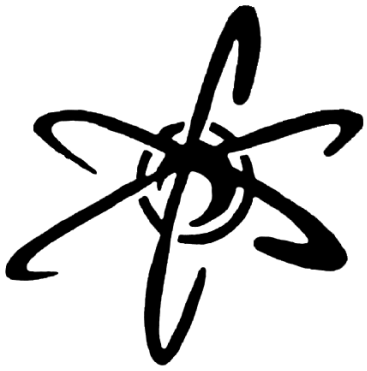

Quantenkryptographie

Marc Rochel

Juni 2002

Inhaltsverzeichnis

1 Einleitung

Heutzutage sind Verschlüsselungsverfahren nicht mehr aus der Welt der EDV wegzudenken. Schon lange Zeit ist es nötig, Daten vor eventuellen Dritten sicher zu verschicken. Denken wir an die Entwicklung des Internets im Bereich der Onlineshops oder des Onlinebankings. Bislang werden dort Verschlüsselungsverfahren eingesetzt, die die Sicherheit der Daten dadurch vermuten lassen, dass die Entschlüsselung, ohne den Schlüssel zu haben, auf klassischen Computern mit bisher bekannten Verfahren nicht in Polynomialzeit möglich ist. Ein bekanntes Beispiel hierfür ist der RSA Algorithmus. 1994 zeigte jedoch Peter Shor mit der Veröffentlichung eines Algorithmuses zur Primfaktorzerlegung und zur Lösung des Diskreten Logarithmuses, dass diese Verfahren nicht mehr sicher sind, sobald Quantencomputer mit entsprechenden Qubitanzahlen existieren. Somit raubt uns die Rechenleistung der Quantencomputer der bisher vermuteten Datensicherheit, jedoch können die Eigenschaften der Quantencomputer auch benutzt werden, um wiederum sicherere Verschlüsselungsverfahren zu entwickeln. Darüber hinaus werden wir sehen, dass die vorgestellten Verfahren zur Quantenkryptographie nicht nur vermutlich sicher sind, wie bisher klassische Verfahren, sondern es wird bewiesen, dass sich selbst mit Hilfe von Quantencomputern die Verschlüsselung nicht überwinden lässt.

Im weiteren Verlauf des Textes werden zunächst in den übrigen Abschnitten der Einleitung Begriffe vereinbart die im folgenden Verwendung finden und die Grundidee der hier behandelten Quantenkryptographieverfahren vorgestellt. In Abschnitt 2 werden drei Quantenkryptographieprotokolle beschrieben. Anschließend wird in Abschnitt 3 Information Reconciliation und Privacy Amplification vorgestellt. Dies sind Verfahren aus der klassischen Kryptographie, die Bestandteil der zuvor präsentierten Quantenkryptographieprotokolle sind. In Abschnitt 4 wird die Sicherheit der Verfahren untersucht und in Abschnitt 5 ein experimenteller Aufbau der Verfahren gezeigt.

1.1 Begriffsdefinitionen

Um eine einfachere Ausdrucksweise zu erzielen, werden für gewöhnlich in Texten über Kryptographie folgende Vereinbarungen getroffen: Mit Alice (A) wird diejenige Person bezeichnet, die eine Nachricht sicher an eine andere Person, diese wird Bob (B) genannt, senden möchte. Ein potentieller Angreifer der die Nachricht entschlüsseln möchte, wird Eve (evedropper) genannt.

1.2 Symmetrische und asymmetrische Verschlüsselungsverfahren

Die heutzutage größtenteils Verwendung findenden Verschlüsselungsverfahren, wie z.B. das RSA Verfahren, verfolgen die Idee, dass Bob zunächst zwei Schlüssel generiert. Einen hält er geheim, dies ist sein privater Schlüssel, den anderen gibt er öffentlich bekannt, sein öffentlicher Schlüssel. Möchte Alice eine Nachricht schicken, verschlüsselt sie sie mittels Bobs öffentlichem Schlüssel. Diese verschlüsselte Nachricht schickt Alice dann über einen offenen Kanal zu Bob, der sie mit seinem privaten Schlüssel entschlüsselt. Die Verschlüsselung ist derart, dass die verschlüsselte Nachricht nicht wieder mit dem öffentlichen Schlüssel entschlüsselt werden kann, zumindest nicht schnell genug, nach heute bekannten Methoden, damit es für Eve noch interessant ist.

Mit der Existenz eines Quantencomputers werden die hierzu bekannten Verfahren jedoch unsicher. Allerdings existieren noch ältere Kryptographieverfahren im Bereich der symmetrischen Verschlüsselungsverfahren, die sich nicht durch Steigerung der Rechenleistung brechen lassen, jedoch eine andere Sicherheitslücke besitzen, die sich mittels Eigenschaften von Quantentheorie schließen lassen.

Zu Beginn der Anwendung von Verschlüsselungsverfahren, lange Zeit vor der Erfindung von Computern, wurden zunächst symmetrische Verschlüsselungsverfahren eingesetzt. Diese beruhen auf der Idee, dass Alice und Bob einen gemeinsamen Schlüssel besitzen, den außer ihnen niemand kennt. Möchte nun Alice Bob eine Nachricht zukommen lassen, verschlüsselt sie diese mit dem geheimen Schlüssel und schickt sie über einen offenen Kanal zu Bob. Daraufhin kann Bob die Nachricht mit dem Schlüssel wieder entschlüsseln. Eve könnte unterwegs am offenen Kanal mithören, jedoch ohne den Schlüssel die Nachricht nicht entschlüsseln. Da der Schlüssel nicht öffentlich bekannt ist, wird er auch als privater Schlüssel bezeichnet. Ein bekanntes Verfahren hierzu ist das folgende: Alice und Bob besitzen einen privaten Schlüssel S. Alice möchte eine Nachricht M schicken. Alice schickt

$$M' := (M \text{ xor } S) \tag{1}$$

an Bob. Daraufhin berechnet sich Bob

$$M' \text{ xor } S = (M \text{ xor } S) \text{ xor } S = M \tag{2}$$

und erhält somit die ursprüngliche Nachricht. Es kann gezeigt werden: Ist der Schlüssel S so lang wie die Nachricht M, so ist das Verfahren sicher. Das heißt Eve hat keine Möglichkeit an M zu kommen durch die Kenntnis von M'. Allerdings ist damit das Verschlüsselungsproblem noch nicht gelöst. Wie bekommen Alice und Bob einen privaten Schlüssel S, ohne dass Eve S kennen lernt?

Klassisch ist dieses Problem nicht lösbar, denn um eine Nachricht sicher zu verschicken, muss eine andere Nachricht derselben Länge sicher verschickt werden, bzw. zwischen Alice und Bob genauso viel Information ausgetauscht werden wie die Nachricht enthält. Man steht vor demselben Problem wie zuvor.

Quantenkryptographie löst dieses Problem. Sie erzeugt einen privaten Schlüssel den Alice und Bob kennen aber Eve nicht. Das restliche Verfahren, die Verschlüsselung und die Versendung der verschlüsselten Nachricht und die Entschlüsselung geschieht klassisch. Im folgenden Abschnitt werden nun Verfahren zur Schlüsselgenerierung beschrieben.

2 Quantenschlüsselgenerierung (Quantum key distribution)

Die hier vorgestellten Quantenschlüsselgenerierungsverfahren (Quantum key distribution, QKD) sind beweisbar sicher. Voraussetzung für die Anwendung der Verfahren ist ein offener Quantenkanal mit einer Fehlerrate unterhalb einer vorgegebenen Schranke.

Eine grundlegende Erkenntnis für die QKD ist folgende Behauptung:

Behauptung: Informationsgewinn impliziert Störungen

Jeder Versuch ein Quantensystem zwischen zwei verschiedenen nicht orthogonal zueinander liegenden Zuständen zu unterscheiden, verändert den Zustand des Quantensystems.

Beweis: Angenommen $|\psi>$ und $|\varphi>$ seien zwei verschiedene nicht orthogonal zueinander liegende Quantenzustände. Ohne Beschränkung der Allgemeinheit kann Eves Versuch ein Quantensystem zwischen diesen beiden Zuständen zu unterscheiden wie folgt modelliert werden: Eve erweitert das Quantensystems um zusätzliche Qubits und wendet Quantenoperationen auf dieses komplette Quantensystem an und versucht, anhand seiner hinzugefügten Qubits anschließend Information über den Zustand des ursprünglichen Quantensystems zu erlangen. Da Eve keine Störung verursachen will, muss für die Quantenoperation folgendes gelten:

$$\begin{aligned} |\psi>|u> &\rightarrow |\psi>|v> \\ |\varphi>|u> &\rightarrow |\varphi>|v> \end{aligned} \qquad (2)$$

wobei $|u>$ den Zustand der zusätzlich von Eve hinzugefügten Qubits entspricht. Eve möchte, dass $|v>$ und $|v'>$ verschieden sind, damit sie durch sie zwischen $|\psi>$ und $|\varphi>$ unterscheiden kann.

Jedoch gilt für unitäre Operatoren im Hilbertraum ([3], Definition 3):

$$\forall U \in L(H).\forall x, y \in H. \quad (Ux, Uy) = (x, y) \tag{3}$$

Folglich muss gelten, da Eves Quantenoperator unitär ist:

$$(|\psi>|u>,|\varphi>|u>) = (|\psi>|v>,|\varphi>|v'>) \tag{4}$$

Nach der Definition des Skalarproduktes ([3], Seite 13) gilt also:

$$<\psi|\varphi><u|u>=<v|v'><\psi|\varphi> \tag{5}$$
$$\Leftrightarrow \quad <u|u>=<v|v'> \tag{6}$$
$$\Leftrightarrow \quad 1=<v|v'> \tag{7}$$
$$\Leftrightarrow \quad |v>=|v'> \tag{8}$$

Folglich kann Eve durch ihre zusätzlichen Qubits den Zustand des Quantensystems nicht zwischen $|\psi>$ und $|\varphi>$ unterscheiden ohne ihn zu verändern.

qed.

2.1 Das BB84 Protokoll

Alice erzeugt zufällig zwei Bitstrings a und b der Länge $(4+\delta)n$ (diese Länge wird später noch wichtig wenn die Sicherheit der QKD behandelt wird) und codiert die einzelnen Bits von a in Qubits, wobei sie anhand von b_k entscheidet, in welcher Basis, entweder X={|0>,|1>} oder Z={(|0>+|1>)/$\sqrt{2}$, (|0>-|1>)/$\sqrt{2}$}, sie a_k kodiert. Formal erhält sie folgenden Zustand $|\psi>$:

$$|\psi> = \bigotimes_{k=1}^{(4+\delta)n} |\psi_{a_k b_k}> \tag{9}$$

wobei a_k das Bit an Stelle k von String a ist, b analog, und

$$
\begin{aligned}
|\psi_{00}> &= |0> \\
|\psi_{10}> &= |1> \\
|\psi_{01}> &= |+> = \frac{(|0> + |1>)}{\sqrt{2}} \\
|\psi_{11}> &= |-> = \frac{(|0> - |1>)}{\sqrt{2}}
\end{aligned}
\tag{10}
$$

Diesen Zustand schickt Alice nun an Bob. Zu bemerken ist, da X und Z nicht orthogonal zueinander sind, Eve nicht mit Sicherheit Kenntnis über den Zustand $|\psi>$ erhalten kann, ohne $|\psi>$ zu verändern. Aufgrund Eves Störungen und des nicht unbedingt fehlerfreien Kanals erhält Bob $\rho = \mathcal{E}(|\psi><\psi|)$. Nun erzeugt auch Bob zufällig einen String b' der Länge $(4+\delta)n$ und entscheidet, analog zu Alice, anhand des k-ten Bits von b', ob er das k-te erhaltene Qubit in X oder Z misst und erhält einen gemessenen String a'. Anschließend veröffentlicht Alice b. Alice und Bob verwerfen alle Bits in a_k bzw. a_k', bei denen $b_k \neq b_k$'. Bis auf die Bits, bei denen durch $\mathcal{E}$ $|\psi>$ verändert wurde, gilt nun a=a'. Das δ kann so gewählt werden dass mit beliebig hoher Wahrscheinlichkeit 2n Bits übrig bleiben.

Alice und Bob können nun untersuchen wie stark der Einfluss von $\mathcal{E}$ war, also wie fehlerhaft der Kanal und wie stark von Eve mitgehört wurde. Dazu vergleichen sie zum Beispiel die Hälfte der Bits von a bzw. a' öffentlich miteinander. Je mehr Bits verschieden sind, desto höher war der Einfluss von $\mathcal{E}$. Übersteigt die Anzahl der unterschiedlichen Bits einen bestimmte Schwelle t, so können Alice und Bob das Protokoll von vorne beginnen. Diese Schwelle t ist so gewählt, dass Alice und Bob durch Information Reconciliation and Privacy Amplification anschließend m geheime Bits erzeugen können. Dies wird getrennt in Abschnitt 3 behandelt.

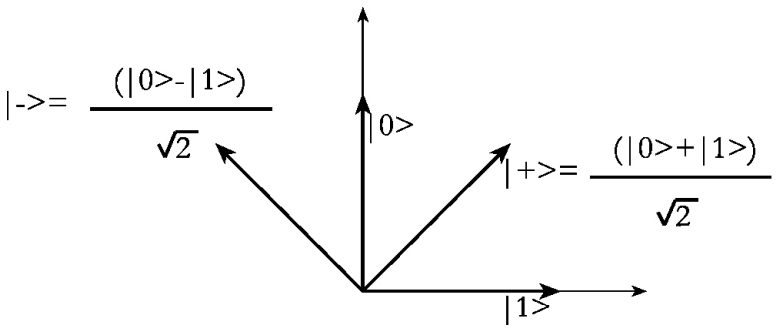

Abbildung 1: Die vier möglichen Zustände der zu sendenden Qubits, bzw. die beiden Basen in denen Bob misst.

2.2 Das B92 Protokoll

Alice erzeugt zufällig einen String a der Länge n. Diesen String kodiert sie wie folgt in Qubits:

$$|\psi>=\bigotimes_{k=1}^{n}|\psi_{a_k}> \tag{11}$$

wobei

$$\begin{aligned}|\psi_0>&=|0>\\ |\psi_1>&=|+>=\frac{(|0>+|1>)}{\sqrt{2}}\end{aligned} \tag{12}$$

Daraufhin schickt Alice $|\psi>$ zu Bob. Bob seinerseits erzeugt sich einen zufälligen String a' der Länge n und entscheidet mit dessen Hilfe, ob er das k-te Qubit in X oder in Z misst und erhält so als Messergebnis einen String b. Im Gegensatz zu BB84 veröffentlicht Bob nun seine Messung b anstatt seinen Messbasenstring a'. Alice und Bob verwerfen nun all diejenigen Bits aus a_k bzw. a_k', bei denen $b_k \neq 1$. Der erzeugte gemeinsame String ist dann für Alice a und für Bob (not a').

Das dadurch zwei gleiche Strings entstehen wird deutlich wenn man alle möglichen Kombinationen durchdenkt, wie es Tabelle 1 zeigt. Wenn $b_k=1$ so gilt a_k=not b_k. Aus der Tabelle lässt sich auch ermitteln, dass der Erwartungswert für die Anzahl der Bits des zum Schluss erhaltenen Schlüssels a gleich n/4 ist.

Alices Bit a_k	Bobs Bit a_k'	Bobs Messung b_k
0	0	0
0	1	0 mit Wahrscheinlichkeit 0.5 1 mit Wahrscheinlichkeit 0.5
1	0	0 mit Wahrscheinlichkeit 0.5 1 mit Wahrscheinlichkeit 0.5
1	1	0

Tabelle 1: Möglichkeiten für Bobs Messung b in Abhängigkeit von den zufällig erzeugten Strings a und a'.

Hierbei wurde jetzt der Einfachheit halber außer acht gelassen, dass die Übertragung von $|\psi>$ unter dem Einfluss von $\mathcal{E}$ steht. Dies ist analog wie beim BB84 Protokoll zu berücksichtigen. Anschließend können sich Alice und

Bob mittels Information Reconciliation and Privacy Amplification einen gemeinsamen geheimen Schlüssel erzeugen.

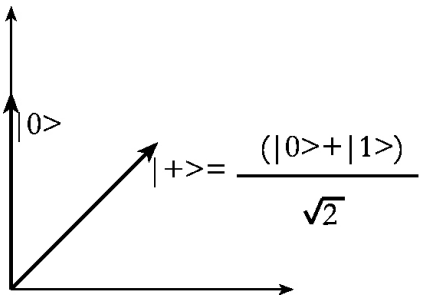

Abbildung 2: Die beiden möglichen Zustände der zu senden Qubits

2.3 Das EPR Protokoll

Ein EPR Paar sind zwei Qubits in folgendem Zustand:

$$\frac{|00>+|11>}{\sqrt{2}} \tag{13}$$

Voraussetzung für dieses Protokoll ist, dass sich Alice und Bob EPR Paare teilen, also Alice je ein Qubit des Paares besitzt und Bob das andere. Dies kann zum Beispiel dadurch erreicht werden, dass Alice und Bob sich vor einiger Zeit getroffen und die EPR Paare erzeugt und geteilt haben. Um nun einen privaten Schlüssel zu erzeugen, mist Alice ihre Qubits und erhält einen String a. Anschließend gibt sie dies öffentlich bekannt, woraufhin Bob seine Qubits mist und einen String a' erhält. Durch die Verschränkung der beiden Qubits eines EPR Paares ist der Zustand von Bobs Qubit gleich dem von Alices und damit die Ergebnisse der Messungen gleich, also a=a', siehe Tabelle 2.

Zustand des EPR Paares vor der Messung	Alices Messung ihres Bits	Zustand des Qubit Paares nach Alices Messung
$\frac{\|00>+\|11>}{\sqrt{2}}$	0	$\|00>$
	1	$\|11>$

Tabelle 2: Verschränkung des EPR Paares. Alices Messung ihres Qubits entspricht einer Messung des gesamten 2 Qubit Systems mit $M_0=|00><00|+|01><01|$ und $M_1=|10><10|+|11><11|$, angenommen Alices Qubit sei das erste.

Da keinerlei Information über den Schlüssel ausgetauscht wurde, konnte Eve nichts über ihn lernen.

3 Information Reconciliation & Privacy Amplification

3.1 Information Reconciliation

Angenommen Alice besitzt einen String X und Bob einen String Y und X und Y seien korreliert. Zusätzlich sei die gemeinsame Information Eves bezüglich X und Y nach oben beschränkt. Dies entspricht der Situation in den zuvor beschriebenen QKD-Protokollen vor der Anwendung der Information Reconciliation und Privacy Amplification.

Information Reconciliation ist eine Fehlerkorrektur, die aus X und Y einen String W erzeugt, den Alice und Bob besitzen. Eine zusätzliche Bedingung ist, dass Eve so wenig wie möglich durch diese Fehlerkorrektur über W erfahren soll.

3.2 Privacy Amplification

Sei Z als Zufallsvariable der String den Eve gewinnt nachdem Alice und Bob ihren String W durch Information Reconciliation erzeugt haben. Z ist dann korreliert mit W. Das Ziel der Privacy Amplification ist nun, diese Korrelation zu minimieren.

Eine Möglichkeit der Privacy Amplification benutzt die Klasse der universalen Hashfunktionen G. Diese Klasse ist wie folgt definiert:

Definition: Klasse der universalen Hashfunktionen G

Sei A eine Menge von n-Bit Strings, B eine Menge von m-Bit Strings. G enthält Funktionen, die von A nach B abbilden. Ferner gilt für G, dass für verschiedene a_1, $a_2 \in A$ und für ein $g \in G$ dass zufällig gewählt wird, die Wahrscheinlichkeit, dass $g(a_1)=g(a_2)$, höchstens $1/|B|$ ist. Formal bedeutet dies:

$$\forall a_1, a_2 \in A \wedge a_1 \neq a_2 .\ \mu\{G(a_1) = G(a_2)\} \leq \frac{1}{|B|} \tag{14}$$

wobei $\Omega = G$ und $\sum = P(G)$.

Die Durchführung der Privacy Amplification ist nicht mehr, als dass Alice und Bob sich öffentlich eine Funktion aus G aussuchen und sie auf W anwenden und S=G(W) erhalten.

Um zu zeigen, dass dies die Korrelation zwischen S und Z minimiert, benutzen wir die Collision Entropy:

Definition: Collision Entropy

Die Collision Entropy einer Zufallsvariable X mit Wahrscheinlichkeitsverteilung p ist definiert als

$$H_c(X) = -\log\left(\sum_x p(x)^2\right) \tag{15}$$

Da der Logarithmus konkav ist, gilt

$$H(X) \geq H_c(X) \tag{16}$$

Die Collision Entropy findet Verwendung in folgendem Theorem, dass an dieser Stelle nicht bewiesen wird:

Theorem 1: Sei X eine Zufallsvariable auf dem Alphabet *X'* mit Wahrscheinlichkeitsverteilung p und Collision Entropy $H_c(X)$. Sei G die gleichverteilte Zufallsvariable die für die zufällige Wahl eines Elements aus der Klasse der universalen Hashfunktionen die von *X* nach $\{0, 1\}^m$ abbilden, verantwortlich ist. Dann gilt

$$H(G(X)\,|\,G) \geq H_c(G(X)\,|\,G) \geq m - 2^{m-H_c(X)} \tag{17}$$

Dieses Theorem lässt sich verwenden, um eine Aussage über die Information zu erhalten, die Eve bezüglich S nicht kennt. Vorausgesetzt, das das Wissen, dass man durch Erfahren von W unter der Bedingung dass man eine Realisierung von Z, also Z=z, kennt, bekommt sei nach unten beschränkt. Also

$$H_c(W\,|\,Z=z) \geq d \tag{18}$$

Die entspricht genau Eves Unwissenheit über W, wenn Z=z. Nach Theorem 1 mit W=X und S=G(W) und der Tatsache dass die Entropie mit der Anzahl der Bits beschränkt ist gilt:

$$m \geq H_c(S\,|\,G,Z=z) \geq m - 2^{m-d} \tag{19}$$

Das heißt, die Information, die Eve durch Erfahren von S bekommen würde, bzw. Eves Unwissen über W, kann durch geeignete Wahl von G ungefähr gleich m werden, was der maximalen Entropie von einem m-Bit String entspricht. Eves Wissen über S sinkt damit auf fast 0. Anschaulich kann man sich das auch so vorstellen: Vor der Anwendung einer Hashfunktion g aus G besitzt Eve Wissen über W. Sie kennt also eine Menge Z' von Kandidaten,

die nach ihrem Wissen W sein könnten. Durch die Anwendung von g wird jedoch die Länge von W reduziert, am besten für Alice und Bob derart, dass die Kardinalität des Wertebereichs von g kleiner gleich der Kardinalität von Z' ist. Dadurch geht Eve das Wissen das sie bisher über W besaß gänzlich verloren, da g(Z') sehr wahrscheinlich der gesamte Wertebereich von g ist. Somit ist S ein sicherer geheimer privater Schlüssel.

Die bisherige Betrachtung ist nicht ganz vollständig. Durch Information Reconciliation erfährt Eve zusätzliche Information über W. Angenommen Alice schickt Bob eine zusätzliche Nachricht u über einen offenen Kanal die es Bob erlaubt seinen String Y zu einem W zu korrigieren. Für die Entropie dieser Nachricht, bzw. die Länge in Bits, k gilt dann

$$k > H(W \mid Y) \tag{20}$$

Die Nachricht u bekommt Eve auch mit, wodurch ihre Collision Entropy von W zu $H_c(W \mid Z = z, U = u)$ verringert wird. Betrachten wir dazu ein weiteres Theorem:

Theorem 2: Seien X und U Zufallsvariablen über den Alphabeten *X'* und *U'*. p(x) sei die Wahrscheinlichkeitsverteilung von X und p(x, u) die gemeinsame Verteilung von U und X. Sei s>0 beliebig. Dann nimmt U mit einer Wahrscheinlichkeit von mindestens $1-2^{-s}$ einen Wert u an, für den gilt

$$H_c(X \mid U = u) \geq H_c(X) - 2\log_2 |U'| - 2s \tag{21}$$

Damit ergibt sich

$$H_c(W \mid Z = z, U = u) \geq H_c(W \mid Z = z) - 2\log_2 |U'| - 2s \geq d - 2(k + s) \tag{22}$$

mit Wahrscheinlichkeit größer gleich $1-2^{s}$ und mit Theorem 1 analog zu (19)

$$m \geq H_c(S \mid G, Z = z, U = u) \geq m - 2^{m-d+2(k+s)} \tag{23}$$

Eves Wissen über S läst sich abschätzen mit

$$H(S) - H_c(S \mid G, Z = z, U = u) \leq m - (m - 2^{m-d+2(k+s)}) = 2^{m-d+2(k+s)} \tag{24}$$

Es ist also maximal $2^{m-d+2(k+s)}$ und lässt sich mit geeigneter Wahl von g aus G bei gegebenem Sicherheitsparameter s beliebig minimieren.

4 Sicherheit der QKD Protokolle

Bisher wurden die QKD Protokolle vorgestellt aber noch nicht gezeigt, dass sie sicher sind. Das ist das Thema dieses Kapitels. Zunächst wird eine untere Schranke für die Fähigkeit eines Quantenkanals, Informationen geheim austauschen zu können hergeleitet. Anschließend wird ein sicheres Protokoll erstellt und dies sukzessiv zu BB84 vereinfacht, wobei die Sicherheit erhalten bleibt.

4.1 Privacy und Kohärente Information

Zunächst definieren wir Privacy, die Fähigkeit eines Quantenkanals, Informationen geheim austauschen zu können, wie folgt: Angenommen Alice sendet einen Zustand ρ_k^A, k=0, 1, … mit Wahrscheinlichkeit p_k^A. Durch Fehler im Kanal und durch Eve empfängt Bob $\rho_k^B = \mathcal{E}(\rho_k^A)$. Benutzen wir folgendes Theorem:

Theorem 3: Der Holevo bound

Angenommen Alice erzeugt Zustände ρ_X, X=0, … , n mit Wahrscheinlichkeiten p_0, … , p_n. Bob führt eine Messung definiert durch die POVM Elemente { E_y } = { E_0, … , E_m } durch und erhält das Ergebnis Y. Der Holevo bound besagt, dass für jede Messung die Bob durchführen kann

$$H(X:Y) \le S(\rho) - \sum_x p_x S(\rho_x) \tag{25}$$

wobei $\rho = \sum_x p_x \rho_x$.

Also gilt für die gemeinsame Information zwischen Bobs Messung und Alices k

$$H_{Bob:Alice} \le \chi^B = S(\rho^B) - \sum_k p_k S(p_k^B) \tag{26}$$

wobei $\rho^B = \sum_x p_x \rho_x^B$ und für die gemeinsame Information zwischen Eves Wert und Alices k

$$H_{Eve:Alice} \leq \chi^E = S(\rho^E) - \sum_k p_k S(p_k^E) \tag{27}$$

Die Privacy P sei dann wie folgt definiert

$$P := \sup(H_{Bob:Alice} - H_{Eve:Alice}) \tag{28}$$

wobei das Supremum über alle Strategien genommen ist, die Alice und Bob anwenden können um den Kanal zu benutzen. Nach dem Holevo-Schumacher-Westmoreland (HSW) Theorem können Alice und Bob nun eine Strategie wählen, so dass $H_{Bob:Alice} = \chi^B$ und $H_{Eve:Alice} \leq \chi^E$ weshalb gilt

$$P \geq \chi^B - \chi^E \tag{29}$$

Die Zustände $\rho_k^A = |\psi_k^A><\psi_k^A|$, die Alice verschicken kann sind reine Zustände und nicht verschränkt mit Eves Startzustand, der, ohne Beschränkung der Allgemeinheit, $|0^E>$ ist. Im schlimmsten Fall für Alice und Bob ist der Quantenkanal an sich fehlerfrei und die Veränderung des Zustands durch $\mathcal{E}$ ist vollständig auf Eve zurückzuführen. Dann ist der Zustand nach der Übertragung

$$|\psi^{EB}> = U|\psi_k^A>|0^E> \tag{30}$$

wobei U die unitäre Operation ist, die Eve auf dem gesammten Quantensystem ausführt und die, auf dem Teilquatensystem das Bob erhält ohne Eves Qubits, wie $\mathcal{E}$ wirkt. Da $|\psi^{EB}>$ ein reiner Zustand ist gilt nach den Eigenschaften der reduzierten Dichtematrizen dass ρ_k^A und ρ_k^B dieselben Eigenwerte ungleich Null besitzen und deshalb gilt

$$S(\rho_k^E) = S(\rho_k^B) \tag{31}$$

Nach (29) und (31) gilt also

$$\begin{aligned} P &\geq \chi^B - \chi^E \\ &= S(\rho^B) - \sum_k p_k S(p_k^B) - S(\rho^E) + \sum_k p_k S(p_k^E) \\ &= S(\rho^B) - S(\rho^E) \\ &= I(\rho, \mathcal{E}) \end{aligned} \tag{32}$$

wobei $I(\rho,\mathcal{E})$ die Quanten kohärente Information ist, die wie folgt definiert ist

$$I(\rho,\mathcal{E}) := S(\mathcal{E}(\rho)) - S(\rho,\mathcal{E}) \tag{33}$$

S ist dabei die von Neumann Entropie.

$I(\rho,\mathcal{E})$ ist also eine untere Schranke für die Privacy P eines Quantenkanals. Dieses Ergebnis ist protokollunabhängig. Allerdings muss, um diese Schranke explizit für einen gegebenen Kanal angeben zu können, $\mathcal{E}$ erst ermittelt werden. Außerdem wissen wir noch nicht, wie eine Strategie auszusehen hat, damit (29) gilt.

4.2 Anforderungen an ein sicheres QKD Protokoll

Unser Kriterium für ein sicheres QKD Protokoll sei:

Sicherheitskriterium: Ein QKD Protokoll heißt sicher, wenn es für jeden Sicherheitsparameter s>0 und l>0 ausgewählt von Alice und Bob und für jede Strategie die Eve anwenden kann, entweder abbricht oder mit einer Wahrscheinlichkeit von mindestens $1-O(2^{-s})$ zum Erfolg führt und es garantiert, dass Eves gemeinsame Information mit dem erzeugten Schlüssel kleiner als 2^{-l} ist. Außerdem muss der erzeugte Schlüssel zufällig sein.

Was bei der bisherigen Beschreibung der Protokolle offen gelassen wurde ist, wie Alice und Bob die obere Schranke t für die Fehler, die durch den Quantenkanal und durch Eves Angriffe während der Übertragung entstehen, ermitteln können. Diese Information brauchen sie für Information Reconciliation. Kennen sie t, kann Alice ihre Qubits in einem t-Fehler korrigierenden Quantencode verschlüsseln und Bob die entstehenden Fehler durch Dekodierung beheben. Unser sicheres QKD Protokoll muss also diese Schranke t ermitteln, damit es genügend Redundanz in die gesendeten Qubits einfügen kann, und letztendlich überhaupt zum Erfolg führen kann. Das zunächst vorgestellte Protokoll löst dies durch zufälliges Übertragen von Prüfqubits und anschließendem öffentlichen Vergleichen der gesendeten und empfangenen Strings. Bezeichnen wie dies als Anforderung 1.

Eine weitere Anforderung 2, die wir an unser finales QKD Protokoll stellen möchten ist, dass nur Operationen und Messungen auf einzelnen Qubits ausreichen sollen um es durchzuführen zu können.

In 2.3 haben wir gesehen, dass das EPR Protokoll sicher ist, jedoch bleibt offen, wie Alice und Bob jeweils an die eine Hälfte der EPR Paare gelangen. Gelingt es, ein Verfahren zu entwickeln, dass Alice und Bob mit EPR Paaren versorgt, so ist dies zusammen mit dem EPR Protokoll ein sicheres QKD Protokoll. Diese Anforderung läst sich sogar noch etwas abschwächen. Wir

zeigen gleich: Wenn es ein Verfahren gibt dass Alice und Bob mit hoher Wahrscheinlichkeit mit EPR Paaren mit Fidelity von mindestens $1-2^{-s}$ versorgt, so ist es sicher.

Nehmen wir also an, Alice hat n EPR Paare, jedes im Zustand

$$|\beta_{00}>=\frac{|00>+|11>}{\sqrt{2}} \tag{34}$$

Durch Fehler, entstanden durch den Quantenkanal und Eve empfängt Bob einen nicht unbedingt reinen Zustand ρ. Betrachten wir folgendes Lemma:

Lemma 1: Hohe Fidelity impliziert niedrige Entropie

Wenn $F(\rho,|\beta_{00}>^{\otimes n})^2 > 1-2^{-s}$, dann gilt

$$S(\rho) < \left(2n+s+\frac{1}{\ln 2}\right)\cdot 2^{-s} + O(2^{-2s}) \tag{35}$$

Beweis:

Aus den Eigenschaften der Fidelity folgt, dass wenn

$$F(\rho,|\beta_{00}>^{\otimes n})^2 = {}^{\otimes n}<\beta_{00}|\rho|\beta_{00}>^{\otimes n} > 1-2^{-s} \tag{36}$$

der größte Eigenwert von ρ größer als $1-2^{-s}$ sein muss. Also ist die Entropie von ρ nach oben beschränkt durch die Entropie von

$$\rho_{\max} = \begin{pmatrix} 1-2^{-s} & 0 & \dots & 0 \\ 0 & \frac{2^{-s}}{(2^{2n}-1)} & 0 & \dots \\ \dots & 0 & \dots & 0 \\ 0 & \dots & 0 & \frac{2^{-s}}{(2^{2n}-1)} \end{pmatrix} \tag{37}$$

Zusammen mit der Definition der von Neumann Entropie folgt

$$S(\rho) \le S(\rho_{\max}) = -(1-2^{-s})\cdot\log_2(1-2^{-s}) - 2^{-s}\log_2\frac{2^{-s}}{2^{2n}-1} \tag{38}$$

qed.

Betrachtet man nun die kompletten EPR Paare als gesendet und die Messung von Alice und Bob als eine einzige, deren Ergebnis XY sei, und Z eine beliebige Messung Eves, so gilt nach dem Holevo bound

$$H(XY:Z) \le S(\rho) < \left(2n + s + \frac{1}{\ln 2}\right) \cdot 2^{-s} + O(2^{-2s}) \tag{39}$$

Die gemeinsame Information die Eve mit dem nach der Übertragung von Alice und Bob durch Messung generierter Schlüssel ist also nach oben beschränkt nach (39). Somit ist gezeigt: Wenn es ein Verfahren gibt, das Alice und Bob mit hoher Wahrscheinlichkeit mit EPR Paaren mit Fidelity von mindestens $1\text{-}2^{-s}$ versorgt, so ist es sicher.

An dieser Stelle läst sich auch über diesen Weg zeigen, dass das EPR sicher ist wenn Alice und Bob EPR Paare besitzen. Dies läst sich betrachten als schickte man $|\beta_{00}>^{\otimes n}$ durch einen perfekten Quantenkanal der den Zustand nicht verändert. Dann ist ρ ein reiner Zustand und nach dem Holevo bound gilt

$$H(XY:Z) \le S(\rho) - S(\rho) = 0 \tag{40}$$

wodurch Eve also keinerlei Information über den generierten Schlüssel hat.

4.3 Die untere Schranke für Fidelity

Im vorherigen Kapitel haben wir gezeigt, um ein sicheres QKD Protokoll zu entwerfen genügt es sicher zu stellen, dass es die untere Schranke für die Fidelity von Alice und Bobs EPR Paaren von Lemma 1 garantiert. Wie schon zuvor erwähnt, lässt sich dies durch zufällige Auswahl übertragener Qubits erreichen, die Alice und Bob auf Fehler untersuchen. Aus der Theorie der Quantenfehlerkorrektur wissen wir, dass der Fehler, der durch die Übertragung eines Qubits durch einen Quantenkanal entsteht, als Operator dargestellt werden kann, der auf das Qubit wirkt und eine Linearkombination aus I, X, Z und XZ ist.

$$E = e_0 I + e_1 X + e_2 Z + e_3 XZ \tag{41}$$

Das einzige, was also einem gesendeten Qubit passieren kann ist nichts, dass ein Bit kippt, dass die Phase kippt, oder dass das Bit und die Phase kippt. Die Bellbasen sind wie folgt definiert:

$$|\beta_{00}>=\frac{|00>+|11>}{\sqrt{2}} \qquad |\beta_{10}>=\frac{|00>-|11>}{\sqrt{2}}$$
$$|\beta_{01}>=\frac{|01>+|10>}{\sqrt{2}} \qquad |\beta_{11}>=\frac{|01>-|10>}{\sqrt{2}} \tag{42}$$

Angenommen, Alice sendet ein Qubit das nun zur Überprüfung der Fidelity mitbenutzt werden soll. Alice und Bob können nun, durch zufällige Auswahl einer Messungen definiert durch die Projektoren

Bitflip: $\Pi_{bf} = |\beta_{01}><\beta_{01}| + |\beta_{11}><\beta_{11}|,\ I - \Pi_{bf}$ (43)

Phasenflip: $\Pi_{pf} = |\beta_{10}><\beta_{10}| + |\beta_{11}><\beta_{11}|,\ I - \Pi_{pf}$ (44)

überprüfen, ob ein Bit oder die Phase gekippt ist. Anzumerken ist, dass diese Messungen den Zustand der Qubits nicht verändern.

Angenommen Alice schickt 2n Qubits und Alice und Bob wählen n Qubits aus zur Überprüfung. Dann sind mit hoher Wahrscheinlichkeit ähnlich viele Qubits der nicht überprüften n Qubits fehlerhaft wie die n überprüften Qubits. Dieses Verfahren lässt sich also benutzen, um die Fidelity über den übertragenen Zustand der n nicht überprüften Qubits, die für das weitere Verfahren verwendet werden, abzuschätzen.

Anzumerken ist, dass die Messungen, obwohl ein Qubit Alice und eins Bob besitzt, lokal durchgeführt werden können, da

$$\Pi_{bf} = (I \otimes I - Z \otimes Z)/2,\ \Pi_{pf} = (I \otimes I - X \otimes X)/2 \tag{45}$$

Alice und Bob können also die Messung durchführen indem sie entweder beide eine Messung auf ihrem Bit durchführen definiert durch Z und I-Z für die Bitflip Überprüfung bzw. X und I-X für die Phasenflip Überprüfung.

4.4 Das modifizierte Lo-Chau Protokoll

Da wir nun in 4.3 gezeigt haben, dass durch zufällige Überprüfung von Qubits die Fidelity von unten beschränkt werden kann und in 4.2 dass dann ein Protokoll sicher ist können wir nun ein erstes sicheres QKD Protokoll entwerfen, dass unser Sicherheitskriterium erfüllt.

Anzumerken ist noch, dass die Sicherheit aus Kapitel 4.3 besagt, dass die gemeinsame Information von Eve mit dem Schlüssel nach oben beschränkt ist. Diese muss noch verringert werden durch Privacy Amplification damit Alice und Bob einen geheimen privaten Schlüssel erhalten. Merken sie, dass bei der Überprüfung der Qubits auf Fehler, zu viele Fehler aufgetreten sind, so können sie ihr Protokoll mit einem größeren t wiederholen. Das bedeutet,

Alice schickt ausreichend mehr Qubits an Bob, damit sie die auftretenden Fehler der anschließenden Messungen von X und Y durch Information Reconciliation zu W entfernen können und durch Privacy Amplification die gemeinsame Information von Eve mit dem Schlüssel minimieren können, während die entstehende Schlüssellänge groß genug bleibt für ihre Anwendung.

Alternativ können Alice und Bob auch Entanglement Distillation als eine Art Quanten Privacy Amplification benutzen. Ist das t ermittelt, so können Alice und Bob einen t-Fehler korrigierenden Quantenfehlerkorrekturcode benutzen um die Qubits zu übertragen.

Dies zusammen mit dem zufälligen Einfügen von Qubits ergibt das modifizierte Lo-Chau Protokoll, unser erstes sicheres QKD Protokoll. Anforderung 1, eine Schranke für t zu ermitteln, wird von ihm durch die Verwendung der Prüfqubits erfüllt.

Das modifizierte Lo-Chau Protokoll

1. Alice erstellt 2n EPR Paare im Zustand $|\beta_{00}>^{\otimes 2n}$.
2. Alice wählt n Prüfqubits aus.
3. Alice erzeugt einen zufälligen Bit-String b der Länge 2n und wendet die Walsh-Hadamard Operation auf das jeweils 2. Qubit des EPR Paares an, an deren Stelle b 1 ist.
4. Alice sendet das jeweils zweite Qubit eines EPR Paares zu Bob
5. Bob gibt öffentlich den Empfang der Qubits bekannt
6. Alice gibt öffentlich b und die Stellen der n Prüfqubits bekannt.
7. Bob wendet Walsh-Hadamard auf die Qubits an, an deren Stelle b 1 ist.
8. Alice und Bob messen ihre n Prüfqubits in der |0>, |1> Basis und geben ihre Ergebnisse öffentlich bekannt. Wenn mehr als t unterschiedlich sind, brechen sie das Protokoll ab, bzw. beginnen erneut mit größerem t.
9. Alice und Bob verwenden einen [n, m] Quantenfehlerkorrekturcode der bis zu t Fehler korrigiert um ihre n verbleibenden Qubits zu korrigieren und paarweise verteilte EPR Paare zu erhalten. (Quanten Information Reconciliation)
10. Alice und Bob messen jeweils ihre Qubits der EPR Paare und erhalten einen geheimen Schlüssel

Dazu ist anzumerken, dass ursprünglich Alice und Bob die Prüfbits zufällig in X, bzw. Z Basis messen sollten, um Bitflip oder Phaseflip festzustellen. In diesem Protokoll wurde nun alternativ während der Übertragung die Basis einiger Qubits durch die Walsh-Hadamard Operation gedreht. Dies ist äquivalent, denn nach der Anwendungsregel von Quantenoperationen auf den Dichteoperator gilt:

$$WXW = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = Z \tag{46}$$

Da die Prüfqubits zufällig dieser Transformation unterzogen werden, wird also auch zufällig auf Bitflip und Phaseflip überprüft, wie zuvor geplant.

4.5 Das Quantenfehlerkorrektur Protokoll

Das modifizierte Lo-Chau Protokoll kann weiter vereinfach werden. Da Alice zunächst zu Beginn EPR Paare erzeugt und zum Schluss Bobs Qubit des Paares durch Messung ihres Qubits zu einem unverschränkten Qubit verändert, kann Alice auch direkt zu Beginn diese Messung durchführen, bzw. erst gar keine EPR Paare erstellen sondern nur eine Menge Qubits, die sie zu Bob sendet.

Die Prüfqubits können einfach durch unverschränkte Qubits ersetzt werden da Alice nach der Übertragung Bob die Positionen der Prüfqubits öffentlich mitteilt und Bob daraufhin diese messen und vergleichen kann.

Die restlichen EPR Paare ersetzen wir wie folgt: Die Qubits nach den Messungen von Alice in Schritt 9 und 10 können angesehen werden als zufällige Qubits enkodiert in einem zufälligen Quantenfehlerkorrekturcode. Dazu betrachten wir einen [n, m] Calenderbank-Shor-Steane Code CSS(C_1, C_2) der m Qubits in n Qubits enkodiert und bis zu t Fehler korrigieren kann. Dann sind die enkodierten Zustände:

$$|v_k + C_2> = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} |v_k + w> \tag{47}$$

wobei v_k für jedes $k \in \{1,...,2^m - 1\}$ für einen Vertreter einer anderen Nebenklasse steht. Außerdem gibt es eine Familie von CSS Codes, die äquivalent zu diesem CSS Code ist, $CSS_{z,x}(C_1, C_2)$:

$$|\xi_{v_k,z,x}> = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{z \cdot w} |v_k + w + x> \tag{48}$$

Da diese Zustände eine Orthonormalbasis im 2^n dimensionalen Hilbertraum bilden, können Alices n EPR Paare wie folgt dargestellt werden:

$$|\beta_{00}>^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n} |j>|j> = \frac{1}{\sqrt{2^n}} \sum_{v_k,z,x} |\xi_{v_k,z,x}>|\xi_{v_k,z,x}> \tag{49}$$

wobei die Qubits so vertauscht wurden, dass das linke Ket für Alices Qubits steht und das rechte für Bobs. Schritt 9 liefert Alice ihr zufälliges x und z und Schritt 10 letztendlich ein zufälliges v_k. Bobs Qubits entsprechen nun einem in $CSS_{z,x}(C_1, C_2)$ |k>. Also erzeugen Alices Messungen zufällige Qubits in einem zufälligen Quatenfehlerkorrekturcode.

Die vorgestellten Änderungen ergeben folgendes Protokoll:

CSS Code Protokoll

1. Alice erzeugt n zufällige Prüfbits und erzeugt entsprechende n Qubits jeweils im Zustand |0> oder |1>. Weiterhin erzeugt sie einen zufälligen m Bit String k und zwei n Bit Strings x und z. Sie enkodiert |k> in $CSS_{z,x}(C_1, C_2)$.
2. Alice platziert die Prüfbits zufällig zwischen den CSS enkodierten Qubits.
3. Alice erzeugt einen zufälligen Bit-String b der Länge 2n und wendet die Walsh-Hadamard Operation auf die Qubits an, an deren Stelle b 1 ist.
4. Alice sendet die Qubits zu Bob.
5. Bob gibt öffentlich den Empfang der Qubits bekannt.
6. Alice gibt öffentlich b, x, z und die Positionen der Prüfbits bekannt.
7. Bob wendet die Walsh-Hadamard Operation auf die Qubits an, an deren Stelle b 1 ist.
8. Bob misst die Prüfbits in der |0>, |1> Basis und gibt sein Ergebnis öffentlich bekannt. Wenn mehr als t Bits falsch sind, bricht das Protokoll ab.
9. Bob dekodiert die restlichen Qubits aus $CSS_{z,x}(C_1, C_2)$.
10. Bob misst seine Qubits und erhält den geheimen Schlüssel k.

4.6 Vereinfachung zu BB84

Unser bisheriges Protokoll erfüllt Anforderung 1. Allerdings benötigen wir weiterhin einen perfekten Quantencomputer für die Berechnung der CSS Codes sowie einen Quantenspeicher, um die Qubits die Bob empfängt bis zur Messung zwischenzuspeichern. Im Weiteren werden wir unser Protokoll soweit verändern, damit auch Anforderung 2 erfüllt wird.

Im bisherigen Protokoll führt Bob direkt nach der Dekodierung seiner Qubits aus dem CSS Code in der Z Basis seine Messung durch. Dabei ist die Phasenkorrekturinformation die Alice in Form von z sendet unnötig. Da C_1 und C_2 jedoch klassische Codes sind, kann Bob alternativ auch erst die Messung durchführen und anschließend klassisch den Fehler korrigieren. Nach einer direkten Messung erhält Bob $v_k + w + x + \varepsilon$, wobei ε für den durch den Quantenkanal verursachten Fehler steht. Da Alice x öffentlich bekannt gibt, kann Bob von seinem String x abziehen und anschließend den Fehler durch

den Fehlerkorrekturcode C_1 korrigieren und erhält $v_k + w$. Der finale Schlüssel ist die Nebenklasse von $v_k + w + C_2$ in C_1. Dieser Schritt entspricht der Privacy Amplification.

Da Alice z nicht mehr öffentlich bekannt gibt, empfängt Bob keinen reinen Zustand mehr, sondern

$$\begin{aligned}\rho_{v_k,x} &= \frac{1}{2^n}\sum_z |\, \xi_{v_k,z,x} >< \xi_{v_k,z,x} \,| \\ &= \frac{1}{2^n \,|\, C_2 \,|}\sum_z \sum_{w_1,w_2 \in C_2} (-1)^{z\cdot(w_1+w_2)} \,|\, v_k + w_1 + x >< v_k + w_2 + x \,| \\ &= \frac{1}{|\, C_2 \,|}\sum_{w \in C_2} |\, v_k + w + x >< v_k + w + x \,|\end{aligned} \qquad (50)$$

Dieser Zustand ist für Alice leicht herzustellen, denn sie kann einfach klassisch zufällig ein $w \in C_2$ auswählen und mittels ihres x und k $|\, v_k + w + x >$ erzeugen. Dies kann noch weiter vereinfacht werden. Da Alice $v_k \in C_1$ zufällig auswählt, ist $v_k + x$ ohnehin ein zufälliger String, auch ohne die Addition eines zufälligen $w \in C_2$. Also kann w weggelassen werden. Weiterhin sind sowohl x als auch v_k jeweils zufällige Strings. Also genügt es, wenn Alice $|\, x >$ über den Quantenkanal sendet und, nachdem Bob die Qubits empfangen und $x + \varepsilon$ gemessen hat, $x - v_k$ öffentlich bekannt gibt. Dann kann Bob durch Subtraktion $v_k + \varepsilon$ berechnen und wie zuvor beschrieben korrigieren.

Eine weitere kleine Verbesserung erhält man, indem man Alice die zu sendenden Qubits direkt in entweder in der |0>, |1> Basis oder der |+>, |-> Basis enkodieren lässt, wodurch man die Walsh-Hadamard Operation einspart.

Bis hierher wurde Anforderung 1 soweit erfüllt, dass kein perfekter Quantencomputer mehr für unser QKD Protokoll benötigt wird, da die CSS Berechnungen klassisch durchgeführt werden. Um auch den Quantenspeicher entfernen zu können gehen wir wie folgt vor:

Bob misst seine empfangen Qubits direkt. Da er zu diesem Zeitpunkt b noch nicht kennt, wählt er zufällig entweder die X oder Z Basis zum messen aus. (Dies entspricht einer zufälligen Walsh-Hadamard Operation und anschließender Messung in |0>, |1> Basis.) Anschließend, nachdem Alice b bekannt gegeben hat, behalten sie nur die Bits, bei denen Bob in der richtigen Basis gemessen hat. Allerdings hat dieses Vorgehen einen negativen Effekt. Da für jedes Bit die Wahrscheinlichkeit die richtige Basis zu wählen 0.5 ist, benötigen Alice und Bob jetzt mindestens doppelt so viele Bits, $(4+\delta)$n Bits, wie zuvor um einen Schlüssel derselben Länge zu erhalten. Zudem muss Alice ihre Entscheidung, welche Bits als Prüfbits dienen sollen bis nach der Verwerfung der falschen Bits verschieben.

Zusammenfassend erhalten wir also folgendes Protokoll, das BB84 entspricht:

Sicheres BB84

1. Alice erzeugt $(4+\delta)$n zufällige Bits.
2. Weiterhin erzeugt sie $(4+\delta)$n Qubits diesem String entsprechend in der Basis einem zufälligen String b entsprechend.
3. Alice sendet die Qubits zu Bob.
4. Alice wählt ein zufälliges $v_k \in C_1$.
5. Bob empfängt die Qubits und misst sie zufällig in X oder Z Basis und gibt den Empfang öffentlich bekannt.
6. Alice gibt b öffentlich bekannt.
7. Alice und Bob verwerfen die falsch gemessenen Bits. Mit hoher Wahrscheinlichkeit bleiben 2n Bits übrig. Von denen wählt Alice 2n die behalten werden sollen zufällig aus und davon wiederum n Prüfbits.
8. Alice und Bob vergleichen öffentlich ihre Prüfbits. Wenn mehr als t unterschiedlich sind, bricht das Protokoll ab. Zu diesem Zeitpunkt besitzt Alice x und Bob $x+\varepsilon$.
9. Alice gibt öffentlich $x-v_k$ bekannt und Bob berechnet sich $v_k+\varepsilon$ und verwendet C_1 um diesen String zu v_k zu korrigieren. (Information Reconiliation)
10. Alice und Bob berechnen die Nebenklasse von v_k+C_2 in C_1 um den privaten Schlüssel k zu erhalten. (Privacy Amplification)

Dieses Protokoll ist somit nach unserem Kriterium sicher und erfüllt die beiden Anforderungen.

4.7 Qubits doch kopierbar?

Am 23. Mai 2002 veröffentlichten Antia Lamas-Linares, Christoph Simon, John C. Howell und Dik Bouwmeester ein Paper, in dem sie ihr Experiment zum Clonen eines Qubits beschrieben. Nach ihrem Verfahren ist es möglich, ein Qubit mit 5/6 Wahrscheinlichkeit zu kopieren, ohne das originale Qubit zu verändern.

Für die Quantenkryptographie stellt dies jedoch keine Bedrohung in Fragen Sicherheit dar. Solange Eves gemeinsame Information mit dem erzeugten Strings geringer als die Entropie des erzeugten Strings ist, können Alice und Bob durch Privacy Amplification einen geheimen privaten Schlüssel erstellen. Lediglich die Anzahl der Bits mit denen Alice und Bob mit dem Protokoll beginnen muss groß genug gewählt werden, damit ein ausreichend langer Schlüssel zum Schluss entsteht.

5 Experimentelle Durchführung von Quantenkryptographie

Zu dem hier vorgestellte BB84 Protokoll existiert ein experimenteller Versuchsaufbau von IBM. Die Testdistanz beträgt 10 km. Photonen werden mittels eines Lasers erzeugt und über Glasfaserkabel verschickt. Die Qubits entsprechen einzelnen Photonen, deren Polarisation die Qubitinformation enthält.

Die Photonen werden dabei zunächst von Bob erzeugt und zu Alice geschickt, damit unerwünschte Effekte des Kanals sich bei der Rücksendung gegenseitig aufheben. Als klassischen Kanal wird ebenfalls dasselbe Glasfaserkabel verwendet mit Photonen einer anderen Wellenlänge.

Die erzielte Geschwindigkeit liegt bei einigen hundert ausgetauschten Schlüsselbits pro Sekunden. Das Verfahren wurde auch bereits über 40 km erfolgreich getestet.

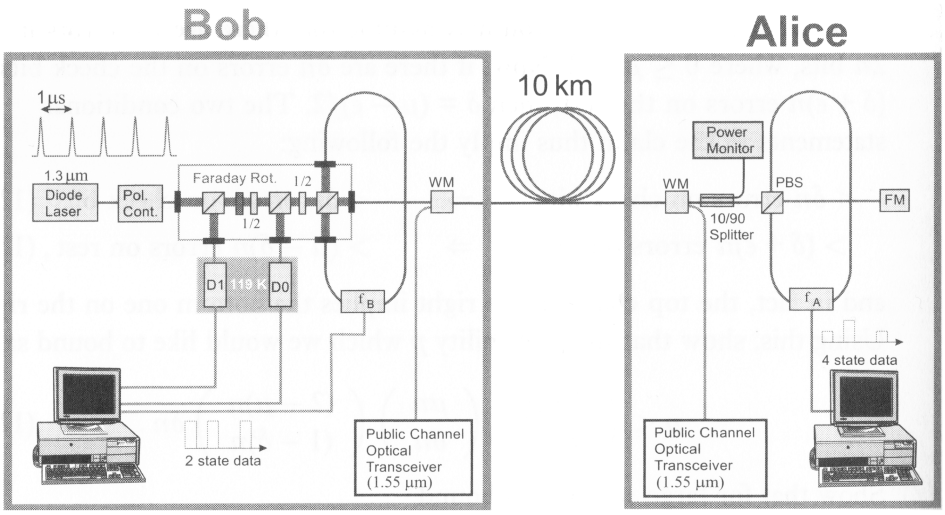

Abbildung 3: Experimenteller Quantenkryptographie Versuchsaufbau

6 Literaturangaben

[1] Nielsen, Michael A. and Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000

[2] Gruska, Jozef, Quantum computing, London: McGraw-Hill, 1999

[3] Heinrich, Stefan, Notes on mathematical foundations of quantum computing, Kaiserslautern, 2002

[4] Shor, Peter W., Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal on Computing, 1997

[5] Lamas-Linares, Antia, Christoph Simon, John C. Howell, Dik Bouwmeester, Experimental Quantum Cloning of Single Photons, University of Oxford, University of California at Santa Barbara, 2002