - D\, log_2(D) - (1 - D)\, log_2(1 - D)]$ erhält man eine hinreichende Bedingung die Fehlerrate D:

$$D\, log_2(D) + (1 - D)\, log_2(1 - D) \leq \frac{1}{2} \tag{3}$$

$$\Longrightarrow D \leq 11\% \tag{4}$$

Das heißt, dass das BB84 - Protokoll für einen QBER von kleiner als 11 % sicher ist!

6 Experimentelle Umsetzung

Es gibt verschiedene Möglichkeiten wie sich die abstrakten qubits experimentell realisieren lassen und die auch teilweise umgesetzt wurden.
Eine Möglichkeit die qubits darzustellen ist die Verwendung verschränkter Zustände, was dann das Ekert - Protokoll als zu bevorzugendes Protokoll nahelegt. Als verschränkte Zustände dienen hierbei Photonenpaare, welche beispielsweise in nicht - linearen Kristallen erzeugt werden können. Der Vorteil dieser Methode ist das gute Signal - Rausch - Verhältnis.
Eine andere Art qubits mit Photonen darzustellen, ist die Verwendung von polarisierten Photonen, welche sich dann auch für die Verwendung des ausführlich besprochenen BB84 - Protokolls eignen. Polarisierte Photonen können zum einen durch Photonengewehre zum anderen durch schwache Laserpulse erzeugt werden. Photonengewehre stellen die ideale Quelle dar, da sie genau ein Photon der gewünschten Polarisation emittieren. Allerdings sind sie für die praktische Anwendung nicht zu verwenden, da ihr Aufbau sehr kompliziert ist und das Vorhandensein von ultrakalten Atomen erfordert.
Verwendet man dagegen schwache Laserpulse ergibt sich als Hauptproblem, dass in jedem Puls genau ein Photon enthalten sein soll, da sonst die Sicherheit nicht garantiert werden kann. Nun ist aber die Photonenzahl pro Puls Poisson - verteilt, das heißt $P_\mu(k) = \frac{\mu^k}{k} e^{-\mu}$, wobei k die Anzahl der Photonen im Puls und μ die mittlere Photonenzahl ist. Daraus folgt, dass das Verhältnis der Wahrscheinlichkeit genau ein Photon ($P_\mu(1)$) und der mehr als ein Photon ($P_\mu(k \geq 2)$) im Puls zu erhalten, steigt je geringer die mittlere Photonenzahl μ ist, denn:

$$\frac{P_\mu(1)}{P_\mu(k \geq 2)} \approx \frac{1}{\mu} - 1$$

Das bedeutet, dass es für die technische Umsetzung umso günstiger ist, je kleiner die mittlere Photonenzahl ist. Aber es gilt außerdem $\frac{P_\mu(0)}{P_\mu(1)} = \frac{e^{-\mu}}{\mu e^{-\mu}} = \frac{1}{\mu}$, also steigt die Zahl der leeren Pulse, der sogenannten „dark counts“ ebenfalls mit sinkender mittlerer Photonenzahl (siehe Abb. 6.1), was zu einem schlechten Signal - Rausch - Verhältnis führt. Trotz dieses großen Nachteils werden meist schwache Laserpulse mit $\mu = 0,1$ zur Erzeugung der qubits verwendet.

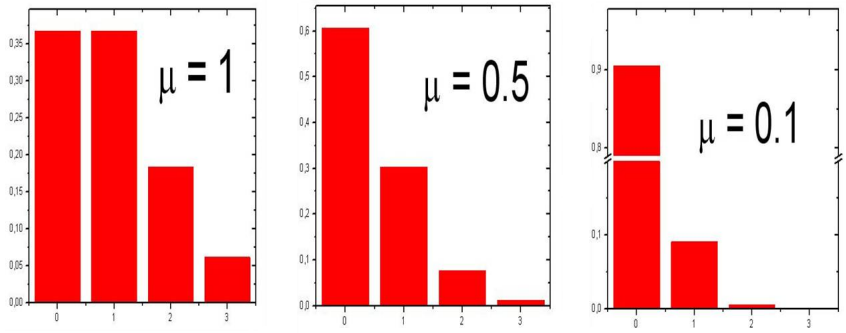

Abbildung 4: Poissonverteilung für verschiedene μ

Werden Photonen verschickt, so stellt sich immer die Frage, welche Wellenlänge zu verwenden ist. Da bieten sich zwei unterschiedliche Wellenlängenbereiche an:

1. $\lambda \approx 800\ nm$
   Zum einen sind in diesem Bereich Quellen und Detektoren vorhanden, zum anderen liegt in diesem Wellenlängenbereich ein Absorptionsminimum der Luft, weshalb sich dieser Wellenlängenbereich besonders

gut zur Satellitenkommunikation eignet, ihn aber für den Kabelbetrieb disqualifiziert, da sich nur spezielle Fasern bei 800 nm zur Leitung von Photonen eignen. Der Nachteil bei Versendung der Photonen durch den freien Raum ist, dass dies nur auf „Sicht“ geschehen kann, also stark wetterabhängig ist. In dem Experiment, in dem die bis jetzt größte Entfernung (23 km) überbrückt wurde, sendete man schwache Laserpulse von der Zugspitze zur westlichen Karwendelspitze. Dies ist im folgenden Bild dargestellt:

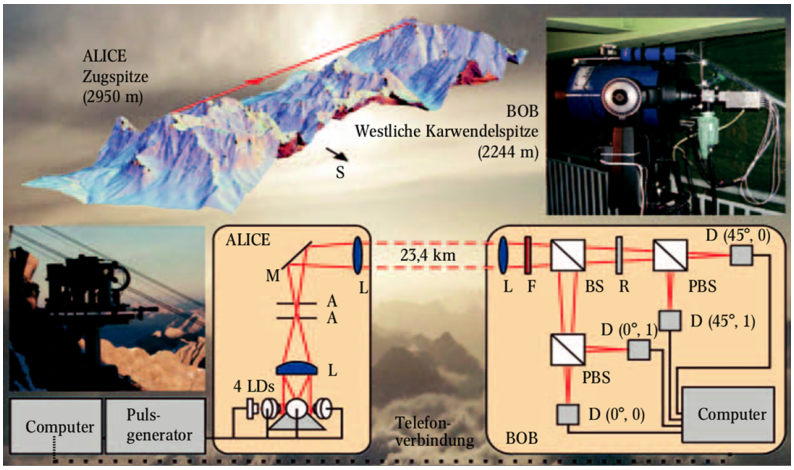

Abbildung 5:

2. $1300\ nm \leq \lambda \leq 1500\ nm$
   Diese Wellenlängen nennt man die Telekommunikationswellenlängen, da die Telekommunikationsunternehmen in diesem Bereich ihre Glasfasernetze betreiben. Die Übertragung durch diese Netze ist dann wetterunabhängig und bis auf effiziente Detektoren ist die Technik einsatzfähig. Die bisher längste Übertragung wurde an der Universität Genf über Leitungen der Schweizer Telekom durchgeführt:

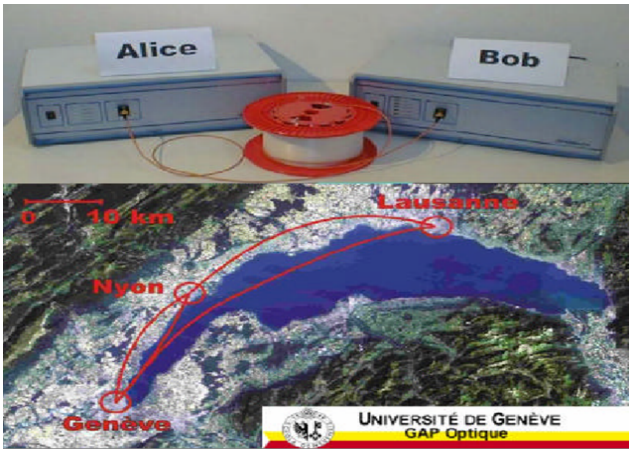

Abbildung 6:

Um die Übertragungslänge weiter zu erhöhen, müssen die Übertragungskanäle, beispielsweise durch Verwendung von Single - Mode - Fasern, weiter verbessert werden. Außerdem ist es notwendig Polarisationseffekte wie die geometrische Phase, Doppelbrechung und „polarization mode dispersion“ minimiert werden. Diese lassen sich unter anderem verringern, indem Bob das Photon aussendet, während Alice dieses mit Faraday - Spiegeln reflektiert und die Information auf das reflektierte Photon aufbringt.