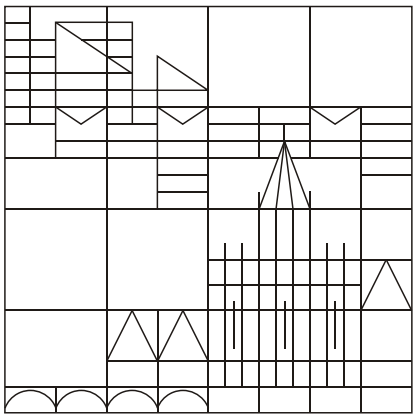
Untersuchungen zur Quantenkryptographie mit unscharfen Messungen

Diplomarbeit



Universität Konstanz
Fachbereich Physik

Verfasser: Sabine Burgdorf
Gr. Kremperstr. 15
25348 Glückstadt
Sabine.Burgdorf@uni-konstanz.de

1. Gutachter: Prof. J. Audretsch

2. Gutachter: Prof. P. Nielaba

Konstanz im März 2007

Inhaltsverzeichnis

Zusammenfassung

Die vorliegende Arbeit befasst sich mit Aspekten der Quantenkryptographie. Sie beschäftigt sich also mit der Frage, wie man mit Hilfe quantentheoretischer Methoden und Prinzipien einen geheimen Schlüssel erzeugt, welcher bei der Übertragung nicht abgehört werden kann. Dieser Schlüssel wird dann genutzt, um die eigentliche Nachricht zu verschlüsseln. Dieses Verfahren ist momentan das einzig bekannte Verfahren, dass wirklich bedingungslos sicher ist, sofern der Schlüssel zufällig generiert wurde und wirklich geheim ist.

Im ersten Teil der Arbeit werden diskrete Quantenkryptographie-Protokolle am Beispiel des BB84- und des SARG-Protokolls behandelt. Nach der Erläuterung der Funktionsweise sowie experimenteller Realisierungen dieser Protokolle wird gezeigt, wie man deren Sicherheit nachweist. Dazu werden zunächst die Prinzipien der Quantenfehlerkorrektur und der Verschränkungspurifizierung vorgestellt. Mit diesen Hilfsmitteln wird dann die Sicherheit des BB84-Protokolls bewiesen.

Im zweiten Teil der vorliegenden Arbeit wird ein neuer Ansatz zur Schlüsselerzeugung untersucht. Die im ersten Teil vorgestellten Protokolle basieren darauf, dass sie ein Schlüsselbit in ein Qubit kodieren. Sie verwenden dabei Zustände, welche in der Blochdarstellung orthogonal aufeinander stehen, da hiermit ein potentieller Lauscher an der Störung durch seinen Lauschangriff am ehesten entdeckt werden kann. Der neue Ansatz untersucht, ob man auch Zustände verwenden kann, die einen kleineren Winkel als 90° einschließen. Diese Zustände kann man beispielsweise durch unscharfe Messungen eines vorher festgelegten Anfangszustands $|\psi\rangle$ erzeugen. Da diese Zustände einen Überlapp haben, muss man die Anzahl der Qubits pro Schlüsselbit erhöhen, um die präparierten Zustände sicher unterscheiden zu können. Ein Bit wird also in einem Ensemble, welches durch unscharfe Messungen erzeugt wird, verschlüsselt.

Das hieraus abgeleitete Verfahren wird mit den entsprechenden Rechnungen vorgestellt und es wird die Sicherheit unter den idealisierten Bedingungen unendlich großer Ensemble pro Schlüsselbit und der Verwendung eines fehlerfreien Quantenkanals gezeigt. Daran anschließend wird untersucht, ob dieses Verfahren auch sicher ist, wenn man auf den fehlerfreien Quantenkanal verzichtet oder endliche Ensemble verwendet. Hierbei werden nur Lauschangriffe mit unscharfen Messungen betrachtet.

Es stellt sich heraus, dass das vorgestellte Verfahren bei Verwendung unendlich großer Ensemble abgehört werden kann, wenn man einen reinen Zustand $|\psi\rangle$ als Anfangszustand verwendet. Die vorgeschlagene Modifikation des Protokolls erweist sich ebenfalls als abhörbar. Allerdings nutzt der Lauschangriff hierbei konkret aus, dass das verwendete Ensemble unendlich groß ist.

Bei Verwendung endlicher Ensemble wird der Schlüssel mit Methoden der Testtheorie ermittelt. Es wird gezeigt, dass man bei geeigneter Wahl der Ensemblegröße den

Schlüssel mit beliebig kleiner Fehlerwahrscheinlichkeit übermitteln kann.

Für einen konkreten Lauschangriff wird zunächst die Wahrscheinlichkeit berechnet, mit der der Lauscher den richtigen Schlüssel erhält. Abschließend wird die Sicherheit gegenüber Lauschangriffen mit unscharfen Messungen mittels der wechselseitigen Information nachgewiesen.

Das vorgestellte Verfahren erweist sich für endliche Ensemble als sicher hinsichtlich der betrachteten Lauschangriffe. Die unbedingte Sicherheit für einen allgemeinen Lauschangriff ist noch zu zeigen.

Abbildungsverzeichnis

Tabellenverzeichnis

Einleitung

Kryptographie befasst sich mit dem Problem, eine Nachricht so zu verschlüsseln, dass ein Lauscher aus der verschlüsselten Botschaft nicht auf die eigentliche Nachricht schließen kann. Im Laufe der Geschichte sind hierfür mehrere Methoden entwickelt worden, so zum Beispiel die Caesar-Chiffre, welche die ursprüngliche Nachricht jeweils um einen konstanten Wert verschoben hat. Diese und auch andere Methoden haben sich als unsicher erwiesen. Bei der Caesar-Chiffre kann man zum Beispiel über einen einfachen Häufigkeitstest oft auf die ursprüngliche Nachricht schließen.

Klassische Kryptographie beruht auf der Komplexität der Berechnungen zur Ermittelung des verwendeten Schlüssels, da ein Lauscher im Allgemeinen unbemerkt die Nachricht kopieren und ermitteln kann, ohne das System zu stören. Das bekannteste Verfahren (RSA) beruht darauf, dass man mit den heutigen Rechnerkapazitäten die Primfaktorzerlegung einer großen Zahl nicht in akzeptabler Zeit berechnen kann. Allerdings sind diese Methoden nicht bedingungslos sicher, da man nicht ausschließen kann, dass diese Probleme in Zukunft gelöst werden.

Quantenkryptographie beruht auf dem von G. Vernam und J. Mauborgne entwickelten Prinzip des Einmal-Schlüssels (*one-time pad*) [4]. Dabei wird die zu verschlüsselnde Nachricht komponentenweiseweise mit einem zufälligen Schlüssel gleicher Länge addiert und dieses so entstandene Kryptogramm versendet. Da der Schlüssel zufällig ist, wird die verschlüsselte Botschaft unabhängig von der Nachricht und kann somit nicht ohne Kenntnis des Schlüssels dekodiert werden. Shannon hat 1949 [5, Th. 13] bewiesen, dass dieses Verfahren, sofern dieser zufällige Schlüssel nur ein einziges Mal verwendet wird, bedingungslos sicher ist.

Die Aufgabe ist somit darauf reduziert, ein Verfahren zu finden, das einen hinreichend zufälligen Schlüssel beim Sender (Alice) und Empfänger (Bob) erzeugt, so dass ein potentieller Lauscher (Eve) mit hoher Wahrscheinlichkeit so gut wie keine Information über diesen Schlüssel besitzt oder ihr Lauschangriff entdeckt wird. Ist dieses der Fall, so wird das Protokoll als sicher betrachtet.

Es stellt sich also das Problem der sicheren Schlüsselübertragung. Ziel der Quantenkryptographie ist es nun, mittels quantentheoretischer Methoden und Prinzipien eine beweisbar bedingungslos sichere Schlüsselübertragung zu gewährleisten. Das heißt, die Sicherheit beruht nur auf den Gesetzen der Quantentheorie und erfordert keine zusätzlichen Annahmen wie die klassische Kryptographie. Wesentlich hierbei sind die folgenden aus der Heisenbergschen Unschärferelation resultierenden Eigenschaften eines quantentheoretischen Systems:

i) Das no-cloning-Theorem; dieses besagt, dass es im Gegensatz zu einem klassischen System nicht möglich ist, einen unbekannten Quantenzustand exakt zu vervielfältigen

ii) Man kann nicht mit Sicherheit zwei nichtorthogonale Zustände durch eine einzige Messung unterscheiden

iii) Jeder Informationsgewinn über ein System bedingt eine mit einer Entropieänderung verbundene Störung des Systems

Diese ermöglichen es Alice und Bob mit hoher Wahrscheinlichkeit festzustellen, ob ihr verwendeter Quantenkanal abgehört wurde. Die dritte Eigenschaft liefert dazu noch die Möglichkeit, unter gewissen Bedingungen die Menge der abgehörten Information abzuschätzen.

Im Laufe der letzten 22 Jahre wurden beginnend mit dem BB84-Protokoll [6], welches 1984 von Bennett und Brassard veröffentlicht wurde, diverse funktionierende Verfahren entwickelt. Im ersten Teil der Arbeit wird das BB84-Protokoll vorgestellt. Zudem wird mit größerem Aufwand gezeigt, dass dieses Protokoll der obigen Anforderung genügt und somit sicher ist. Hierbei wird ein Beweisprinzip benutzt, welches zunächst die Sicherheit eines anderen Protokolls zeigt, aus dem man dann die Sicherheit der oben genannten Protokolle ableitet. Diese Methode wurde von Lo und Chau [7] entwickelt und von Shor und Preskill [8] (siehe auch [9, 10]) verbessert. Sie verwenden dabei das quantentheoretische Phänomen der Verschränkung. In diesem Zusammenhang werden sowohl mathematische Sätze der Quanteninformationstheorie bewiesen und angewendet als auch essentielle Methoden wie die Quantenfehlerkorrektur (QECC), also der Fehlerkorrektur von quantentheoretischen Zuständen behandelt. Dabei betrachten wir die Fehlerkorrektur mit Calderbank-Shor-Steane(CSS)-Codes und Verschränkungspurifizierung, also der Erhöhung der Verschränkung zwischen zwei Zuständen, und deren Zusammenhänge [11].

Ein weiterer Aspekt ist die Anwendbarkeit des Protokolls. Daher werden experimentelle Realisierungsmöglichkeiten vorgestellt, um einen Bezug zur Wirklichkeit herzustellen. Durch den Wunsch nach einer Realisierung ergeben sich weitere Schwierigkeiten, so kann man zum Beispiel nicht von perfekten Bedingungen ausgehen und muss die technischen Möglichkeiten beachten. Darauf basierend wurde das SARG-Protokoll [12] entwickelt, welches eine sicherere Methode der Schlüsselübertragung liefert als das BB84-Protokoll. Dieses Protokoll wird sowohl in der Theorie als auch in einer möglichen Realisierung vorgestellt.

Im zweiten Teil dieser Arbeit wird ein neuer Ansatz zur Schlüsselübertragung untersucht. Dieser Ansatz beruht im Gegensatz zu herkömmlichen diskreten Quantenkryptographie-Protokollen auf der Verschlüsselung eines Bits in ein quantentheoretisches Ensemble. Wir versuchen, die Schlüsselübertragung mit nicht-komplementären Zuständen zu generieren, das heißt, die zugehörigen Blochvektoren dieser Zustände schließen einen kleineren Winkel als 90° ein. Diese Zustände kann man beispielsweise durch unscharfe Messungen eines vorher festgelegten Anfangszustands $|\psi\rangle$ erzeugen. Da die Zustände nun einen größeren Überlapp haben, muss man die Anzahl der Qubits pro Schlüsselbit

erhöhen, um die verschiedenen Zustände sicher zu unterscheiden. Daher nutzen wir für jedes Bit ein Ensemble, welches von Alice durch unscharfe Messungen bezüglich der z-Basis (für das Schlüsselbit 0) oder der x-Basis (für das Schlüsselbit 1) präpariert wird. Durch eine sogenannte tomographische Messung kann Bob die Dichtematrix dieses Ensembles und damit dessen Entropie ermitteln. Hierdurch kann aufgrund der oben genannten Eigenschaft iii) festgestellt werden, ob der Kanal abgehört wurde.

Dieser Ansatz wurde für unendliche und endliche Ensemblegrößen auf Sicherheit bezüglich verschiedener Lauschangriffe untersucht. Dier Ergebnisse dieser Untersuchungen sind im zweiten Teil dieser Arbeit dargestellt.

Konkret gliedert sich die Arbeit also wie folgt:

- Im ersten Kapitel legen wir die in im Rahmen dieser Diplomarbeit benötigten quantentheoretischen und mathematischen Grundlagen dar. Dabei gehen wir auf Aspekte der Quantenkryptographie ein.

- Im ersten Teil der Arbeit behandeln wir diskrete Quantenkryptographie-Protokolle am Beispiel des BB84- und des SARG-Protokolls. Die Funktionsweise dieser Protokolle sowie experimentelle Realisierungen werden in den Kapiteln 2 und 3 erläutert. Um die Sicherheit dieser Protokolle in Kapitel 5 zu beweisen, benötigen wir die Theorie der Quantenfehlerkorrektur. Diese wird in Kapitel 4 dargestellt.

- Im zweiten Teil der Arbeit untersuchen wir einen neuen Ansatz zur Quantenschlüsselübertragung. Dieser wird ausführlich in Kapitel 6 dargelegt. Dabei werden verschiedene Varianten des Protokolls betrachtet und die Sicherheit unter idealen Bedingungen gezeigt. Anschließend werden spezielle Lauschangriffe mit unscharfen Messungen unter Verwendung unendlich großer Ensemble untersucht. Dabei stellt man fest, dass das vorgestellte Protokoll abgehört werden kann. Daher wird eine Modifikation des Protokolls vorgesschlagen und im folgenden auf ihre Sicherheit bei speziellen Lauschangriffen untersucht.

  Wir schließen diesen Abschnitt mit der Betrachtung endlicher Ensemble und Überlegungen zur bedingungslosen Sicherheit. Es ist im Rahmen dieser Arbeit allerdings nicht gelungen, die bedingungslose Sicherheit unter Verwendung endlicher Ensemble zu beweisen oder zu widerlegen.

- Im Anhang sind die Berechnungen der im zweiten Teil verwendeten Größen aufgeführt.

Danksagung

Ich danke Prof. Audretsch für die Ermöglichung dieser Diplomarbeit und seiner Arbeitsgruppe für ihre Unterstützung. Spezieller Dank gilt hierbei Prof. Thomas Konrad für die Betreuung der Arbeit. Er war auch nach seinem Wechsel an die Universität von KwaZulu-Natal immer bereit, meine Fragen zu beantworten. Weiter danke ich Michael Nock für viele kleine Ratschläge und seine Korrekturen. Martin Schäfer verdanke ich hilfreiche Hinweise zur Statistik. Da ich einen Teil der Bearbeitungszeit mit Unterstützung des DAAD an der Universität von KwaZulu-Natal verbracht habe, möchte ich allen beteiligten danken. Insbesondere danke ich Prof. Pretuccione und seiner Arbeitsgruppe für die angenehme, produktive Zeit in Durban. Abschließend möchte ich noch Thomas Schluck danken, der dafür gesorgt hat, dass diese Arbeit rechtzeitig ihren Bestimmungsort erreicht hat. Allen anderen Beteiligten, die mich auf verschiedene Art und Weise unterstützt haben, danke ich unnamentlich.

Teil I

Diskrete Quantenkryptographie

1 Grundlagen für die Quantenkryptographie

Im Folgenden sollen zunächst einige grundlegende Begriffe und Techniken der Quantenkryptographie erläutert werden. Neben der Behandlung des Vernam-Schlüssels sind die erforderlichen quantentheoretischen und mathematischen Grundlagen aufgeführt. Weiter folgt eine ausgedehnte Darstellung des Entropiebegriffs. Abschließend werden noch einige Abhörstrategien und mögliche Definitonen der Sicherheit eines Protokolls diskutiert. Sofern es nicht anders angegeben ist, wurde als Referenz stets [13] und [14] verwendet.

1.1 Der Vernam-Schlüssel

In der Kryptographie geht es darum, verschlüsselte Botschaften über einen öffentlichen Kanal zu verschicken, so dass diese geheim bleiben, d.h. nur vom gewünschten Empfänger entschlüsselt werden können. Ein Prinzip, welches man hierfür verwendet, ist das des Einmal-Schlüssels (*one-time pad*), welches zu Anfang des 20. Jahrhunderts von Gilbert Vernam und Joseph Mauborgne entwickelt wurde [4]. Hierbei ist der wesentliche Bestandteil der geheime Schlüssel, welcher aus einer zufällig generierten Zeichenfolge von gleicher Länge wie die der zu verschlüsselnden Nachricht besteht. Die Nachricht selbst wird als Zeichenfolge komponentenweise mit diesem Schlüssel addiert und man erhält das sogenannte Kryptogramm. Dieses wird dann über einen öffentlichen Kanal verschickt. Ein Empfänger kann dann das Kryptogramm nur entschlüsseln, wenn er den geheimen Schlüssel kennt. Dann erhält er den Quelltext durch Subtraktion des Schlüssels.

Ein besonders einfacher Fall liegt vor, wenn der Absender den Quelltext in einer Binärfolge, d.h. einer Folge bestehend aus Nullen und Einsen, vorliegen hat. Diese wird dann mit einem binären Schlüssel komponentenweise addiert. Der Empfänger kann dann, indem er den Schlüssel erneut addiert, das Kryptogramm entschlüsseln. Hierfür geben wir ein kurzes Beispiel:

Quelltext	1	1	1	0	0	1	0	0	1	1
Schlüssel	1	0	1	1	0	1	0	0	0	1
Kryptogramm	0	1	0	1	0	0	0	0	1	0
Schlüssel	1	0	1	1	0	1	0	0	0	1
Quelltext	1	1	1	0	0	1	0	0	1	1

Der Einfachheit halber und im Hinblick auf die spätere Anwendung betrachten wir hier nur Binärsysteme, unsere Nachricht und unser Schlüssel sind also Folgen bestehend aus Nullen und Einsen.

Wird der geheime Schlüssel zufällig generiert und nur einmal (one-time) verwendet, dann ist das Kryptogramm unabhängig vom Quelltext und das Verfahren ist sicher, wie 1949 von C. Shannon [5, Th. 13] gezeigt wurde. Weiter darf auch keine sonstige Information z. B. über den Aufbau der Nachricht zugänglich sein, vgl. [7, Ref. 16.]. Durch zweimaliges Verwenden des gleichen Schlüssels entstehen Redundanzen und die Sicherheit des Verfahrens kann nicht mehr gewährleistet werden.

Wir befassen uns im Folgenden mit dem Problem der sicheren Schlüsselübertragung. Hierzu verwenden wir Quantensysteme und nutzen deren Quanteneigenschaften aus. Im Allgemeinen Sprachgebrauch wird diese Theorie, welche die quantenphysikalischen Eigenschaften des Informationsträger mit einbezieht, als Quantenkryptographie bezeichnet. Korrekterweise sollte man dieses Quanten-Schlüsselübertragung (*quantum key distribution* (QKD)) nennen. Im folgenden soll es also um Möglichkeiten gehen, wie man mittels quantentheoretischer Methoden und Prinzipien einen Schlüssel zwischen zwei Parteien (Sender und Empfänger) generieren kann, der einem potentiellen (passiven) Lauscher mit hoher Wahrscheinlichkeit nicht zugänglich ist, ohne entdeckt zu werden.

Diese Verfahren erzeugen genauso wie klassische Verfahren einen geheimen Schlüssel, von dem der Empfänger mit hoher Wahscheinlichkeit eine exakte Kopie besitzt. Außerdem ermöglichen sie, die Fehlerrate zwischen den Schlüsseln des Senders und des Empfängers abzuschätzen und die Fehler gegebenenfalls zu korrigieren. Quantentheoretische Verfahren bieten gegenüber klassischen Verfahren zusätzlich den Vorteil, dass sich die maximale Information, die ein Lauscher über den Schlüssel ermittelt haben kann, abschätzen lässt. Dadurch ist gewährleistet, dass diese im Gegensatz zu den klassischen Verfahren auch in Zukunft sicher bleiben - unabhängig vom technologischen Fortschritt.

Kryptographieverfahren werden jeweils durch ein (QKD-)Protokoll beschrieben. Dieses besteht aus einer schrittweisen Anleitung zur Durchführung des Verfahrens. Dabei wird der Absender stets mit Alice, der Empfänger mit Bob und ein potentieller Lauscher mit Eve (*eavesdropper*) bezeichnet. Diese Bezeichnungen werden im Folgenden übernommen.

1.2 Quantentheoretische Grundlagen

Die nachfolgenden Grundlagen sind der Vollständigkeit halber aufgeführt. Sie orientieren sich überwiegend an [13].

1.2.1 Qubits

Wir betrachten hier nur Zwei-Niveau-Quantensysteme, die durch einen zweidimensionalen komplexen Hilbertraum $\mathcal{H}_2$ beschrieben werden. Ein reiner Zustand eines Zwei-Niveau-Systems ist ein Zustand, welcher nach der Messung einer nicht-trivialen Observablen $O \neq \alpha\mathbf{1}$ mit einem bestimmten Messergebnis vorliegt. Er lässt sich als normier-

ter Vektor $|\psi\rangle \in \mathcal{H}_2$ in der Rechenbasis $|0\rangle, |1\rangle$ schreiben. Man kann einen allgemeinen reinen Zustand also darstellen durch $|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle$ mit $|c_0|^2 + |c_1|^2 = 1$.

Die Beschreibung ist eindeutig bis auf einen globalen Phasenfaktor $e^{i\varphi}$. Eine relative Phase erzeugt einen anderen Zustand, die Zustände $c_0 |0\rangle + c_1 |1\rangle$ und $c_0 |0\rangle + e^{i\varphi} c_1 |1\rangle$ sind also verschieden.

Alternativ lassen sich Qubits auch über Dichtematrizen beschreiben. Eine Dichtematrix ρ ist ein positiver Operator mit Spur 1, d.h. die Eigenwerte von ρ sind stets größer oder gleich 0 und summieren sich zu 1. Für ein Qubit im Zustand $|\psi\rangle$ ist dies der Projektionsoperator $\rho_\psi = |\psi\rangle \langle\psi|$. Er erfüllt die Gleichung $\mathrm{tr}[\rho_\psi^2] = \mathrm{tr}[\rho_\psi] = 1$.

Ein statistisches Gemisch beschreibt Systeme, deren Zustand nicht eindeutig bekannt ist. Befindet sich das betrachtete System mit Wahrscheinlichkeit p_i im Zustand $|\psi_i\rangle$, so wird dieses System beschrieben durch das Gemisch

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i| .$$

Hierfür gilt im Allgemeinen $\mathrm{tr}[\rho^2] \leq 1$. Dabei gilt die Gleichheit genau dann, wenn ρ ein reiner Zustand ist.

Bemerkung 1.1. Als Realisierung von Qubits bieten sich für die Quantenkryptographie Spin 1/2-Systeme an oder polarisierte Photonen. Dabei entspricht der Zustand $|0\rangle$ horizontaler Polarisierung und der Zustand $|1\rangle$ vertikaler Polarisierung. Hierbei ist auch die Bildung von Superpositionen besonders anschaulich. Zum Beispiel entsprechen dem Zustand $|0_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ gerade diagonal polarisierte Photonen. Ebenso können anstatt diagonal polarisierter Photonen auch links-/rechts-zirkular polarisierte Photonen betrachtet werden, indem man eine zusätzliche Phasenverschiebung zwischen den beiden Zuständen erzeugt.

Eine generalisierte Messung $\mathcal{M}$ mit Messergebnissen $a, b, \cdots \in \Omega$ wird durch eine Menge zugehöriger Messoperatoren $M_a, M_b, \ldots$ beschreiben. Diese Operatoren operieren auf dem Zustandsraum $\mathcal{H}$ und erfüllen die Vollständigkeitsrelation $\sum_{a\in\Omega} E_a = \mathbf{1}$ mit den zugehörigen Effekten $E_a = M_a^d agger M_a$.

Die Wahrscheinlichkeit, bei Messung von $|\psi\rangle$ das Messergebnis a zu erhalten, ist gegeben durch

$$p_\psi(a) = \langle\psi| E_a |\psi\rangle$$

Diese hängt konkret vom gemessenen Zustand $|\psi\rangle$ ab. Durch die Vollständigkeitsrelation ist gewährleistet, dass die Wahrscheinlichkeiten normiert sind, d.h. deren Summation über alle Ereignisse ist 1. Die Messung transformiert den Zustand $|\psi\rangle$ auf

$$|\psi'\rangle = \frac{M_a |\psi\rangle}{\sqrt{p_\psi(a)}}.$$

Für einen allgemeinen Zustand, gegeben durch die Dichtematrix ρ gilt

$$p_\rho(a) = \mathrm{tr}[E_a \rho]$$

und

$$\rho' = \frac{M_a \rho M_a^\dagger}{p_\rho(a)}.$$

Unter einer unscharfen Messung verstehen wir eine generalisierte Messung, beschrieben durch Operatoren $M_a, M_b, \ldots$, bei der alle Effekte $E_a = M_a^\dagger M_a$ kommutieren, d.h. es gilt $[E_a, E_b] = 0$ für alle $a, b \in \Omega$ [15].

Observablen auf dem $\mathcal{H}_2$ werden durch hermitesche 2×2-Matrizen beschrieben. Eine Basis für hermitesche 2×2-Matrizen bilden die Pauli-Matrizen σ_k zusammen mit der Einheitsmatrix. Die Pauli-Matrizen sind dabei gegeben durch

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.1}$$

Eine Observable A kann dann dargestellt werden durch

$$A = \frac{1}{2}\operatorname{tr}(A)\mathbf{1} + \frac{1}{2}\sum_{k=x,y,z} \operatorname{tr}(A\sigma_k)\sigma_k. \tag{1.2}$$

Der Erwartungswert eines Operators bezüglich eines zu messenden Zustands mit der Dichtematrix ρ ist gegeben durch

$$\langle A \rangle_\rho = \operatorname{tr}(\rho A).$$

Wir betrachten später Systeme aus mehreren Qubits. n Qubits bilden dabei einen Hilbertraum $\mathcal{H}^n$ der Dimension 2^n. Dieser ist das Tensorprodukt der Hilberträume $\mathcal{H}_2^{(i)}$ der einzelnen Qubits, also $\mathcal{H}^n = \mathcal{H}_2^{(1)} \otimes \cdots \otimes \mathcal{H}_2^{(n)}$. Man kann die Zustände $|\psi_i\rangle$ der einzelnen Hilberträume $\mathcal{H}_2^{(i)}$ zu einem Produktzustand

$$\left|\psi^{1\ldots n}\right\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle = |\psi_1, \ldots, \psi_n\rangle \tag{1.3}$$

zusammensetzen und erhält somit einen reinen Zustand in $\mathcal{H}^n$. Allerdings gilt die Umkehrung im Allgemeinen nicht. Dies wird im Abschnitt 1.2.4 über Verschränkung behandelt.

Hat man für jeden Hilbertraum $\mathcal{H}_2^{(i)}$ eine Basis $\{|j_i\rangle\}_j$ gegeben, erhält man als Basis von $\mathcal{H}^n$ die Menge der direkten Produkte der Einzel-Qubit-Basen. Man kann also einen Produktzustand $|\psi\rangle \in \mathcal{H}^n$ allgemein darstellen durch

$$|\psi\rangle = \sum_{j_1,\ldots,j_n} \alpha_{j_1\cdots j_n} |j_1, \ldots, j_n\rangle .$$

Analog zu den Produktzuständen erhält man auch Produktoperatoren

$$A = A_1 \otimes \cdots \otimes A_n$$

der einzelnen Operatoren A_i auf $\mathcal{H}_2^{(i)}$. Die Operatoren A_i operieren lokal auf dem $i-$ten Teilsystem. Der Produktoperator A setzt sich also aus lokalen Abbildungen zusammen.

Wir definieren für eine Sequenz $[s] = (s_1, \ldots, s_n)$ und einen Operator A auf $\mathcal{H}_2$ den Operator $A^{[s]} := A^{s_1} \otimes A^{s_2} \otimes \cdots \otimes A^{s_n}$ auf $\mathcal{H}^n$, wobei $A^0 = \mathbf{1}$ die Identitätsabbildung ist.

1.2.2 Blochdarstellung

Als nützliches Hilfsmittel erweist sich die Blochdarstellung von Qubits. Die reinen Zustände eines Qubits lassen sich als Punkte auf der Oberfläche einer Kugel, der sogenannten Blochkugel, im dreidimensionalen Raum darstellen. Dabei wird jedem Zustand $|\psi\rangle$ eindeutig ein Vektor $\mathbf{r}$ im $\mathbb{R}^3$ zugeordnet.

Wir definieren mit den Pauli-Matrizen (1.1) und den Einheitsvektoren $\mathbf{e_x}, \mathbf{e_y}, \mathbf{e_z}$ den Vektor $\sigma = \sigma_x \mathbf{e_x} + \sigma_y \mathbf{e_y} + \sigma_z \mathbf{e_z}$. Mit Gleichung (1.2) folgt dann für jedes hermitesche ρ mit $\mathrm{tr}(\rho) = 1$

$$\rho = \frac{1}{2}(\mathbf{1} + \mathbf{r}\sigma) \tag{1.4}$$

mit $\mathbf{r} = \mathrm{tr}(\rho\sigma)$ Dies gilt also insbesondere für jede Dichtematrix.

Beginnt man mit einem reinen Zustand $|\psi\rangle$ und formt Gleichung (1.4) um, erhält man die eindeutige Zuordnung

$$\mathbf{r} = \langle\psi| \sigma |\psi\rangle ,$$

welche jedem Zustand $|\psi\rangle$ einen Vektor $\mathbf{r}$, den *Blochvektor*, zuordnet.

Einen beliebigen Zustand $|\psi\rangle$ kann man mittels Polarkoordinaten darstellen in der Form

$$|\psi\rangle = \cos(\vartheta/2) |0\rangle + e^{i\varphi} \sin(\vartheta/2) |1\rangle . \tag{1.5}$$

Der zugehörige Blochvektor ist dann

$$\mathbf{r} = (\sin\vartheta\cos\varphi, \sin\vartheta\sin\varphi, \cos\psi),$$

also der entsprechende Vektor in Kugelkoordinaten. Damit haben wir eine einfache Relation zwischen $|\psi\rangle$ und $\mathbf{r}$, welche die Äquivalenz der beiden Darstellungen beschreibt.

Punkte im Inneren der Kugel entsprechen Qubits, die als Gemische vorliegen. Die kartesischen Koordinaten von $\mathbf{r}$ entsprechen dabei den Faktoren $\mathrm{tr}(\rho\sigma_k)$ in der Pauli-darstellung (1.2). Somit wird das totale Gemisch $\frac{1}{2}\mathbf{1}$ durch den Mittelpunkt der Kugel repräsentiert.

1.2.3 Parität

Die Parität eines Qubit-Zustands ist gegeben durch die Summe aller seiner Bits modulo 2, d.h. $|\psi_1\rangle = |0011\rangle$ hat Parität 0 und $|\psi_2\rangle = |0111\rangle$ hat Parität 1. Die Parität eines realen Zustands $|\psi\rangle$, gegeben durch ein polarisiertes Photon, ist definiert über die Messergebnisse einer Z-Messung. Die Parität $P(\psi)$ ist dann gegeben durch $\sigma_z(\psi) = (-1)^{P(\psi)}$. D.h. eine parallele Polarisation bzgl. der $z-$Achse ($\sigma_z(\psi) = 1$) entspricht der Parität 0 und eine antiparallele Polarisation ($\sigma_z(\psi) = -1$) der Parität 1.

1.2.4 Verschränkung

Das Qubit spielt in der Quanteninformationstheorie eine ähnliche Rolle wie das Bit in der klassischen Informationstheorie, es fungiert ebenfalls als Datenträger einer Informationseinheit. Zwischen Qubits und Bits besteht jedoch auch eine Relation. In n

Qubits lassen sich maximal n klassische Bits speichern und zuverlässig wieder extrahieren. Allerdings ist dabei nicht notwendigerweise jedes klassische Bit in genau einem Qubit gespeichert. Die Information steckt häufig in der Verschränkung der Zustände.

Verschränkung tritt nur in zusammengesetzen Quantensytemen auf. Wir betrachten hier nur den Spezialfall eines 2-Qubit-Systems, also einen Hilbertraum $\mathcal{H}^{AB} = \mathcal{H}_2^A \otimes \mathcal{H}_2^B$. Liegt im System A sowie im System B jeweils ein reiner Zustand $|\psi_A\rangle$ bzw. $|\psi_B\rangle$ vor, dann ist der Zustand des zusammengesetzten Systems ebenfalls ein reiner Zustand und gegeben durch die Produktdarstellung

$$|\psi_A\rangle \otimes |\psi_B\rangle \,. \tag{1.6}$$

Reine Zustände, welche sich in einer solchen Produktdarstellung schreiben lassen, nennt man *separabel*.

Einen allgemeinen Zustand $\sum_{i,j} c_{ij} |i_A\rangle |j_B\rangle$ auf $\mathcal{H}^{AB}$, welcher nicht wie in (1.6) faktorisiert werden kann, heißt *verschränkt*.

Beispielsweise erhält man, dass sich die vier Zustände

$$|\phi_\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \qquad \text{und} \qquad |\Psi_\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{1.7}$$

nicht faktorisieren lassen und somit verschränkt sind. Diese vier Zustände bilden sogar eine Basis des $\mathcal{H}^{AB} = \mathcal{H}^2$, die sogenannte *Bell-Basis*.

Wir identifizieren die vier Bellzustände $|\phi_\pm\rangle, |\Psi_\pm\rangle$ jeweils durch zwei logische klassische Bits, indem wir jedem Bellzustand je ein Phasen- und ein Paritätsbit nach nebenstehender Tabelle zuordnen. Das rechte Bit beschreibt dabei die Parität, also die Ausrichtung der Spins oder Polarisationsrichtungen zueinander (parallel, antiparallel), das linke Bit beschreibt die lokale Phase (± 1) zwischen den Zuständen.

Bell-Zustand	log. Bits
ϕ^+	00
ϕ^-	10
Ψ^+	01
Ψ^-	11

1.2.5 Treue als Verschränkungsmaß

Um zwei Zustände miteinander vergleichen zu können, braucht man so etwas wie ein Abstandsmaß, welches angibt, wie „nah“ sich zwei Zustände sind. Dabei gibt es verschiedene Möglichkeiten. Wir nutzen hier die Größe der *Treue* F (fidelity). Diese ist für zwei beliebige Zustände, welche durch ihre Dichtematrizen ρ und σ gegeben sind, definiert durch [14]

$$F(\rho, \sigma) = \mathrm{tr}(\sqrt{\rho^{1/2}\sigma\rho^{1/2}}). \tag{1.8}$$

Weiter gilt $0 \leq F(\rho, \sigma) \leq 1$, wobei $F(\rho, \sigma) = 1$ genau dann gilt, wenn $\rho = \sigma$ ist.

1.2.6 Quantenzustandstomographie

Die Quantenzustandstomographie befasst sich mit dem Problem einen unbekannten Quantenzustand experimentell zu ermitteln. Hat man viele gleich präparierte Qubits (Kopien), so kann man durch Messung geeigneter Observablen den Quantenzustand bestimmen. Dazu misst man üblicherweise

$$\frac{\mathbf{1}}{\sqrt{2}}, \frac{X}{\sqrt{2}}, \frac{Y}{\sqrt{2}} \text{ und } \frac{Z}{\sqrt{2}}.$$

Die Dichtematrix des unbekannten Qubit-Zustands ergibt sich dann mit Gleichung (1.2) als

$$\rho = \frac{1}{2}(\mathrm{tr}[\rho]\mathbf{1} + \mathrm{tr}[\rho X]X + \mathrm{tr}[\rho Y]Y + \mathrm{tr}[\rho Z]Z). \tag{1.9}$$

Dabei gilt wieder $\mathrm{tr}[\rho A] = \langle A \rangle_\rho$. Man bestimmt also einen Zustand durch Bestimmung der Erwartungswerte eines geeigneten Satzes von Observablen. Für ein endliches System aus n Kopien kann man die Wahrscheinlichkeiten nicht exakt bestimmen und erhält nur relative Häufigkeiten $h(A, n)$. Dabei liegt nach dem schwachen Gesetz der großen Zahl 1.6 eine Standardabweichung von $\sim \frac{1}{\sqrt{n}}$ vor und man erhält eine fehlerbehaftete Zustandsschätzung.

1.3 Charakteristische Eigenschaften eines Quantensystems

Die folgenden drei Eigenschaften bilden die Basis eines jeden QKD-Protokolls. Sie gelten jeweils für nicht-orthogonale Zustände.

- Man kann durch eine einzelne Messung nicht eindeutig zwischen zwei nicht-orthogonalen Zuständen unterscheiden.
- Man kann einen unbekannten Zustand nicht exakt kopieren.
- Man kann keine Informationen über den Zustand eines Systems erlangen, ohne diesen zu verändern.

Orthogonale Zustände können als klassische Zustände interpretiert werden und die Eigenschaften verlieren ihre Gültigkeit. Im folgenden werden wir diese Eigenschaften beweisen [14].

Satz 1.2. *Man kann durch eine Messung nicht eindeutig zwischen zwei nichtorthogonalen Zuständen unterscheiden.*

Beweis. [14, S.87] Angenommen, eine solche Messung existiert. Diese wird dann dargestellt durch einen Satz Messoperatoren M_i und eine Strategie f, welche jedem Messergebnis j einen Zustand $|\psi_i\rangle$ zuordnet.

Liegt der Zustand $|\psi_1\rangle$ vor, dann gilt für diese Messung $p(j : f(j) = 1) = 1$, d.h. die Wahrscheinlichkeit, dass bei der Messung ein Messergebnis j auftritt, welches der Strategie zufolge auf den Zustand $|\psi_1\rangle$ schließen lässt, tritt in jedem Fall ein.

Wir setzen nun $E_i := \sum_{j:f(j)=i} M_j^\dagger M_j$. Dann gilt

$$\langle\psi_1| E_1 |\psi_1\rangle = 1 \quad \text{und} \quad \langle\psi_2| E_2 |\psi_2\rangle = 1. \tag{1.10}$$

Aus der Normiertheit der E_i folgt dann weiter $\langle\psi_1| E_2 |\psi_1\rangle = 0$, also $\sqrt{E_2}\,|\psi_1\rangle = 0$. Wir zerlegen $|\psi_2\rangle$ in den Anteil parallel und den Anteil senkrecht zu $|\psi_1\rangle$, also

$$|\psi_2\rangle = \alpha\,|\psi_1\rangle + \beta\,|\varphi\rangle$$

mit $\langle\psi_1|\,\varphi\rangle = 0$, $|\alpha|^2 + |\beta|^2 = 1$. Hierfür gilt $\beta < 1$, da $|\psi_1\rangle$ und $|\psi_2\rangle$ nicht orthogonal zueinander sind. Damit folgt dann $\sqrt{E_2}\,|\psi_2\rangle = \beta\sqrt{E_2}\,|\varphi\rangle$ und weiter

$$\langle\psi_2| E_2 |\psi_2\rangle = |\beta|^2 \langle\varphi| E_2 |\varphi\rangle \leq |\beta|^2 \sum_i \langle\varphi| E_i |\varphi\rangle = |\beta|^2 \langle\varphi|\,\varphi\rangle = |\beta|^2 < 1 \tag{1.11}$$

im Widerspruch zu (1.10). □

Diese Eigenschaft macht es für Eve unmöglich, das Signal abzufangen, zu messen und erneut exakt zu präparieren. Eve präpariert mit einer gewissen Wahrscheinlichkeit einen falschen Zustand, wodurch sie dann potentiell entdeckt werden kann.

Satz 1.3. *Man kann einen unbekannten Zustand nicht exakt kopieren.*

Beweis. [14, S.532] Angenommen, es existiert ein Apparat, welcher $|\psi\rangle\,|s\rangle$ bestehend aus einem beliebigen, unbekannten Zustand $|\psi\rangle$ und einen reinen Zustand $|s\rangle$ durch eine unitäre Transformation U abbildet auf $|\psi\rangle\,|\psi\rangle$. Dann gilt für zwei reine Zustände $|\psi\rangle$ und $|\varphi\rangle$:

$$U(|\psi\rangle\,|s\rangle) = |\psi\rangle\,|\psi\rangle \quad \text{und} \quad U(|\varphi\rangle\,|s\rangle) = |\varphi\rangle\,|\varphi\rangle$$

und damit

$$\begin{aligned}\langle\psi|\varphi\rangle^2 &= \langle\psi|\,\varphi\rangle\,\langle\psi|\,\varphi\rangle = \langle\psi|\,\langle\psi|\,\varphi\rangle\,|\varphi\rangle \\ &= \langle s|\,\langle\psi|\,U^\dagger U\,|\varphi\rangle\,|s\rangle = \langle s|\,\langle\psi|\,\varphi\rangle\,|s\rangle \\ &= \langle\psi|\,\varphi\rangle\,\langle s|\,s\rangle = \langle\psi|\,\varphi\rangle\end{aligned} \tag{1.12}$$

Sind nun $|\psi\rangle$ und $|\varphi\rangle$ nicht orthogonal, folgt aus der Normiertheit und Gleichung (1.12) schon $|\psi\rangle = |\varphi\rangle$. Da im Allgemeinen die Orthogonalität zwischen verschiedenen Zuständen nicht gegeben ist, folgt die Behauptung. □

Somit ist es einem Lauscher nicht möglich, Kopien eines abgehörten Systems zu erstellen und diese separat zu messen. Weiter erhält man hiermit, dass es bei Verwendung nichtorthogonaler Zustände $|\psi\rangle$ und $|\varphi\rangle$ nicht möglich ist, Informationen über diese Zustände zu erhalten, ohne das System zu stören, wie der folgende Satz zeigt.

Satz 1.4. *Es ist im Allgemeinen nicht möglich, Informationen über den Zustand eines System zu erlangen, ohne diesen zu verändern.*

Beweis. Wir betrachten ein Signal bestehend aus einem Produkt zweier nicht-orthogonaler Zustände $|\psi\rangle$ und $|\varphi\rangle$.

Nach 1.3 kann das Signal nicht kopiert werden. Um Informationen über den Zustand des Systems zu erhalten, müssen wir an diesem eine Messung durchführen. Diese kann man im Allgemeinen dadurch ausdrücken, dass man das System mit einem Hilfssystem S erweitert, am Gesamtsystem eine unitäre Transformation ausführt und am Hilfssytem ein Projektionsmessung durchführt [14, S.93f].

Angenommen, es existiert eine unitäre Transformation U, welche die Signalzustände unverändert lässt, das heißt, welche den Zustand $|\psi\rangle\,|s\rangle$ auf den Zustand $|\psi\rangle\,|s_\psi\rangle$ abbildet und den Zustand $|\varphi\rangle\,|s\rangle$ auf $|\varphi\rangle\,|s_\varphi\rangle$. Die Zustände $|s_\psi\rangle$ und $|s_\varphi\rangle$ des Hilfssystems werden projektiv gemessen.

Analog zum no-cloning Theorem 1.3 erhalten wir dann

$$\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle\langle s_\psi|s_\varphi\rangle$$

und damit $|s_\psi\rangle = |s_\varphi\rangle$. Die Zustände des Hilfssystems sind also nicht unterscheidbar. Damit existiert keine Messung, welche zwischen $|\varphi\rangle$ und $|\psi\rangle$ unterscheiden kann, ohne diese zu verändern. □

Somit ist jeder Versuch von Eve, das System abzuhören mit einer Störung des Systems verbunden, wodurch sie potentiell entdeckt werden kann.

Um die Wahrscheinlichkeit, dass Eve entdeckt wird, möglichst groß zu machen, nutzen wir später komplementäre Basen. Dieses sind die Basen der Eigenräume zu komplementären Observablen, d.h. die Kenntnis des Wertes der einen Observablen bedingt die vollständige Unkenntnis der anderen. Zueinander komplementäre Observablen werden durch zueinander orthogonale Richtungen in der Bloch-Sphäre beschrieben. Damit ist sofort ersichtlich, dass beispielsweise die z- und die x-Basis komplementär sind.

1.4 Mathematische Hilfsmittel

1.4.1 Einiges aus der Wahrscheinlichkeitstheorie

Die Quantentheorie arbeitet mit Wahrscheinlichkeitsaussagen. Die in dieser Arbeit benötigten stochastischen Grundlagen und Sätze sollen hier aufgeführt werden.

Grundlage der Wahrscheinlichkeitstheorie ist das Konzept der Zufallsvariablen. Eine Zufallsvariable X ist eine Funktion, welche jedem Ereignis $\omega_i \in \Omega$ eines Zufallsexperiments (z.B. einer Messung einer Observablen) einen Wert x_i zuordnet. Ist der Wahrscheinlichkeitsraum Ω diskret, besteht er also nur aus abzählbar vielen Ereignissen, so ist X eine diskrete Zufallsvariable. Für unsere Anwendungen genügt es, nur diskrete Zufallsvariablen zu betrachten.

Es ist allerdings im Allgemeinen nicht das konkrete Ereignis ω_i von Interesse, sondern nur der zugehörige Wert x_i (z.B. das Messergebnis) und die Häufigkeit, mit der das Ergebnis x_i auftritt. Eine Zufallsvariable ist also charakterisiert durch Angabe der Werte x_i und der zugehörigen Wahrscheinlichkeiten $p(x_i)$.

Indem wir einem Wert x_i eine Präparation in $|\psi_i\rangle$, welcher bei Messung der entsprechenden Observablen den Messwert x_i liefert, zuordnen, können wir auch unsere Signalquelle mathematisch durch eine Zufallsvariable ausdrücken, welche die „Werte“ $|\psi_i\rangle$ mit der Wahrscheinlichkeit $p(|\psi_i\rangle)$ ausgibt.

Somit können wir Methoden und Ergebnisse der klassischen Wahrscheinlichkeitstheorie nutzen.

Ein wichtiges Hilfsmittel ist der Satz von Bayes [16], welcher eine Beziehung zwischen a-priori und a-posteriori Wahrscheinlichkeiten herstellt.

Satz 1.5 (Bayes)**.** *Für zwei Ereignisse A und B gilt*

$$p(A|B) = \frac{p(B|A)p(A)}{p(B)}.$$

Hat man ein endliches System vorliegen, so kann man durch n Messungen nur die relativen Häufigkeiten $h(x_i, n)$ der Messergebnisse x_i bestimmen. Die relative Häufigkeit $h(x_i, n)$ ist dabei gegeben durch die Anzahl der aufgetretenen Ereignisse x_i dividiert durch n, die Anzahl aller aufgetretenen Ereignisse. Dass sich diese jedoch den exakten Wahrscheinlichkeiten $p(x_i)$ für große n sinnvoll nähern, liefert uns das Gesetz der großen Zahl. Zudem erhalten wir hierdurch eine Abschätzung, wie weit der geschätzte Wert vom tatsächlichen Wert entfernt ist. Dabei bezeichnet $E(X) = \sum_i p(x_i)x_i$ den Erwartungswert und $\mathrm{Var}(X) = E(X^2) - E(X)^2 = (\Delta X)^2$ die Varianz einer Zufallsvariablen X.

Satz 1.6 (schwaches Gesetz der großen Zahl [16])**.** *Für unabhängige, quadratintegrable Zufallsvariablen $X_1, X_2, \ldots$ und für jedes $\varepsilon > 0$ gilt für alle $n \in \mathbb{N}$*

$$P(|\frac{1}{n}\sum_{i=1}^{n}(X_i - E(X_i))| \geq \varepsilon) \leq \frac{1}{\varepsilon^2 n^2}\sum_{i=1}^{n} Var(X_i).$$

Hiervon benötigen wir den Spezialfall von binomial-gleichverteilten, unabhängigen Zufallsvariablen X_i. Die Binomialverteilung beschreibt die Verteilung der möglichen Ereignisse bei n gleichen Zufallsexperimenten, wobei jeweils genau zwei Ergebnisse möglich sind. In unserem Fall beschreibt sie die Häufigkeit eines bestimmten Messergebnisses x bei n unabhängigen Messungen von gleich präparierten Zuständen. Sei die Messwahrscheinlichkeit gegeben durch p. Dann ist die Wahrscheinlichkeit, dass genau k mal dieser Messwert auftritt, gegeben durch

$$p(h(x, n) = k/n) = \binom{n}{k} p^k (1-p)^{n-k}.$$

Der Erwartungswert der relativen Häufigkeit ist $E(h) = np/n = p$ und die Varianz $\sigma^2 = np(1-p)/n^2 = p(1-p)/n$.

Es ist also $E(X_i) = p$ und $\mathrm{Var}(X_i) = p(1-p)$ für jedes i. Hiermit folgt dann für die relative Häufigkeit $h(A,n)$ eines Ereignisses A bei n Messungen:

$$P(|h(A,n) - p(A)| \geq \varepsilon) = P(|\frac{1}{n}\sum_{i=1}^{n}(X_i - E(X_i))| \geq \varepsilon) \leq \frac{1}{\varepsilon^2 n}p(1-p). \tag{1.13}$$

Für endliche Ensemble müssen wir daher auf die Testtheorie zurückgreifen [17]. In der Testtheorie geht es darum anhand einer endlichen Stichprobe eine Hypothese bezüglich der Gesamtheit zu testen. Die Hypothese besteht dabei aus einer Aussage über die Wahrscheinlichkeitsverteilung der Gesamtheit, sie kann zum Beispiel aus einer Wahrscheinlichkeit, einem Mittelwert oder einer Varianz bestehen. In dieser Arbeit besteht die verwendete Hypothese aus einer Wahrscheinlichkeit, welche an einem endlichen Ensemble verifiziert werden soll. Desweiteren betrachten wir nur eine einseitige Probe, d.h. wir testen die Hypothese $p = p_0$ auf die Alternative $p < p_0$. Das Testen der Hypothese läuft dabei wie folgt ab. Mit der Hypothese $p = p_0$ und bekannter Stichprobenzahl N ermitteln wir das sogenannte Konfidenzintervall, in dem die Hypothese angenommen wird. Bei der Festlegung des Konfidenzintervalls legen wir eine obere Schranke für einen erlaubten Fehler erster Art zugrunde. Ein Fehler erster Art tritt ein, wenn wir die Hypothese verwerfen, obwohl sie richtig ist. Die Wahrscheinlichkeit für einen Fehler erster Art wird mit der Konfidenzzahl α bezeichnet. Daneben tritt im Allgemeinen auch ein Fehler zweiter Art auf. Dieser Fehler besteht darin, dass wir die Hypothese annehmen, obwohl sie falsch ist. Diese Wahrscheinlichkeit wird mit $1-\beta$ bezeichnet. Ziel ist es, beide Fehler zu minimieren. Da diese Fehler miteinander korreliert sind, muss man stets einen Kompromiss finden. Die praktische Vorgehensweise besteht darin, dass man zunächst die untere Grenze c des Konfidenzintervalls festlegt. Gilt für die ermittelte relative Häufigkeit $h(x,n) > c$, so wird die Hypothese angenommen, ist $h(x,n) \leq c$, so wird die Hypothese verworfen und die Alternativhypothese angenommen.

Diese Grenze ermittelt man aus der Bedingung, dass die ermittelte relative Häufigkeit $h(x,n)$ bei einer Stichprobengröße von n mit der Wahrscheinlichkeit α außerhalb des Konfidenzintervalls liegt, wenn die Hypothese richtig ist. Dieses lässt sich mahematisch formulieren in der Form

$$P(h(x,n) \leq c)_{p_0} = \alpha. \tag{1.14}$$

Die Größe c ergibt sich dann aus den tabellierten Werten [17] der gaußschen Φ-Funktion unter Benutzung der Relation

$$P(h(x,n) \leq c) = \Phi\left(\frac{c - h(x,n)}{\sigma}\right)$$

mit der Varianz $\sigma = \sqrt{p_0(1-p_0)}/\sqrt{n}$. Das Argument $\frac{c-h(x,n)}{\sigma}$ von ϕ wird dann als $(1-\alpha/2)$-Fehlerquantil $u_{1-\alpha/2}$ bezeichnet. Es gilt also $\phi(u_{1-\alpha/2}) = \alpha$. Hiermit kann

man dann anschließend die Wahrscheinlichkeit β für einen Fehler zweiter Art berechnen, indem man entsprechend zu Gleichung (1.14) die Wahrscheinlichkeit $P(h(x,n) > c)_{p'}$ unter Annahme der Alternativhypothese $p = p'$ berechnet. Liegt der Fehler 2. Art ebenfalls unterhalb der festgelegten oberen Schranke, so wird der Stichprobenumfang akzeptiert. Andernfalls erhöht man den Umfang der Stichprobe.

1.4.2 Entropie und Information

Eine wichtige Größe über den Informationsgehalt einer Nachricht ist die Entropie. Dabei unterscheidet man je nach Anwendung zwischen verschiedenen Größen, welche auf Entropieberechungen basieren. Einige von ihnen sollen im Hinblick auf spätere Anwendungen hier kurz erläutert werden. Dabei orentieren wir uns an [14].

Generell unterscheidet man zwischen klassischer und quantentheoretischer Information. Hierbei bestehen wesentliche Unterschiede. Klassische Information ist immer komplett auslesbar. Andererseits kann sie auch kopiert werden. Quanteninformation beschreibt die Information, die durch einen Zustand ρ repräsentiert wird. Sie ist nicht direkt ablesbar und muss durch Messung in klassische Information umgewandelt werden.

Die Shannon-Entropie $H(X)$ einer Zufallsvariablen X ist das Basiskonzept der Informationstheorie. Sie ist ein Maß für die mittlere klassische Information eines Signals, die wir aus einem Wert x von X erhalten. Wenn die Entropie pro Bit einen Wert von 1 hat, dann ist X zufällig verteilt, d.h. wir wissen überhaupt nichts über den Informationstext außer genau diesem einen Wert. Bei einer kleineren Entropie enthält der Informationstext Redundanzen oder statistische Regelmäßigkeiten und wir können aus einem Teil des Textes eventuell auf den ganzen Text schließen. Bei Entropie Null besitzen wir mit x die volle Information über X. Die Entropie kann man also auch auffassen als Maß dafür, wie viel von einem Bit im Durchschnitt fehlt, um auf die komplette Nachricht zu schließen. Daher ist es in der Kryptographie wünschenswert, die Entropie für einen Lauscher möglichst groß zu gestalten.

Mathematisch ist sie charakterisiert durch die Wahrscheinlichkeiten $p(x)$ der verschiedenen Werte x von X.

Definition 1.7. Die *Shannon-Entropie* einer Zufallsvariable X mit Werten x und Wahrscheinlichkeiten $p(x)$ ist gegeben durch

$$H(X) = -\sum_x p(x) \log p(x). \tag{1.15}$$

Diese kann man rekursiv in natürlicher Weise auf mehrere Zufallsgrößen verallgemeinern durch

$$H(X,Y) = -\sum_{x,y} p(x,y) \log p(x,y).$$

Als Beispiel betrachten wir die Shannon-Entropie für ein Zwei-Zustands-System mit den Basiszuständen 0 und 1. Die Nachricht bestehe aus einer Folge aus Nullen und Einsen, wobei mit der Wahrscheinlichkeit p an einer festen Stelle eine Null auftritt und mit Wahrscheinlichkeit $1-p$ eine Eins. Die Shannon-Entropie ist dann abhängig von p und hat einen Verlauf nach nebenstehender Abbildung 1.1. Sie wird maximal für $p = 1/2$ also in dem Punkt mit dem größten Unwissen.

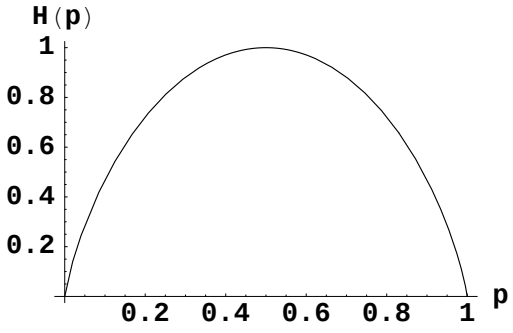


Abbildung 1.1: Entropieverlauf $H(p)$ eines Zwei-Zustands-Systems

Sind wir an der quantentheoretischen Information eines Zustandes interessiert, so betrachten wir die *von-Neumann Entropie* $S(\rho)$ für die Dichtematrix $\rho = \sum_x \lambda_k |\psi_k\rangle \langle\psi_k|$ mit den Eigenwerten λ_k, so gilt:

$$S(\rho) := -\operatorname{tr}[\rho \log \rho] = -\sum_k \lambda_k \log \lambda_k. \tag{1.16}$$

Daneben gibt es noch weitere Größen, die für uns von Belang sind, da sie sich auf zwei Zufallsgrößen X und Y und ihr Verhältnis zueinander beziehen. Da wir letztendlich nur an der klassischen Information interessiert sind, werden die folgenden Größen hier nur für die Shannon-Entropie definiert, gelten aber entsprechend für die von-Neumann Entropie.

Definition 1.8. Die *bedingte Entropie* $H(X|Y)$ ist gegeben durch

$$\begin{aligned} H(X|Y) &= H(X,Y) - H(Y) \\ &= \sum_y p(y) \log p(y) - \sum_{x,y} p(x,y) \log p(x,y) \\ &= \sum_{x,y} p(x,y) \log p(x|y) \end{aligned} \tag{1.17}$$

und beschreibt die mittlere Information über X bei Kenntnis von Y.

Ist $H(X|Y)$ groß, so weiß man wenig über X, wenn man Y kennt, d.h. Eve kennt mit Y, welches sie z.B. durch eine öffentliche Nachricht von Alice an Bob erfährt, höchstens $H(X|Y)$ über X. Damit ist klar, dass wir auch diesen Wert möglichst maximieren wollen.

Beispiel 1.9. Wir betrachten X mit Werten $\psi_i \in \{|00\rangle, |10\rangle, |01\rangle, |11\rangle\}$ als ein gleichverteiltes System aus zwei Qubits, d.h. jeder der vier Zustände in X tritt mit gleicher Wahrscheinlichkeit auf. Dann ist die Shannon-Entropie von X gegeben durch

$$H(X) = -4\frac{1}{4}\log\frac{1}{4} = \log 4 = 2.$$

Anschaulich gesprochen, muss man also zwei Bits geschickt bekommen, um den Zustand und damit die Nachricht zu kennen. Wir betrachten zunächst als Zufallsvariable Y_1 die Menge $\{|0\rangle, |1\rangle\}$ mit $p(|0\rangle) = p(|1\rangle) = \frac{1}{2}$. Dies entspricht der Dichtematrix $\rho = \frac{1}{2}\mathbf{1}$ und beschreibt den Zustand des ersten Qubits. Die Shannon-Entropie von Y_1 ist $H(Y_1) = 2\frac{1}{2}\log\frac{1}{2} = 1$. Wieviel Information gewinnen wir nun dadurch, dass wir wissen, dass das erste Qubit eines uns unbekannten 2-Qubit-Systems entweder der Zustand $|0\rangle$ oder $|1\rangle$ ist? Dieses ist durch die bedingte Entropie gegeben und berechnet sich zu

$$\begin{aligned} H(X|Y_1) = H(X,Y_1) - H(Y_1) &= -\frac{1}{2}\log\frac{1}{2} - \frac{2}{4}\log\frac{1}{4} - \frac{1}{2}\log\frac{1}{2} - \frac{2}{4}\log\frac{1}{4} - 1 \\ &= \log 2 + \log 4 - 1 = 2 = H(X). \end{aligned}$$

Wir erhalten also, wie zu erwarten war, hierdurch keine neue Information. Ist uns allerdings der erste Qubitzustand bekannt (z.B. $|0\rangle$), sieht das Ganze anders aus. Wir setzen ohne Einschränkung $Y_2 = \{|0\rangle, |1\rangle\}$ mit $p(|0\rangle) = 1, p(|1\rangle) = 0$, dann ist $H(Y_2) = -1\log 1 - 0\log 0 = 0$, da der Zustand eindeutig festliegt und wir jegliche Information besitzen. Die bedingte Entropie ist dann

$$H(X|Y_2) = -\frac{1}{2}\log\frac{1}{2} - \frac{1}{2}\log\frac{1}{2} = \log 2 = 1.$$

Damit haben wir unser Unwissen halbiert, uns fehlt nun im Durchschnitt 1 Bit, um den endgültigen Zustand zu kennen (nämlich gerade das zweite Bit).

Eine weitere Kenngröße ist die Korrelationsentropie (collision entropy). Sie beschreibt die Wahrscheinlichkeit, dass zwei unabhängige Realisierungen einer Zufallsvariablen total korreliert sind und genau die gleiche Nachricht entsteht. Sie ist wichtig im Zusammenhang der Verschwiegenheitsverstärkung, welche wir später behandeln werden.

Definition 1.10. Die *Korrelationsentropie* einer Zufallsvariablen X ist definiert als

$$H_c(X) = -\log\left(\sum_x p(x)^2\right). \tag{1.18}$$

Die wesentliche Größe in Bezug auf das Wissen eines Lauschers ist die wechselseitige Information (mutual information):

Definition 1.11. Die *wechselseitige Information* $H(X:Y)$ von X und Y ist definiert als

$$H(X:Y) = H(X) - H(X|Y) = H(X) + H(Y) - H(X,Y) \tag{1.19}$$

und ist ein Maß für die Information, die X und Y gemeinsam haben.

Diese Größe sollte im Hinblick auf einen Lauschangriff möglichst klein werden, so dass der Lauscher möglichst wenig Information über X bei Kenntnis von Y erhält. Die wechselseitige Information zwischen Alice und Bob soll dagegen möglichst groß werden, so dass eine hohe Korrelation zwischen ihnen besteht.

Mit Abbildung 1.2 ist klar, dass die wechselseitige Information symmetrisch ist, dass also $H(X:Y) = H(Y:X)$ gilt.

Mit $0 \leq H(X|Y) \leq H(X)$ folgt sofort $0 \leq H(X:Y) \leq H(Y)$.

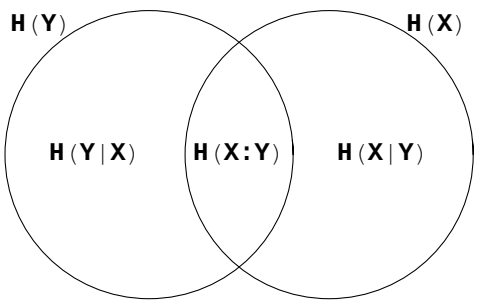


Abbildung 1.2: Veranschaulichung der Beziehungen zwischen Entropie und wechselseitiger Information

Im Falle des obigen Beispiels 1.9 ergibt sich für die wechselseitige Information $H(X : Y_1) = 0$ und $H(X : Y_2) = 1$. Die beiden Zufallsvariablen X und Y_1 haben also keinerlei Information gemeinsam, X und Y_2 dagegen genau 1 Bit an Information, nämlich das erste Bit.

Die wechselseitige Information ist in der Quantenkryptographie eine bedeutende Größe, da sie Aussagen über die Sicherheit eines Protokolls erlaubt. Ein nützliches Hilfsmittel ist der 1978 von Csiszár und Körner gezeigte Satz 1.12 [18]. Die im Satz verwendeten Verfahren der Fehlerkorrektur und Verschwiegenheitsverstärkung entstammen der klassischen Kryptographie und werden im Abschnitt 2.1 erläutert. Der Übersichtlichkeit halber bezeichnen wir die Zufallsvariable von Alice mit A, von Bob mit B und von Eve mit E.

Satz 1.12 (Csiszár, Körner)**.** *Für gegebene Zufallsvariablen A, B und E können Alice und Bob genau dann aus A und B einen sicheren Schlüssel mittels Fehlerkorrektur und klassischer Verschwiegenheitsverstärkung erzeugen, wenn für die wechselseitige Information gilt:*

$$H(A:B) > \min\{H(A:E), H(B:E)\}.$$

Wir müssen also bei der Sicherheitsbetrachtung prüfen, ob die wechselseitige Information zwischen Alice und Bob stets größer ist als die bezüglich Eve.

Wir können außerdem mit der folgenden Holevo-Schranke die wechselseitige Information mit Hilfe der von-Neumann Entropie abschätzen. Dabei ist ρ_X eine Abkürzung für alle bezüglich einer Zufallsvariablen X möglichen präparierbaren Dichtematrizen ρ_x mit $x \in X$.

Proposition 1.13. *Sei X eine Zufallsvariable zum Zustand ρ_X und Y die Zufallsvariable, welche ein Messergebnis von ρ_X beschreibt. Dann gilt für jede solche Messung Y*

$$H(X:Y) \leq S(\rho) - \sum_x p(x) S(\rho_x) \leq S(\rho),$$

wobei $\rho = \sum_x p(x)\rho_x$ gilt.

1.5 Abhörstrategien

Ein QKD-Protkoll benötigt im Allgemeinen klassische Kommunikation, da Bob ohne Informationsaustausch nicht feststellen kann, ob Eve das Signal abgehört hat. Eve befindet sich dann außerdem bei einem Ein-Weg-Protokoll in einer symmetrischen Position zu Bob und kann in gleicher Weise wie er ihre Messergebnisse auswerten. Ein präparierter Zustand ohne Information erscheint immer wie ein totales Gemisch, aus dem man keine Informationen erhalten kann. Der Austausch der klassischen Information sorgt für die Korrelation zwischen Alice und Bob. Nun ist es natürlich möglich, den klassischen Kommunikationskanal abzuhören. Dabei gehen wir davon aus, dass der Lauscher dabei nicht entdeckt wird. Sonst könnten wir gleich mit rein klassischen Methoden arbeiten.

Der Lauscher kann aber auch eine sogenannte 'man in the middle'-Position einnehmen, die Nachricht abhören und verändern, so dass wir keinen sicheren klassischen Kommunikationskanal mehr haben. Wir wissen dann nicht mehr, ob die erhaltene Nachricht tatsächlich von Alice stammt. Dadurch wird unser Protokoll zerstört. Man kann aber über klassische Authentifizierungsverfahren dieses Problem beheben, so dass wir davon ausgehen können, dass Eve den klassischen Kanal nur passiv abhört. Da eine klassische Nachricht übermittelt wird, ändert sich die Nachricht durch das Abhören von Eve nicht. Wir gehen also von folgender Situation aus [1].

Eve hat auf den Quantenkanal zwischen Alice und Bob vollen Zugriff, wobei sie jedoch bei ihrem Lauschangriff die Rückkopplung ihrer Messung mit dem System beachten muss. Auf den klassichen Kanal hat sie nur passiven Zugriff und kann diesen nur abhören, jedoch nichts verändern. Dieses ist noch einmal in der folgenden Abbildung veranschaulicht.

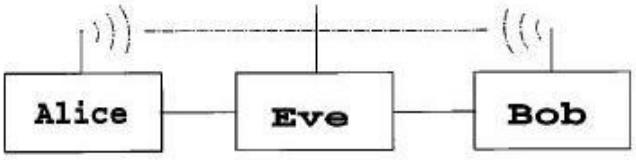


Abbildung 1.3: Schematische Veranschaulichung des betrachteten Lauschangriffs [1]

Einen Lauschangriff von Eve auf den Quantenkanal kann man allgemein so ausdrücken, dass sie das Signal mit einem ihr bekannten Zustand eines Hilfssystems verschränkt und ihren Zustand später misst, um an die Information zu gelangen. Ihre Messung entspricht dabei einer unitären Transformation auf dem Gesamtsystem [14, S.93f]. Dabei gibt es im idealisierten System die folgenden Möglichkeiten [3].

individuelle Attacke Eve misst jeweils nur ein Qubit oder verschränkt jedes Qubit mit einem eigenen Hilfssystem und misst diese einzeln zu einem beliebigen Zeitpunkt.

kollektive Attacke Eve verschränkt jedes Signal mit einem eigenen Hilfssystem, kann aber zu einem beliebigen Zeitpunkt alle Hilfssysteme kollektiv messen

kohärente Attacke Eve hat zeitgleichen Zugriff auf alle übermittelten Signale (z.B. durch einen Speicherprozess), welche sie dann mit einem einzigen Hilfssytem verschränkt und dieses dann misst. Dadurch kann sie sowohl Informationen über die Korrelationen zwischen den einzelnen Signalen erhalten als auch Korrelationen in das System integrieren.

Diese Attacken sind sogenannte *intercept/resend*-Attacken. Eve unterbricht hierbei den Quantankanal, führt ihren Angriff bzw. die Verschränkung mit ihrem System durch und schickt die abgefangenen Qubits anschließend weiter. Die Betrachtung dieser Angriffe reicht für die theoretische Sicherheitsbetrachtung aus [3].

Bei heutzutage realisierten Protokollen sind weitere Angriffsstrategien möglich, welche die nicht perfekten Eigenschaften der verwendeten Bauteile nutzen. Diese werden später kurz im Abschnitt 3 über Realisierungsmöglichkeiten der Protokolle behandelt.

1.6 Sicherheit

Die Sicherheit eines Protokolls ist über die Beschränkung der wechselseitigen Information von Eve gegeben. Dabei sind verschiedene Ansätze möglich. Allerdings sind nicht alle sinnvoll.

Es ist naheliegend zu verlangen, dass für die wechselseitige Information von Eve $H(S : E) < \delta N$ bei einer Schlüssellänge von N Bits gilt. Diese Schranke ist aber zu schwach, da Eve hierbei immer ein paar Bits der Nachricht ($\approx \delta N$) ermitteln kann, ohne entdeckt zu werden. Hat sie zusätzlich noch Informationen über die Struktur der zu verschlüsselnden Nachricht, so kann sie unter Umständen gerade die für sie wichtigen Bits entschlüsseln, vgl. [7, Ref. 16.] oder [10].

Fordert man dagegen $H(S : E) < e^{-\alpha N}$ für jeden Lauschangriff, so hat man eine zu starke Forderung, welche niemals realisiert werden kann. Nehmen wir an, Eve ersetzt alle Qubits von Alice durch eigene. Dann besteht nur eine sehr geringe Wahrscheinlichkeit, dass sie nicht entdeckt wird. In diesem unwahrscheinlichen Fall aber besitzt sie die volle Information über den Schlüssel und verletzt somit die geforderte Ungleichung.

Die folgende Definition der Sicherheit eines Protokolls wird heutzutage allgemein verwendet. Dabei wird neben einer realistischen Schranke für die wechselseitige Information auch noch eine gewisse Effektvität des Protokolls zugrunde gelegt. Alice und Bob sollen mit hoher Wahrscheinlichkeit auch einen gemeinsamen Schlüssel besitzen.

Definition 1.14. [10] Ein Protokoll heißt *sicher*, falls für gewählte Parameter $s, l > 0$ und für jede Lauschangriffs-Strategie das Protokoll entweder verlassen wird (da der

Lauschangriff entdeckt wurde) oder mit $1 - O(2^{-s})$ einen gemeinsamen Schlüssel von Alice und Bob mit genügender Länge erzeugt und garantiert, dass Eve's wechselseitige Information über diesen Schlüssel kleiner als 2^{-l} ist.

2 Quantenschlüsselübertragung am Beispiel BB84

Wir stellen hier das bekannteste diskrete QKD-Protokoll BB84 [6] vor. Es basiert auf vier Zuständen bezüglich zweier nicht orthogonaler Basen zur Schlüsselübertragung und nutzt die Eigenschaften aus Abschnitt 1.3. Dabei untergliedert es sich in zwei Phasen. In der ersten Phase wird mit quantentheoretischen Methoden eine Binärfolge, der sogenannte Rohschlüssel R, übermittelt. Dieser wird dann mittels klassischer Methoden weiter bearbeitet, um einen höheren Grad an Genauigkeit und eine größere Sicherheit zu erhalten. Wir beginnen mit der Erläuterung der zweiten Phase, da diese unabhängig vom Protokoll ist und auch für andere QKD-Protokolle verwendet werden kann.

2.1 klassische Verfahren zur Verbesserung der Sicherheit

Zu Beginn der zweiten Phase eines jeden Protokolls hat man einen klassischen Rohschlüssel, also eine Binärfolge R, vorliegen. Dadurch kann man nun auch auf Methoden der klassischen Kryptographie zurückgreifen, von denen wir hier ein geeignetes Fehlerkorrekturverfahren und die Verschwiegenheitsverstärkung vorstellen wollen .

2.1.1 Fehlerkorrektur

Bei der Übertragung eines Zustands durch einen Quantenkanal kann sich durch Wechselwirkungsprozesse (z.B. Wechselwirkung mit der Umgebung oder Wechselwirkung durch einen Lauschangriff) der übermittelte Zustand ändern, so dass die Messung, welche die Quanteninformation in klassische Information umwandelt, ein anderes Ergebnis liefert als für den ursprünglichen Zustand. Dadurch treten Fehler auf. Alice und Bob besitzen also nicht den exakt gleichen Schlüssel. Um diese Fehler zu beheben, tauschen Alice und Bob klassische Informationen aus, welche sie in Übereinstimmung bringen. Daher spricht man hier auch von *Informationsabgleich* (information reconciliation).

Alice und Bob besitzen jeweils eine binäre Zufallsfolge. Der Schlüssel, welcher von Alice gesendet wird, sei mit R bezeichnet. Bob erhält einen eventuell fehlerhaften Schlüssel R'. Da diese jedoch nicht übereinstimmen müssen, muss man einen Weg finden, diese beiden Folgen abzugleichen, ohne dass Eve aus den dazu ausgetauschten Informationen den Schlüssel R konstruieren kann.

Dazu wählt Alice beliebige Zufallsfolgen s_i von gleicher Länge wie der Schlüssel R. Hiervon bestimmt sie dann jeweils die Paritäten. Dazu berechnet sie zunächst s_iR, multipliziert also die beiden Folgen s_i und R komponentenweise. Die Parität $P(s_i)$

ergibt sich dann als Summer aller Komponenten der Folge $s_i R$ modulo 2. Anschließend teilt sie Bob s_i und die zugehörigen Paritäten $P(s_i)$ öffentlich mit. Durch geschickte Wahl kann sie die Anzahl der Folgen minimieren, so dass Bob aus den Paritäten von Alice und seiner Folge R' die Folge R exakt kombinieren kann. Hierzu werden häufig klassische lineare Codes verwendet. Diese werden in Abschnitt 4.1.1 behandelt.

Wir geben ein Beispiel. Wir gehen von 7 Bits in der Nachricht aus, welche durch die Übertragung maximal einen Bitflip-Fehler aufweisen, d.h. es wird von höchstens einem Bit der Nachricht der Bitwert vertauscht ($0 \leftrightarrow 1$). Wir bestimmen die Paritäten bezüglich der folgenden Matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Jede Zeile ($i = 1, 2, 3$) entspricht einer Sequenz s_i, dessen Parität wir bezüglich R ermitteln. Der Einfachheit halber gehen wir davon aus, dass Alice die Nachricht 0000000 sendet. Dann ergeben sich die Werte von Bob nach folgender Tabelle 2.1.

Bobs Ergebnis	$P(s_1)$	$P(s_2)$	$P(s_3)$
0 0 0 0 0 0 0	0	0	0
1 0 0 0 0 0 0	0	0	1
0 1 0 0 0 0 0	0	1	0
0 0 1 0 0 0 0	0	1	1
0 0 0 1 0 0 0	1	0	0
0 0 0 0 1 0 0	1	0	1
0 0 0 0 0 1 0	1	1	0
0 0 0 0 0 0 1	1	1	1

Tabelle 2.1: Paritäten bzgl. H am Beispiel der Nachricht 0000000

Man erkennt, dass $P := P(s_1), P(s_2), P(s_3)$ die Stelle des Fehlers in Binärdarstellung angibt. Damit kann Bob R konstruieren, indem er einfach das P-te Bit ändert. Im Allgemeinen ergibt die komponentenweise Differenz der Paritäten ΔP von Alice und Bob das sogenannte *Fehlersyndrom*, welches für unser Beispiel gerade wieder die Stelle des Fehlers in Binärdarstellung angibt. Ändert Bob nun die Stelle entsprechend des Syndroms, erhält er die ursprüngliche Nachricht von Alice. Zur Veranschaulichung betrachten wir die Nachricht 1001110. Dann erhält Alice $P_A(s_1) = 1, P_A(s_2) = 1$ und $P_A(s_3) = 0$ und für Bob ergeben sich die Möglichkeiten nach Tabelle 2.2.

Durch die ausgetauschte Nachricht u, bestehend aus den Folgen s_i und den entsprechenden Paritäten, erhält Eve zusätzliche Information. Hat Eve aus ihrem Lauschangriff die Information E erhalten, so kann sie ihre Korrelationsentropie $H_c(A|E)$ verbessern zu

$$H_c(A|E, u) \geq H_c(A|E) - H(U). \tag{2.1}$$

Bob's Ergebnis	$P(s_1)$	$P(s_2)$	$P(s_3)$	$\Delta P(s_1)$	$\Delta P(s_2)$	$\Delta P(s_3)$
1 0 0 1 1 1 0	1	1	0	0	0	0
0 0 0 1 1 1 0	1	1	1	0	0	1
1 1 0 1 1 1 0	1	0	0	0	1	0
1 0 1 1 1 1 0	1	0	1	0	1	1
1 0 0 0 1 1 0	0	1	0	1	0	0
1 0 0 1 0 1 0	0	1	1	1	0	1
1 0 0 1 1 0 0	0	0	0	1	1	0
1 0 0 1 1 1 1	0	0	1	1	1	1

Tabelle 2.2: Paritäten bzgl. H am Beispiel der Nachricht 10011110 und Differenzen ΔP

Dabei besteht U aus allen möglichen Nachrichten, welche man aus A, der Menge aller möglichen von Alice versendbaren siebenstelligen Nachrichten, nach dem oben beschriebenen Verfahren erhalten kann. Damit ist U eine von A abhängige Zufallsvariable.

Für die Korrelationsentropie gilt sogar folgender Satz, welchen wir hier jedoch nicht beweisen werden [14]. Er gibt eine bessere Schranke als in Gleichung (2.1) an.

Satz 2.1. *Seien A, U Zufallsvariablen mit Wahrscheinlichkeitsverteilung $p(a)$ von A und $p(a,u)$ von U in Abhängigkeit von A. Sei $s \in \mathbb{N}$ beliebig. Dann gilt mit mindestens der Wahrscheinlichkeit $1-2^{-s}$ die folgende Abschätzung:*

$$H_c(A|u) \geq H_c(A) - 2\log|u| - 2s.$$

Dabei ist $|u|$ die Anzahl der Bits in der generierten Nachricht $u \in U$.

Damit gilt fast sicher, also mit Wahrscheinlichkeit $p \geq 1-2^{-s}$,

$$H_c(R|E,u) \geq H_c(R|E) - 2(m+s), \tag{2.2}$$

wobei s als Sicherheitsparameter beliebig gewählt werden kann und m die Anzahl der Bits in u ist.

2.1.2 Verschwiegenheitsverstärkung

Da man im Allgemeinen nicht zwischen Fehlern, welche durch die Umgebung an sich (Rauschen) bedingt sind, und solchen, die aus einem Lauschangriff resultieren, unterscheiden kann, muss man immer von einem möglichen Lauscher ausgehen. Daher wird der nun korrigierte Rohschlüssel R weiter bearbeitet, um den Informationsgehalt für Eve zu minimieren. Dieser Schritt wird als *Verschwiegenheitsverstärkung* (privacy amplification) bezeichnet.

Diese basiert mathematisch auf der Klasse der sogenannten universellen Hash-Funktionen

$$\mathcal{G} = \{h : \{0,1\}^n \to \{0,1\}^k \mid \forall a_1, a_2 \in \{0,1\}^n : a_1 \neq a_2 : p(h(a_1) = h(a_2)) \leq 2^{-k}\}$$

in Abhängigkeit von n und k. Dieses sind Funktionen, die für verschiedene Argumente mit hoher Wahrscheinlichkeit verschiedene Funktionswerte liefert.

Ein einfaches Beispiel für eine solche Klasse ist gegeben durch die Klasse aller linearen Abbildungen $h : \{0,1\}^n \to \{0,1\}^k$, wie man durch einfaches Nachrechnen sieht.

Somit können wir auch hier das Beispiel aus dem vorherigen Kapitel aufgreifen. Wir wählen 'zufällig' die universelle Hash-Funktion, welche durch die Matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

gegeben ist.

Damit ergibt sich der endgültige Schlüssel S aus dem Rohschlüssel R als die durch H festgelegten Paritäten. Beispielsweise erhalten wir die Ergebnisse der nebenstehenden Tabelle.

Rohschlüssel R	Schlüssel S
1 0 0 1 1 1 0	110
0 0 0 1 1 1 0	111
1 1 0 1 1 1 0	100
1 0 1 1 1 1 0	101
1 1 0 1 1 0 1	101

Hieran sieht man, dass man selbst dann, wenn nur ein Bit unbekannt ist und dieses falsch geraten wird, im Allgemeinen einen anderen Schlüssel erhält. Weiter sieht man, dass die endgültigen Schlüssel mit unterschiedlichen Rohschlüsseln erzeugt werden können, da der Bildraum wesentlich kleiner als der Definitionsraum ist. Dadurch kann es passieren, dass man durch geschicktes Raten von fehlenden Bits den Schlüssel dennoch erhält. Diese Wahrscheinlichkeit ist jedoch nach Definition der universellen Hash-Funktionen kleiner als 2^{-k}. Mit dem folgenden Satz lässt sich die Korrelationsentropie für Eve abschätzen [14].

Satz 2.2. *Sei X eine Zufallsvariable mit Wahrscheinlichkeitsverteilung $p(x)$. Sei $h \in \mathcal{G}$ zufällig gewählt. Dann gilt:*

$$H(h(X)|h) \geq H_c(h(X)|h) \geq k - 2^{k-H_c(X)}.$$

Alice wählt also öffentlich eine zufällige Funktion $h \in \mathcal{G}$ für ein vorher festgelegtes k, welches die Länge des endgültigen Schlüssels bestimmt. Diese wenden Alice und Bob nun auf ihren gemeinsamen Rohschlüssel R an und erhalten dadurch einen neuen, kürzeren Schlüssel $S = h(R)$ über den Eve weniger Information besitzt als über R.

2.1.3 Folgerungen für die Entropie

Damit erhalten wir eine quantitative Abschätzung von Eves möglichem Informationsgewinn. Können wir Eves Korrelationsentropie nach ihrem Lauschangriff nach unten

abschätzen durch $H_c(A|E) > d$, so gilt nach der Fehlerkorrektur nach Gleichung (2.2) mit einer Wahrscheinlichkeit $\geq 1 - 2^{-s}$, dass

$$H_c(A|E, u) \geq d - 2(m + s).$$

Nach der Verschwiegenheitsverstärkung erhalten wir dann mit Satz 2.2, dass

$$H(S|E, u) \geq H_c(S|E, u) \geq k - 2^{k-d+2(m+s)}.$$

Damit gilt dann für die wechselseitige Information

$$I(S : E) \leq 2^{k-d+2(m+s)}. \tag{2.3}$$

2.2 BB84

Dieses Protokoll ist das erste und bekannteste QKD-Protokoll. Es wurde 1994 von Charles Bennett und Gilles Brassard veröffentlicht [6]. Es basiert auf den vier Zuständen $|0\rangle, |1\rangle, |0_x\rangle$ und $|1_x\rangle$. Wichtig hierbei ist, dass diese Zustände Eigenzustände zu zwei nicht kommutierenden Observablen (hier Z und X) sind, damit die Eigenschaften für nichtorthogonale Zustände aus Abschnitt 1.3 genutzt werden können.

Alice und Bob gehen dazu folgendermaßen vor. Der Einfachheit halber betrachten wir zunächst den Fall, dass der verwendete Quantenkanal rauschfrei ist.

- Alice präpariert eine zufällige Folge aus den vier Zustände $|0\rangle, |1\rangle, |0_x\rangle$ oder $|1_x\rangle$ und sendet diese an Bob,
- Bob gibt die Ankunft öffentlich bekannt und misst die erhaltene Folge in der $z-$Basis oder der $x-$Basis in zufälliger Reihenfolge,
- Alice und Bob vergleichen ihre Basiswahl (z oder x) und behalten nur die Bits mit gleicher Basis; die Messergebnisse hiervon bilden den Rohschlüssel R_0,
- Alice wählt aus R_0 die Hälfte zufällig aus und gibt diese mit ihren erwarteten Messergebnissen öffentlich bekannt,
- Bob vergleicht diese mit seinen Messergebnissen; treten Fehler auf, wurde der Kanal abgehört, da ein rauschfreier Kanal keine Fehler verursacht,
- wurde das Protokoll akzeptiert, bilden die verbleibenden Messergebnisse den Schlüssel S.

Bob muss die erhaltenen Zustände sofort messen, da bei einer späteren Messung das Messergebnis durch die unitäre Dynamik der Zustände verfälscht sein kann.

Damit Eve entdeckt werden kann, darf sie vor ihrem Angriff nicht wissen, welche Basis Alice gewählt hat, da dann aus ihrer Sicht orthogonale Zustände vorliegen, die sie fehlerfrei kopieren kann. Daher gibt Alice ihre Basis erst bekannt, wenn sie weiß,

dass Eve keinen direkten Zugriff mehr auf die Zustände hat.

Wir betrachten ein Beispiel, um zu veranschaulichen wie man auf den Rohschlüssel kommt.

Beispiel 2.3.

Basis Alice	X	Z	X	X	Z	X	Z	Z	Z	X
Zufallsfolge a	1	1	0	0	1	0	1	1	0	1
Präparation	$\|1_x\rangle$	$\|1\rangle$	$\|0_x\rangle$	$\|0_x\rangle$	$\|1\rangle$	$\|0_x\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1_x\rangle$
Basis Bob	Z	Z	Z	X	Z	X	Z	X	X	X
Messergebnis	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0_x\rangle$	$\|1\rangle$	$\|0_x\rangle$	$\|1\rangle$	$\|1_x\rangle$	$\|1_x\rangle$	$\|1_x\rangle$
Ergebnis	0	1	0	0	1	0	1	1	1	1
Rohschlüssel R_0		1		0	1	0	1			1

Tabelle 2.3: Beispiel zum BB84-Protokoll

Die folgende Abbildung veranschaulicht die Funktionsweise. Dabei bilden polarisierte Photonen die einzelnen Qubits. Die z-Basis ist durch horizontale (0) und vertikale (1) Polarisation beschreiben, die x-Basis entsprechend durch diagonale Polarisation.

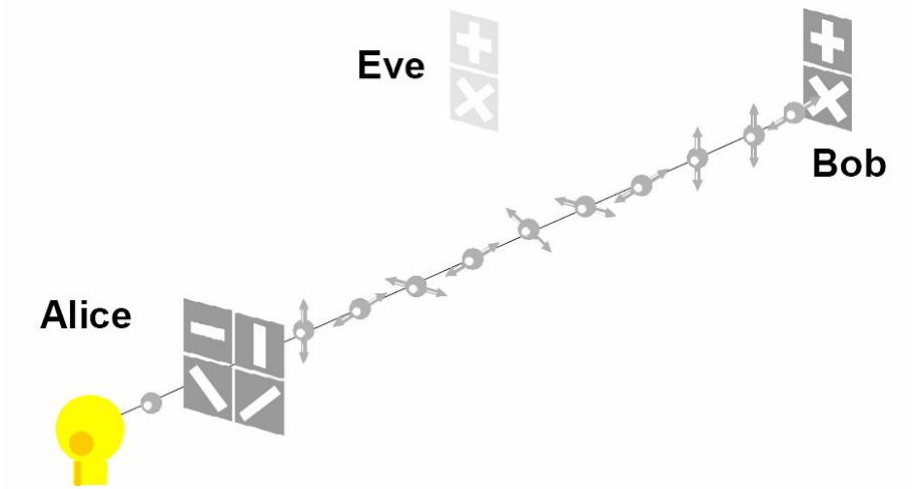


Abbildung 2.1: Veranschaulichung der Funktionsweise des BB84-Protokolls [2]

Um zu berücksichtigen, dass ein Quantenkanal im Allgemeinen verrauscht ist, muss das Protokoll noch weiter verbessert werden. Dazu erweitert man das Protokoll um die beiden im Abschnitt 2.1 vorgestellten Verfahren der Fehlerkorrektur und Verschwiegenheitsverstärkung. Außerdem muss man eine typische Fehlerrate, verursacht durch den Kanal, erlauben.

Das Resultat dieser Erweiterung ist im folgenden mit den für die Berechnungen benötigten Bezeichnungen aufgeführt.

1. Alice wählt zwei binäre Zufallsfolgen a und b von genügender Länge (mindestens 4N bei einer gewünschten Schlüssellänge von N),

2. Alice präpariert
$$|\psi\rangle = \bigotimes_k |\psi_{a_k b_k}\rangle \,,$$
wobei $|\psi_{00}\rangle = |0\rangle \,, |\psi_{10}\rangle = |1\rangle \,, |\psi_{01}\rangle = |+\rangle$ und $|\psi_{11}\rangle = |-\rangle$ ist, und sendet diesen an Bob,

3. Bob erhält $|\psi'\rangle = \mathcal{E}(|\psi\rangle \langle\psi|)$, gibt die Ankunft öffentlich bekannt und misst $|\psi'\rangle$ bezüglich einer Zufallsfolge b', d.h. er misst bei $b'_k = 0$ bezüglich der $z-$Basis und bei $b'_k = 1$ bezüglich der $x-$Basis,

4. Alice gibt ihre Basiswahl, also die Zufallsfolge b bekannt, nachdem sie Bobs Bestätigung erhalten hat,

5. Alice und Bob vergleichen b und b' und behalten nur die Bits mit $b_k = b'_k$; diese sollten mit hoher Wahrscheinlichkeit eine Folge der Länge (mindestens) 2N sein und bilden den Rohschlüssel R_0,

6. Alice wählt aus R_0 die Hälfte, also N Bits zufällig aus; diese bilden die Testbits C, die anderen die Schlüsselbits R,

7. Alice gibt die Testbits C öffentlich bekannt,

8. Alice und Bob vergleichen die Messergebnisse von C auf Fehler: Da C zufällig ist, können sie dadurch auf eine mittlere Fehlerrate der gesamten Folge R_0 schließen und mit der bekannten Fehlerrate ihres Kanals vergleichen; bei Überschreiten einer Toleranzgrenze wird das Protokoll abgebrochen, da mit hoher Wahrscheinlichkeit ein Lauschangriff vorliegt; liegt die Fehlerrate unter diesem Toleranzwert, wird R akzeptiert,

9. Alice und Bob betreiben Fehlerkorrektur durch Informationsabgleich, vgl. Abschnitt 2.1.1,

10. Durch Verschwiegenheitsverstärkung (Abschnitt 2.1.2) wird der endgültige Schlüssel S (der Länge $k < N$) erzeugt.

Bei der Betrachtung eines Lauschangriffs steht man Eve alle quantentheoretischen Freiheiten zu. Üblicherweise geht man davon aus, dass sie einen perfekten (also rauschfreien) Quantenkanal besitzt und das Rauschen des eigentlichen Kanals durch ihren Lauschangriff erzeugt. Geht man zunächst von der einfachsten Attacke aus, dass Eve ebenso wie Bob die Qubits zufällig in der z- oder der x-Basis misst, so liegt sie in der Hälfte der Fälle mit ihrer Basiswahl richtig, wird also nicht bemerkt, da sich der Zustand durch ihre Messung nicht verändert hat. Liegt sie falsch, projeziert sie in der

Hälfte der Fälle auf die richtige Basis, in der anderen Hälfe auf die falsche. Dieses äußert sich als Fehler beim Vergleich der Testbits von Alice und Bob. Damit erzeugt Eve eine durchschnittliche Fehlerrate von 25%. Liegt die Fehlerrate des Kanals also über 25%, so kann Eves Lauschangriff nicht detektiert werden und das Protokoll ist unsicher. Bei typischen Verlustraten im Kanal von $\eta = 10^{-0.025ldB/km}$ [12] ergibt sich damit eine maximale Reichweite von 240 km, wenn man keine weiteren Detektorverluste zugrunde legt. Hieran sieht man, dass man im nichtidealen Fall auf neue Probleme treffen kann. Ein Teil dieser Probleme soll im folgenden Kapitel 3 neben den experimentellen Realisierungsmöglichkeiten des BB84-Protokolls vorgestellt werden.

3 Realisierungsmöglichkeiten

Wir stellen hier Realisierungsmöglichkeiten mittels polarisierter Photonen und mittels lokaler Phasendifferenzen vor. Dabei geht man davon aus, dass der Sender jeweils ein einziges Photon mit einer bestimmten Polarisation abschickt. Ein Lauscher müsste beim Abhören ein neues Photon erzeugen, um nicht bemerkt zu werden. Dieses ist bei nichtorthogonalen Polarisationszuständen nicht exakt möglich.

3.1 BB84

Bei der Realisierung des BB84-Protokolls werden vier verschiedene Polarisationszustände benötigt. Hierzu wählt man je zwei Basiszustände aus zwei zueinander komplementären Basen. Es werden horizontal/vertikal polarisierte Photonen und je nach Aufbau entweder rechts-/linkszirkular oder diagonal polarisierte Photonen verwendet. Diese entsprechen dann den Zuständen $|0\rangle, |1\rangle, |0_x\rangle$ und $|1_x\rangle$. Alice sendet also eine Reihe von Photonen, die sie bezüglich ihrer Zufallsfolgen entsprechend polarisiert hat, an Bob. Bob wählt nun entsprechend b' seine Basis und misst die Polarisation. Der Rest des Protokolls benutzt nur noch die Zufallsfolgen und die Messergebnisse, verwendet also ausschließlich klassische Größen und kann über einen Algorithmus generiert werden.

Der folgende Aufbau wurde 1989 von Bennett et al. [19, 20] bei der ersten experimentellen Realisierung genutzt.

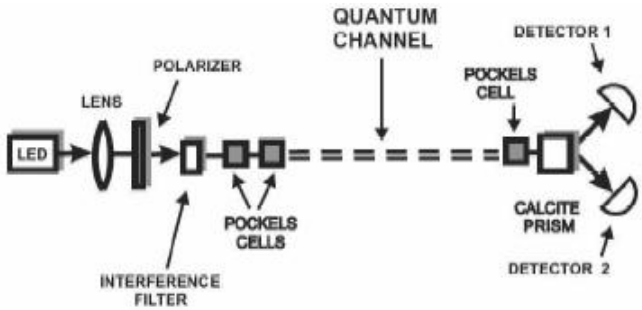


Abbildung 3.1: Schema der ersten experimentellen Realisierung von BB84 [3]

Eine LED-Diode emittiert Lichtpulse, die über einen Interferenzfilter (interference filter) abgeschwächt und mit einem Polarisator (polarizer) horizontal polarisiert werden. Die Photonenzahl pro Puls beträgt dann im Mittel 0.1 und simuliert hierdurch einen Ein-Photonen-Zustand. Die folgenden zwei Pockelszellen (pockels cell) erzeugen die vier gewünschten Polaritationszustände (horizontal, vertikal, links-, rechtszirkular). Der Quantenkanal besteht aus 32 cm reinem Luftweg. Die Pockelszelle bei Bob vertauscht linear und zirkular polarisiertes Licht bei Anlegen einer Spannung und dient

somit zur Basiswahl der zu messenden Polarisation. Mit einem Kalkspat-Prisma (calcite prism) werden die vertikalen und horizontalen Polarisationsanteile des Lichtpulses in zwei Wege aufgespaltet. An beiden Ausgängen findet eine Detektion (detector 1,2) durch Photomultiplier statt.

Wir betrachten noch einmal Beispiel 2.3 im Photonenbild.

Zufallsfolge b	1	0	1	1	0	1	0	0	0	1
Polarisationsbasis	◯	+	◯	◯	+	◯	+	+	+	◯
Zufallsfolge a	1	1	0	0	1	0	1	1	0	1
Polarisation	↻	↕	↺	↺	↕	↺	↕	↕	↔	↻
Zufallsfolge b'	0	0	0	1	0	1	0	1	1	1
Polarisationsbasis	+	+	+	◯	+	◯	+	◯	◯	◯
gemessen	↔	↕	↔	↺	↕	↺	↕	↻	↻	↻
Ergebnis	0	1	0	0	1	0	1	1	1	1
Rohschlüssel R		1		0	1	0	1			1

Tabelle 3.1: Beispiel zum BB84-Protokoll mit polarisierten Photonen

Eine andere Möglichkeit als die Kodierung über verschiedene Polarisationszustände besteht in der Kodierung über eine lokale Phasenverschiebung zwischen zwei Pulsen in einem Mach-Zehnder-Interferometer.

Alice kontrolliert dabei die Phasenverschiebung in einem Arm des Interferometers und Bob im anderen. Das Ergebnis ihrer Wahl kann Bob dann durch das Interferenzbild interpretieren. Liegt zwischen beiden Pulsen eine Phasendifferenz von 0 oder π vor, hat man in einem Ausgang konstruktive und im anderen Ausgang destruktive Interferenz. Man detektiert also abhängig von der Phasendifferenz entweder in dem einen oder in dem anderen Ausgang ein Photon. Dieser Fall liefert also ein deterministisches Ergebnis. Liegt eine andere Phasendifferenz vor, so kann man keine Aussage treffen, da die Messergebnisse zufällig sind.

Alice kodiert nun ihre Photonen, indem sie in ihrem Arm der Interferometers eine Phasenverschiebung von 0 ($|0\rangle$) , $\pi/2$ ($|0_x\rangle$), π ($|1\rangle$) oder $3\pi/2$ ($|1_x\rangle$) vollzieht. Bob vollzieht in seinem Arm eine Phasenverschiebung von entweder 0 (z-Basis) oder $\pi/2$ (x-Basis).

Dies ist äquivalent zur Verwendung von Polarisationszuständen, da man sich vorstellen kann, dass die Polarisation des einen Pulses die z-Achse festlegt. Die Phasendifferenz des anderen Pulses legt dann die Orientierung der Polarisation bezüglich der durch den ersten Puls festgelegten z-Achse fest. Bei einer Phasendifferenz von 0 oder π ist der Puls horizontal oder vertikal polarisiert, bei einer Phasendifferenz von $\pm\pi/2$ diagonal. Dieses hat den Vorteil, dass man anstatt durch Polarisationsfilter die Zustände durch Interferenzeffekte bei kohärenter Überlagerung dieser beiden Pulse unterscheiden kann und das System damit weniger störanfällig für eine globale Verschiebung der

Polarisationsrichtung ist.

Allerdings ist es schwierig, dieses System stabil zu halten. Daher wird ein anderer Aufbau verwendet, welcher aber der gleichen Funktionsweise folgt. Man benutzt hierbei zwei gleiche Mach-Zehnder-Interferometer nach folgendem Aufbau 3.2.

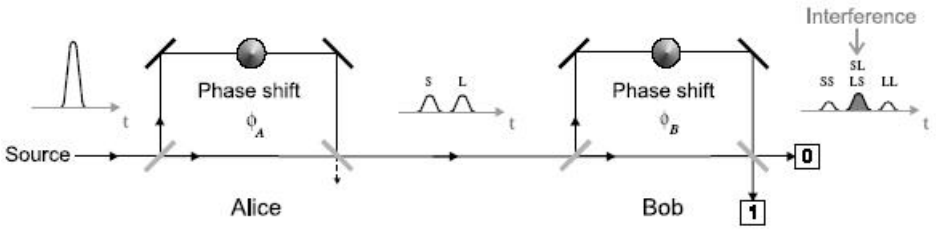


Abbildung 3.2: Schematische Darstellung der experimentellen Realisierung von BB84 über Phasenkodierung [3]

Die Wegdifferenz im Interferometer ist größer als die Ausdehnung des Laserpulses. Die Fälle, bei dem nun das Photon zuerst durch den kurzen Arm (S) bei Alice und dann durch den langen Arm (L) bei Bob läuft, ist nicht zu unterscheiden vom umgekehrten Fall (LS), bei dem das Photon zunächst den langen und dann den kurzen Arm durchläuft. Dieser Fall wird durch eine genaue Zeitauflösung herausgefiltert. Das System verhält sich dann wie ein einzelnes stabilisiertes Mach-Zehnder-Interferometer. Alice kontrolliert dabei die Phasenverschiebung im ersten Interferometer und Bob im zweiten.

3.1.1 Nachteil - PNS-Attacke

Die PNS(Photon Number Splitting)-Attacke ist eine spezielle Attacke, die die Unvollkommenheit der verwendeten Ein-Photonen-Quellen und Quantenkanäle nutzt.

Im oben dargestellten Aufbau 3.2 benutzt man einen auf 0.1 Photonen pro Puls abgeschwächten Laserstrahl, wobei die Anzahl der Photonen pro Puls Poisson-verteilt ist. Dadurch ist es natürlich möglich, dass in manchen Fällen mehr als ein Photon pro Puls auftritt. In diesem Fall kann Eve eines dieser Photonen abzweigen und dieses messen, ohne entdeckt zu werden.

Hierzu geht Eve folgendermaßen vor: Sie fängt alle gesendeten Pulse ab und bestimmt die Anzahl der Photonen pro Puls mit einer Messung welche den Polarisationszustand nicht zerstört. Solche Messungen existieren und werden als QND-Messungen bezeichnet. Sie blockt alle 1-Photon-Pulse komplett ab und zweigt bei allen Pulsen mit mehr als zwei Photonen eines ab und speichert dieses. Die übrigen Photonen schickt sie dann durch einen fehlerfreien Quantenkanal an Bob. Sie wartet bis Alice ihre Basiswahl bekannt gibt und misst die gespeicherten Photonen entsprechend. Dadurch besitzt Eve von jedem geblockten Photon die volle Information über den Zustand, da sie ja nur

zwischen zwei orthogonalen Zuständen unterscheiden muss. Da Eve die Photonen speichert, bis Alice ihre Basis bekannt gibt, spricht man auch von einer *Speicher-Attacke* (storage attack).

Ist die Menge der von Eve geblockten Photonen unterhalb der statistischen Verlustrate des verwendeten Quantenkanals zwischen Alice und Bob, bemerkt Bob keinen Unterschied. Legt man die heutzutage üblichen Verlustwerte von $\eta = 10^{-0.025ldB/km}$ und einen Detektorverlust von 10% zugrunde, so ergibt sich eine kritische Länge von 53,7 km, ab der dieser Angriff uneingeschränkt funktioniert [12]. Unterhalb dieser kann Eve nur einen Teil der 1-Photonen-Pulse blocken und erhält damit auch nur einen Teil des Rohschlüssels.

Für eine Schlüsselübertragung über große Entfernungen ist das BB84-Protokoll also nicht sinnvoll, da Eve ab einer Länge von 54km sämtliche Informationen erhält. Eine Möglichkeit, die Reichweite sicher zu erhöhen, liegt im SARG-Protokoll von Scarani, Acín, Ribordy und Gisin [12].

3.2 Das SARG-Protkoll

Beim SARG-Protokoll [12] wird das Bit nicht im Zustand selbst verschlüsselt sondern durch die Basiswahl des Zustands. Dabei verwendet man wieder komplementäre Basen. Das Protokoll folgt in weiten Teilen dem BB84-Protokoll, lediglich die Rohschlüsselermittlung ist abgewandelt. Alice und Bob gehen nun folgendermaßen vor.

1. Alice wählt zwei binäre Zufallsfolgen a und b und präpariert hiermit wie im BB84-Protokoll
$$|\psi\rangle = \bigotimes_k |\psi_{a_k b_k}\rangle \,,$$
2. Alice sendet $|\psi\rangle$ an Bob,
3. Bob erhält $|\psi'\rangle$, gibt die Ankunft öffentlich bekannt und misst $|\psi'\rangle$ bezüglich einer Zufallsfolge b',
4. Alice gibt nun pro Bit jeweils zwei mögliche Zustände, davon einen in jeder Basis, bekannt; d.h. sie veröffentlicht jeweils $A_{\omega,\omega'} := \{|\omega_x\rangle\,, |\omega'_z\rangle\}$ mit $\omega, \omega' \in \{\uparrow, \downarrow\}$,
5. Hiermit kann Bob in 1/4 der Fälle das verschlüsselte Bit logisch bestimmen (siehe folgendes Beispiel) und erhält R_0,
6. Alice teilt R_0 in Testbits C und Schlüsselbits R ein; dann gibt sie C bekannt,
7. Alice und Bob vergleichen C und entscheiden, ob der Rohschlüssel R akzeptiert oder verworfen wird,
8. Durch Fehlerkorrektur und Verschwiegenheitsverstärkung wird der endgültige Schlüssel S erzeugt.

Wir geben für die Ermittlung des Rohschlüssels ein Beispiel:

Beispiel 3.1. Wir nehmen an, Alice sendet den Zustand $|\uparrow_x\rangle$, dann erhält Bob als mögliche Messergebnisse bei Messung in der x-Basis stets $+1$ und bei Messung in der z-Basis ± 1 jeweils mit der Wahrscheinlichkeit 1/2. In Abhängigkeit von Alice' Angabe $A_{\omega,\omega'}$ ergibt sich folgende Auswertung:

$A_{\omega,\omega'}$	Bob's Basis	Messergebnis	Auswertung
$\uparrow\uparrow$	X	+1	?
	Z	+1	?
	Z	-1	X
$\uparrow\downarrow$	X	+1	?
	Z	+1	X
	Z	-1	?

Tabelle 3.2: Beispiel zur Auswertung im SARG-Protokoll

Dieses bedeutet folgendes. Nehmen wir an, Alice gibt $A_{\uparrow\uparrow}$ bekannt. Dann hat sie entweder $|\uparrow_x\rangle$ oder $|\uparrow\rangle$ geschickt. Erhält Bob in der z-Basis das Ergebnis -1, also $|\downarrow\rangle$, so weiß er, dass er in der falschen Basis gemessen hat und kann somit darauf schließen, dass Alice den Zustand $|\uparrow_x\rangle$ gesendet hat. Misst er $+1$ in der x- oder der z-Basis, so kann er keine solche Aussage treffen und somit auch nicht auf das verschlüsselte Bit schließen. Da Bob mit Wahrscheinlichkeit 1/2 in der z-Basis misst und hierbei mit Wahrscheinlichkeit 1/2 das Ergebnis -1 erhält, kann er nur in ein Viertel aller Fälle auf das Bit schließen. Die anderen Möglichkeiten verlaufen analog.

3.2.1 Realisierung

Eine experimentelle Realisierung dieses Verfahrens wird unter anderem von der Firma IdQuantique vertrieben [21]. Der Aufbau erlaubt neben der Implementierung des SARG-Protokolls auch eine Implementierung des BB84-Protokolls, indem man einfach die Auswertung nach der Quantenübertragung entsprechend abändert. Das hier vorgestellte Verfahren verwendet linear polarisiertes Licht, d.h. die z-Basis wird durch horizontal/vertikal polarisiertes und die x-Basis durch diagonal polarisiertes Licht realisiert. Dabei wird die Information als Phasenbeziehung zweier 1-Photonen-Pulse kodiert.

Der schematische Aufbau ist in Abbildung 3.3 dargestellt. Es ähnelt dem vorherigen Aufbau 3.2. Aus technischen Gründen wurde das Protokoll um einige Schritte vorab erweitert. Die Funktionsweise ist jedoch prinzipiell dieselbe.

Bob sendet einen linear polarisierten Laserpuls (L) mit der Telekom-Wellenlänge[1] an Alice. Dieser wird durch den 50/50-Strahlteiler (BS) aufgeteilt. Der Puls auf dem

[1] 1310-1550 nm

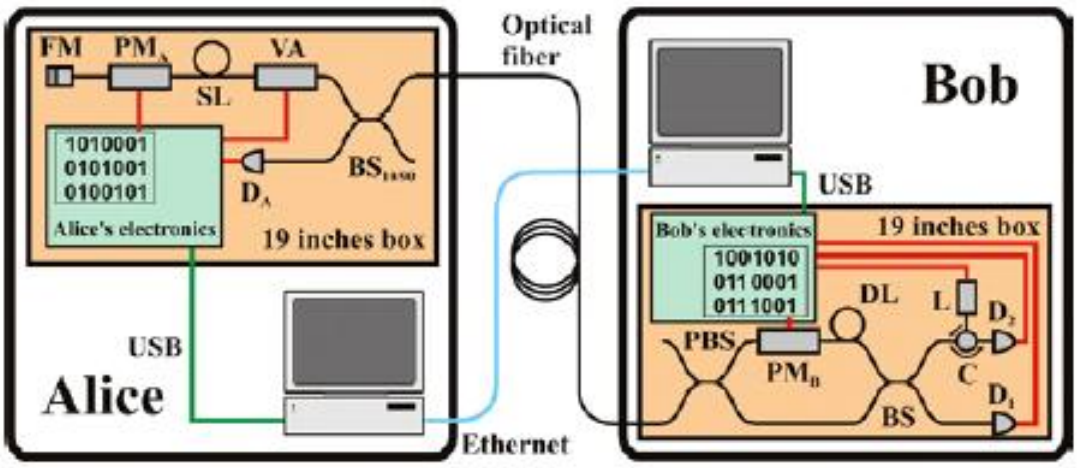


Abbildung 3.3: Experimentelle Realisierung der Firma IdQuantique [22]; die wesentlichen Bauteile sind im Text erläutert

oberen Weg erhält eine Phasenverschiebung (PM_B) von 90° und wird um 30ns zeitverzögert, der Puls auf dem unteren Weg erhält keine Phasenverschiebung. Der Polarisationsstrahlteiler (PBS) leitet beide Pulse (zeitversetzt) an Alice weiter. Alice koppelt 90% der Intensität der Pulse über einen Strahlteiler (BS) ab, um einerseits die Intensität der Pulse zu bestimmen und andererseits die exate zeitliche Kopplung des Phasenschiebers zu ermöglichen. Beide Pulse werden nun an einem Faradayspiegel (FM) reflektiert und erhalten dabei eine Phasenverschiebung von 90°.

Nun beginnt das eigentliche Protokoll. Alice lässt den ersten Puls passieren und versieht den zweiten mit einer Phasenverschiebung ϕ_A von $0, \pi$ für einen Zustand in der z-Basis oder $\pi/2, 3\pi/2$ in der x-Basis. Beide Pulse werden anschließend (VA) in der Intensität auf das Ein-Photonen-Niveau abgesenkt und zurück an Bob geschickt.

Durch die Phasenverschiebung am Faradayspiegel sind die ursprünglichen Polarisationen um 90° gedreht, so dass durch den Polarisationsstrahlteiler (PBS) nun der erste Puls den langen Weg durchläuft und dabei eine Phasenverschiebung von 90° erhält und der zweite Puls den kurzen Weg passiert. Dadurch ist gewährleitet, dass beide Pulse gleichzeitig am 50/50-Strahlteiler ankommen. Um nun zwischen den beiden möglichen Basen x und z zu wählen, versieht Bob den ersten Puls mit einer zusätzlichen Phasenverschiebung ϕ_B von $\pi/2$, wenn er in der x-Basis messen will. Insgesamt erreichen also beide Pulse gleichzeitig mit einer Gesamtphasenverschiebung von $\phi = \phi_A - \phi_B$ den 50/50-Strahlteiler und erzeugen somit ein entsprechendes Interferenzbild in den beiden Detektoren D0 und D1.

Dieses Interferenzbild ist in folgender Tabelle aufgelistet. Man erkennt, dass Bob genau dann einen eindeutigen Detektornachweis (D0 oder D1) erhält, wenn er die gleiche Basis wie Alice gewählt hat.

Der Detektornachweis ist mit der Phasendifferenz ϕ korreliert, so dass Bob dann eindeutig den gesendeten Zustand kennt. Misst er in der falschen Basis, also mit einer Phasendifferenz von $\pm\pi/2$, erhält er entweder in beiden Detektoren einen Nachweis oder zufällig in einem von beiden. Somit kann er keine Aussage über den gesendeten Zustand treffen. Mit seinen Messergebnissen kann er nun algorithmisch das jeweilige Protokoll beenden.

ϕ_A	ϕ_B	ϕ	D0	D1
0	0	0	+	-
0	$\pi/2$	$-\pi/2$	+	+
$\pi/2$	$\pi/2$	0	+	-
π	0	π	-	+
$\pi/2$	0	$\pi/2$	+	+
π	$\pi/2$	$\pi/2$	+	+
$3\pi/2$	0	$-\pi/2$	+	+
$3\pi/2$	$\pi/2$	π	-	+

Da linear polarisiertes Licht auf dem Weg durch das Glasfaserkabel elliptisch polarisiert wird, wurde dieses Protokoll modifiziert. Diese Änderung beruht auf dem Prinzip der „Faraday orthoconjugation“ [23]. Durch die Drehung der Polarisation am Faradayspiegel werden die Polarisationsfluktuationen, die beim Durchgang durch das Glasfaserkabel aufgetreten sind, auf dem Rückweg kompensiert. Dadurch kommt das linear polarisierte Licht von Bob auch wieder linear polarisiert zurück. Allerding ist die Polarisation im Vergelich zur ursp”runglichen um 90° gedreht. Das bedeutet beispielsweise, dass horizontal polarisiertes Licht vertikal polarisiert zurückkommt und umgekehrt - unabhängig von den Störfaktoren des Glasfaserkabels.

Es sind noch weitere technische Komponenten in Abbildung 3.3 zu sehen. Diese sollen hier aber nicht weiter erläutert werden.

3.2.2 kritische Übertragungslänge

Das SARG-Protokoll ist bei gleicher mittlerer Photonenzahl pro Puls beweisbar sicherer als das BB84-Protokoll hinsichtlich der oben beschriebenen PNS-Attacke [12]. Durch das Abfangen eines Photons erhält Eve nicht mehr die gesamte Informtaion, da Alice das Bit bezüglich zweier nichtorthogonaler Zustände verschlüsselt hat. Man kann allerdings auch zeigen [12], dass Eve mit einer speziellen PNS-Attacke, der IRUD(intercept-resend with unambigious discrimination)-Attacke, ab einer kritischen Übertragungslänge von 102,5km ebenfalls volle Information über den Schlüssel erhält. Kombiniert man BB84 mit dem SARG-Protokoll [24], kann man sogar eine kritische Übertragungslänge von 125km erreichen.

Mit den heutigen technologischen Möglichkeiten sind die vorgestellten Protokolle also alle ab einer gewissen kritischen Übertragungslänge nicht sicher gegenüber PNS-Attacken. Allerdings muss man dabei beachten, dass diese Attacken ebenfalls mit den heutigen bekannten Möglichkeiten nicht realisierbar sind.

4 Methoden zur Fehlerbehebung

Hier werden die Grundlagen für den Sicherheitsnachweis der QKD-Protokolle gelegt. Zunächst behandeln wir die Quantenfehlerkorrektur, welche uns klassisch schon in Abschnitt 2.1.1 begegnet ist. Anschließend wenden wir uns dem Problem zu, dass verschränkte Zustände durch Wechselwirkung mit der Umgebung an Verschränkung verlieren können. Das heißt, wir müssen die auftretenden Quantenfehler korrigieren, ohne jedoch den Zustand selbst zu zerstören, da wir an maximal verschränkten Zuständen bzw. Zuständen mit hoher Treue zu einem maximal verschränkten Zustand interessiert sind. Dieses Problem wird durch Verschränkungs-Purifzierungs-Protokolle gelöst. Abschließend zeigen wir den Zusammenhang zwischen beiden Verfahren.

Wichtig für eine spätere Anwendung ist, dass wir hierbei lediglich lokale Operationen und klassische Kommunikation (LOCC) verwenden.

Abschnitt 4.1 über Quantenfehlerkorrektur orientiert sich dabei an [14], die folgenden Abschnitte über Verschränkungs-Purifizierung an [11].

4.1 Quantenfehlerkorrektur

Klassische Zustände kann man beliebig oft messen, ohne den Zustand zu zerstören. Hierauf basiert die Fehlerkorrektur durch Informationsabgleich in Abschnitt 2.1.1. Die *Quantenfehlerkorrektur* (quantum error correction) befasst sich mit dem Problem, wie man Fehler von Quantenzuständen, welche bei der Übertragung durch einen Quantenkanal auftreten, wieder beheben kann, ohne den Zustand selbst zu zerstören. Dabei transformiert man den Zustand $|\psi\rangle$ durch eine unitäre Transformation U in einen Zustand $|\psi'\rangle = U|\psi\rangle$, welcher neben dem Zustand selbst noch redundante Informationen erhält. Man spricht davon, dass man den Zustand $|\psi\rangle$ durch einen Code kodiert hat in $|\psi'\rangle$. Der Zustand $|\psi'\rangle$ wird dann an Stelle von $|\psi\rangle$ durch den Kanal geschickt. Anschließend wird eine Syndrom-Messung durchgeführt, welche Informationen über den Fehler liefert. Dieser kann dann korrigiert und der Zustand durch U^{-1} wieder zurücktransformiert (dekodiert) werden. Das Verfahren wird also durch einen Fehlerkorrekturcode (QECC) beschrieben. Hier werden zunächst die linearen Codes vorgestellt, welche auch für die Fehlerkorrektur von klassischen Bits genutzt werden. Anschließend werden die Calderbank-shor-Steane(CSS)-Codes, welche auf linearen Codes basieren, behandelt. Zuletzt wird noch kurz die Implementierung der Codes und der Fehlerkorrekturverfahren dargestellt.

Da wir hier nur auf linearen Transformationen basierende Codes betrachten, genügt es die Transformation der Basiszustände anzugeben. Die Basiszustände eines QECC im Binärsystem bilden eine Teilmenge $C \subset \mathbb{F}_2^n$, sie werden auch als Codewörter bezeichnet. Der Raum $\mathbb{F}_2^n$ ist dabei der n-dimensionale Vektorraum über dem Körper $\mathbb{F}_2$ bestehend

aus 0 und 1. Wir bezeichnen Codes, welche eine k-Bit-Folge x in eine n-Bit-Folge y transformieren als $[n, k]$-Codes.

4.1.1 Lineare Codes

Lineare Codes lassen sich durch eine $n \times k$-Matrix über dem $\mathbb{F}_2$ darstellen, die Generatormatrix G. Dann ist das Codewort y von x gegeben durch $y = Gx$. Somit hat man hier eine kompakte Darstellung des Codes.

Beispiel 4.1 (3-Qubit-Bitflip-Code)**.** Dieser Code bildet den Zustand $|0\rangle$ auf $|0_L\rangle = |000\rangle$ ab und $|1\rangle$ auf $|1_L\rangle = |111\rangle$. Eine allgemeine Superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ wird damit abgebildet auf $|\psi'\rangle = \alpha|000\rangle + \beta|111\rangle$. Der 3-Qubit-Bitflip-Code ist also ein $[3, 1]$-Code. Die zugehörige Generatormatrix ist somit gegeben durch

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Man beachte hierbei, dass der Zustand dabei nicht kopiert wird, da $\alpha|000\rangle + \beta|111\rangle \neq (\alpha|0\rangle + \beta|1\rangle)^{\otimes 3}$ ist.

Dieser kodierte Zustand wird nun gesendet und somit einem Rauschen ausgesetzt. Wie können wir jetzt hiermit die dabei aufgetretenen Fehler beheben?

Dazu gehen wir zu einer anderen Darstellung der linearen Codes über. Man kann einen linearen Code C auch durch seine sogenannte *Paritätsmatrix* H darstellen. Dabei ist H so gewählt, dass $\ker(H) = C$ gilt, dass also genau die Codewörter $y \in C$ die Gleichung $Hy = 0$ erfüllen. Diese Matrix H ist eine $n - k \times n$-Matrix über $\mathbb{F}_2$ und existiert immer. Zum Beispiel ist die Paritätsmatrix H für den 3-Qubit-Bitflip-Code gegeben durch

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Hiermit kann man nun Fehlerkorrektur betreiben.

Sei $y = Gx$ die kodierte Nachricht x, weiter sei $y' = y + e$ die kodierte Nachricht, nachdem sie einen Kanal durchlaufen hat, e bezeichne den Fehler von y. Da $\ker(H) = C$ gilt, ist $Hy' = Hy + He = He$. Somit liefert die Messung von H das sogenannte *Fehlersyndrom* He. Berechnet man nun He_k für alle möglichen Fehler e_k, so kann man durch Vergleich dieser Werte mit He auf den Fehler e schließen und diesen durch eine geeignete Transformation korrigieren.

Beispiel 4.2. Wir nehmen an, dass höchstens einem Qubit im Kanal ein Bitflip widerfährt. Dann kann der 3-Qubit-Bitflip-Code diese Fehler korrigieren.

Dazu vergleicht man die Parität (entsprechend zu H) des ersten und zweiten Qubits mit der des zweiten und dritten Qubits. Beginnen wir mit dem kodierten Zustand $|\psi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$, so liefert uns der Code für die möglichen Zustände $|\psi'\rangle = \alpha|0'_L\rangle + \beta|1'_L\rangle$.

$\|\psi'\rangle$	$P(110)$	$P(011)$
$\alpha\|000\rangle + \beta\|111\rangle$	0	0
$\alpha\|100\rangle + \beta\|011\rangle$	1	0
$\alpha\|010\rangle + \beta\|101\rangle$	1	1
$\alpha\|001\rangle + \beta\|110\rangle$	0	1

Aus der nebenstehenden Tabelle ist ersichtlich, dass wir aus den Paritäten bezüglich H eindeutig festlegen können, welches Bit geflipt werden muss, um den ursprünglichen Zustand y zu erhalten. Hieran sieht man auch, dass wir zwar den Fehler kennen, aber keinerlei Information über den Zustand $|\psi\rangle$ erhalten haben, da uns α und β auch nach der Messung völlig unbekannt sind. Durch unsere Messung der Paritäten dürfen wir keine Information gewinnen, da sonst der Zustand gestört wird.

Es ist zu beachten, dass nicht jeder Code jeden Fehler korrigieren kann. So korrigiert der 3-Qubit-Bitflip-Code lediglich Bitflip- und keine Phasenfehler und auch nur dann, wenn höchstens ein solcher Fehler pro Zustand auftritt. Daher muss man der Situation entsprechend einen geeigneten Code wählen. Die Existenz solcher Codes wird durch die Quanten-Hamming-Schranke (4.1) begrenzt. Diese liefert als notwendige Bedingung für die Existenz eines linearen $[n, k]$-Codes C, welcher bis zu t Fehler korrigiert, dass

$$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n \tag{4.1}$$

gelten muss. Eine hinreichende Bedingung für die Existenz liefert die Gilbert-Varshanov-Schranke, die

$$\frac{k}{n} \geq 1 - H(\frac{2t}{n}) \quad \text{mit } H(x) = -x\log x - (1-x)\log(1-x) \tag{4.2}$$

fordert. Beachtet man diese Schranken, so kann man stets davon ausgehen, dass ein geeigneter Code existiert, sofern man nicht mit zu wenig Qubits zu viele Fehler korrigieren will.

Beispiel 4.3. Ein weiteres bekanntes Beispiel für einen linearen Code ist der $[7, 4]$-Hamming-Code, welcher 4 Qubits in 7 Qubits umwandelt und einen Bitflip-Fehler korrigieren kann. Er ist charakterisiert durch folgende Generatormatrix G, bzw. Paritätsmatrix H:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \qquad H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix},$$

Betrachtet man die sich ergebenden Codewörter nach Tabelle 4.1, so fällt auf, dass sich die einzelnen Codewörter um mindestens 3 Stellen voneinander unterscheiden. Daher kann man bei nur einem Bitflip wieder auf den ursprünglichen Zustand korrigieren, da sich der Zustand nur an einer Stelle hiervon unterscheidet und von allen anderen um mindestens zwei Stellen.

x	Gx	x	Gx
0 0 0 0	0 0 0 0 0 0 0	1 1 1 1	1 1 1 1 1 1 1
1 0 0 0	1 0 0 0 0 1 1	0 1 1 1	0 1 1 1 1 0 0
0 1 0 0	0 1 0 0 1 0 1	1 0 1 1	1 0 1 1 0 1 0
0 0 1 0	0 0 1 0 1 1 0	1 1 0 1	1 1 0 1 0 0 1
0 0 0 1	0 0 0 1 1 1 1	1 1 1 0	1 1 1 0 0 0 0
1 1 0 0	1 1 0 0 1 1 0	0 0 1 1	0 0 1 1 0 0 1
0 1 1 0	0 1 1 0 0 1 1	1 0 0 1	1 0 0 1 1 0 0
1 0 1 0	1 0 1 0 1 0 1	0 1 0 1	0 1 0 1 0 1 0

Tabelle 4.1: Codewörter des $[7, 4]$-Hamming-Codes

Ermittelt man hier die Paritäten bezüglich H, so ergibt sich beispielhaft am Codewort 1001100 folgendes Bild nach Tabelle 4.2. Der Vorteil des Hamming-Codes ist, dass

Bob's Ergebnis	$P(0001111)$	$P(0110011)$	$P(1010101)$
1 0 0 1 1 0 0	0	0	0
0 0 0 1 1 0 0	0	0	1
1 1 0 1 1 0 0	0	1	0
1 0 1 1 1 0 0	0	1	1
1 0 0 0 1 0 0	1	0	0
1 0 0 1 0 0 0	1	0	1
1 0 0 1 1 1 0	1	1	0
1 0 0 1 1 0 1	1	1	1

Tabelle 4.2: Paritäten bzgl. H am Beispiel der Nachricht 1001100

das Fehlersyndrom gerade die Stelle als Binärcode angibt, an der der Bitflip aufgetreten ist. Dadurch ist es hiermit sehr einfach, Fehler zu lokalisieren und zu korrigieren.

Bemerkung 4.4. Die Paritätsmatrix H ist uns schon im Abschnitt 2.1.1 über Fehlerkorrektur mittels Informationsabgleich begegnet. Auch hier haben wir Hx bestimmt und daraus den ursprünglichen klassischen Zustand abgeleitet. Dabei mussten wir allerdings unsere Messergebnisse mit denen von Alice abstimmen. Da wir hier schon wissen, dass wir ein Codewort suchen, brauchen wir diesen Schritt nicht mehr, da alle Codewörter $Hy = 0$ liefern. Dafür muss Alice uns aber mitteilen, welchen Code sie

benutzt hat. Betrachten wir als Code C' denjenigen Code, der entsteht, wenn man die Codewörter jeweils um einen festen Wert v ändert. Dann kann man ebenfalls den Fehler korrigieren, sofern man Hv kennt. Dabei ist es unerheblich, welchen Wert v konkret hat. Somit ergibt sich hier genau die gleiche Situation wie bei der klassischen Fehlerkorrektur und diese Schritte sind äquivalent. Wir haben also die klassische Fehlerkorrektur mit linearen Codes auf die Fehlerkorrektur von Quantenzuständen erweitert.

4.1.2 CSS-Codes

Calderbank-Shor-Steane-Codes basieren auf linearen Codes und den dazu gehörenden dualen Codes. Ist C ein $[n,k]$-Code mit Generatormatrix G und Paritätsmatrix H, so ist der duale Code $C^\perp$ ein $[n,n-k]$-Code und gegeben durch die Generatormatrix $G^\perp = H^T$ und die Paritätsmatrix $H^\perp = G^T$. Er besteht aus allen Codewörtern $z \in \mathbb{F}_2^n$, die senkrecht auf allen Codewörtern $x \in C \subset \mathbb{F}_2^n$ im $\mathbb{F}_2^n$ stehen. Daher kommt auch die Bezeichnung $C^\perp$.

Wir können aus zwei linearen Codes C_1 und C_2 den $CSS(C_1,C_2)$-Code konstruieren. Sei dazu C_1 ein $[n,k_1]$-Code mit Generatormatrix G_1 und Paritätsmatrix H_1 und C_2 (mit G_2 und H_2) ein $[n,k_2]$-Code mit $C_2 \subset C_1$. Dann ist die Menge $C_1/C_2 = \{x + C_2 : x \in C_1\}$ wohldefiniert und bildet den $CSS(C_1,C_2)$-Code. Es gilt

$$\begin{aligned} x_1 + C_2 = x_2 + C_2 \quad &\Leftrightarrow \quad x_1 - x_2 \in C_2 \\ x_1 + C_2 \perp x_2 + C_2 \quad &\Leftrightarrow \quad x_1 - x_2 \notin C_2. \end{aligned} \tag{4.3}$$

Da man hierbei also von den 2^{k_1} Codewörtern jeweils 2^{k_2} Codewörter gleichsetzt (diese unterscheiden sich nur um ein Codewort $y \in C_2$), besteht der neue Code aus $2^{k_1-k_2}$ Codewörtern und bildet somit einen $[n,k_1-k_2]$-Code.

Ein beliebiger Zustand $|x\rangle$ wird mittels $CSS(C_1,C_2)$-Code also abgebildet auf

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle \,. \tag{4.4}$$

Beispiel 4.5. Wir wählen als $C_1 =: C$ den $[7,4]$-Hamming-Code mit Matrizen G und H aus dem vorherigen Abschnitt und als C_2 den dazu dualen $[7,3]$-Code $C^\perp$ mit Generatormatrix $G_2 = H^T$ und Paritätsmatrix $H_2 = G^T$. Hierfür gilt $C_2 \subset C_1$, wie man durch Vergleich von H und H_2 sofort sieht. Der hieraus resultierende $CSS(C_1,C_2)$-Code ist ein $[7,1]$-Code und wird als Steane-Code bezeichnet. Berechnet man zunächst C_1 und C_2, so erhält man als mögliche Codewörter die Ergebnisse der folgenden Tabelle 4.3. Damit erhält man als logische Codewörter der Basiszustände

$$\begin{aligned} |0_L\rangle &= \frac{1}{\sqrt{8}}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |0001111\rangle + \\ &\qquad + |1101001\rangle + |0111100\rangle + |1011010\rangle + |1100110\rangle) \\ |1_L\rangle &= \frac{1}{\sqrt{8}}(|1111111\rangle + |0101010\rangle + |1001100\rangle + |1110000\rangle + \\ &\qquad + |0010110\rangle + |1000011\rangle + |0100101\rangle + |0011001\rangle). \end{aligned}$$

x	Gx	x	Gx	x'	$G^{\perp}x'$
0 0 0 0	0 0 0 0 0 0 0	1 1 1 1	1 1 1 1 1 1 1	0 0 0	0 0 0 0 0 0 0
1 0 0 0	1 0 0 0 0 1 1	0 1 1 1	0 1 1 1 1 0 0	0 0 1	1 0 1 0 1 0 1
0 1 0 0	0 1 0 0 1 0 1	1 0 1 1	1 0 1 1 0 1 0	0 1 0	0 1 1 0 0 1 1
0 0 1 0	0 0 1 0 1 1 0	1 1 0 1	1 1 0 1 0 0 1	1 0 0	0 0 0 1 1 1 1
0 0 0 1	0 0 0 1 1 1 1	1 1 1 0	1 1 1 0 0 0 0	1 1 1	1 1 0 1 0 0 1
1 1 0 0	1 1 0 0 1 1 0	0 0 1 1	0 0 1 1 0 0 1	1 1 0	0 1 1 1 1 0 0
0 1 1 0	0 1 1 0 0 1 1	1 0 0 1	1 0 0 1 1 0 0	1 0 1	1 0 1 1 0 1 0
1 0 1 0	1 0 1 0 1 0 1	0 1 0 1	0 1 0 1 0 1 0	0 1 1	1 1 0 0 1 1 0

Tabelle 4.3: Codewörter des CSS-Codes in Beispiel 4.5

Korrigieren C_1 und C_2 jeweils bis zu t Fehler, so korrigiert der CSS-Code ebenfalls bis zu t Fehler. Dabei ist die Korrektur von Phasen- und Bitflip-Fehlern unabhängig voneinander, was sich später als nützliche Eigenschaft dieses Codes erweisen wird. Der CSS-Code kann ebenfalls durch eine Paritätsmatrix H der folgenden Gestalt beschrieben werden.

$$H = \left(\begin{array}{c|c} H_2^{\perp} & 0 \\ 0 & H_1 \end{array} \right)$$

Dabei gibt die linke Seite die Matrix an, mit der man Phasenfehler korrigiert, und die rechte Seite beschreibt die Matrix für die Bitflip-Fehler. Dies wird im folgenden deutlich.

Der kodierte Zustand $|x + C_2\rangle$ wird zunächst durch einen Kanal geschickt. Sei der dabei resultierende Bitflip-Fehler beschrieben durch e_1 und der Phasenfehler durch e_2. Dann besitzt der verrauschte Zustand $|x + C_2\rangle' = \mathcal{E}(|x + C_2\rangle \langle x + C_2|)$ folgende Gestalt

$$|x + C_2\rangle' = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)e_2} |x + y + e_1\rangle . \tag{4.5}$$

Wir korrigieren zunächst den Bitflip-Fehler e_1. Dazu koppeln wir unser System mit einem Hilfs-System $|0\rangle^{\otimes n-k}$ und transformieren den Zustand $|x + y + e_1\rangle |0\rangle^{\otimes n-k}$ durch Kopplung bezüglich H_1 auf $|x + y + e_1\rangle |H_1(x + y + e_1)\rangle = |x + y + e_1\rangle |H_1 e_1\rangle$. Eine Messung von $H_1 e_1$ liefert dann das Fehlersyndrom und wir können analog zu den linearen Codes den Bitflip-Fehler durch eine geeignete unitäre Transformation korrigieren, ohne den Zustand selbst verändert zu haben. Damit haben wir nach diesem Schritt den Zustand

$$|x + C_2\rangle'' = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)e_2} |x + y\rangle \tag{4.6}$$

vorliegen.

Die Korrektur des Phasenfehlers erfolgt über eine Hadamardtransformation H. Wir erhalten

$$\mathrm{H} |x + C_2\rangle'' = \frac{1}{\sqrt{2^n |C_2|}} \sum_z \sum_{y \in C_2} (-1)^{(x+y)(e_2+z)} |z\rangle$$

$$= \frac{1}{\sqrt{2^n|C_2|}} \sum_{z'} \sum_{y \in C_2} (-1)^{(x+y)z'} |z' + e_2\rangle \quad \text{mit } z' := z + e_2.$$

Führt man die Summe über $y \in C_2$ aus, so ergibt sich mit (4.3)

$$\sum_{y \in C_2} (-1)^{yz'} = \begin{cases} |C_2| & \text{für } z' \in C_2^\perp \\ 0 & \text{für } z' \notin C_2^\perp \end{cases}$$

und damit

$$\mathrm{H} |x + C_2\rangle'' = \frac{|C_2|}{\sqrt{2^n|C_2|}} \sum_{z' \in C_2^\perp} (-1)^{xz'} |z' + e_2\rangle . \tag{4.7}$$

Somit können wir hier analog zum Bitflip-Fehler den Fehler durch ein entsprechendes Hilfs-System und Messung von $H_2^\perp e_2 = G_2 e_2$ korrigieren und erhalten den Zustand

$$\frac{|C_2|}{\sqrt{2^n|C_2|}} \sum_{z' \in C_2^\perp} (-1)^{xz'} |z'\rangle . \tag{4.8}$$

Eine wiederholte Anwendung der Hadamardtransformation überführt diesen Zustand dann in $|x + C_2\rangle$ und wir haben die Fehler korrigiert.

Da wir die Fehler mit den linearen Codes C_1 bzw. $C_2^\perp$ korrigieren, ist somit klar, dass der CSS-Code bis zu t Fehler korrigiert, wenn C_1 und $C_2^\perp$ bis zu t Fehler korrigieren.

Die Existenz solcher CSS-Codes ist ebenfalls durch eine Gilbert-Varshamov-Schranke gegeben, die besagt, dass ein $[n, k]$-CSS-Code existiert, der bis zu t Fehler korrigiert, falls gilt:

$$\frac{k}{n} \geq 1 - 2H(\frac{2t}{n}) \quad \text{mit } H(x) = -x \log x - (1 - x) \log(1 - x). \tag{4.9}$$

Somit können wir auch hier davon ausgehen, dass ein CSS-Code existiert, sofern wir n entsprechend zu t groß genug wählen.

Ein Spezialfall der CSS-Codes ist dadurch gegeben, dass wir das Codewort zusätzlich mit einem konkreten Phasen- und Bitflip (charakterisiert durch zwei Binärfolgen u und v) versehen. Dieses wird dann mit $CSS_{u,v}$ bezeichnet und bildet das Codewort x ab auf den Zustand

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{uy} |x + y + v\rangle . \tag{4.10}$$

Da u und v fest gewählt sind, ist $C_{u,v} \cong C$. Damit ist dieser Code äquivalent zum CSS-Code mit $u = 0$ und $v = 0$.

Der zusätzliche Bitflip v ist genau der gleiche Bitflip wie in Bemerkung 4.4. Bei der Verwendung linearer Codes wird meistens die Phase vernachlässigt. Wählen wir also $C_2 = 0$, so haben wir eine weitere äquivalente Darstellung der Fehlerkorrektur in Abschnitt 2.1.1 gefunden.

4.1.3 Implementierung der CSS-Codes

Hier werden beispielhaft einige Quantenschaltungen zur Implementierung der Codes im vorherigen Abschnitt 4.1.2 angegeben. Zur Schreibweise der Quantengatter sei auf die Literatur, z.B. [14], verwiesen.

Der lineare $[7, 4]$-Hamming-Code G lässt wie in Abbildung 4.1 implementieren. Dabei ist sofort offensichtlich, dass die angegebene Schaltung einer Operation von G entspricht.

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

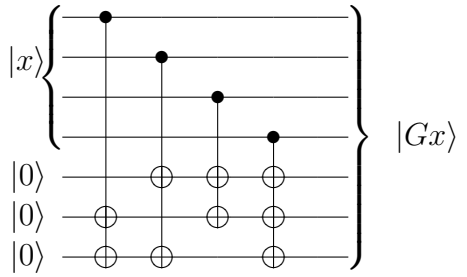


Abbildung 4.1: Implementierung des [7,4]-Hamming-Codes

Der daraus abgeleitete Stean-Code implementiert sich nach folgendem Schema.

$$G_2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

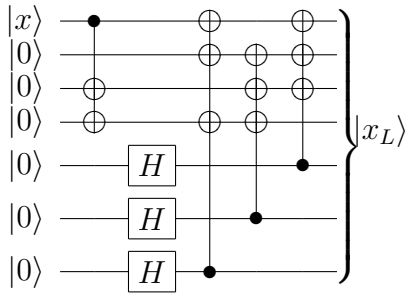


Abbildung 4.2: Implementierung des Stean-Codes

Die erste CNOT-Operation liefert den Zustand $|0000000\rangle$ für $|x\rangle = |0\rangle$ und den Zustand $|1011000\rangle$ für $|x\rangle = |1\rangle$. Dadurch wird jeweils ein Vertreter des logischen Codebits ($|0_L\rangle$ oder $|1_L\rangle$) erzeugt. Das gesamte Codewort eines Codebits besteht entsprechend Gleichung (4.4) aus einer Superposition des Vertreters selbst und den dazu addierten Codewörtern aus C_2. Um dies zu implementieren, erzeugen wir zunächst die gleichgewichtete Superposition aller Drei-Qubit-Zustände, indem wir auf drei Qubitzustände $|0\rangle$ jeweils eine Hadamard-Transformation anwenden. Im weiteren wenden wir entsprechend der Einträge in G_2 CNOT-Operationen auf diese Superposition an. Dies entspricht der Addition der Superposition von Zuständen aus C_2 mit dem zuvor erzeugten Vertreter.

Die Implementierung der Fehlerkorrektur ist somit ebenfalls klar. Es wird eine Schaltung implementiert, welche einer Operation der Paritätsmatrix auf die Codequbits entspricht. Da die Parität der Zustände $|\psi\rangle$ durch die Polarisation bezüglich der $z-$Achse gegeben ist, misst man in nebenstehender Schaltung Z für die drei Hilfs-Qubits und erhält hierdurch das Fehlersyndrom He_1. Daraus kann man dann den ermittelten Fehler durch eine geeignete Transformation σ_1 korrigieren.

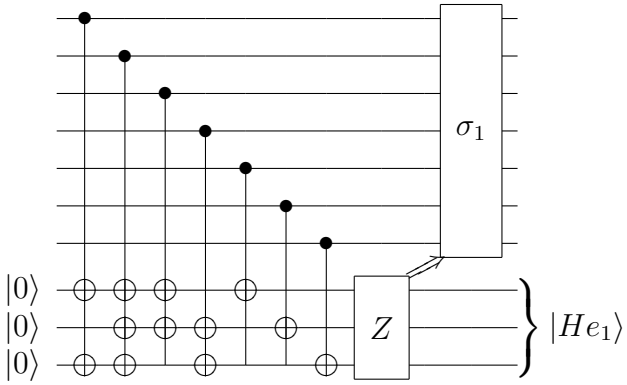


Abbildung 4.3: Implementierung der Fehlerkorrektur

Die Fehlerkorrektur bezüglich der Phasenflip-Fehler erfolgt auf ähnliche Weise. Man schaltet eine Hadamard-Transformation davor und misst nun bezüglich $H_2 = G^T$.

Zur Dekodierung werden die CNOT-Gatter der Kodierung umgekehrt, d.h. Kontroll- und Zielqubits werden im Kodierungsschema vertauscht. Damit ergibt sich beispielsweise die Dekodierung des $[7, 4]$ Hamming-Codes nach nebenstehender Schaltung.

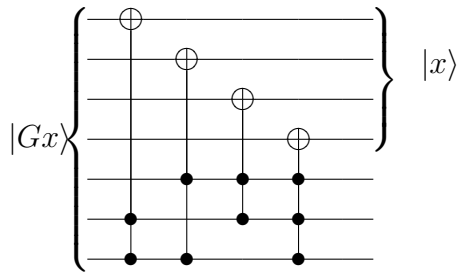


Abbildung 4.4: Implementierung der Dekodierung

4.2 Verschränkungs-Purifizierung

Verfahren, um ausgehend von einem Gemisch reinere Zustände zu erhalten, bezeichnet man als *Purifizierung* (purification). Verfahren zur Erhöhung der Verschränkung von Zuständen sind als *Verschränkungsdestillation* (entanglement distillation) bekannt [11]. Wir werden hier ein kombiniertes Verfahren vorstellen, welches sowohl die Reinheit unseres Gemisches als auch die Verschränkung erhöht. Dieses Verfahren wird dann im Allgemeinen mit *Verschränkungspurifizierung* (entanglement purification (EP)) bezeichnet. Wir betrachten hier Verfahren, welche mit einseitiger Kommunikation auskommen, d.h. Alice kann an Bob klassische Information übermitteln, Bob allerdings nicht an Alice. Diese Protokolle bezeichnen wir dann als 1-EPP um sie gegenüber Protokollen mit zweiseitiger Kommunikation abzugrenzen. Der Grund für diese Einschränkung wird in Abschnitt 4.3 ersichtlich, in dem wir zeigen werden, wie man aus einem 1-EPP ein QECC-Protokoll erhält.

EP-Protokolle basieren auf der wiederholten Anwendung der folgenden drei Schritte:

(i) Alice und Bob führen an ihren Zuständen lokale unitäre Operationen U durch,

(ii) Alice und Bob messen ($\mathcal{M}$) einige ihrer Qubits,

(iii) Alice und Bob vergleichen ihre Messwerte und legen hierauf basierend die nächsten lokalen unitären Operationen für Schritt (i) fest.

Dabei gehen wir ohne Einschränkung davon aus, dass Alice und Bob von-Neumann-Messungen durchführen. Kommutieren die Operatoren dieses Verfahrens, so kann man alles in einem Schritt durchführen, das Prinzip bleibt aber das selbe. Das Verfahren ist in Abbildung 4.5 dargestellt.

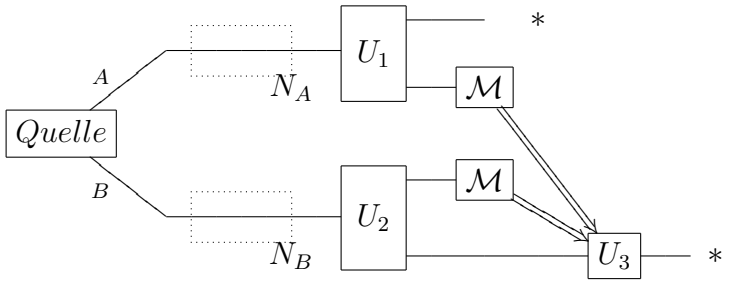


Abbildung 4.5: Schematische Darstellung eines 1-EPP; N_A und N_B repräsentieren das Rauschen im Kanal

Der Einfachheit halber gehen wir davon aus, dass der Zustand $|\psi\rangle' = \mathcal{E}(|\psi\rangle\langle\psi|)$, nachdem er den Kanal durchlaufen hat, ein Wernerzustand ist

$$W_F = F\left|\phi^+\right\rangle\left\langle\phi^+\right| + \frac{1-F}{3}(\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \left|\phi^-\right\rangle\left\langle\phi^-\right| + \left|\Psi^-\right\rangle\left\langle\Psi^-\right|).$$

Dies stellt prinzipiell keine Einschränkung dar, da man durch eine umkehrbare Verzwirbelung (twirl) [11] jedes Gemisch auf diese Form bringen kann. Wir betrachten also nur EP-Protokolle für diese Gemische und können uns somit der klassischen Wahrscheinlichkeitstheorie bedienen.

Die vier Bell-Zustände sind unter den folgenden Operationen invariant:

(1) unilaterale Rotationen π_u um den Winkel π : Dabei dreht (ohne Einschränkung) Alice ihr Qubit um π um eine feste Achse; diese Operation wird beschrieben durch $\sigma_k \otimes \mathbf{1}$, wobei σ_k eine der drei Paulimatrizen σ_x, σ_y oder σ_z ist.

(2) bilaterale Rotationen $\pi/2_b$ um den Winkel $\pi/2$: Dabei drehen Alice und Bob jeweils ihr Qubit eines verschränkten Paares um $\pi/2$ um eine feste Achse; sie wird beschrieben durch $B_k = b_k \otimes b_k$ $(k = x, y, z)$ mit

$$b_x = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}, b_y = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, b_z = \frac{1}{\sqrt{2}} \begin{pmatrix} 1-i & 0 \\ 0 & 1+i \end{pmatrix}$$

(3) bilaterales CNOT, auch bezeichnet als BXOR: Alice und Bob führen jeweils mit ihren Hälften zweier Qubitpaare ein CNOT durch, wobei ein Qubitpaar als Kontrollpaar und eines als Zielpaar fungiert.

Die BXOR-Operation wird beschrieben durch die Abbildung

$$\left|x^A, x^B\right\rangle \left|y^A, y^B\right\rangle \overset{\text{BXOR}}{\longrightarrow} \left|x^A, x^B\right\rangle \left|x^A + y^A, x^B + y^B\right\rangle . \tag{4.11}$$

BXOR folgt dem folgenden Schaltbild.

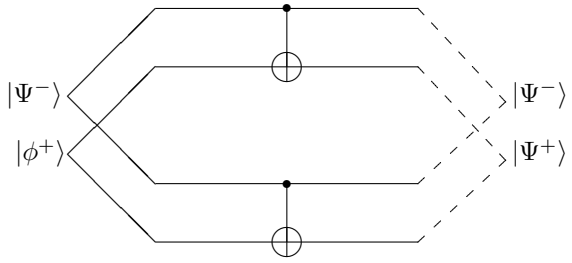


Abbildung 4.6: Schematische Darstellung der bilateralen CNOT-Operation

Wir geben hier einige Beispiele für die Berechnungen der Bilder der Bellzustände unter diesen Operationen.

Beispiel 4.6. Wir betrachten die unilaterale Rotation π_u um die x-Achse. Die Abbildungsvorschrift ist dann gegeben durch $\sigma_x \otimes \mathbf{1}$. Dies bedeutet

$$\sigma_x \otimes \mathbf{1} \left|00\right\rangle = -\left|10\right\rangle \qquad \sigma_x \otimes \mathbf{1} \left|11\right\rangle = -\left|01\right\rangle$$
$$\sigma_x \otimes \mathbf{1} \left|01\right\rangle = -\left|11\right\rangle \qquad \sigma_x \otimes \mathbf{1} \left|10\right\rangle = -\left|00\right\rangle$$

Damit folgt für die Bellzustände

$$\sigma_x \otimes \mathbf{1} \left|\phi^\pm\right\rangle = \frac{1}{\sqrt{2}}(\sigma_x \otimes \mathbf{1} \left|00\right\rangle \pm \sigma_x \otimes \mathbf{1} \left|11\right\rangle) = -\frac{1}{\sqrt{2}}(\left|10\right\rangle \pm \left|01\right\rangle) = \left|\Psi^p m\right\rangle$$

$$\sigma_x \otimes \mathbf{1} \left|\Psi^\pm\right\rangle = \frac{1}{\sqrt{2}}(\sigma_x \otimes \mathbf{1} \left|10\right\rangle \pm \sigma_x \otimes \mathbf{1} \left|01\right\rangle) = -\frac{1}{\sqrt{2}}(\left|00\right\rangle \pm \left|11\right\rangle) = \left|\phi^p m\right\rangle$$

Als Beispiel einer bilateralen Rotation betrachten wir $B_y = b_y \otimes b_y$. Diese bilden folgendermaßen ab

$$b_y |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad b_y |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Die Bilder der Rechenbasis sind dann

$$\begin{aligned}
B_y |00\rangle &= \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle + |11\rangle - |01\rangle - |10\rangle) \\
B_y |11\rangle &= \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |11\rangle + |01\rangle + |10\rangle) \\
B_y |01\rangle &= \frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle - |11\rangle + |01\rangle - |10\rangle) \\
B_y |10\rangle &= \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |11\rangle - |01\rangle + |10\rangle).
\end{aligned}$$

Damit folgt für die Bellzustände beispielsweise

$$\begin{aligned}
B_y \left|\phi^+\right\rangle &= \frac{1}{\sqrt{2}}(B_y |00\rangle + B_y |11\rangle) \\
&= \frac{1}{2\sqrt{2}}(|00\rangle + |11\rangle - |01\rangle - |10\rangle + |00\rangle + |11\rangle + |01\rangle + |10\rangle) \\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \left|\phi^+\right\rangle
\end{aligned}$$

$$\begin{aligned}
B_y \left|\phi^-\right\rangle &= \frac{1}{\sqrt{2}}(B_y |00\rangle - B_y |11\rangle) \\
&= \frac{1}{2\sqrt{2}}(|00\rangle + |11\rangle - |01\rangle - |10\rangle - |00\rangle - |11\rangle - |01\rangle - |10\rangle) \\
&= -\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \left|\Psi^+\right\rangle
\end{aligned}$$

und entsprechend $B_y |\Psi^+\rangle = \phi^-, B_y |\Psi^-\rangle = B_y |\Psi^-\rangle$ für die $|\Psi^\pm\rangle$ Zustände.

Zur Verdeutlichung der BXOR-Operation ist ebenfalls ein Beispiel angegeben. Dabei entsprechen die ersten beiden Qubits dem Kontrollpaar und die beiden hinteren dem Zielpaar.

$$\begin{aligned}
\left|\Psi^-\right\rangle \left|\phi^+\right\rangle \quad &= \quad \frac{1}{2}((|01\rangle - |10\rangle)(|00\rangle + |11\rangle)) \\
&= \quad \frac{1}{2}(|01\rangle |00\rangle + |01\rangle |11\rangle - |10\rangle |00\rangle - |10\rangle |11\rangle) \\
&\xrightarrow{\text{BXOR}} \quad \frac{1}{2}(|01\rangle |01\rangle + |01\rangle |10\rangle - |10\rangle |10\rangle - |10\rangle |01\rangle)
\end{aligned}$$

$$\begin{aligned} &= \frac{1}{2}((|01\rangle - |10\rangle)(|01\rangle + |10\rangle)) \\ &= \left|\Psi^-\right\rangle \left|\Psi^+\right\rangle \end{aligned}$$

Insgesamt erhält man damit die folgenden Zustandsabbildungen nach Tabelle 4.4.

		Eingangszustand			
	Operation	$\|\Psi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|\Psi^+\rangle$
π_u	I	$\|\Psi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|\Psi^+\rangle$
	σ_x	$\|\phi^-\rangle$	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$	$\|\phi^+\rangle$
	σ_y	$\|\phi^+\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$	$\|\phi^-\rangle$
	σ_z	$\|\Psi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\Psi^-\rangle$
$\pi/2_b$	I	$\|\Psi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|\Psi^+\rangle$
	B_x	$\|\Psi^-\rangle$	$\|\phi^-\rangle$	$\|\Psi^+\rangle$	$\|\phi^+\rangle$
	B_y	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^-\rangle$
	B_z	$\|\Psi^-\rangle$	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\Psi^+\rangle$
		Kontrollpaar			
	Ziel	$\|\Psi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|\Psi^+\rangle$
BXOR	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\Psi^-\rangle$
		$\|\phi^-\rangle$	$\|\Psi^-\rangle$	$\|\Psi^-\rangle$	$\|\phi^-\rangle$
	$\|\phi^-\rangle$	$\|\Psi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\Psi^-\rangle$
		$\|\Psi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^-\rangle$	$\|\Psi^-\rangle$
	$\|\phi^+\rangle$	$\|\Psi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|\Psi^+\rangle$
		$\|\Psi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|\Psi^+\rangle$
	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$	$\|\phi^-\rangle$	$\|\phi^+\rangle$	$\|\Psi^+\rangle$
		$\|\phi^+\rangle$	$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	$\|\phi^+\rangle$

Tabelle 4.4: Zusammenstellung der Abbildungen, unter denen die Bellzustände invariant sind

Wir stellen zunächst die grundlegende Idee am Beispiel zweier Wernerzustände vor, wie man mittels der BXOR-Operation und einer Messung die Treue des anderen Zustandes erhöhen kann. Wir starten also mit zwei Wernerzuständen

$$\begin{aligned} \rho_s &= F\left|\phi^+\right\rangle\left\langle\phi^+\right| + \frac{1-F}{3}(\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \left|\phi^-\right\rangle\left\langle\phi^-\right| + \left|\Psi^-\right\rangle\left\langle\Psi^-\right|) \text{ und} \\ \rho_t &= F\left|\phi^+\right\rangle\left\langle\phi^+\right| + \frac{1-F}{3}(\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \left|\phi^-\right\rangle\left\langle\phi^-\right| + \left|\Psi^-\right\rangle\left\langle\Psi^-\right|). \end{aligned}$$

Die Anwendung der CNOT-Operation auf zwei beliebige Zustände

$$|\psi\rangle_s = \alpha|0\rangle + \beta|1\rangle \quad \text{und} \quad |\varphi\rangle_t = \gamma|0\rangle + \delta|1\rangle$$

liefert

$$|\psi'\rangle_s = (\alpha\gamma + \alpha\delta)|0\rangle + (\beta\gamma + \beta\delta)|1\rangle \quad \text{und}$$

$$|\varphi'\rangle_t = (\alpha\gamma + \beta\delta)\,|0\rangle + (\alpha\delta + \beta\gamma)\,|1\rangle\,. \tag{4.12}$$

Hieraus resultieren die Ergebnisse nach Tabelle 4.5. Sie stellt zum einen dar, wie die auftretenden Kombinationen der Bellzustände abgebildet werden (analog zu Tabelle 4.4), und gibt außerdem den nach (4.12) ermittelten Vorfaktor der Ausgangszustände an.

Vorfaktor	Eingang	Ausgang	Vorfaktor	Eingang	Ausgang
F^2	$\|\phi^+\rangle_s \|\phi^+\rangle_t$	$\|\phi^+\rangle_s \|\phi^+\rangle_t$	$\frac{F(1-F)}{3}$	$\|\Psi^+\rangle_s \|\phi^+\rangle_t$	$\|\Psi^+\rangle_s \|\Psi^+\rangle_t$
$\frac{F(1-F)}{3}$	$\|\phi^+\rangle_s \|\phi^-\rangle_t$	$\|\phi^-\rangle_s \|\phi^-\rangle_t$	$\frac{(1-F)^2}{9}$	$\|\Psi^+\rangle_s \|\phi^-\rangle_t$	$\|\Psi^-\rangle_s \|\Psi^-\rangle_t$
$\frac{F(1-F)}{3}$	$\|\phi^+\rangle_s \|\Psi^+\rangle_t$	$\|\phi^+\rangle_s \|\phi^+\rangle_t$	$\frac{(1-F)^2}{9}$	$\|\Psi^+\rangle_s \|\Psi^+\rangle_t$	$\|\Psi^+\rangle_s \|\phi^+\rangle_t$
$\frac{F(1-F)}{3}$	$\|\phi^+\rangle_s \|\Psi^-\rangle_t$	$\|\phi^-\rangle_s \|\Psi^-\rangle_t$	$\frac{(1-F)^2}{9}$	$\|\Psi^+\rangle_s \|\Psi^-\rangle_t$	$\|\Psi^-\rangle_s \|\phi^-\rangle_t$
$\frac{F(1-F)}{3}$	$\|\phi^-\rangle_s \|\phi^+\rangle_t$	$\|\phi^-\rangle_s \|\phi^+\rangle_t$	$\frac{F(1-F)}{3}$	$\|\Psi^-\rangle_s \|\phi^+\rangle_t$	$\|\Psi^+\rangle_s \|\Psi^-\rangle_t$
$\frac{(1-F)^2}{9}$	$\|\phi^-\rangle_s \|\phi^-\rangle_t$	$\|\phi^+\rangle_s \|\phi^-\rangle_t$	$\frac{(1-F)^2}{9}$	$\|\Psi^-\rangle_s \|\phi^-\rangle_t$	$\|\Psi^-\rangle_s \|\Psi^-\rangle_t$
$\frac{(1-F)^2}{9}$	$\|\phi^-\rangle_s \|\Psi^+\rangle_t$	$\|\phi^-\rangle_s \|\Psi^+\rangle_t$	$\frac{(1-F)^2}{9}$	$\|\Psi^-\rangle_s \|\Psi^+\rangle_t$	$\|\Psi^-\rangle_s \|\phi^+\rangle_t$
$\frac{(1-F)^2}{9}$	$\|\phi^-\rangle_s \|\Psi^-\rangle_t$	$\|\phi^+\rangle_s \|\Psi^-\rangle_t$	$\frac{(1-F)^2}{9}$	$\|\Psi^-\rangle_s \|\Psi^-\rangle_t$	$\|\Psi^+\rangle_s \|\phi^-\rangle_t$

Tabelle 4.5: Bild der BXOR-Operation, aufgeteilt nach den einzelnen Summanden

Messen wir nun den Zustand des Zielqubits mit $Z \otimes Z$, so können wir durch Vergleich der Messergebnisse darauf schließen, ob das Zielqubit im Zustand $|\phi^\pm\rangle$ oder $|\Psi^\pm\rangle$ vorliegt. Bei gleichem Messergebnis liegt der Zustand $|\phi^\pm\rangle$ vor, bei unterschiedlichem Messergebnis $|\Psi^\pm\rangle$. Dabei erhalten wir allerdings keine Information über die Phase.

Bemerkung 4.7. Da Alice und Bob im Allgemeinen voneinander entfernt sind, können sie keine nichtlokale Messung $Z \otimes Z$ durchführen. Stattdessen messen sie $Z \otimes \mathbf{1}$ und $\mathbf{1} \otimes Z$ und vergleichen ihre Messergebnisse. Sie selektieren hierbei nur nach dem Produkt der Messergebnisse, wodurch dann der gleiche Zustand wie nach der Messung von $Z \otimes Z$ vorliegt. Unter anderem werden so Bellzustände auf Bellzustände abbildet.

Haben wir beispielsweise $|\phi^\pm\rangle$ gemessen, so liegt der Zustand

$$\rho' = F' \left|\phi^+\right\rangle \left\langle\phi^+\right| + \frac{1-F'}{3}(\left|\Psi^+\right\rangle \left\langle\Psi^+\right| + \left|\phi^-\right\rangle \left\langle\phi^-\right| + \left|\Psi^-\right\rangle \left\langle\Psi^-\right|) \tag{4.13}$$

mit Treue

$$F' = \frac{F^2 + (1-F)^2/9}{F^2 + 2F(1-F)/3 + 5(1-F)^2/9} \tag{4.14}$$

vor. Die Treue ergibt sich dabei aus der Summe der Vorfaktoren, welche $|\phi^+\rangle$ als Kontrollpaar im Ausgangszustand haben dividiert durch die Summe aller Vorfaktoren mit $|\phi^+\rangle$ als Zielzustand. Wir berechnen also die Wahrscheinlichkeit, dass wir den Zustand $|\phi^+\rangle$ als Kontrollpaar vorliegen haben, wenn wir $|\phi^+\rangle$ messen.

Hat man $|\Psi^{\pm}\rangle$ als Zielzustand vorliegen, so erhält man nach Transformation mit σ_x das analoge Ergebnis. Für $F > 1/2$ gilt dann $F' > F$. Somit können wir aus zwei Zuständen ρ mit Treue F einen Zustand ρ' mit Treue $F' > F$ erhalten. Wir erhalten nur einen verschränkten Zustand, da wir den gemessenen Zielzustand aufgrund der Messung nicht weiter nutzen können.

Durch Selektieren unserer Zustände anhand der Messergebnisse (bei $|\phi^{\pm}\rangle$ wird der Zustand behalten, bei $|\Psi^{\pm}\rangle$ wird σ_x auf den Zustand angewendet und wir erhalten ebenfalls $|\phi^{\pm}\rangle$) wird also die Treue der verbliebenen Qubits auf Kosten der Gesamtanzahl der Qubits erhöht. Im folgenden zeigen wir zwei effizientere Methoden, die im Allgemeinen die gleiche Erhöhung bei geringerem Verlust an verschränkten Qubits ermöglicht. Diese Verfahren werden später für den Sicherheitsnachweis der Protokolle genutzt.

4.2.1 Einweg-Hashing Methode

Diese Methode erlaubt es, N Paare von Wernerzuständen in $m \approx N(1 - S(W))$ Paare mit höherer Treue zu transformieren. Dieses Protokoll benutzt nur lokale Operationen aus obiger Tabelle 4.4 und einseitige Kommunikation, ist also ein 1-EPP. Dieses Verfahren werden wir später benutzen, um zu verifizieren, ob die von Alice und Bob geteilten Zustände maximal verschränkt sind oder nicht.

Wir beginnen wieder mit einem klassischen Gemisch von Bellzuständen, zum Beispiel einer Folge von Wernerzuständen. Indem wir eventuell eine Bell-Messung an unserem System durchführen, können wir davon ausgehen, dass unser Zustand ein Produkt von Bellzuständen ist. Da wir nur Operationen aus Tabelle 4.4 verwenden werden, kommutiert unsere Operation mit der Bell-Messung und die Messergebnisse sind demnach unabhängig davon, ob wir diese Messung durchführen oder nicht (bzw. irgendwann später). Wir haben also ohne Einschränkung eine Folge von N Bellzuständen vorliegen.

Hierzu wählen wir eine zufällige Binärfolge s der Länge $2N$. Dann sind jedem Bellzustand genau zwei Bits der Folge s zugeordnet. Dabei können jeweils die Kombinationen $00, 01, 10$ und 11 auftreten. Betrachten wir dazu ein Beispiel:

Beispiel 4.8.

Bellzustände:	ϕ^+	ϕ^-	Ψ^+	ϕ^-	Ψ^-
Zufallsfolge s:	01	00	10	11	10

Wir operieren nun auf dem $i-$ten Zustand entsprechend der zugeordneten Zweiergruppe s_i. Wir lassen den vorliegenden Zustand unberührt bei $s_i = 00$ oder $s_i = 01$, wenden die bilaterale Operation B_y an bei $s_1 = 10$ und operieren mit $B_x\sigma_x$ bei $s_i = 11$. Aus Tabelle 4.4 erhält man dann die Ergebnisse der nebenstehenden Tabelle.

	Qubits			
s_i	ϕ^+	Ψ^+	ϕ^-	Ψ^-
00	ϕ^+	Ψ^+	ϕ^-	Ψ^-
01	ϕ^+	Ψ^+	ϕ^-	Ψ^-
10	ϕ^+	ϕ^-	Ψ^+	Ψ^-
11	ϕ^+	Ψ^+	Ψ^-	ϕ^-

Anschließend werden alle Bellzustände außer die bezüglich 00 mittels BXOR in das erste Paar mit $s_i \neq 00$ addiert, welches dann mit $Z \otimes Z$ gemessen wird. Diese Prozedur entspricht also folgender Schaltung.

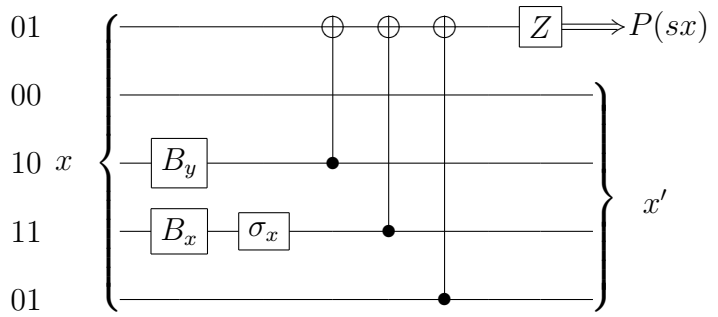


Abbildung 4.7: Beispielhaftes Schaltbild der Einweg-Hashing-Methode

Für unser Beispiel ergibt sich damit folgendes Ergebnis. Dabei bezeichnet BXOR(i,j) die BXOR-Operation mit dem $i-$ten (Ziel-) und $j-$ten (Kontroll-) Qubit. Die Ergebnisse dieser Operation ergeben sich ebenfalls aus Tabelle 4.4.

Anfangszustand	s_i	BXOR(1,3)	BXOR(1,4)	BXOR(1,5)
ϕ^+	ϕ^+	ϕ^+	Ψ^+	ϕ^+
ϕ^-	ϕ^-			
Ψ^+	ϕ^-	ϕ^-		
ϕ^-	Ψ^-		Ψ^+	
Ψ^-	Ψ^-			Ψ^-

Tabelle 4.6: Transfomation der Zustände durch obige Schaltung (Abb. 4.7)

Die Bedeutung dieser Ergebnisse wird klar, wenn man die Bellzustände mit den entsprechenden logischen Bits (siehe Abschnitt 1.2.4) identifiziert. Dann ergibt sich für unser Beispiel folgendes Bild. Zunächst die Ergebnisse der s_i-Operationen.

Bellzustände	ϕ^+	ϕ^-	Ψ^+	ϕ^-	Ψ^-
logische Folge x	00	01	10	10	11
Zufallsfolge s	01	00	10	11	01
Ergebnis	00	01	10	11	11

Tabelle 4.7: logisches Äquivalent der entsprechenden s_i-Operationen

Hieran sieht man, dass wir jeweils die Paritäten $s_i x_i$ der einzelnen Qubits für $s_i \neq 00$ jeweils in das rechte (Paritäts)Bit geschrieben haben. Anhand der obigen Tabelle der

zu s_i entsprechenden Abbildungen kann man sehen, dass dieses auch für alle anderen Fälle gilt. Man braucht also hierfür den vorliegenden Bellzustand nicht zu kennen.

Die BXOR-Operationen ergeben dann abschließend folgendes Ergebnis:

Anfangszustand	logisch	s_i	BXOR(1,3)	BXOR(1,4)	BXOR(1,5)
ϕ^+	00	00	00	01	00
ϕ^-	10	10			
Ψ^+	01	10	10		
ϕ^-	10	11		01	
Ψ^-	11	11			11

Tabelle 4.8: logisches Äquivalent BXOR-Operationen

Man liest ab, dass die Parität sx der logischen Bits ins Paritätsbit des Zielpaares transformiert wurde. Eine Messung von Z auf beiden Seiten und anschließendem Vergleich der Messergebnisse zeigt uns wieder, ob das Qubit im Zustand $|\phi^{\pm}\rangle$ oder $|\Psi^{\pm}\rangle$ vorliegt. Dies entspricht dann einer Parität von 0 für $|\phi^{\pm}\rangle$ oder 1 für $|\Psi^{\pm}\rangle$.

Wir haben also eine Methode gefunden, wie wir zufällige Paritäten von Produkten von Bellzuständen ermitteln können, aber nur einen Bellzustand dafür messen müssen. Dies ermöglicht es, unsere Folge in analoger Weise zur Fehlerkorrektur zu purifizieren, indem wir sie beispielsweise auf $0000\ldots$ korrigieren. Dies entspricht dann einer Purifizierung bezüglich $|\phi^+\rangle^{\otimes m}$.

Die Einweg-Hashing-Methode beruht also auf $N-m$ Durchgängen der folgenden Schritte. Zu Beginn des $k-$ten Durchgangs besitzen Alice und Bob $N-k+1$ ungemessene verschränkte Paare, deren Zustand durch eine $2(N-k+1)-$Bitfolge x_{k-1} beschrieben wird. Hiermit verfahren sie dann wie folgt:

(i) Alice wählt eine Zufallsfolge s_k der Länge $2(N-k+1)$ und teilt diese Bob mit

(ii) Alice und Bob führen entsprechend s_k lokale unitäre Operationen f_{s_k} durch.

(iii) Alice und Bob messen ein vorher festgelegtes Paar bezüglich Z und besitzen nun $N-k$ ungemessene Paare, welche durch die $2(N-k)$-Bitfolge $x_k = f_{s_k}(x_{k-1})$ beschrieben ist.

Nach $N-m$ Durchgängen besitzen Alice und Bob dann m ungemessene Paare im Zustand $x_{N-m} = f_{s_1\ldots s_{N-m}}(x)$ mit der bekannten Hashing-Funktion $f := f_{s_1\ldots s_{N-m}}$. Durch Vergleich ihrer Messwerte und Kenntnis von f können Alice und Bob analog wie bei der Fehlerkorrektur mit hoher Wahrscheinlichkeit erschließen, in welchen Zustände sich die einzelnen ungemessenen Bellzustände befinden. Diese können sie dann zu dem gewünschten Zustand $|\phi^+\rangle^m$ korrigieren. Dabei gilt die folgende Schranke.

Lemma 4.9. *Die Wahrscheinlichkeit, dass nach r Schritten zwei verschiedene Sequenzen x_r und y_r existieren, welche die gleichen Paritäten in jedem Schritt geliefert haben, ist beschränkt durch 2^{-r}. Es gilt also $p(x_r \neq y_r \wedge \forall_{k=1}^{r} s_k x = s_k y) \leq 2^{-r}$.*

Beweis. Es seien x_k, y_k die Sequenzen von zwei Ausgangssequenzen x, y nach dem $k-$ten Schritt. Dann gilt:

$$\begin{aligned} p(x_r \neq y_r \wedge \forall_{k=1}^{r} s_k x_k = s_k y_k) &= p(x_r \neq y_r) \prod_{k=1}^{r} p(s_k x_k = s_k y_k | x_r \neq y_r) \\ &\overset{(*)}{=} p(x_r \neq y_r) \prod_{k=1}^{r} p(s_k x_k = s_k y_k \wedge x_k \neq y_k) \\ &= p(x_r \neq y_r) \prod_{k=1}^{r} p(x_k \neq y_k) p(s_k x_k = s_k y | x_k \neq y_k) \\ &\leq 2^{-r} \end{aligned}$$

Es gilt $(*)$, da mit $x_k = y_k$ zugleich $x_r = y_r$ gilt und somit dieser Faktor dann entfällt. Die letzte Abschätzung ergibt sich aus $p(x_k \neq y_k) \leq 1$ und $p(s_k x_k = s_k y | x_k \neq y_k) \leq 1/2$ für alle $k = 1, \ldots, r$. □

Diese Abschätzung genügt uns später für den Sicherheitsbeweis. Man kann allerdings eine noch bessere Schranke erhalten.

Nehmen wir an, wir besitzen eine Folge Bellzuständen, wobei die Verteilung der Bellzustände charakterisiert ist durch die Dichtematrix

$$\rho_j = \sum_{i=1}^{4} p_i \left|\chi_i\right\rangle \left\langle\chi_i\right| \quad \text{mit } \left|\chi_i\right\rangle \in \{\left|\phi^+\right\rangle, \left|\phi^-\right\rangle, \left|\Psi^+\right\rangle, \left|\Psi^-\right\rangle\}$$

Es liegt also insgesamt die Dichtematrix $\rho = \bigotimes_j \rho_j$ vor. Dann ist nach dem Satz über typische Sequenzen [14, Thm.12.2] (für die Shannon Entropie) oder [14, Thm.12.5] (für die von-Neumann Entropie) ist die Anzahl ν typischer Sequenzen beschränkt durch

$$\nu \leq 2^{N(S(\rho)+\varepsilon)}$$

und die Wahscheinlichkeit, dass unsere Folge keine typische Sequenz (vgl. [14]) ist, ist von der Ordnung $O(\exp(-\varepsilon^2 N))$. Damit ist die Wahrscheinlichkeit p_f, dass das Verfahren nicht exakt funktioniert hat, beschränkt durch die Wahrscheinlichkeit, dass eine typische Sequenz vorliegt, aber mehr als eine Lösung nach $N - m$ Paritätstests zulässt, plus die Wahrscheinlichket, dass eine untypische Folge vorliegt. Dieses ergibt [11, B.3.]

$$p_f \leq 2^{N(S(\rho)+\varepsilon)} 2^{-(N-m)} + O(\exp(-\varepsilon^2 N)). \tag{4.15}$$

Durch geschickte Wahl der Parameter ($N - m = N(S(\rho) + 2\varepsilon)$ mit $\varepsilon \approx N^{-1/4}$) kann man erreichen, dass $p_f \to 0$ und $N - m \to N(S(\rho))$ für große N gilt.

Durch geeignete Wahl der Hashing-Funktionen ist es möglich, auch endliche Qubitfolgen exakt zu purifizieren [11]. Auch wenn dieses im Hinblick auf die reale Anwendung von Interesse ist, wollen wir diesen Punkt hier nicht näher ausführen, da es im Prinzip genauso wie für das unendlichdimensionale System funktioniert, außer dass man bei der Wahl der Hashing-Funktionen wesentlich sorgfältiger vorgehen muss.

4.2.2 CSS-Methode

Diese Mehode ist ähnlich zur Einweg-Hashing-Methode. Dabei soll allerdings bei einem Übergang des Purifizierungs-Protokolls hin zur Fehlerkorrektur, welcher im folgenden Kapitel beschrieben wird, genau der im Abschnitt 4.1.2 beprochene CSS-Code herauskommen. Dazu ist es notwendig, dass lediglich σ_x und σ_z-Operationen neben den BXOR-Operationen verwendet werden.

Wir gehen von einer Folge verschränkter Bellzustände aus. Weiter liegen zwei Paritätsmatrizen H_1 und $H_2^\perp$ vor, die die Bedingungen der CSS-Codes (Abschnitt 4.1.2) erfüllen. Jede Hälfte der verschränkten Qubits wird nun auf gleiche Art gemessen. Zunächst messen Alice und Bob jeweils Z entsprechend der Matrix H_1. Durch Vergleich der Ergebnisse kann Bob analog zur Fehlerkorrektur mittels linearer Codes auf die Bitflip-Fehler schließen. Bei diesem Schritt gehen $n-k$ verschränkte Qubits, die gemessen wurden, verloren. Anschließend messen beide X bezüglich der Matrix $H_2^\perp$ und können den Phasenfehler korrigieren. Dabei verlieren sie wieder $n-k$ Qubits. Die korrigierte Folge der verbliebenen $m := n-2(n-k)$ Zustände besitzt nun die Treue 1, sofern nicht mehr als t Fehler bei Verwendung eines entsprechenden Codes aufgetreten sind.

Für einen allgemeinen Anfangszustand ρ kann man die Treue abschätzen durch [9]

$$F(\rho, |\phi+\rangle^m) \geq \operatorname{tr}\left[\prod \rho\right], \tag{4.16}$$

wobei $\prod$ die Projektion auf den Raum der Bellzustände mit maximal t Fehlern darstellt.

Damit kann die Treue eines beliebigen Zustands nach dem CSS-Verfahren abgeschätzt werden durch die Wahrscheinlichkeit, dass nicht mehr als t Fehler auftreten. Diese Wahrscheinlichkeit können Alice und Bob anhand ihrer Ergebnisse aus dem Vergleich der Testbits ermitteln. Legt dieser Vergleich eine Fehlerrate von $\delta-\varepsilon$ nahe, dann ist die Wahrscheinlichkeit p_e, dass mehr als $t=\delta m$ Fehler in den Codebits und weniger als $(\delta-\varepsilon)m$ Fehler in den Testbits auftreten, asymptotisch beschränkt durch [8]

$$\exp\left(-\frac{\varepsilon^2 m}{4\delta(1-\delta)}\right).$$

Zusammenfassend erhalten wird folgendes Lemma:

Lemma 4.10. *Die Treue $F(\rho, |\phi+\rangle^m)$ des Zustandes ρ nach Anwendung der CSS-Methode kann in Abhängigkit von der zugelassenen Fehlerrate $[\delta-\varepsilon, \delta]$ beschränkt werden durch*

$$F(\rho, |\phi+\rangle^m) \geq \operatorname{tr}\left[\prod \rho\right] = 1 - p_e \geq 1 - \exp\left(-\frac{\varepsilon^2 m}{4\delta(1-\delta)}\right).$$

Durch das CSS-Verfahren haben Alice und Bob ihre Qubitfolge in einen $CSS_{u,v}$-Code abgebildet. Dabei sind u und v durch die Messergebnisse von Alice bestimmt. Somit erfolgt dieses Verfahren analog zur Fehlerkorrektur mit Informationsabgleich

aus Abschnitt 2.1.1. Der Unterschied besteht darin, dass zunächst quantentheoretische und keine klassischen Zustände vorliegen und Alice erst nach der Messung sagen kann, welchen Code sie zur Fehlerkorrektur verwendet hat.

4.3 Übergang von 1-EPP zu QECC

Wir zeigen nun, wie man von einem Protokoll der Verschränkungspurifizierung auf ein Protokoll der Quantenfehlerkorrektur kommt. Dabei setzen wir voraus, dass Alice und Bob nur einseitige Kommunikation benutzen und nur Operationen aus Tabelle 4.4 (in beliebiger Reihenfolge) verwenden. Setzen wir weiter voraus, dass nur Bobs Kanal einem Rauschen unterliegt, so kann man das 1-EPP in ein äquivalentes QECC-Schema umwandeln [11]. Dieses ist für unseren Fall gegeben, da Alice später ihr Qubit bei sich behält und somit gar keinen Quantenkanal benutzt.

Wir gehen von folgender Situation aus. Alice und Bob besitzen eine Folge verschränkter Zustände, welche sie mit einem 1-EPP purifizieren, so dass sie hinterher mindestens einen maximal verschränkten Zustand $|\psi\rangle$ besitzen. Diesen nutzen sie nun, um über eine Bellmessung $\mathcal{M}_B$ einen Zustand $|\xi\rangle$ von Alice zu Bob zu teleportieren. Da der Zustand$|\psi\rangle$ maximal verschränkt ist, wird $|\xi\rangle$ hierbei fehlerfrei übertragen. Dieses ist noch einmal im folgenden Schaubild 4.8 dargestellt.

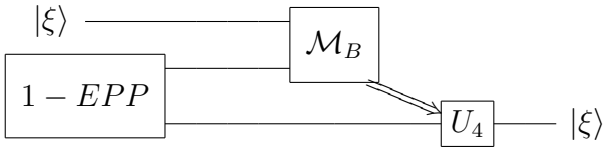


Abbildung 4.8: Schematische Darstellung der betrachteten Situation; ein purifizierter Zustand wird genutzt, um einen unbekannten Zustand $|\xi\rangle$ fehlerfrei zu übertragen, die Transformation U_4 (siehe Text) ist dabei Bestandteil der Teleportation.

Betrachten wir zunächst noch einmal das Purifizierungs-Protokoll, vgl. dazu Abbildung 4.7. Dazu nehmen wir an, unsere Quelle erzeugt nur $|\phi^+\rangle$ Zustände. Dann lässt sich unser Ausgangszustand $|\psi\rangle_i$ darstellen als Gemisch über alle möglichen Kombinationen von $|0\rangle|0\rangle$ und $|1\rangle|1\rangle$. Bei N Paaren ergeben sich 2^N Möglichkeiten. Diese seien in festgelegter Reihenfolge, parametrisiert durch x, geordnet. Damit ergibt sich

$$|\psi\rangle_i = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_A |x\rangle_B .$$

Nach der unitären Transformation U_1 von Alice liegt dann der Zustand

$$|\psi\rangle_f = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (U_1)_{x,y} |y\rangle_A |x\rangle_B$$

vor. Durch Vertauschen der Variablenbezeichnung x und y unter Berücksichtigung von

$$(U_1)_{y,x} = (U_1)^T_{x,y}$$

ergibt sich

$$|\psi\rangle_f = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} |y\rangle_A \, (U_1)^T_{x,y} \, |x\rangle_B \, .$$

Damit liefert das Purifizierungs-Verfahren genau die gleichen Ergebnisse, wenn Alice statt der Transformation U_1 an ihren Qubits die Transformation U_1^T an Bobs Qubit durchführt, bevor diese durch den Kanal geschickt werden. Hierbei haben wir verwendet, dass bei Alice kein Rauschen vorliegt.

Der Rest des Purifizierungsprotokolls besteht neben Bobs Transformation U_2 aus $N-m$ Messungen von $Z \otimes Z$ und einer abschließenden Korrektur U_3. Da U_1 (und damit auch U_1^T) mit der Messung von $Z \otimes Z$ vertauscht (beide haben die Bellzustände als Eigenzustände), kann Alice auch erst ihre Z-Messung an ihren Qubits durchführen und dann U_1^T auf Bobs Qubits anwenden. Da die Bellzustände durch die Z-Messung jeweils auf den Eigenzustand $|00\rangle$ oder $|11\rangle$ projeziert werden, kann Alice ebenso Bobs Qubits direkt präparieren. Dabei können wir ohne Einschränkung davon ausgehen, dass sie immer mit $|0\rangle$ beginnt.

Betrachten wir nun noch die Teleportation. Diese bestand aus einer Bellmessung $\mathcal{M}_B$ von Alice Qubit von $|\phi^+\rangle$ und einem unbekannten Zustand $|\xi\rangle$. Das Ergebnis wird Bob mitgeteilt, welcher dann mit einer entsprechenden Transformation U_4 aus seinem Qubit den Zustand $|\xi\rangle$ erzeugt. Da auch die Bellmessung mit allen bisherigen Operationen vertauscht, kann Alice diese noch vor allen anderen Operationen durchführen. Da aber eine Bellmessung mit einem maximal verschränkten Zustand nur die Zustände vertauscht, kann sie auch gleich mit dem Zustand $|\xi\rangle$ anstelle ihrer Qubithälfte beginnen und die Transformation U_4 vernachlässigen.

Damit ergibt sich abschließend folgendes Bild 4.9, welches exakt dem Schema einer Quantenfehlerkorrektur gleicht.

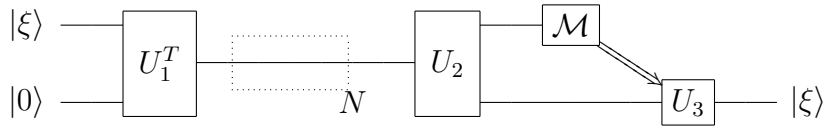


Abbildung 4.9: Purifizierungsprotokoll nach den oben erläuterten Transformationen; es ergibt sich das Schema der Fehlerkorrektur.

Wir haben also unser Purifizierungsprotokoll in ein Fehlerkorrekturprotokoll überführt. Wichtig hierbei war, dass die durchgeführten Transformationen U_i mit den Messungen vertauschen und die Reihenfolge damit für die Messergebnisse unerheblich ist.

Diesen Vorgang werden wir im folgenden Kapitel, in dem wir die Sicherheit des BB84-Protokolls zeigen werden, verwenden, um von einem sicheren Protokoll, welches mit Verschränkungspurifizierung arbeitet, zum BB84-Protokoll mit Fehlerkorrektur zu gelangen.

5 Sicherheit von QKD-Protokollen

Wir befassen uns hier im Wesentlichen mit der Sicherheit des BB84-Protokolls. Aus dem Beweis wird aber ersichtlich, dass wir damit analog auch die Sicherheit des SARG-Protkolls erfasst haben.

5.1 Die Beweisidee

Der hier vorgestellte Beweis basiert auf der Arbeit von Lo und Chau [7] sowie der Verbesserung des Beweises durch Shor und Preskill [8].

Hierbei bedient man sich folgenden Tricks: Man beginnt mit einem auf Verschränkung basierenden Protokoll, dem Lo-Chau-Protokoll, aus dem man eine konkrete Schranke für die wechselseitige Information von zwischen Alice, Bob und Eve ableiten kann. Modifiziert man dann dieses Protokoll entsprechend, ohne die Sicherheit zu zerstören, ergibt sich die Sicherheit des vorgestellten BB84-Protokolls.

Wir setzen voraus, dass unsere EPR-Quellen perfekte Quellen sind. Diese Fehler werden also nicht betrachtet und wir brauchen die PNS-Attacken nicht zu berücksichtigen.

Weiter nehmen wir an, dass Fehlerquellen, die durch den Kanal selbst, durch einen fehlerhaften Speicherprozess oder fehlerhaften Quantenberechnungen entstehen, nicht auftreten. Die letzten beiden Fehlerquellen können wir durch Anwendung von fehlertoleranten Quantenfehlerkorrekturverfahren [14, Abs.10.6.] unschädlich machen. Fehler durch den Kanal werden zunächst komplett vernachlässigt. Durch Fehlerkorrektur mittels Informationsabgleich (Abschnitt 2.1.1) wird diesem später Rechnung getragen.

5.2 Beweis von Lo und Chau

Wir beschränken uns auf ein Protokoll, bei dem also ein fehlerfreier Kanal und ideale Ausrüstung vorliegt.

Wir zeigen zunächst, dass das folgende (rauschfreie) Lo-Chau-Protokoll sicher ist.

5.2.1 Lo-Chau Protokoll

1. Alice erzeugt N EPR-Paare im Zustand $|\phi^+\rangle$ und wählt eine Zufallsfolge b der Länge N,

2. Alice erzeugt $|\psi\rangle$ durch Anwendung von $1 \otimes \mathcal{H}^b$ auf $|\phi^+\rangle^N$, d.h. sie wendet $1 \otimes \mathcal{H}$ auf den $k-$ten Zustand $|\phi^+\rangle$ an, falls $b_k = 1$ ist, und sonst die Identität $1 \otimes 1$,

3. Alice sendet jeweils das zweite Qubit von $|\psi\rangle$ an Bob,

4. Bob erhält $|\psi\rangle'$, dieser unterscheidet sich von $|\psi\rangle$ nur dann, wenn ein Lauschangriff stattgefunden hat. Er speichert den Zustand und gibt die Ankunft öffentlich bekannt,

5. Alice veröffentlicht b und Bob transformiert $|\psi'\rangle$ mit $\mathcal{H}^b$. Für $|\psi'\rangle = |\psi\rangle$ teilen sich Alice und Bob dann genau N maximal verschränkte Zustände $|\phi^+\rangle$,

6. Alice und Bob testen ihre Paare auf Verschränkung mit der Hashing-Methode (siehe Abschnitt 4.2.1 oder Abschnitt 5.2.2),

7. War diese erfolgreich, messen Alice und Bob die verbliebenen Qubits in der $z-$Basis und erhalten den Schlüssel S.

Dabei gewährleisten die Schritte 2 und 5, dass die gesendeten Qubits im Allgemeinen nicht orthogonal zueinander sind und somit nicht unbemerkt abgehört werden können (vgl. Abschnitt 1.3).

5.2.2 Hashing-Verfahren

Durch ihren Lauschangriff hat Eve den Zustand $|\psi\rangle$ mit einem Hilfssystem bei sich verschränkt und dadurch den Zustand $|\psi'\rangle$ präpariert. Aufgabe von Alice und Bob ist es nun, herauszufinden, ob es sich bei ihrem geteilten Zustand um $|\phi^+\rangle^N$ handelt oder nicht. Dabei sollen sie nur lokale Operationen und klassische Kommunikation (LOCC) verwenden.

Gemäß unserer Identifizierung eines Bellzustands mit zwei logischen Bits, identifizieren wir unseren Produktzustand aus N Bellzuständen mit der entsprechenden $2N$-Bitfolge.

Das klassische Analogon zu unserem Problem, mit wenigen Messungen $m < N$ herauszufinden, ob unser Zustand eine Folge nur aus $|\phi^+\rangle$-Zuständen ist, entspricht dann der Aufgabe, mit m Paritätsabfragen herauszufinden, ob die Folge $x = 0000\ldots$ vorliegt [7].

Die naheliegende Strategie, nach den Paritäten m zufälliger Bits zu fragen, ist nicht sinnvoll. Ersetzt Eve nur ein einziges Bit der Folge, so ist die Wahrscheinlichkeit, dass dies nicht entdeckt wird, mindestens

$$\frac{2N-m}{2N} = 1 - \frac{m}{2N}.$$

Da im Allgemeinen sogar $m \ll N$ ist, geht diese Wahrscheinlichkeit gegen 1.

Daher benutzen Alice und Bob die Hashing-Methode (random hashing idea). Dazu wählen sie m zufällige Teilfolgen s_k und fragen nach deren Paritäten in der Folge, d.h. sie bestimmen $x \cdot s_k \mod 2$. Hierbei verfahren sie genauso wie bei der in Abschnitt 4.2.1 beschriebenen Einweg-Hashing-Methode. Hierdurch verlieren sie m verschränkte Paare, da die Messung die Verschränkung zerstört, und erhalten einen Zustand ρ

bestehend aus $N - m$ Zutänden. Aber sie können dafür mit hoher Wahrscheinlichkeit feststellen, welcher Zustand vorliegt, d.h. mit Wahrscheinlichkeit größer oder gleich $1 - 2^{-m}$ identifizieren sie ihren Zustand richtig und mit der Wahrscheinlichkeit von höchstens 2^{-m} wird Eve nicht entdeckt, obwohl sie angegriffen hat. Damit können sie die Treue ihres Zustands bezüglich $|\phi^+\rangle^{N-m}$ abschätzen. Diese Abschätzung soll im nächsten Abschnitt durchgeführt werden.

5.2.3 Sicherheit des Lo-Chau-Protokolls

Eve wählt ihre Abhör-Strategie natürlich so, dass sie eine reelle Chance hat, nicht entdeckt zu werden. Wir nehmen an, dass sie mit mindestens 2^{-r} für ein $r \in \mathbb{N}$ nicht entdeckt wird.

Um nun die Treue des Zustandes ρ bzgl. $|\phi^+\rangle^{\otimes N-m}$ abzuschätzen, genügt eine Abschätzung der Treue des ursprünglichen Zustands $|\psi\rangle$ bzgl. $|\phi^+\rangle^{\otimes N}$. Auf Grund der Konvexität der Treue, gilt

$$F(\rho, \left|\phi^+\right\rangle^{\otimes N-m}) \geq F(|\psi\rangle, \left|\phi^+\right\rangle^{\otimes N}) \tag{5.1}$$

und somit erhalten wir hierdurch auch eine Abschätzung für $F(\rho, |\phi^+\rangle^{\otimes N-m})$.

Sei p_1 die Wahrscheinlichkeit dafür, dass $|\psi\rangle = |\phi^+\rangle^{\otimes N}$ ist. Dann wird Eve mit $p = 1$ nicht entdeckt, hat aber auch nicht eingegriffen. Ist $|\psi\rangle \neq |\phi^+\rangle^{\otimes N}$, so wird dieser Fehler und damit Eve mit $p \leq 2^{-m}$ bei m Schritten nach Lemma 4.9 nicht entdeckt. Die Gesamtwahrscheinlichkeit p_{Eve}, dass sie nicht entdeckt wird, kann somit abgeschätzt werden durch

$$2^{-r} \leq p_{Eve} \leq p_1 + (1 - p_1)2^{-m} \leq p_1 + 2^{-m}. \tag{5.2}$$

Umformen liefert

$$p_1 \geq 2^{-r}(1 - 2^{-(m-r)}). \tag{5.3}$$

Da $\frac{p_1}{p_1+2^{-m}}$ monoton mit p_1 wächst, erhalten wir hiermit für die Treue (im Falle eines akzeptierten Zustands ρ):

$$\begin{aligned} F(|\psi\rangle, \left|\phi^+\right\rangle^{\otimes N})^2 &= \frac{p(|\psi\rangle = |\phi^+\rangle^{\otimes N})}{p_{Eve}} \\ &\geq \frac{p_1}{p_1 + 2^{-m}} \\ &\geq \frac{2^{-r}(1 - 2^{-(m-r)})}{2^{-r}(1 - 2^{-(m-r)+2^{-m}})} = 1 - 2^{-(m-r)}. \end{aligned} \tag{5.4}$$

Diese Abschätzung ist hilfreich im Hinblick auf das folgende Lemma, welches uns eine Abschätzung für die Entropie in Abhängigkeit von der Treue liefert.

Lemma 5.1 (Lo, Chau)**.** *Gilt $F(\rho, |\phi^+\rangle^{\otimes n})^2 > 1 - 2^{-s}$ für ein $s \in \mathbb{N}$, so ist $S(\rho) < (2n + s + \frac{1}{\ln 2})2^{-s} + O(2^{-2s})$.*

Beweis. $F(\rho, |\phi^+\rangle^{\otimes n})^2 = \langle\phi^+|\rho|\phi^+\rangle^{\otimes n} > 1 - 2^{-s}$. Also ist der größte Eigenwert von ρ größer als $1-2^{-s}$. Damit gilt, da die Entropie konkav ist, für die von-Neumann Entropie $S(\rho) \leq S(\rho_{max})$ mit $\rho_{max} = \mathrm{diag}(1-2^{-s}, \frac{2^{-s}}{2N-1}, \ldots, \frac{2^{-s}}{2N-1})$.
Für $S(\rho_{max})$ gilt:

$$\begin{aligned}
S(\rho_{max}) &= -\operatorname{tr}[\rho_{max} \log \rho_{max}] \\
&= -(1-2^{-s})\log(1-2^{-s}) - 2^{-s}\log\left(\frac{2^{-s}}{2N-1}\right) \\
&= 2^{-s}\left(\log(1-2^{-s} - \log(2^{-s} + \log(2^{2N}-1))\right) - \log(1-2^{-s}) \\
&< 2^{-s}(0+s+2N) + \frac{1}{\ln 2}2^{-s} + O(2^{-2s}) \\
&= \left(2N + s + \frac{1}{\ln 2}\right)2^{-s} + O\left(2^{-2s}\right)
\end{aligned}$$

□

Gleichung (5.4) liefert uns $s = m - r$. Damit gilt dann mit Lemma 5.1

$$S(\rho) \leq 2^{-(m-r)}\left(2(N-m) + m - r + \frac{1}{\ln 2}\right). \tag{5.5}$$

Mit Hilfe der Holevo-Schranke (1.13) folgt dann für die wechselseitige Information $H(S:E)$, also der Information, die Eves Messergebnisse E mit dem Schlüssel S gemeinsam haben:

$$H(S:E) \leq 2^{-(m-r)}\left(2(N-m) + m - r + \frac{1}{\ln 2}\right). \tag{5.6}$$

Wählt man $l = m - r - \log(2(N-m) + m - r + \frac{1}{\ln 2})$, so ist $H(S:E) \leq 2^{-l}$, und mit $s' := m$ kann das Protokoll mit einer Wahrscheinlichkeit von $1 - p_f = 1 - O(2^{-s'})$ erfolgreich beendet werden. Somit ist das Lo-Chau-Protokoll sicher.

5.3 Beweis von Shor und Preskill

Wir beginnen nun mit der Modifizierung des Lo-Chau Protokolls, von dem wir nach dem vorherigen Abschnitt wissen, dass es sicher ist. Dabei ersetzen wir die Hashing-Methode durch die CSS-Methode aus Abschnitt 4.2.2. Da hierfür ebenfalls nach Lemma 4.10 eine untere Schranke für die Treue existiert, ist auch dieses Protokoll nach Abschnitt 5.2.3 sicher.

Schritt 6 wird also folgendermaßen ersetzt:

6a. Alice und Bob wählen aus den $2N$ Qubits N zufällig aus, messen diese in der z-Basis und vergleichen ihre Ergebnisse. Dadurch erhalten sie eine mittlere Fehlerrate ihrer Zustände. Ist die Fehlerrate zu groß, wird das Protokoll verlassen.

6b. Die restlichen N Paare durchlaufen ein $CSS-$EP Protokoll nach Abschnitt 4.2.2.

Wie in Abschnitt 4.3 gezeigt, können wir durch geeignete Vertauschung kommutierender Operatoren ein Purifizierungs-Protokoll äquivalent in ein Fehlerkorrekturprotokoll umwandeln.

Wesentlich dabei ist, dass die X-Messungen den Phasenfehler bestimmen und diese im QKD-Protokoll keinen Einfluss auf den Schlüssel haben. Sie liefern lediglich ein Anzeichen dafür, ob Eve gelauscht hat oder nicht. Diese Operationen können also weggelassen oder ans Ende der Operationenfolge geschoben werden, ohne die Ergebnisse zu beeinflussen.

Der wesentliche Schritt in der Umformung des Protokolls von Shor und Preskill (oder auch von Lo und Chau) zum BB84-Protokoll besteht darin, dass alle Operationen des Kanals (also von Eve) und von Bob lokale Operationen sind und sie somit mit allen Operationen von Alice kommutieren. Daher kann Alice alle ihre Operationen vor dem Senden an Bob an ihren Qubithälften durchführen.

Ein Vergleich mit Abschnitt 4.1.3 zeigt, dass die entsprechenden Messungen gerade der Kodierung des Eingangszustands in einen $CSS_{u,v}$-Code entsprechen, wobei u und v durch die Messergebnisse der Z- und X-Messungen gegeben sind, da nicht notwendigerweise mit den Anfangszuständen $|0\rangle$ kodiert wurde. Daher kann Alice ebenso einen vorher zufällig generierten Schlüssel aus klassischen Bits direkt in einen zufälligen $CSS_{u,v}$-Code kodieren und diesen an Bob senden.

Das Ergebnis der entsprechenden Umformungen ist der Vollständigkeit halber noch einmal aufgeführt.

1. Alice erzeugt N zufällige Testbits und wählt zwei Zufallsfolgen k (mit Länge N) und b (mit Länge $N + m$) ; dabei entspricht k der Zufallsfolge, die sie durch die Messergebnisse ihrer σ_z-Messung am Ende des Protokolls erhalten hätte, also dem Schlüssel,

2. Alice wählt zwei weitere Zufallsfolgen u und v der Länge N; diese Folgen entsprechen den Messergebnissen, die Alice durch die Z- und X-Messungen bezüglich der Paritätsmatrix des CSS-Codes erhalten hätte,

3. Alice erzeugt $|k\rangle$ und kodiert diesen Zustand mit dem $CSS_{u,v}$-Code und erhält N Codebits sowie m Testbits, welche den ursprünglich gemessenen Qubits entsprechen,

4. Alice wendet $1 \otimes H^b$ entsprechend b an. Dadurch erzeugt sie einen Zustand $|\psi\rangle$, welcher ein Produktzustand aus $|0\rangle, |1\rangle, |0_x\rangle$ und $|1_x\rangle$ ist,

5. Alice sendet jeweils das zweite Qubit von $|\psi\rangle$ an Bob,

6. Bob erhält $|\psi\rangle'$ und gibt dessen Ankunft bekannt,

7. Alice veröffentlicht b und N, Bob misst $|\psi\rangle'$ bezüglich b (Z-Basis für $b_k = 0$ und X-Basis für $b_k = 1$); dies ist äquivalent dazu, dass er zunächst $|\psi\rangle'$ mittels b korrigiert und dann in der Z-Basis misst,

8. Alice veröffentlicht die m Testbits, sie vergleichen diese und bestimmen damit die Fehlerrate. Hiermit entscheiden beide, ob das Protokoll verlassen wird oder nicht,

9. Alice veröffentlich u und v und Bob korrigiert seine Codebits analog zur klassischen Fehlerkorrektur; dieses entspricht den Z- und X-Messungen sowie den σ_z- und σ_x-Operationen von Bob im CSS-Protokoll,

10. Bob dekodiert den Code und erhält durch Z-Messungen den Schlüssel k.

Lemma 4.10 liefert uns nun eine untere Schranke für die Treue in Abhängigkit von der zugelassenen Fehlerrate $[\delta - \varepsilon, \delta]$. Mit den Ausführungen zum Lo-Chau-Protokoll aus Abschnitt 5.2.3 folgt dann, dass das CSS-Protokoll sicher ist.

Dieses Protokoll hat große Ähnlichkeit mit dem BB84-Protokoll. Wir führen nun noch ein paar weitere Veränderungen durch und gelangen so zu einer äquivalenten Variante des Originalprotokolls.

Da Bob die Phase des Codeworts nicht interessiert, kann Alice genausogut auf die Bekanntgabe von u verzichten. Sie sendet dann effektiv den über u gemittelten Zustand

$$\frac{1}{2^n|C_2|}\sum_{w_1,w_2\in C_2}(-1)^{(w_1+w_2)u}\left|k+w_1+v\right\rangle\left\langle k+w_2+v\right| = \\ = \frac{1}{|C_2|}\sum_{w\in C_2}\left|k+w+v\right\rangle\left\langle k+w+v\right|.$$

Bob erhält somit nach seiner z-Messung $k+w+v+e$ für ein $w \in C_2$, wobei e den durch den Kanal verursachten Fehler beschreibt. Hiervon zieht er v ab und korrigiert $k+w+e$ zu $k+w \in C_1$. Der Schlüssel ergibt sich dann als der vorher festgelegte Vertreter zu der Klasse $k+w$. Dieser Prozess ist äquivalent zur Verschwiegenheitsverstärkung.

Den Speicherprozess in Schritt 4 können wir dadurch ersetzen, dass Alice die doppelte Anzahl an Qubits an Bob sendet. Er misst diese sofort bezüglich seiner vorher festgelegten Zufallsfolge b'. Dann vergleichen beide b und b', wobei sie wie im BB84-Protkoll auch nur den übereinstimmenden Teil der Qubits behalten.

Damit haben wir die Sicherheit des BB84-Protokoll gezeigt.

Die Sicherheit des SARG-Protokoll erfolgt analog, da das SARG-Protokoll ebenfalls den Sicherheitstest mit einer gewissen Anzahl an Testqubits durchführt und nach der Rohschlüsselermittelung die gleichen klassischen Verfahren anwendet. Man muss dabei lediglich einen anderen Code als den CSS-Code betrachten. Der Rest des Beweises verläuft dann analog.

Teil II

Kryptographie mit unscharfen Messungen

6 Das Protokoll

Hier soll ein neuer Ansatz für ein Protokoll zur Schlüsselübertragung vorgestellt werden. Diskrete QKD-Protokoll basieren darauf, dass sie ein Schlüsselbit in ein Qubit kodieren, wobei die verschiedenen Bits (0 und 1) jeweils in zueinander komplementären Zuständen kodiert sind. Die verwendeten Zustände stehen also senkrecht aufeinander in der Blochdarstellung. Eine naheliegende Frage ist nun, ob man auch Zustände verwenden kann, die einen kleineren Winkel als 90° einschließen. Diese Zustände kann man beispielsweise durch unscharfe Messungen eines vorher festgelegten Anfangszustands $|\psi\rangle$ erzeugen. Da die Zustände nun einen größeren Überlapp haben, muss man die Anzahl der Qubits pro Schlüsselbit erhöhen, um zu garantieren, dass Alice und Bob am Ende den gleichen Schlüssel besitzen. Wir verschlüsseln ein Bit also in einem Ensemble, welches durch unscharfe Messungen erzeugt wird. Dieser Ansatz soll im folgenden untersucht werden.

Wir beginnen zunächst mit dem Verfahren zur Schlüsselübertragung und dem Sicherheitstest. Dabei verwenden wir den Anfangszustand $|\uparrow_y\rangle$. Danach zeigen wir den Übergang zu einem allgemeinen reinen Anfangszustand. Hierbei tritt eine besondere Eigenschaft unseres Verfahrens zu Tage. Anschließend behandeln wir noch kurz die Möglichkeit eines Gemisches als Anfangszustand. Abschließend zeigen wir, dass das vorgestellte Protokoll unter idealen Bedingungen funktioniert und sicher ist.

6.1 Schlüsselübertragung

Ein Schlüsselbit 0 oder 1 wird jeweils in ein Ensemble kodiert, wobei dieses Ensemble durch unscharfe Messungen eines Anfangszustands $|\psi\rangle$ erzeugt wird. Dabei verwendet Alice je nach Schlüsselbit eine unscharfe Messung in der z-Basis oder in der x-Basis. Sie präpariert also das Ensemble ρ_A der Gestalt

$$\rho_M = \mathrm{M}_+^{\mathrm{A}}\,\rho\,\mathrm{M}_+^{\mathrm{A}\dagger} + \mathrm{M}_-^{\mathrm{A}}\,\rho\,\mathrm{M}_-^{\mathrm{A}\dagger}$$

für ein Schlüsselbit 0 oder

$$\rho_N = \mathrm{N}_+^{\mathrm{A}}\,\rho\,\mathrm{N}_+^{\mathrm{A}\dagger} + \mathrm{N}_-^{\mathrm{A}}\,\rho\,\mathrm{N}_-^{\mathrm{A}\dagger}$$

für ein Schlüsslbit 1 mit $\rho = |\psi\rangle\langle\psi|$.

Die unscharfen Messungen $M_\pm^A$ und $N_\pm^A$ sind hierbei konkret gegeben durch

$$\mathrm{M}_+^{\mathrm{A}} = \sqrt{p_0}\,|\uparrow\rangle\langle\uparrow| + \sqrt{p_1}\,|\downarrow\rangle\langle\downarrow|\,, \tag{6.1}$$

$$\mathrm{M}_-^{\mathrm{A}} = \sqrt{1-p_0}\,|\uparrow\rangle\langle\uparrow| + \sqrt{1-p_1}\,|\downarrow\rangle\langle\downarrow|\,, \tag{6.2}$$

$$\mathrm{N}_{+}^{\mathrm{A}} = \sqrt{p_0}\,|\uparrow_x\rangle\langle\uparrow_x| + \sqrt{p_1}\,|\downarrow_x\rangle\langle\downarrow_x| \quad \text{und} \tag{6.3}$$

$$\mathrm{N}_{-}^{\mathrm{A}} = \sqrt{1-p_0}\,|\uparrow_x\rangle\langle\uparrow_x| + \sqrt{1-p_1}\,|\downarrow_x\rangle\langle\downarrow_x| \tag{6.4}$$

für frei wählbare Parameter $p_0, p_1 \in [0,1]$. Da Alice entweder ρ_M oder ρ_N präpariert, ist die Vollständigkeitsrelation $\mathrm{M}_{+}^{\mathrm{A}\dagger}\mathrm{M}_{+}^{\mathrm{A}} + \mathrm{M}_{-}^{\mathrm{A}\dagger}\mathrm{M}_{-}^{\mathrm{A}} = \mathrm{N}_{+}^{\mathrm{A}\dagger}\mathrm{N}_{+}^{\mathrm{A}} + \mathrm{N}_{-}^{\mathrm{A}\dagger}\mathrm{N}_{-}^{\mathrm{A}} = \mathbf{1}$ erfüllt. Die zugehörigen Effekte kommutieren trivialerweise jeweils für die $\mathrm{M}_{\pm}^{\mathrm{A}}$- und die $\mathrm{N}_{\pm}^{\mathrm{A}}$-Messung. Damit beschreiben diese Operatoren unscharfe Mesungen. Für den Grenzfall $\Delta p = p_0 - p_1 = 1$ gehen die unscharfen Messungen $\mathrm{M}_{\pm}^{\mathrm{A}}$ und $\mathrm{N}_{\pm}^{\mathrm{A}}$ über in die Projektionsmessungen P_z und P_x. Im folgenden schließen wir diesen Fall aus.

Wir beschreiben, wie ein Schlüsselbit übertragen wird. Für jedes weitere Bit wird das Verfahren wiederholt. Wir beginnen zunächst mit dem Anfangszustand $|\uparrow_y\rangle$, da dieser Fall besonders einfach ist. Die entsprechenden Berechnungen für einen allgemeinen reinen Anfangszustand werden im Abschnitt 6.3 aufgeführt.

Berechnet man ρ_A für den nun vorliegenden Fall $|\psi\rangle = |\uparrow_y\rangle$, so ergibt sich sowohl für die $\mathrm{M}_{\pm}^{\mathrm{A}}$- also auch für die $\mathrm{N}_{\pm}^{\mathrm{A}}$-Messung die Dichtematrix

$$\rho_A = \rho_M = \rho_N = \frac{1}{2}\begin{pmatrix} 1 & -ia \\ ia & 1 \end{pmatrix}$$

mit

$$a = \sqrt{p_0 p_1} + \sqrt{(1-p_0)(1-p_1)}. \tag{6.5}$$

Damit besitzen die Ensemble ρ_M und ρ_N die gleiche Dichtemtrix und sind ohne zusätzliche Information nicht voneinander zu unterscheiden.

Alice erzeugt ein Ensemble ρ_A durch unscharfe Messung von N Qubits, notiert sich die Reihenfolge ihrer Messergebnisse ($+$ oder $-$) und sendet ρ_A an Bob. Dabei achtet sie darauf, dass bei der Übertragung die Reihenfolge der gemessenen Qubits erhalten bleibt.

Bob misst das erhaltene Ensemble projektiv bezüglich Z. Er erhält also für jedes Qubit entweder das Ergebnis $\uparrow$ oder $\downarrow$. Entsprechend seiner Messergebnisse sortiert er das Ensemble nun in zwei Unterensemble. Hierfür notiert er sich die Nummern der Qubits mit Messergebnis $\uparrow$ für das eine Ensemble und die übrigen Nummern der Qubits mit Messergebnis $\downarrow$ für das andere Ensemble.

Alice teilt ihm nun die gewählten Parameter p_0, p_1 sowie die Reihenfolge ihrer Messergenisse mit. Hiermit kann Bob dann seine Unterensemble weiter unterteilen. Er sortiert also die Qubits nach "$\uparrow$ und $+$", "$\uparrow$ und $-$","$\downarrow$ und $+$" und "$\downarrow$ und $-$". Durch Abzählen erhält er hieraus die Anzahl n aller Qubits, die Anzahl $n_\uparrow$ der Qubits mit Messergebnis $\uparrow$, die Anzahl $n_\downarrow$ für $\downarrow$ sowie die Anzahl der Teilchen $n(\uparrow,+), n(\uparrow,-), n(\downarrow,+)$ und $n(\downarrow,-)$ im jeweiligen Unterensemble. Damit ergeben sich dann die entsprechenden

relativen Häufigkeiten aus

$$h(+|\uparrow, n) = \frac{n(\uparrow,+)}{n_\uparrow} \qquad h(-|\uparrow, n) = \frac{n(\uparrow,-)}{n_\uparrow} \tag{6.6}$$

$$h(+|\downarrow, n) = \frac{n(\downarrow,+)}{n_\downarrow} \qquad h(-|\downarrow, n) = \frac{n(\downarrow,-)}{n_\downarrow}. \tag{6.7}$$

Dieses ist noch einmal beispielhaft in folgendem Schema dargestellt.

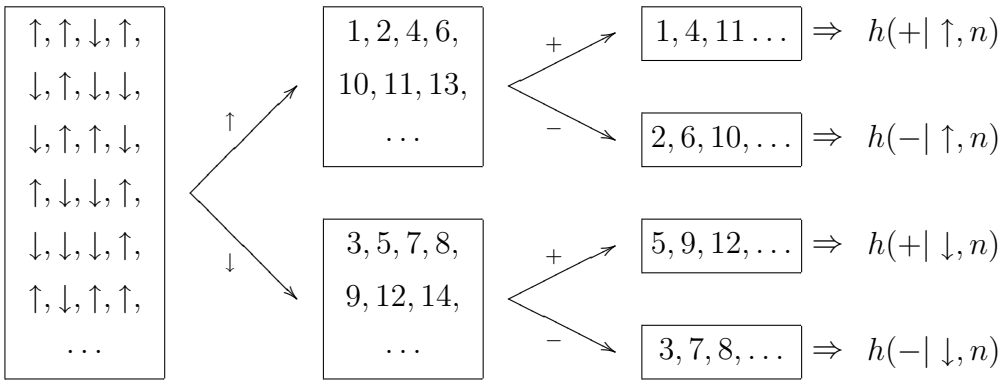


Abbildung 6.1: Schematische Darstellung der Ermittlung der relativen Häufigkeiten

Da Bob die Parameter p_0 und p_1 kennt, kann er berechnen, welche relativen Häufigkeiten $p(+|\uparrow, M)$, $p(-|\uparrow, M), \ldots$ zu erwarten wären, wenn Alice das Ensemble mit $\mathrm{M}^{\mathrm{A}}_{\pm}$ präpariert hat und welche Häufigkeiten $p(+|\uparrow, N)$, $p(-|\uparrow, N), \ldots$ bei Präparation mit $\mathrm{N}^{\mathrm{A}}_{\pm}$ auftreten. Diese berechnen sich wie folgt

$$\begin{aligned} p(+|\uparrow, M) = p(\mathrm{M}^{\mathrm{A}}_{+} \,|\, \uparrow) &= \frac{p(|\uparrow\rangle \,|\, \mathrm{M}^{\mathrm{A}}_{+}) p(\mathrm{M}^{\mathrm{A}}_{+})}{p(|\uparrow\rangle)} \\ &= \frac{p(|\uparrow\rangle\,, \mathrm{M}^{\mathrm{A}}_{+})}{p(|\uparrow\rangle)} = \frac{\mathrm{tr}[|\uparrow\rangle\langle\uparrow| \,\mathrm{M}^{\mathrm{A}\dagger}_{+} \mathrm{M}^{\mathrm{A}}_{+} |\uparrow_y\rangle\langle\uparrow_y|]}{\mathrm{tr}[|\uparrow\rangle\langle\uparrow| \,|\uparrow_y\rangle\langle\uparrow_y|]} \\ &= \frac{\langle\uparrow_y| \,\mathrm{M}^{\mathrm{A}\dagger}_{+} |\uparrow\rangle\langle\uparrow| \,\mathrm{M}^{\mathrm{A}}_{+} |\uparrow_y\rangle}{|\langle\uparrow \,|\, \uparrow_y\rangle|^2} = \frac{1}{2} \langle\uparrow_y| \,\mathrm{M}^{\mathrm{A}\dagger}_{+} |\uparrow\rangle\langle\uparrow| \,\mathrm{M}^{\mathrm{A}}_{+} |\uparrow_y\rangle\,. \end{aligned} \tag{6.8}$$

und entsprechend für die anderen Größen. Hiermit ergeben sich dann die Werte

$$\begin{aligned} p(\mathrm{M}^{\mathrm{A}}_{+} \,|\, \uparrow) &= p_0 & p(\mathrm{M}^{\mathrm{A}}_{+} \,|\, \downarrow) &= p_1 \\ p(\mathrm{N}^{\mathrm{A}}_{+} \,|\, \uparrow) &= \frac{p_0 + p_1}{2} & p(\mathrm{N}^{\mathrm{A}}_{+} \,|\, \downarrow) &= \frac{p_0 + p_1}{2} \quad \text{und} \\ p(\mathrm{M}^{\mathrm{A}}_{-} \,|\, \uparrow) &= 1 - p_0 & p(\mathrm{M}^{\mathrm{A}}_{-} \,|\, \downarrow) &= 1 - p_1 \\ p(\mathrm{N}^{\mathrm{A}}_{-} \,|\, \uparrow) &= \frac{2 - p_0 - p_1}{2} & p(\mathrm{N}^{\mathrm{A}}_{-} \,|\, \downarrow) &= \frac{2 - p_0 - p_1}{2}. \end{aligned}$$

Bob vergleicht nun die ermittelten relativen Häufigkeiten $h(+|\uparrow, n)$, $h(-|\uparrow, n), \ldots$ mit den bedingten Wahrscheinlichkeiten $p(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow)$, $p(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow)$, $p(\mathrm{M}_-^{\mathrm{A}} \mid \uparrow)$, $p(\mathrm{N}_-^{\mathrm{A}} \mid \uparrow), \ldots,$ um festzustellen, welche Präparation Alice gewählt hat. Praktisch vergleicht er beispielsweise, ob

$$h(+|\uparrow, n) = p_0 = p(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow)$$

gilt oder nicht. Liegt Übereinstimmung vor, so hat Alice die $\mathrm{M}_\pm^{\mathrm{A}}$-Präparation gewählt und das Schlüsselbit ist 0, ansonsten wurde mit $\mathrm{N}_\pm^{\mathrm{A}}$ präpariert und das Schlüsselbit hat den Wert 1.

Bemerkung 6.1. Im Falle eines endlichen Ensembles sind die relativen Häufigkeiten im allgemeinen um die entsprechenden bedingten Wahrscheinlichkeiten verteilt. Die Verteilung ist binomial und weist eine gewisse Streuung auf. Daher verwendet Bob bei endlichen Ensemblen Methoden der Testtheorie, um (mit einem gewissen Fehler) abzuschätzen, welche Wahrscheinlichkeit er im Grenzfall erhalten hätte.

Bob kann anstelle der Z-Basis auch in der X-Basis messen. Dadurch ändert sich am Verfahren nichts. Wir haben lediglich die Basen vertauscht und erhalten dadurch andere bedingte Wahrscheinlichkeiten $p(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow_x)$, $p(\mathrm{M}_+^{\mathrm{A}} \mid \downarrow_x)$, $p(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow_x), \ldots$. Diese berechnen sich analog zu Gleichung 6.8 und ergeben

$$\begin{aligned}
p(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow_x) &= p_0 & \qquad p(\mathrm{N}_+^{\mathrm{A}} \mid \downarrow_x) &= p_1 \\
p(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow_x) &= \frac{p_0 + p_1}{2} & \qquad p(\mathrm{M}_+^{\mathrm{A}} \mid \downarrow_x) &= \frac{p_0 + p_1}{2} \\
p(\mathrm{N}_-^{\mathrm{A}} \mid \uparrow_x) &= 1 - p_0 & \qquad p(\mathrm{N}_-^{\mathrm{A}} \mid \downarrow_x) &= 1 - p_1 \\
p(\mathrm{M}_-^{\mathrm{A}} \mid \uparrow_x) &= \frac{2 - p_0 - p_1}{2} & \qquad p(\mathrm{M}_-^{\mathrm{A}} \mid \downarrow_x) &= \frac{2 - p_0 - p_1}{2}.
\end{aligned}$$

Damit kann er genauso wie im ersten Fall verfahren.

Bemerkung 6.2. Beim Vergleich der relativen Häufigkeiten mit den bedingten Wahrscheinlichkeiten kann Bob nur dann ein eindeutiges Ergebnis erhalten, wenn

$$p(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow) \neq p(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow)$$

also

$$p_0 \neq \frac{p_0 + p_1}{2}$$

ist. Daher fordern wir ab jetzt:

Alice muss die Parameter p_0 und p_1 verschieden wählen !

Damit ist das Verfahren zur Schlüsselübertragung geklärt. Es ist noch einmal schematisch in Abbildung 6.2 veranschaulicht.

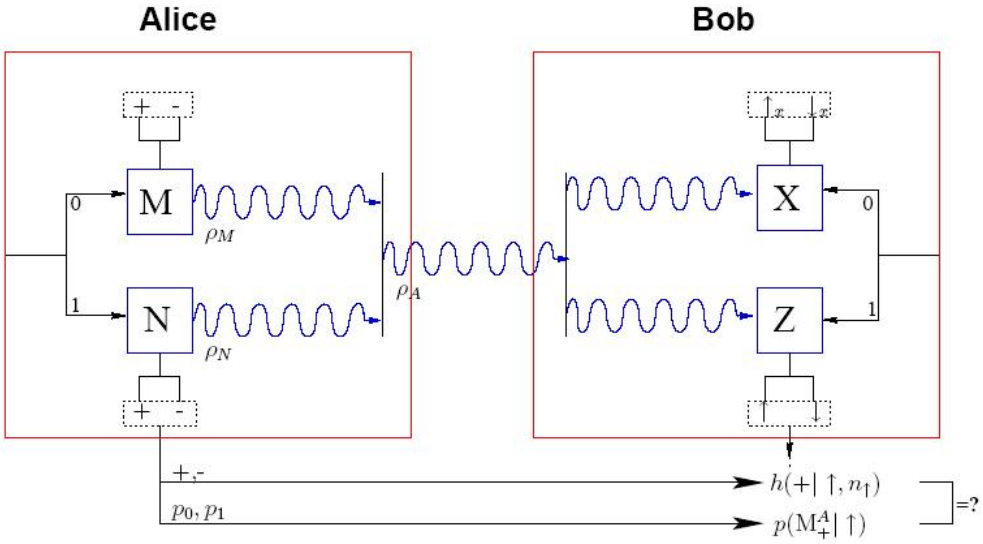


Abbildung 6.2: Schematische Darstellung der Schlüsselübermittlung; aus Symmetriegründen misst Bob entweder in der X- oder in der Z-Basis

6.2 Sicherheitstest

Nutzen wir den gleichen Sicherheitstest wie im BB84-Protokoll, bei dem man die Hälfte des potentiellen Schlüssels opfert, um die Werte direkt zu vergleichen, so verbrauchen wir jedes zweite gesendete Qubit. Wir stellen nun eine Möglichkeit vor, bei der wir im Schnitt nur jedes dritte Qubit benötigen. Das Verfahren ist also effektiver.

Durch die Verwendung eines Ensembles ist es nun möglich, tomographische Messungen am Ensemble durchzuführen und die erhaltene Dichtematrix ρ_B sowie die Entropie $S(\rho_B)$ zu bestimmen. Da Alice das Ensemble ρ_A präpariert hat, kann sie auch dessen Entropie bestimmen. Diese ergibt sich in Abhängigkeit vom Parameter $a = \sqrt{p_0 p_1} + \sqrt{(1-p_0)(1-p_1)}$ (6.5) zu

$$S(\rho_A) = -(\frac{1}{2} + \frac{a}{2}) \log(\frac{1}{2} + \frac{a}{2}) - (\frac{1}{2} - \frac{a}{2}) \log(\frac{1}{2} + \frac{a}{2}). \tag{6.9}$$

Diese ist nebenstehend dargestellt. Man sieht, dass mit abnehmendem a die Entropie zunimmt. Durch diese Zunahme kann ein Lauscher entdeckt werden, da eine Störung des Systems immer mit einer Entropieänderung verbunden ist, vgl. 1.4.

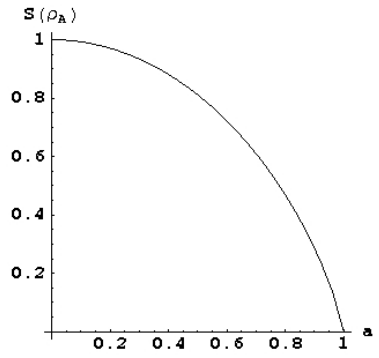


Abbildung 6.3: Entropie $S(\rho_A)$ in Abhängigkeit von a

Konkret bildet der Sicherheitstest eine Vorstufe zur Schlüsselermittlung. Bob misst das erhaltene Ensemble ρ_B nun tomographisch, d.h. er misst anstelle einer

Projektionsmessung in der X- oder der Z-Basis nun gleichverteilt X, Y und Z. Hiermit bestimmt er dann mit (1.9)

$$\rho = \frac{1}{2}(\mathrm{tr}(\rho)I + \mathrm{tr}(\rho X)X + \mathrm{tr}(\rho Y)Y + \mathrm{tr}(\rho Z)Z)$$

die Dichtematrix ρ_B und hieraus die Entropie $S(\rho_B)$.

Alice gibt $S(\rho_A)$ bekannt und Bob vergleicht die beiden Werte. Ist die Differenz

$$\Delta S = S(\rho_B) - S(\rho_A)$$

größer als eine vorgegebene Schranke, so verwirft er das Protokoll, da die Störung des Systems während der Übertragung durch den Quantenkanal zu groß war.

Durch den Sicherheitstest sind die Qubits projektiv gemessen, daher kann Bob das ursprüngliche Verfahren zur Schlüsselermittlung nicht mehr anwenden. Allerdings hat er 2/3 der Qubits entweder in der X- oder der Z-Basis gemessen. Diese Messergebnisse kann er nun zur Schlüsselbit-Ermittlung nutzen. Dadurch entstehen Redundanzen in der Auswertung, da er obiges Verfahren zweimal anwendet. Allerdings ist die Anzahl n der in der entsprechenden Basis gemessenen Qubits geringer, so dass diese Redundanzen genutzt werden können, um die Fehlerwahrscheinlichkeit in der Schlüsselermittlung zu erniedrigen. Er bestimmt mit beiden Messungen das Schlüsselbit. Bei Übereinstimmung akzeptiert es das Ergebnis, ansonsten verwirft er es. Hat jedes Verfahren eine Fehlerwahrscheinlichkeit von p_f, so liegt die Fehlerwahrscheinlichkeit nach dem Vergleich bei p_f^2, wenn man in Kauf nimmt, kritische Ensemble (mit verschiedenen Ergebnissen in der Auswertung) zu verwerfen.

Das Schema zur Schlüsselübertragung (Abbildung 6.2) muss damit nur leicht abgeändert werden. Bob misst nun jedes Qubits zufällig entweder in der X-, Y- oder Z-Basis und wertet die einzelnen Unterensemble jeweils separat aus. Dabei wird das Unterensemble der Y-Messung nur zur Entropiebestimmung genutzt.

6.3 Allgemeiner reiner Anfangszustand

Die berechneten bedingten Wahrscheinlichkeiten $p(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow), p(\mathrm{M}_+^{\mathrm{A}} \mid \downarrow), p(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow), \ldots$ der unscharfen Messungen zeigen eine besondere Eigenschaft. Während die Wahrscheinlichket $p_\psi(a)$ eines Messresultats a einer unscharfen Messung vom Anfangszustand $|\psi\rangle$ abhängt, ist die bedingte Wahrscheinlichkeit in bestimmten Fällen unabhängig vom Anfangszustand. Dieses tritt dann ein, wenn man $|\psi\rangle$ zunächst unscharf $\mathrm{M}_\pm^{\mathrm{A}}$ oder $\mathrm{N}_\pm^{\mathrm{A}}$ misst und anschließend eine Projektionsmessung in der gleichen Basis durchführt.

Lemma 6.3. *Für fast alle $\psi, \psi' \in \mathcal{H}_2$ gilt*

$$p_\psi(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow) = p_{\psi'}(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow) \qquad p_\psi(\mathrm{M}_+^{\mathrm{A}} \mid \downarrow) = p_{\psi'}(\mathrm{M}_+^{\mathrm{A}} \mid \downarrow)$$
$$p_\psi(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow_x) = p_{\psi'}(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow_x) \qquad p_\psi(\mathrm{N}_+^{\mathrm{A}} \mid \downarrow_x) = p_{\psi'}(\mathrm{N}_+^{\mathrm{A}} \mid \downarrow_x)$$

und entsprechend für $\mathrm{M}_-^{\mathrm{A}}$ und $\mathrm{N}_-^{\mathrm{A}}$.

Hierbei schließen wir die Zustände $|\psi\rangle \in \{|\uparrow\rangle, |\downarrow\rangle\ |\uparrow_x\rangle, |\downarrow_x\rangle\}$ aus. Da sich die Eigenzustände der Z-Messung bei unscharfer Messung mit $\mathrm{M}_{\pm}^{\mathrm{A}}$ nicht ändern, sind die Wahrscheinlichkeiten $p_{\uparrow}(\mathrm{M}_{\pm}^{\mathrm{A}} \mid \downarrow)$ nicht definiert und können somit nicht verglichen werden. Gleiches gilt für die Eigenzustände der X-Messung und unscharfe Messung mit $\mathrm{N}_{\pm}^{\mathrm{A}}$.

Wir zeigen obige Eigenschaft nur für den ersten Fall, also $p_{\psi}(\mathrm{M}_{+}^{\mathrm{A}} \mid \uparrow) = p_{\psi'}(\mathrm{M}_{+}^{\mathrm{A}} \mid \uparrow)$. Die übrigen Fälle folgen analog.

$$
\begin{aligned}
p_{\psi}(\mathrm{M}_{+}^{\mathrm{A}} \mid \uparrow) &= \frac{\langle\uparrow| \mathrm{M}_{+}^{\mathrm{A}\dagger} |\psi\rangle \langle\psi| \mathrm{M}_{+}^{\mathrm{A}} |\uparrow\rangle}{\langle\uparrow |\psi\rangle \langle\psi| \uparrow\rangle} \\
&= \frac{\langle\psi| \mathrm{M}_{+}^{\mathrm{A}\dagger} |\uparrow\rangle \langle\uparrow| \mathrm{M}_{+}^{\mathrm{A}} |\psi\rangle}{|\langle\uparrow |\psi\rangle|^2} = \frac{\langle\psi| \mathrm{M}_{+}^{\mathrm{A}\dagger} |\uparrow\rangle \langle\uparrow| \uparrow\rangle \langle\uparrow| \mathrm{M}_{+}^{\mathrm{A}} |\psi\rangle}{|\langle\uparrow |\psi\rangle|^2} \\
&= \frac{\langle\psi| \uparrow\rangle \langle\uparrow| \mathrm{M}_{+}^{\mathrm{A}\dagger} \mathrm{M}_{+}^{\mathrm{A}} |\uparrow\rangle \langle\uparrow| \psi\rangle}{|\langle\uparrow |\psi\rangle|^2} = \frac{|\langle\uparrow |\psi\rangle|^2 \langle\uparrow| \mathrm{M}_{+}^{\mathrm{A}\dagger} \mathrm{M}_{+}^{\mathrm{A}} |\uparrow\rangle}{|\langle\uparrow |\psi\rangle|^2} = \langle\uparrow| \mathrm{M}_{+}^{\mathrm{A}\dagger} \mathrm{M}_{+}^{\mathrm{A}} |\uparrow\rangle
\end{aligned}
$$

Hierbei wurde verwendet, dass $\mathrm{M}_{+}^{\mathrm{A}}$ mit $|\uparrow\rangle\langle\uparrow|$ vertauscht. Der Wert von $p_{\psi}(\mathrm{M}_{+}^{\mathrm{A}} \mid \uparrow)$ hängt also nicht mehr vom Anfangszustand $|\psi\rangle$ ab. Damit ist die Aussage gezeigt.

Da für den Beweis der Operator der unscharfen Messung mit dem Projektionsoperator vertauschen muss, ist klar, dass diese Aussage nicht mehr gilt, wenn man Operatoren bezüglich verschiedener Basen verwendet.

Somit können Alice und Bob das für den Anfangszustand $|\uparrow_y\rangle$ vorgestellte Verfahren übernehmen. Alice muss nur darauf achten, dass die entsprechenden bedingten Wahrscheinlichkeiten, also beispielsweise $p_{\psi}(\mathrm{M}_{+}^{\mathrm{A}} \mid \uparrow)$ und $p_{\psi}(\mathrm{N}_{+}^{\mathrm{A}} \mid \uparrow)$ verschieden sind. Wegen Lemma 6.3 kann Alice dabei sogar darauf verzichten, den Anfangszustand $|\psi\rangle$ bekannt zu geben.

Das Protokoll gliedert sich also wie folgt.

1. Alice wählt einen Anfangszustand ψ und präpariert hiermit ein Ensemble ρ_A entsprechend des zu verschlüsselnden Bits,
2. dieses schickt sie an Bob,
3. Bob misst das erhaltene Ensemble mit $P_{x,y,z}$-Messungen tomographisch, bestimmt ρ_B und damit $S(\rho_B)$,
4. Alice gibt $S(\rho_A)$ bekannt
   $\rightarrow$ liegt $\Delta S = S(\rho_B) - S(\rho_A)$ im Toleranzbereich, so wird das Protokoll fortgesetzt, ansonsten abgebrochen,
5. Alice gibt ihre Messergebnisse $(+/-)$ und die Parameter p_0, p_1 bekannt,
6. Bob bestimmt die relativen Häufigkeiten $h(+| \uparrow, n), h(-| \uparrow, n)$, usw. aus seinen Messergebnissen,

7. Bob vergleicht die bedingte Wahrscheinlichkeit $p_\psi(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow) = p_0$ mit der relativen Häufigkeit $h(+|\uparrow, n)$ und erhält dadurch eine Aussage über die von Alice gewählte Basis und damit das übertragene Bit,

8. Zur Fehlerkorrektur verfährt Bob analog mit den Wahrscheinlichkeiten zur X-Messung, bei Übereinstimmung akzeptiert er das Schlüssselbit ansonsten wird es verworfen.

Die Ergebnisse der für das Protokoll notwendigen Berechnungen der Entropie und der bedingten Wahrscheinlichkeiten werden im folgenden aufgeführt. Für die entsprechenden Rechnungen sei auf den Anhang verwiesen.

Die Berechnungen erfolgen in der Darstellung, in der die Zustände durch ihre Blochvektoren beschrieben werden. Für die Operatoren $M_\pm$,$N_\pm$ der unscharfen Messung ergibt sich hierfür

$$\mathrm{M}_+^{\mathrm{A}} = \mathrm{M}_+^{\mathrm{A}\dagger} = \begin{pmatrix} \sqrt{p_0} & 0 \\ 0 & \sqrt{p_1} \end{pmatrix} \tag{6.10}$$

$$\mathrm{N}_+^{\mathrm{A}} = \mathrm{N}_+^{\mathrm{A}\dagger} = \frac{1}{2}\begin{pmatrix} \sqrt{p_0}+\sqrt{p_1} & \sqrt{p_0}-\sqrt{p_1} \\ \sqrt{p_0}-\sqrt{p_1} & \sqrt{p_0}+\sqrt{p_1} \end{pmatrix} \tag{6.11}$$

$$\mathrm{M}_-^{\mathrm{A}} = \mathrm{M}_-^{\mathrm{A}\dagger} = \begin{pmatrix} \sqrt{1-p_0} & 0 \\ 0 & \sqrt{1-p_1} \end{pmatrix} \tag{6.12}$$

$$\mathrm{N}_-^{\mathrm{A}} = \mathrm{N}_-^{\mathrm{A}\dagger} = \frac{1}{2}\begin{pmatrix} \sqrt{1-p_0}+\sqrt{1-p_1} & \sqrt{1-p_0}-\sqrt{1-p_1} \\ \sqrt{1-p_0}-\sqrt{1-p_1} & \sqrt{1-p_0}+\sqrt{1-p_1} \end{pmatrix}. \tag{6.13}$$

Der allgemeine Anfangszustand $|\psi\rangle = \begin{pmatrix} \cos\vartheta/2 \\ e^{i\varphi}\sin\vartheta/2 \end{pmatrix}$ liefert als Ausgangsmatrix

$$\rho = \begin{pmatrix} \cos\vartheta/2 \\ e^{i\varphi}\sin\vartheta/2 \end{pmatrix}\left(\cos\vartheta/2,\ \ e^{-i\varphi}\sin\vartheta/2\right) = \frac{1}{2}\begin{pmatrix} 1+\cos\vartheta & e^{-i\varphi}\sin\vartheta \\ e^{i\varphi}\sin\vartheta & 1-\cos\vartheta \end{pmatrix}.$$

Damit ergeben sich die Ensembledarstellungen

$$\rho_M = \frac{1}{2}\begin{pmatrix} 1+\cos\vartheta & ae^{-i\varphi}\sin\vartheta \\ ae^{i\varphi}\sin\vartheta & 1-\cos\vartheta \end{pmatrix} \tag{6.14}$$

und analog

$$\rho_N = \frac{1}{2}\begin{pmatrix} 1+a\cos\vartheta & \sin\vartheta(\cos\varphi - ia\sin\varphi) \\ \sin\vartheta(\cos\varphi + ia\sin\varphi) & 1-a\cos\vartheta \end{pmatrix}. \tag{6.15}$$

Für die Entropie dieser Ensembles gilt

$$S(\rho_A) = -\lambda_+\log\lambda_+ - \lambda_-\log\lambda_-$$

mit

$$\lambda_{\pm}^{(M)} = \frac{1}{2} \pm \frac{1}{2}\sqrt{1-(1-a^2)\sin^2\vartheta}, \tag{6.16}$$

$$\lambda_{\pm}^{(N)} = \frac{1}{2} \pm \frac{1}{2}\sqrt{a^2(1-\sin^2\vartheta\cos^2\varphi)}. \tag{6.17}$$

Wir erhalten nach Lemma 6.3 bei gleicher Basiswahl die selben Ergebnisse wie für den Anfangszustand $|\uparrow_y\rangle$. Es gilt also

$$\begin{aligned} p_\psi(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow) &= p_0 & p_\psi(\mathrm{M}_+^{\mathrm{A}} \mid \downarrow) &= p_1 \\ p_\psi(\mathrm{M}_-^{\mathrm{A}} \mid \uparrow) &= 1-p_0 & p_\psi(\mathrm{M}_-^{\mathrm{A}} \mid \downarrow) &= 1-p_1 \\ p_\psi(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow_x) &= p_0 & p_\psi(\mathrm{N}_+^{\mathrm{A}} \mid \downarrow_x) &= p_1 \\ p_\psi(\mathrm{N}_-^{\mathrm{A}} \mid \uparrow_x) &= 1-p_0 & p_\psi(\mathrm{N}_-^{\mathrm{A}} \mid \downarrow_x) &= 1-p_1. \end{aligned}$$

Die bedingten Wahrscheinlichkeiten der nichtkommutierenden Observablen lauten

$$p_\psi(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow_x) = \frac{p_0+p_1+(p_0-p_1)\cos\vartheta+2\sqrt{p_0p_1}\sin\vartheta\cos\varphi}{2(1+\sin\vartheta\cos\varphi)}$$

$$p_\psi(\mathrm{M}_-^{\mathrm{A}} \mid \uparrow_x) = \frac{1-p_0+1-p_1+(p_1-p_0)\cos\vartheta+2\sqrt{(1-p_0)(1-p_1)}\sin\vartheta\cos\varphi}{2(1+\sin\vartheta\cos\varphi)}$$

$$p_\psi(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow) = \frac{p_0+p_1+(p_0-p_1)\sin\vartheta\cos\varphi+2\sqrt{p_0p_1}\cos\vartheta}{2(1+\cos\vartheta)}$$

$$p_\psi(\mathrm{N}_-^{\mathrm{A}} \mid \uparrow) = \frac{2-p_0-p_1+(p_1-p_0)\sin\vartheta\cos\varphi+2\sqrt{(1-p_0)(1-p_1)}\cos\vartheta}{2(1+\cos\vartheta)}$$

$$p_\psi(\mathrm{M}_+^{\mathrm{A}} \mid \downarrow_x) = \frac{p_0+p_1+(p_0-p_1)\cos\vartheta-2\sqrt{p_0p_1}\sin\vartheta\cos\varphi}{2(1-\sin\vartheta\cos\varphi)}$$

$$p_\psi(\mathrm{M}_-^{\mathrm{A}} \mid \downarrow_x) = \frac{2-p_0-p_1+(p_1-p_0)\cos\vartheta-2\sqrt{(1-p_0)(1-p_1)}\sin\vartheta\cos\varphi}{2(1-\sin\vartheta\cos\varphi)}$$

$$p_\psi(\mathrm{N}_-^{\mathrm{A}} \mid \downarrow) = \frac{p_0+p_1+(p_0-p_1)\sin\vartheta\cos\varphi-2\sqrt{p_0p_1}\cos\vartheta}{2(1-\cos\vartheta)}$$

$$p_\psi(\mathrm{N}_-^{\mathrm{A}} \mid \downarrow) = \frac{2-p_0-p_1+(p_1-p_0)\sin\vartheta\cos\varphi-2\sqrt{(1-p_0)(1-p_1)}\cos\vartheta}{2(1-\cos\vartheta)}$$

Diese Größen hängen konkret von ϑ und φ, also vom Anfangszustand $|\psi\rangle$ ab.

6.4 Ununterscheidbarkeit der Ensemble

Beginnen wir mit $|\psi\rangle = |\uparrow_y\rangle$, so gilt $\rho_A = \rho_M = \rho_N$, d.h. Eve kann nicht schon anhand der Dichtematrix ρ_A auf die von Alice gewählte Basis schließen. Dieses sollte auch für

einen beliebigen Anfangszustand gelten. Daher muss ρ_A immer so gewählt sein, dass es hierzu einen Zustand $|\psi\rangle$ und einen Zustand $|\psi\rangle'$ gibt mit

$$\rho_A = \mathrm{M}_+^{\mathrm{A}}\,\rho\,\mathrm{M}_+^{\mathrm{A}\dagger} + \mathrm{M}_-^{\mathrm{A}}\,\rho\,\mathrm{M}_-^{\mathrm{A}\dagger} = \mathrm{N}_+^{\mathrm{A}}\,\rho'\,\mathrm{N}_+^{\mathrm{A}\dagger} + \mathrm{N}_-^{\mathrm{A}}\,\rho'\,\mathrm{N}_-^{\mathrm{A}\dagger}, \tag{6.18}$$

wobei $\rho = |\psi\rangle\langle\psi|$ und $\rho' = |\psi'\rangle\langle\psi'|$ ist. Die zugehörigen Winkel von $|\psi\rangle$ werden wir mit ϑ und φ bezeichnen, und entsprechend mit ϑ' und φ' für den Zustand $|\psi\rangle'$.

Die Blochdarstellung von ρ_M und ρ'_N ist dann

$$\rho_M = \frac{1}{2}\begin{pmatrix} 1+\cos\vartheta & ae^{-i\varphi}\sin\vartheta \\ ae^{i\varphi}\sin\vartheta & 1-\cos\vartheta \end{pmatrix} = \frac{1}{2}(1+\mathbf{r}\sigma)$$
$$\rho'_N = \frac{1}{2}\begin{pmatrix} 1+a\cos\vartheta' & \sin\vartheta'(\cos\varphi' - ia\sin\varphi') \\ \sin\vartheta'(\cos\varphi' + ia\sin\varphi') & 1-a\cos\vartheta' \end{pmatrix} = \frac{1}{2}(1+\mathbf{r}'\sigma)$$

mit den zugehörigen Blochvektoren $\mathbf{r}$ bzw. $\mathbf{r}'$ der Gestalt

$$\mathbf{r} = \begin{pmatrix} a\sin\vartheta\cos\varphi \\ a\sin\vartheta\sin\varphi \\ \cos\vartheta \end{pmatrix} \qquad \text{und} \qquad \mathbf{r}' = \begin{pmatrix} \sin\vartheta'\cos\varphi' \\ a\sin\vartheta'\sin\varphi' \\ a\cos\vartheta' \end{pmatrix}. \tag{6.19}$$

Hieran erkennt man auch das Transformationsverhalten von $M_\pm$ und $N_\pm$. Der Operator $M_\pm$ transformiert die Blochkugel auf ein Rotationsellipsoid um die z-Achse mit Hauptachsen der Länge a senkrecht zur z-Achse. Der Operator $N_\pm$ transformiert die Blochkugel ebenso in ein Rotationselipsoid, welches nun aber an der x-Achse orientiert ist.

Damit nun (6.18) gilt, müssen wir also den Schnitt dieser beiden Rotationsellipsoide berechnen. Da wir mit reinen Zuständen anfangen, welche alle auf dem Rand der Blochkugel liegen, erhalten wir einen Oberflächenschnitt, welcher in Abbildung 6.4 veranschaulicht ist.

Für alle Punkte in dieser Schnittmenge gilt $\mathbf{r} = \mathbf{r}'$ für entsprechende Winkel ϑ, φ und ϑ', φ'. Es gilt also

$$\begin{aligned} a\sin\vartheta\cos\varphi &= \sin\vartheta'\cos\varphi' \\ a\sin\vartheta\sin\varphi &= a\sin\vartheta'\sin\varphi' \\ \cos\vartheta &= a\cos\vartheta' \end{aligned} \tag{6.20}$$

Löst man dieses Gleichungssystem nach φ auf, so ergeben sich für $\varphi \neq n\frac{\pi}{2}$ folgende Abhängigkeiten zwischen den Winkeln

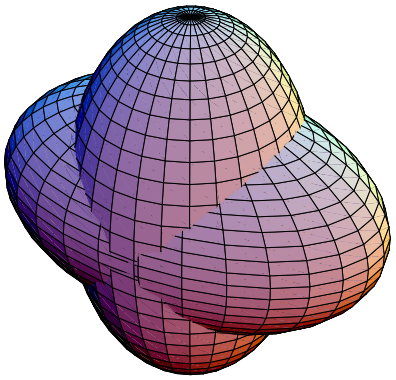


Abbildung 6.4: Schnitt der beiden Rotationsellipsoide

$$\begin{aligned}
\vartheta &= \pm \arccos\left(\pm a\sqrt{\frac{a^2\cos^2\varphi + \sin^2\varphi - 1}{a^4\cos^2\varphi + a^2\sin^2\varphi - 1}}\right) \\
\vartheta' &= \pm \arccos\left(\pm\sqrt{\frac{a^2\cos^2\varphi + \sin^2\varphi - 1}{a^4\cos^2\varphi + a^2\sin^2\varphi - 1}}\right) \\
\varphi' &= \arctan(\frac{1}{a}\tan\varphi).
\end{aligned} \tag{6.21}$$

Für den Fall $\varphi = \frac{\pi}{2}$ ergibt sich $\vartheta = \varphi' = \vartheta' = \frac{\pi}{2}$. Dieses entspricht dem vorher schon behandelten Zustand $|\uparrow_y\rangle$. Da damit $\psi = \psi'$ gilt, bestätigt sich noch einmal, dass für den $|\uparrow_y\rangle$-Zustand $\rho_M = \rho'_N = \rho_N =$ gilt.

Wählt Alice nicht den Anfangszustand $|\uparrow_y\rangle$, so darf sie den Anfangszustand ψ nicht mehr bekannt geben, da Eve dann anhand der Dichtematrix ρ_A auf die Präparation und damit auf das Schlüsselbit schließen kann. Alice kann zwar bekannt geben, dass sie entweder ψ oder ψ' verwendet hat, da diese Information nicht genügt, um die verschiedenen Ensemble zu unterscheiden, sie ist aber nach Lemma 6.3 nicht notwendig für die Auswertung von Bob.

6.5 Gemisch als Anfangszustand

Eine weitere mögliche Verallgemeinerung besteht darin, dass Alice ihr Ensemble nicht mehr mit einem festen Anfangszustand sondern mit endlich vielen Zuständen in beliebiger Reihenfolge präpariert. Alice beginnt also mit einem Gemisch, sie muss allerdings darauf achten, dass ein Ensemble mit Entropie < 1 erzeugt wird. Der Einfachheit halber betrachten wir nur endliche Gemische.

Die bedingten Wahrscheinlichkeiten berechnen sich als Konvexkombinationen der bedingten Wahrscheinlichkeiten der einzelnen Zustände. Für das Anfangsgemisch

$$\rho = \sum_{k=1}^{m} \lambda_k \left|\psi_k\right\rangle \left\langle\psi_k\right|$$

ergibt sich also beispielsweise

$$p_\rho(\mathrm{M}^{\mathrm{A}}_{\pm} \mid \uparrow) = \sum_{k=1}^{m} \lambda_k p_{\psi_k}(\mathrm{M}^{\mathrm{A}}_{\pm} \mid \uparrow).$$

Damit gilt Lemma 6.3 auch für Gemische und das Auswertungsverfahren zur Schlüsselermittlung kann einfach übernommen werden. Die Berechnung der Entropie stellt auch kein Problem dar.

Die Ununterscheidbarkeit der einzelnen Ensemble ist hier wesentlich einfacher. Da wir mit einem Gemisch beginnen, wird aus unserem Oberflächenschnitt der Ellipsoide der entsprechende Volumenschnitt. Damit kann Alice mit allen Gemischen beginnen, deren Bild innerhalb dieses Volumenschnitts liegen. Durch die Bekanntgabe der Entropie $S(\rho_A)$ ist der Paramter a aus Gleichung (6.5) festgelegt. Beginnt Alice nun miteinem Gemisch, das in der Blochdarstellung innerhalb einer Kugel mit Radius a um den Ursprung, also das totale Gemisch, liegt, so liegt das Bild dieses Gemisches garantiert im Volumenschnitt der Ellipsen, da die $\mathrm{M}^{\mathrm{A}}_{\pm}$ und $\mathrm{N}^{\mathrm{A}}_{\pm}$-Messungen den Blochvektor nur drehen und (eventuell) verkürzen.

Damit lassen sich alle benötigten Werte berechnen und man kann das Protokoll auch mit einem Gemisch durchführen.

6.6 Sicherheit unter idealen Bedingungen

Das vorgestellte Protokoll muss zumindest unter idealen Bedingungen absolut sicher sein, um später die Sicherheit unter realistischeren Bedingungen gewährlseisten zu können. Außerdem erfolgt die Schlüsselübertragung in diesem Fall ohne Fehler. Unter idealen Bedingungen verstehen wir hier die Verwendung beliebig vieler Qubits pro Ensemble und eines perfekten Quantenkanals.

Durch die Voraussetzung eines beliebig (unendlich) großen Ensembles, ist es möglich das Ensemble mit beliebiger Genauigkeit zu präparieren und die Entropie $S(\rho_A)$ exakt anzugeben. Bei der tomographischen Messung erhält Bob relative Häufigkeiten der Messergebnisse, welche nach dem Gesetz der großen Zahl für große Ensemble gegen die Erwartungswerte streben. Daher kann Bob die Entropie $S(\rho_B))$ exakt bestimmen.

Da die Übertragung über einen perfekten Quantenkanal erfolgt, wird das Ensemble bei der Übertragung nicht gestört. Die Entropieänderung muss also exakt Null sein. Da man nach 1.4 keine Information über das System erhalten kann, ohne das System zu stören, muss ein Lauscher eine nicht-unitäre Transformation des Systems vornehmen, um an Informationen zu gelangen. Eine nicht-unitäre Störung des Systems bedingt aber eine Änderung der Entropie, da sich die Eigenwerte des Systems ändern.

Diese Entropieänderung kann Bob feststellen. Somit ist das Protokoll unter idealen Bedingungen nicht abhörbar.

Da auch die bedingten relativen Häufigkeiten $h(+|\uparrow, n), \ldots$ für große Ensemble gegen die bedingten Wahrscheinlichkeiten streben und die Streuung gegen Null geht, weist der Test zur Ermittelung des Schlüssels keinen Fehler auf.

Damit ist das Protokoll prinzipiell sicher und funktionsfähig. Um zu einem realistischen Protokoll zu gelangen, müssen wir einerseits auf den perfekten Quantenkanal verzichten und andererseits zu einem endlichen Ensemble pro Bit übergehen.

7 Lauschangriffe durch unscharfe Messungen

Bei unbekanntem Anfangszustand $|\psi\rangle$ ist eine Projektionsmessung nur in der x- oder z-Basis sinnvoll, da nur dann gewisse bedingte Wahrscheinlichkeiten bekannt sind. Da projektive Messungen die Entropie eines unbekannten Ensembles im Allgemeinen stark ändern, wird nur eine Entropieänderung ΔS_t zugelassen, welche kleiner ist als die Entropieänderung bei projektiver Messung in der x- oder z-Basis. Dadurch kann Eve diese Projektionsmessungen nicht mehr durchführen. Da das zu messende Ensemble unbekannt ist, kann sie allerdings auch keinen anderen Projektionsmessungen durchführen, ohne das Risiko einzugehen, entdeckt zu werden. Wir betrachten daher nun Angriffe durch minimale[1] unscharfe Messungen von Eve. Der Einfachheit halber beschränken wir uns auf unscharfe Messungen bezüglich der relevanten Basen x und z.

7.1 Unscharfe Messungen

Die betrachteten Lauschangriffe durch unscharfe Messungen besitzen die folgenden Operatordarstellungen

$$\begin{aligned}
\mathrm{M}_{+}^{\mathrm{E}} &= q_0 \left|\uparrow\right\rangle\left\langle\uparrow\right| + q_1 \left|\downarrow\right\rangle\left\langle\downarrow\right|, && (7.1)\\
\mathrm{M}_{-}^{\mathrm{E}} &= (1-q_0) \left|\uparrow\right\rangle\left\langle\uparrow\right| + (1-q_1) \left|\downarrow\right\rangle\left\langle\downarrow\right| \quad \text{und} && (7.2)\\
\mathrm{N}_{+}^{\mathrm{E}} &= q_0 \left|\uparrow_x\right\rangle\left\langle\uparrow_x\right| + q_1 \left|\downarrow_x\right\rangle\left\langle\downarrow_x\right|, && (7.3)\\
\mathrm{N}_{-}^{\mathrm{E}} &= (1-q_0) \left|\uparrow_x\right\rangle\left\langle\uparrow_x\right| + (1-q_1) \left|\downarrow_x\right\rangle\left\langle\downarrow_x\right| && (7.4)
\end{aligned}$$

mit zunächst für Eve frei wählbaren Parametern $q_0, q_1 \in [0,1]$. Die unscharfen Messungen $\mathrm{M}_{\pm}^{\mathrm{E}}, \mathrm{N}_{\pm}^{\mathrm{E}}$ gehen für $\Delta q = 1$ ebenfalls über in die projektiven Messungen $\left|\uparrow\right\rangle\left\langle\uparrow\right|, \left|\downarrow\right\rangle\left\langle\downarrow\right|$ und $\left|\uparrow_x\right\rangle\left\langle\uparrow_x\right|, \left|\downarrow_x\right\rangle\left\langle\downarrow_x\right|$.

Da Alice und Bob nur eine Entropieänderung ΔS_t zulassen, sind nicht alle Parameter (q_0, q_1) erlaubt. Um dieses zu sehen, betrachten wir noch einmal den einfachsten Fall, dass Alice den Anfangszustand $|\uparrow_y\rangle$ wählt. Alice sendet dann das Ensemble

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & -ia \\ ia & 1 \end{pmatrix}$$

mit $a = \sqrt{p_0 p_1} + \sqrt{(1-p_0)(1-p_1)}$. Nach Messung am Ensemble ρ_A mit $\mathrm{M}_{\pm}^{\mathrm{E}}$ oder $\mathrm{N}_{\pm}^{\mathrm{E}}$ schickt Eve das Ensemble über ihren perfekten Quantenkanal weiter an Bob. Dieser

[1] minimal bedeutet, dass die Effekte $M^\dagger M$ der Messung keinen unitären Anteil besitzen, es gilt also $|M| = M$

erhält dann

$$\begin{aligned}\rho_B &= \mathrm{M}_{+}^{\mathrm{E}\,\dagger}\,\rho_A\,\mathrm{M}_{+}^{\mathrm{E}} + \mathrm{M}_{-}^{\mathrm{E}\,\dagger}\,\rho_A\,\mathrm{M}_{-}^{\mathrm{E}} \\ &= \mathrm{N}_{+}^{\mathrm{E}\,\dagger}\,\rho_A\,\mathrm{N}_{+}^{\mathrm{E}} + \mathrm{N}_{-}^{\mathrm{E}\,\dagger}\,\rho_A\,\mathrm{N}_{-}^{\mathrm{E}} \\ &= \frac{1}{2}\begin{pmatrix} 1 & -iab \\ iab & 1 \end{pmatrix}\end{aligned}$$

mit

$$b = \sqrt{q_0 q_1} + \sqrt{(1-q_0)(1-q_1)}. \tag{7.5}$$

Dieses Ensemble hat dann eine von-Neumann-Entropie von

$$S(\rho_E) = -(\frac{1}{2} + \frac{ab}{2})\log(\frac{1}{2} + \frac{ab}{2}) - (\frac{1}{2} - \frac{ab}{2})\log(\frac{1}{2} + \frac{ab}{2}). \tag{7.6}$$

Da $0 < b < 1$ gilt, ist $ab < a$. Betrachtet man noch einmal Abbildung 6.3, so ist klar, dass hierurch die Entropie erhöht wurde. Daher muss Eve b nahe 1 wählen, um nicht entdeckt zu werden. Dadurch ist sie in der Wahl ihrer Parameter beschränkt.

Mit bekanntem $S(\rho_A)$ und ΔS_t kann man nun eine obere Schranke für b finden. Hierzu ein numerisches Beispiel.

Beispiel 7.1. Wir wählen p_0 und p_1 so, dass $a = 0.8$ gilt. Dann ist $S(\rho_A) = 0.469$. Erlauben wir nun eine Entropieänderung von $\Delta S_t \leq 0.1$, so folgt für Eve, dass $b \geq 0.915$ sein muss, um nicht entdeckt zu werden. Umgerechnet ist damit eine Differenz $|q_0 - q_1|$ von maximal 0.41 erlaubt. Setzen wir $\Delta S \leq 0.01$, so ergibt sich $b \geq 0.993$ und damit $|q_0 - q_1| \leq 0.16$. Wie wir später sehen werden, entsprechen diese Entropieänderungen typischen Werten bei Verwendung endlicher Ensemble.

Wir gehen zunächst von einer Auswertung von Eve analog zu Bob's Verfahren aus. Daher müssen wir auch ihre bedingten Wahrscheinlichkeiten berechnen. Es ergeben sich die folgenden Werte für den Anfangszustand $|\uparrow_y\rangle$ (Berechnung siehe Anhang).

$$\begin{aligned}p(\mathrm{M}_{+}^{\mathrm{A}} \,|\, \mathrm{M}_{+}^{\mathrm{E}}) &= \frac{q_0 p_0 + q_1 p_1 + 2\sqrt{q_0 q_1}\sqrt{p_0 p_1}a}{q_0 + q_1 + 2\sqrt{q_0 q_1}a} \\ p(\mathrm{N}_{+}^{\mathrm{A}} \,|\, \mathrm{N}_{+}^{\mathrm{E}}) &= \frac{q_0 p_0 + q_1 p_1 + 2\sqrt{q_0 q_1}\sqrt{p_0 p_1}a}{q_0 + q_1 + 2\sqrt{q_0 q_1}a} \\ p(\mathrm{N}_{+}^{\mathrm{A}} \,|\, \mathrm{M}_{+}^{\mathrm{E}}) &= \frac{q_0(p_0 + p_1) + q_1(p_0 + p_1) + 4\sqrt{q_0 q_1}\sqrt{p_0 p_1}a}{2[q_0 + q_1 + 2\sqrt{q_0 q_1}a]} \\ p(\mathrm{M}_{+}^{\mathrm{A}} \,|\, \mathrm{N}_{+}^{\mathrm{E}}) &= \frac{q_0(p_0 + p_1) + q_1(p_0 + p_1) + 4\sqrt{q_0 q_1}\sqrt{p_0 p_1}a}{2[q_0 + q_1 + 2\sqrt{q_0 q_1}a]}\end{aligned} \tag{7.7}$$

Die Ergebnisse der $-$-Messungen erhält man dadurch, dass man die ensprechenden Parameter p_i (bei $\mathrm{M}_{-}^{\mathrm{A}}, \mathrm{N}_{-}^{\mathrm{A}}$) oder q_i (bei $\mathrm{M}_{-}^{\mathrm{E}}, \mathrm{N}_{-}^{\mathrm{E}}$) durch $1 - p_i$ bzw. $1 - q_i$ ersetzt.

Für einen allgemeinen Anfangszustand mit Dichtematrix ρ folgt entsprechend:

$$\begin{aligned} p_\psi(\mathrm{M}_+^\mathrm{A} \,|\, \mathrm{M}_+^\mathrm{E}) &= \frac{\langle\psi|\, \mathrm{M}_+^{\mathrm{A}\,\dagger}\, \mathrm{M}_+^\mathrm{E}\, \rho\, \mathrm{M}_+^{\mathrm{E}\,\dagger}\, \mathrm{M}_+^\mathrm{A}\, |\psi\rangle}{\langle\psi|\, \mathrm{M}_+^\mathrm{E}\, \rho\, \mathrm{M}_+^{\mathrm{E}\,\dagger}\, |\psi\rangle} \\ &= \frac{q_0 p_0 (1+\cos\vartheta)^2 + q_1 p_1 (1-\cos\vartheta)^2 + 2\sqrt{q_0 q_1}\sqrt{p_0 p_1} a \sin^2\vartheta}{q_0(1+\cos\vartheta)^2 + q_1(1-\cos\vartheta)^2 + 2\sqrt{q_0 q_1} a \sin^2\vartheta} \end{aligned} \tag{7.8}$$

$$\begin{aligned} &p_\psi(\mathrm{N}_+^\mathrm{A} \,|\, \mathrm{N}_+^\mathrm{E}) = \\ &= \frac{q_0 p_0 (1+\sin\vartheta\cos\varphi)^2 + q_1 p_1 (1-\sin\vartheta\cos\varphi)^2 + 2a\sqrt{q_0 q_1}\sqrt{p_0 p_1}(\cos^2\vartheta + \sin^2\vartheta\sin^2\varphi)}{q_0(1+\sin\vartheta\cos\varphi)^2 + q_1(1-\sin\vartheta\cos\varphi)^2 + 2a\sqrt{q_0 q_1}(\cos^2\vartheta + \sin^2\vartheta\sin^2\varphi)} \end{aligned} \tag{7.9}$$

$$\begin{aligned} &p_\psi(\mathrm{N}_+^\mathrm{A} \,|\, \mathrm{M}_+^\mathrm{E}) = \\ &= \frac{q_0(1+a\cos\vartheta)(p_0+p_1+(p_0-p_1)\sin\vartheta\cos\varphi + 2\sqrt{p_0 p_1}\cos\vartheta)}{2q_0(1+a\cos\vartheta)(1+\cos\vartheta) + 2q_1(1-\cos\vartheta) + 4\sqrt{q_0 q_1}(\sin^2\vartheta\cos^2\varphi + a\sin^2\vartheta\sin^2\varphi)} + \\ &+ \frac{q_1(1-a\cos\vartheta)(p_0+p_1+(p_0-p_1)\sin\vartheta\cos\varphi - 2\sqrt{p_0 p_1}\cos\vartheta)}{2q_0(1+a\cos\vartheta)(1+\cos\vartheta) + 2q_1(1-\cos\vartheta) + 4\sqrt{q_0 q_1}(\sin^2\vartheta\cos^2\varphi + a\sin^2\vartheta\sin^2\varphi)} + \\ &+ \frac{2\sqrt{q_0 q_1}((p_0-p_1)\sin\vartheta\cos\varphi + (p_0+p_1)\sin^2\vartheta\cos^2\varphi + 2a\sqrt{p_0 p_1}\sin^2\vartheta\sin^2\varphi)}{2q_0(1+a\cos\vartheta)(1+\cos\vartheta) + 2q_1(1-\cos\vartheta) + 4\sqrt{q_0 q_1}(\sin^2\vartheta\cos^2\varphi + a\sin^2\vartheta\sin^2\varphi)} \end{aligned} \tag{7.10}$$

$$\begin{aligned} &p_\psi(\mathrm{M}_+^\mathrm{A} \,|\, \mathrm{N}_+^\mathrm{E}) = \\ &= [q_0(1+a\sin\vartheta\cos\varphi)(p_0+p_1+(p_0-p_1)\cos\vartheta + 2\sqrt{p_0 p_1}\sin\vartheta\cos\varphi) + \\ &\quad + q_1(1-a\sin\vartheta\cos\varphi)(p_0+p_1+(p_0-p_1)\cos\vartheta - 2\sqrt{p_0 p_1}\sin\vartheta\cos\varphi) + \\ &\quad + 2\sqrt{q_0 q_1}((p_0-p_1)\cos\vartheta + (p_0+p_1)cos^2\vartheta + 2a\sqrt{p_0 p_1}\sin^2\vartheta(1-\cos^2\varphi)]/ \\ &\quad /[2q_0(1+\sin\vartheta\cos\varphi)(1+a\sin\vartheta\cos\varphi) + 2q_1(1-\sin\vartheta\cos\varphi)(1-a\sin\vartheta\cos\varphi) + \\ &\quad + 4\sqrt{q_0 q_1}(\cos^2\vartheta + a\sin^2\vartheta(1-\cos^2\varphi))]. \end{aligned} \tag{7.11}$$

Diese Größen sind ohne Kenntnis des Anfangszustands $|\psi\rangle$ noch nicht zur Schlüsselermittlung geeignet, da sie alle von ϑ und φ abhängen. Durch ihre Messung erhält Eve aber ebenso wie Bob weitere Information durch die unbedingten Wahrscheinlichkeiten ihrer Messergebnisse. Für diese gilt

$$\begin{aligned} p(\mathrm{M}_+^\mathrm{E}) &= \mathrm{tr}(\mathrm{M}_+^{\mathrm{E}\,\dagger}\, \mathrm{M}_+^\mathrm{E}\, \rho_A) = q_0 \rho_{A00} + q_1 \rho_{A11} \\ p(\mathrm{N}_+^\mathrm{E}) &= \mathrm{tr}(\mathrm{N}_+^{\mathrm{E}\,\dagger}\, \mathrm{N}_+^\mathrm{E}\, \rho_A) = \frac{1}{2}(q_0+q_1)(\rho_{A00}+\rho_{A11}) + \frac{1}{2}(q_0-q_1)(\rho_{A01}+\rho_{A10}) \end{aligned}$$

mit

$$\begin{aligned}
\rho_{A00} &= \frac{1}{2}(1+\cos\vartheta) = \frac{1}{2}(1+a\cos\vartheta') \\
\rho_{A11} &= \frac{1}{2}(1-\cos\vartheta) = \frac{1}{2}(1-a\cos\vartheta') \\
\rho_{A01}+\rho_{A10} &= a\sin\vartheta\cos\varphi = \sin\vartheta'\cos\varphi' \\
\rho_{A00}+\rho_{A11} &= \operatorname{tr}\rho_A = 1.
\end{aligned}$$

Es gilt also

$$p(\mathrm{M}_+^{\mathrm{E}}) = \frac{1}{2}(q_0+q_1+(q_0-q_1)\cos\vartheta) = \frac{1}{2}(q_0+q_1+(q_0-q_1)a\cos\vartheta') \tag{7.12}$$

$$\begin{aligned}
p(\mathrm{N}_+^{\mathrm{E}}) &= \frac{1}{2}(q_0+q_1)+\frac{1}{2}(q_0-q_1)a\sin\vartheta\cos\varphi \\
&= \frac{1}{2}(q_0+q_1)+\frac{1}{2}(q_0-q_1)\sin\vartheta'\cos\varphi'.
\end{aligned} \tag{7.13}$$

Zusammen mit der von Alice bekanntgegebenen Entropie $S(\rho_A)$ kann sie nun ihre Messergebnisse in folgender Weise sinnvoll nutzen.

Für die von-Neumann-Entropie gilt $S(\rho_A) = -\lambda_+\log\lambda_+ - \lambda_-\log\lambda_-$ mit

$$\lambda_\pm = \frac{1}{2}\pm\frac{1}{2}\sqrt{1-(1-a^2)\sin^2\vartheta} = \frac{1}{2}\pm\frac{1}{2}\sqrt{a^2(1-\sin^2\vartheta'\cos^2\varphi')}.$$

Sie hängt also bei einer $\mathrm{M}_\pm^{\mathrm{A}}$ Präparation nur von a und $\sin^2\vartheta$ ab und bei einer $\mathrm{N}_\pm^{\mathrm{A}}$-Präparation von a und $\sin\vartheta'\cos\varphi'$.

Wir nehmem zunächst an, dass Alice mit $\mathrm{M}_\pm^{\mathrm{A}}$ präpariert hat. Dann gelten jeweils die ersten Formeln und Eve erhält

- aus $p(\mathrm{M}_+^{\mathrm{E}})$ die Größe $\cos\vartheta$
- aus $S(\rho_A)$ die Größe a und
- aus $p(\mathrm{N}_+^{\mathrm{E}})$ noch $\sin\vartheta\cos\varphi$.

Hat Alice mit $\mathrm{N}_\pm^{\mathrm{A}}$ präpariert, so folgt

- aus $p(\mathrm{N}_+^{\mathrm{E}})$ die Größe $\sin\vartheta'\cos\varphi'$,
- aus $S(\rho_A)$ wieder a und
- aus $p(\mathrm{M}_+^{\mathrm{E}})$ schließlich $\cos\vartheta'$.

Eve erhält damit zwar nicht die volle Information über den Anfangszustand $|\psi\rangle$, aber sie kennt nun alle aus $|\psi\rangle$ folgenden relevanten Größen für ihre bedingten Wahrscheinlichkeiten.

Bemerkung 7.2. Es ist zu beachten, dass bei der Auswertung der Messergebnisse angenommen wurde, dass Alice mit $\mathrm{M}_{\pm}^{\mathrm{A}}$ präpariert, um Aussagen über $|\psi\rangle$ zu erhalten. Um Aussagen über $|\psi'\rangle$ zu erhalten, wurde angenommen, dass Alice mit $\mathrm{N}_{\pm}^{\mathrm{A}}$ präpariert hat. Eve kann also nicht anhand ihrer Ergebnisse zwischen $|\psi\rangle$ und $|\psi\rangle'$ unterscheiden, was der Ununterscheidbarkeit der Ensemble ρ_M und ρ_N widersprechen würde.

Die bedingten Wahrscheinlichkeiten sind nach dieser Berechnung nur noch von den Größen p_0, p_1 sowie q_0, q_1 abhängig, von denen Eve q_0 und q_1 sogar kennt. Gibt Alice die Parameter p_0 und p_1 bekannt, so kann Eve analog zu Bob auf die von Alice gewählte Basis schließen, indem sie die theoretisch aus (7.8)-(7.11) ermittelten Werte mit ihren relativen Häufigkeiten vergleicht.

Im Falle unendlich großer Ensemeble gehen auch Eves relative Häufigkeiten beliebig nahe gegen die entsprechenden bedingten Wahrscheinlichkeiten. Damit ist klar, dass Eve hiermit im Grenzfall unendlich großer Ensemble unbemerkt das Protokoll abhören kann.

Dieses Resultat ist nicht weiter erstaunlich, wenn man bedenkt, dass Eve und Bob bisher bei der Auswertung ihrer Messergebnisse eine symmetrische Position eingenommen haben. Ist die Entropieänderung zwischen ρ_A und ρ_B akzeptiert, tauscht Bob mit Alice keine Information mehr aus. Daher ist Eve ab diesem Zeitpunkt in der gleichen Position wie Bob. Beide vergleichen die theoretisch berechneten Werte mit ihren ermittelten relativen Häufigkeiten. Da keine Streuung vorliegt, sind lediglich die Zahlenwerte verschieden.

Daher müssen wir das Protokoll derart ändern, dass diese Symmetrie gebrochen wird.

Im Falle eines endlichen Ensembles liegen füe Bob und Eve verschieden große Streuungen vor. Daher ist es möglich, dass das ursprüngliche Protokoll dann sicher gegenüber diesem Angrif ist. Dieses wird später untersucht.

7.2 Modifikation des Protokolls

Da Eve, wie wir gesehen haben, auf den Anfangszustand $|\psi\rangle$ bzw. $|\psi\rangle'$ schließen kann, kann Alice diese ebensogut auch bekannt geben. Dann brauchen wir allerdings eine andere unbekannte Größe, welche Eve nicht aus ihren Messergebnissen ableiten kann, um die Symmetrie zu brechen. Die einzigen verbleibenden Größen, welche Eve nicht berechnen kann, sind p_0 und p_1. Daher fordern wir:

Alice darf die Parameter p_0 und p_1 nicht bekannt geben !

7.2.1 Bobs Auswertung

Da Alice nun die für Bobs Auswertung benötigten Parameter p_0 und p_1 nicht mehr bekannt gibt, müssen wir ein anderes Verfahren finden, wie Bob dennoch an die ver-

schlüsselte Information gelangt.

Dieses kann beispielsweise folgendermaßen geschehen.

Alice wählt sich zwei verschiedene Anfangszustände ψ_1 und ψ_2, welche

$$p_{\psi_1}(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow) \neq p_{\psi_2}(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow)$$

und

$$p_{\psi_1}(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow_x) \neq p_{\psi_2}(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow_x)$$

erfüllen.

Hiermit erzeugt sie dann durch $\mathrm{M}_\pm^{\mathrm{A}}$- oder $\mathrm{N}_\pm^{\mathrm{A}}$-Messung zwei Subensemble, welche sie dann zu einem Ensemble beliebig zusammensetzt. Der Einfachheit halber gehen wir davon aus, dass Alice zunächst das erste Subensemble schickt und separat davon das zweite. Die Parameter p_0 und p_1 haben dabei in beiden Subensemblen die gleichen Werte.

Nach Bobs Messung teilt sie ihm die Entropie des Gesamtensembles, ihre Aufteilung in die zwei Subensemble und die jeweilige Aufteilung nach $+/-$ mit.

Für Bob gilt nach Lemma 6.3

$$\begin{aligned} &p_{\psi_1}(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow_x) \neq p_{\psi_2}(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow_x), && p_{\psi_1}(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow) \neq p_{\psi_2}(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow) \quad \text{und} \\ &p_{\psi_1}(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow) = p_{\psi_2}(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow), && p_{\psi_1}(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow_x) = p_{\psi_2}(\mathrm{N}_+^{\mathrm{A}} \mid \uparrow_x). \end{aligned}$$

Die bedingten Wahrscheinlichkeiten und damit auch die entsprechenden relativen Häufigkeiten ändern sich also beim Wechsel des Anfangszustands, wenn er eine andere Basis als Alice gewählt hat, und bleiben unverändert bei gleicher Basiswahl. Betrachtet man die Differenz der bedingten Wahrscheinlichkeiten $p_{\psi_1}(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow) - p_{\psi_2}(\mathrm{M}_+^{\mathrm{A}} \mid \uparrow), \ldots$ der Unterensemble, so sind diese Null, also unabhängig von den Parametern p_0, p_1. Gleiches gilt (mit entsprechender Streuung) für die relativen Häufigkeiten, wenn Bob in der gleichen Basis wie Alice gemessen hat.

Damit kann er ohne Angabe von p_0 und p_1 auf die von Alice gewählte Basis und damit auf das übertragene Bit schließen, indem er vergleicht, ob sich die relativen Häufigkeiten bei Änderung des Ensembles verändern oder nicht. Dieses entspricht einem Test zweier Wahrscheinlichkeitsverteilungen und ist äquivalent dazu, die Differenz der relativen Häufigkeitenen auf den Erwartungswert Null zu testen.

Das prinzipielle Protokoll bleibt also erhalten. Die Verschlüsselung des Bits erfolgt nun allerdings durch Auswertung und Vergleich zweier Ensemble, wodurch doppelt so viele Qubits wie ursprünglich benötigt werden.

Für Eve gilt im Allgemeinen stets die Ungleichheit der relativen Häufigkeiten, unabhängig davon, ob sie die gleiche oder eine andere Basis als Alice gewählt hat. Damit kann sie nicht mehr ihr ursprüngliches Verfahren nutzen und die Symmetrie in der Auswertung ist gebrochen. Das Protokoll ist nun sicher gegenüber obigem einfachen Lauschanriff durch unscharfe Messungen. Diese Sicherheit gilt sogar für den Fall beliebig großer Ensemble.

7.3 Verallgemeinerter Angriff

Wir haben gesehen, dass das modifizierte Protokoll sicher ist gegenüber einfachen Lauschangriffen. Nun erlauben wir Eve alle Freiheiten bezüglich der Messoperatoren $\mathrm{M}^{\mathrm{E}}_{\pm}$ und $\mathrm{N}^{\mathrm{E}}_{\pm}$. Sie darf beispielsweise verschiedene Parameter wählen oder $\mathrm{M}^{\mathrm{E}}_{\pm}$- und $\mathrm{N}^{\mathrm{E}}_{\pm}$-Messungen beliebig abwechseln. Allerdings lassen wir der Einfachheit halber keine weiteren Messoperatoren in anderen Basen als der x- oder z-Basis zu.

Es wird sich herausstellen, das das Protokoll im Falle unendlich großer Ensmeble nicht mehr sicher ist gegen den allgemeineren Lauschangriff durch unscharfe Messungen. Dazu betrachten wir zunächst den einfachsten (hypothetischen) Fall, Präparation mit dem Anfangszustand $|\uparrow_y\rangle$. Hier kann man recht einfach zeigen, dass Eve durch Messung von $\mathrm{M}^{\mathrm{E}}_{\pm}$ oder $\mathrm{N}^{\mathrm{E}}_{\pm}$ und geeigneter Auswertung aus die von Alice gewählte Präparation schließen kann. Anschließend wenden wir uns dem allgemeinen Fall zu, bei dem wir einen konkreten Lauschangriff mit unscharfen Messungen angeben, mit dem Eve die gewünscht Information erhält. Dieser Angriff basiert allerdings darauf, dass wirklich unendlich viele Qubits pro Ensemble vorliegen und kann nicht auf endliche Ensemble übertragen werden.

7.3.1 Anfangszustand $|\uparrow_y\rangle$

Wir erinnern an die (vereinfachte) vorliegende Ausgangslage. Dabei ist Eve bekannt, welche Anfangszustände Alice gewählt hat. Alice präpariert mit unscharfen Messungen ausgehen vom Zustand $|\uparrow_y\rangle$ ein Unterensemble. Dieses wird von Eve unscharf mit $\mathrm{M}^{\mathrm{E}}_{\pm}$ (oder $\mathrm{N}^{\mathrm{E}}_{\pm}$) gemessen und anschließend an Bob geschickt. Alice schickt ein zweites (anderes) Unterensemble, so dass Bob den Schlüssel ermitteln kann. Dieses zweite Ensemble bleibt von Eve unberührt. Anschließend gibt Alice $S(\rho_A)$ sowie die Reihenfolge ihrer $+/-$-Ergebnisse bekannt.

Die bedingten Wahrscheinlichkeiten für Eves Messergebnisse sind dann (7.7)

$$
\begin{aligned}
p(\mathrm{M}^{\mathrm{A}}_{+} \,|\, \mathrm{M}^{\mathrm{E}}_{+}) &= \frac{q_0 p_0 + q_1 p_1 + 2\sqrt{q_0 q_1}\sqrt{p_0 p_1}\,a}{q_0 + q_1 + 2\sqrt{q_0 q_1}\,a} \\
p(\mathrm{N}^{\mathrm{A}}_{+} \,|\, \mathrm{N}^{\mathrm{E}}_{+}) &= \frac{q_0 p_0 + q_1 p_1 + 2\sqrt{q_0 q_1}\sqrt{p_0 p_1}\,a}{q_0 + q_1 + 2\sqrt{q_0 q_1}\,a} \\
p(\mathrm{N}^{\mathrm{A}}_{+} \,|\, \mathrm{M}^{\mathrm{E}}_{+}) &= \frac{q_0(p_0 + p_1) + q_1(p_0 + p_1) + 4\sqrt{q_0 q_1}\sqrt{p_0 p_1}\,a}{2[q_0 + q_1 + 2\sqrt{q_0 q_1}\,a]} \\
p(\mathrm{M}^{\mathrm{A}}_{+} \,|\, \mathrm{N}^{\mathrm{E}}_{+}) &= \frac{q_0(p_0 + p_1) + q_1(p_0 + p_1) + 4\sqrt{q_0 q_1}\sqrt{p_0 p_1}\,a}{2[q_0 + q_1 + 2\sqrt{q_0 q_1}\,a]}
\end{aligned}
$$

und entsprechend für die $-$-Messungen.

Eve kennt hiervon die Parameter q_0, q_1 und a. Der Parameter p_1 kann mit Gleichung (6.5) nach p_0 und a aufgelöst werden, so dass der einzige verbleibende unbekannte Parameter p_0 ist.

Eve kann nun anhand ihrer Messergebnisse

$$h(+, \mathrm{M}^{\mathrm{E}}_{+}, n), h(+, \mathrm{M}^{\mathrm{E}}_{-}, n), h(-, \mathrm{M}^{\mathrm{E}}_{+}, n) \text{ und } h(-, \mathrm{M}^{\mathrm{E}}_{-}, n)$$

nicht auf Alice' Basis schließen, wenn es p_0 und p'_0 gibt mit

$$\begin{aligned} p(\mathrm{M}^{\mathrm{A}}_{+} \,|\, \mathrm{M}^{\mathrm{E}}_{+})_{p_0} &= p(\mathrm{N}^{\mathrm{A}}_{+} \,|\, \mathrm{M}^{\mathrm{E}}_{+})_{p'_0} \quad \text{und} \\ p(\mathrm{M}^{\mathrm{A}}_{+} \,|\, \mathrm{M}^{\mathrm{E}}_{-})_{p_0} &= p(\mathrm{N}^{\mathrm{A}}_{+} \,|\, \mathrm{M}^{\mathrm{E}}_{-})_{p'_0}. \end{aligned}$$

Die Gleichheit der bedingten Wahrscheinlichkeiten mit $\mathrm{M}^{\mathrm{A}}_{-}, \mathrm{N}^{\mathrm{A}}_{-}$ ist dann aus Symmetriegründen automatisch erfüllt. Dabei müssen p_0 und p'_0 zum gleichen Wert a führen, da dieser Eve bekannt ist.

Es muss also gelten

$$q_0p_0 + q_1p_1 + 2\sqrt{q_0q_1}\sqrt{p_0p_1}a = \frac{1}{2}q_0(p'_0 + p'_1) + \frac{1}{2}q_1(p'_0 + p'_1) + 2\sqrt{q_0q_1}\sqrt{p'_0p'_1}a \quad (7.14)$$

$$\begin{aligned} (1-q_0)p_0 + (1-q_1)p_1 + 2\sqrt{(1-q_0)(1-q_1)}\sqrt{p_0p_1}a = \\ = \frac{1}{2}(1-q_0)(p'_0 + p'_1) + \frac{1}{2}(1-q_1)(p'_0 + p'_1) + 2\sqrt{(1-q_0)(1-q_1)}\sqrt{p'_0p'_1}a \end{aligned} \quad (7.15)$$

undter der Nebenbedingung

$$a = \sqrt{p_0p_1} + \sqrt{(1-p_0)(1-p_1)} = \sqrt{p'_0p'_1} + \sqrt{(1-p'_0)(1-p'_1)} = a'. \quad (7.16)$$

Setzt man (7.14) in (7.15) ein, erhält man

$$2a(\sqrt{p_0p_1} - \sqrt{p'_0p'_1})(\sqrt{q_0q_1} - \sqrt{(1-q_0)(1-q_1)}) = p_0 + p_1 + p'_0 + p'_1. \quad (7.17)$$

Existiert nun für jedes Paar q_0, q_1 eine Lösung p_0, p_1, p'_0, p'_1 mit $a = a'$, so wäre das Verfahren sicher gegenüber diesem Lauschangriff. Betrachtet man die Funktion

$$Q := \left|(\sqrt{q_0q_1} - \sqrt{(1-q_0)(1-q_1)})\right| = \left|\frac{p_0 + p_1 + p'_0 + p'_1}{2a(\sqrt{p_0p_1} - \sqrt{p'_0p'_1})}\right|$$

mit der Nebenbedingung $a = a'$, so stellt man fest, dass das Minimum von Q für $a = a' = 1$ bei 1 liegt und sonst > 1 ist. Hierzu wurde numerische Minimierung mit Mathematica genutzt. Da aber stets $0 \leq Q \leq 1$ gelten muss, exisitert somit nur für $Q = 1$ eine theoretische Lösung, welche praktisch aber nicht von Nutzen ist. Aus $a = a' = 1$ folgt mit Gleichung (6.5), dass $p_0 = p_1$ und $p'_0 = p'_1$ gilt. Bob kann also diesem Fall seine Messergebnisse ebenfalls nicht auswerten, da sie zufällig erscheinen. Somit kann Eve mit ihrem Lauschangriff das Protokoll abhöhren.

7.3.2 Allgemeiner reiner Anfangszustand

Wir befinden uns in der gleichen Ausgangslage wie zuvor, nur dass Alice nun zwei beliebige Anfangszustände $|\psi_1\rangle$ und $|\psi_2\rangle$ verwendet. Der vorgestellte Angriff nutzt nur eines dieser Unterensemble. Daher beschränken wir uns auf den Fall $|\psi_1\rangle = |\psi\rangle$. Betrachten wir die dazu gehörenden bedingten Wahrscheinlichkeiten (7.8)-(7.11), so kann man diese nach den unbekannten Parametern p_0 und p_1 auflösen. Es ergeben sich dann jeweils Gleichungen der Gestalt

$$p_\psi(X|Y) = p_0 f_{X|Y} + p_1 g_{X|Y} + \sqrt{p_0 p_1} h_{X|Y} \tag{7.18}$$

mit bekannten Funktionen $f_{X|Y}, g_{X|Y}$ und $h_{X|Y}$. Der Einfachheit halber lassen wir im Folgenden den Index $X|Y$ weg. Nutzt man nun wieder $a = \sqrt{p_0 p_1} + \sqrt{(1-p_0)(1-p_1)}$ (6.5), so kann man Gleichung (7.18) nach p_0 auflösen und erhält die folgenden vier Lösungen :

$$p_0 = \frac{1}{2\beta_+}(\alpha_+ \pm \sqrt{\alpha_+^2 - 4\beta_+\gamma}) \qquad \text{und}$$
$$p_0 = \frac{1}{2\beta_-}(\alpha_- \pm \sqrt{\alpha_-^2 - 4\beta_-\gamma})$$

mit

$$\begin{aligned}
\alpha_\pm &= 2(p_\psi - (1-a^2)g)(f-g) + 4a^2 p_\psi g + (1-a^2)h^2 \pm 2ah(p_\psi + (1-a^2)g)(f-g) \\
\beta_\pm &= (f-g)^2 + 2a^2 fg + h^2 \pm 2ah(f+g) \\
\gamma &= (p_\psi - (1-a^2)g)^2.
\end{aligned}$$

Somit kann Eve aus jeder Gleichung (7.8)-(7.11) bis zu vier mögliche Lösungen ermitteln. Ein einfacher Vergleich der Lösungen zu (7.8) und (7.11) sowie entsprechend von (7.9) und (7.10) liefert dann entweder

- genau eine Lösung p_0 und damit die Basis, oder
- mehrere Lösungen für die eine Basis und keine für die andere Basis, oder
- eine (oder mehrere) Lösung für die x- und eine (andere) für die z-Basis.

Nur im letzten Fall kann Eve nicht eindeutig auf Alice' Basis schließen. Daher untersuchen wir nur diesen Fall im Speziellen.

Dazu betrachten wir folgende Funktion

$$\begin{aligned}
f(q_0, q_1, p_0, p_0', \mathbf{x}) = {} & |p_\psi(\mathrm{M}_+^\mathrm{A} \,|\, \mathrm{M}_+^\mathrm{E}) - p_{\psi'}(\mathrm{N}_+^\mathrm{A} \,|\, \mathrm{M}_+^\mathrm{E})| + |p_\psi(\mathrm{M}_+^\mathrm{A} \,|\, \mathrm{N}_+^\mathrm{E}) - p_{\psi'}(\mathrm{N}_+^\mathrm{A} \,|\, \mathrm{N}_+^\mathrm{E})| + \\
& + |p_\psi(\mathrm{M}_+^\mathrm{A} \,|\, \mathrm{M}_-^\mathrm{E}) - p_{\psi'}(\mathrm{N}_+^\mathrm{A} \,|\, \mathrm{M}_-^\mathrm{E})| + |p_\psi(\mathrm{M}_+^\mathrm{A} \,|\, \mathrm{N}_-^\mathrm{E}) - p_{\psi'}(\mathrm{N}_+^\mathrm{A} \,|\, \mathrm{N}_-^\mathrm{E})|,
\end{aligned}$$

wobei $p_\psi(\mathrm{M}_+^\mathrm{A} \,|\, \cdot\,)$ von p_0 und $p_{\psi'}(\mathrm{N}_+^\mathrm{A} \,|\, \cdot\,)$ von p_0' abhängen, da wir ja verschiedene Lösungen p_0 und p_0' für die verschiedenen Präparationen M_+^A und N_+^A zulassen. Der Parameter

$\mathbf{x}$ beschreibt die übrigen bekannten Koeffizienten (a,$\cos\vartheta, \sin\vartheta\cos\varphi, \dots$) und ist durch die Wahl des Anfangzustands von Alice und die Entropie festgelegt.

Der kritische Fall tritt nun genau dann ein, wenn zu von Eve gewählten Parametern q_0, q_1 eine Lösung (p_0, p_0') zu $f(q_0, q_1, p_0, p_0', \mathbf{x}) = 0$ existiert. Dann kann Alice den Anfangszustand $|\psi\rangle$ mit $\mathrm{M}_+^{\mathrm{A}} = p_0 \,|\uparrow\rangle\langle\uparrow| + p_1 \,|\downarrow\rangle\langle\downarrow|$ (und $\mathrm{M}_-^{\mathrm{A}}$ entsprechend) oder den Anfangszustand $|\psi'\rangle$ mit $\mathrm{N}_+^{\mathrm{A}} = p_0' \,|\uparrow_x\rangle\langle\uparrow_x| + p_1' \,|\downarrow_x\rangle\langle\downarrow_x|$ (und $\mathrm{N}_-^{\mathrm{A}}$ enstprechend) präpariert haben. Hierfür gilt dann $p_\psi(\mathrm{M}_+^{\mathrm{A}} \,|\, \mathrm{M}_+^{\mathrm{E}}) = p_{\psi'}(\mathrm{N}_+^{\mathrm{A}} \,|\, \mathrm{M}_+^{\mathrm{E}})$, $p_\psi(\mathrm{M}_+^{\mathrm{A}} \,|\, \mathrm{N}_+^{\mathrm{E}}) = p_{\psi'}(\mathrm{N}_+^{\mathrm{A}} \,|\, \mathrm{N}_+^{\mathrm{E}})$, $p_\psi(\mathrm{M}_+^{\mathrm{A}} \,|\, \mathrm{M}_-^{\mathrm{E}}) = p_{\psi'}(\mathrm{N}_+^{\mathrm{A}} \,|\, \mathrm{M}_-^{\mathrm{E}})$ und $p_\psi(\mathrm{M}_+^{\mathrm{A}} \,|\, \mathrm{N}_-^{\mathrm{E}}) = p_{\psi'}(\mathrm{N}_+^{\mathrm{A}} \,|\, \mathrm{N}_-^{\mathrm{E}})$, da der Absolutbetrag stets ≥ 0 ist und somit schon jeder Summand $= 0$ sein muss. Somit kan Eve anhand ihrer Messergebnisse nicht auf die von Alice gewählte Basis schließen. Korrekterweise müssen in der Betrachtung auch noch die Nebenbedingungen (6.20) für die möglichen Anfangszustände erfüllt sein. Die Betrachtung des vereinfachten Falls ist jedoch ausreichend, um die Sicherheit des Protokolls zu widerlegen. Die bisherigen Vorgehensweise lief im Wesentlichen analog zum Fall $|\psi\rangle = |\uparrow_y\rangle$. Für den allgemeinen Fall konnte aber leider kein analoger Beweis gefunden werden. Numerische Minimierungsversuche von f lieferten keine eindeutige Aussage darüber, ob für jedes erlaubte Paar q_0, q_1 eine Nullstelle exisitert. Daher geben wir im folgenden eine Strategie an, mit der Eve in jedem Fall eine eindeutige Lösung ihres Problems erhält.

Es kann also durachaus möglich sein, eine Lösung zu $f(q_0, q_1, p_0, p_0', \mathbf{x}) = 0$ für bestimmte Parameter q_0, q_1 zu finden. Da Alice jedoch Eve's Wahl der Parameter q_0, q_1 bei der Wahl ihrer Parameter für $M_\pm, N_\pm$ nicht kennt, muss die Lösung zu $f(q_0, q_1, p_0, p_0', \mathbf{x}) = 0$ für alle von Eve wählbaren Parameter $q_0, q_1 \in [0,1] \times [0,1]$ gelten. Wir werden zeigen, dass bei geschickter Wahl der Parameter von Eve analog zum Abschnitt 7.3.1 nur dann kein Informationsgewinn von Eve über Alice' Basis auftreten kann, wenn dieses ebenso für Bob gilt.

Hierfür nutzen wir den Identitätssatz der Funktionentheorie. Dazu noch einmal zur Erinnerung [25] (für mehrere Variablen siehe [26]):

Definition 7.3. Eine stetige Funktion $f : \mathbb{C} \longrightarrow \mathbb{C}$ heißt holomorph, falls sie komplex differenzierbar ist. Äquivalent dazu ist, dass sie lokal durch eine konvergente Potenzreihe darstellbar ist.

Eine Funktion $f : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ ist holomorph, falls sie in jeder Unbestimmten holomorph ist.

Insbesondere sind also Polynome stets holomorph, da sie stetig und ihre eigene Potenzreihe sind.

Satz 7.4 (Identitätssatz)**.** *Sei G ein Gebiet, also eine offene, zusammenhängende Menge. Seien $f, g : G \to \mathbb{C}$ holomorphe Funktionen, die auf einer nichtleeren Teilmenge W von G, welche in G einen Häufungspunkt besitzt, übereinstimmen. Dann gilt schon $f = g$ auf ganz G.*

Dieses gilt ebenso für mehrdimensionale holomorphe Funktionen.

Es gilt $f(q_0, q_1, p_0, p_0', \mathbf{x}) = 0$ genau dann, wenn alle Summanden $|p_\psi(\mathrm{M}_+^\mathrm{A} \,|\, \mathrm{M}_+^\mathrm{E}) - p_{\psi'}(\mathrm{N}_+^\mathrm{A} \,|\, \mathrm{M}_+^\mathrm{E})|$, $|p_\psi(\mathrm{M}_+^\mathrm{A} \,|\, \mathrm{N}_+^\mathrm{E}) - p_{\psi'}(\mathrm{N}_+^\mathrm{A} \,|\, \mathrm{N}_+^\mathrm{E})|, \ldots$ Null sind. Wir betrachten ohne Einschränkung den ersten Summanden. Bringt man diesen auf den Hauptnenner, dann gilt für $(q_0, q_1) \neq (0, 0)$, dass genau dann $p_\psi(\mathrm{M}_+^\mathrm{A} \,|\, \mathrm{M}_+^\mathrm{E}) - p_{\psi'}(\mathrm{N}_+^\mathrm{A} \,|\, \mathrm{M}_+^\mathrm{E}) = 0$ ist, wenn der Zähler $\tilde{F}(q_0, q_1, p_0, p_0', \mathbf{x})$ Null ist.

Weiter fassen wir $\tilde{F}$ als Polynom in den Unbestimmten q_0, q_1 auf. Die Parameter p_0, p_0' und $\mathbf{x}$ beschreiben dabei die Koeffizienten. Die genaue Gestalt von $\tilde{F}$ ist unerheblich. Wichtig ist nur, dass für $(q_0, q_1) \neq (0, 0)$ genau dann $f = 0$ gilt, wenn $\tilde{F} = 0$ ist.

Indem wir den Definitionsbereich erweitern, setzen wir dieses Polynom $\tilde{F}$ nun fort zu einem Polynom F auf $\mathbb{C}^2$. Dann ist F für feste $p_0, p_0', \mathbf{x}$ holomorph auf ganz $\mathbb{C}^2$.

Wir bezeichnen die Menge der von Eve bei ihrem Angriff gewählten Parameter q_0, q_1 mit W. Nehmen wir nun an, es existiert für alle von Eve gewählten $(q_0, q_1) \in W$ eine gemeinsame Nullstelle $(p_0, p_0', \mathbf{x})$ von F. Dann gilt $F(q_0, q_1, p_0, p_0', \mathbf{x}) = 0$ auf W. Besitzt W nun einen Häufungspunkt, so ist nach dem Identitätssatz 7.4 $F(q_0, q_1) = 0$ auf ganz $\mathbb{C}^2$.

Damit gilt dies insbesondere für $(q_0, q_1) = (1, 0)$. Nach obigen Überlegungen ist mit F dann auch $p_\psi(\mathrm{M}_+^\mathrm{A} \,|\, \mathrm{M}_+^\mathrm{E}) - p_{\psi'}(\mathrm{N}_+^\mathrm{A} \,|\, \mathrm{M}_+^\mathrm{E}) = 0$ für $(q_0, q_1) = (1, 0)$. Diese Parameter entsprechen aber gerade einer projektiven Messung von $|\uparrow\rangle$. Daher gilt dann auch für Bob $p_\psi(\mathrm{M}_+^\mathrm{A} \,|\, \uparrow) = p_{\psi'}(\mathrm{N}_+^\mathrm{A} \,|\, \uparrow)$ und er kann seine Messergebnisse nicht auswerten.

Eve kann bei unendlich vielen Qubits pro Ensemble beispielsweise nach folgender Strategie messen und somit eine Menge W mit Häufungspunkt erzeugen. Dazu wählt sie bei ihren Messungen den Parameter q_1 fest und variiert den Parameter $q_0 := q_1 + \frac{1}{n}$ nach n. Dann stellt W ein um q_1 verschobenes Intervall dar und besitzt somit einen Häufungspunkt. Mit einem geeigneten Abzählverfahren (n=2,2,3,2,3,4,2,3,4,5,...) kann sie es dabei sogar erreichen, dass sie alle Parameter beliebig oft misst und dadurch die gewünschte Genauigkeit ihrer Ergebnisse erhält. Hierbei geht wesentlich die unendliche Anzahl der Qubits pro Ensemble ein.

Damit ist das Protokoll für diese Angriffsstrategie abhörbar, da wir gezeigt haben, dass Eve ihre Messergebnisse eindeutig nach der von Alice gewählten Basis auflösen kann.

Es konnte bisher kein einfacherer analystischer Beweis für den allgemeinen Anfangszustand gefunden werden, welcher den Umstand des unendlich großen Ensembles nicht nutzt. Daher ist es durchaus möglich, dass das vorgestellte Protokoll für ein endliches Ensemble sicher ist.

7.4 Unendliches → großes System

Bisher haben wir ein System mit unendlich vielen Qubits pro Ensemble betrachtet. Diesen Umstand kann der Lauscher auch konkret in seiner Angriffsstrategie nutzen. Da

ein unendliches System nicht realisierbar ist und in der Realität nur durch ein großes System approximiert wird, muss das endliche System nicht mehr abhörbar sein.

Unendlich viele Messparameter, welche für den oben angegebenen Lauschangriff nötig sind, sind gar nicht realisierbar. Eve kann nun aus diesen unendlich vielen Parametern endlich viele zufällig auswählen und hoffen, dass hierfür eine Lösung (p_0, p_0') exisitert, welche Alice' Basiswahl eindeutig bestimmt. Aber durch den Übergang zum endlichen System kann sie die bedingten Wahrscheinlichkeiten nicht mehr mit beliebiger Genauigkeit bestimmen. Dieses ist anschaulich klar und soll hier in einer ersten Näherung durch das schwache Gesetz der großen Zahl (1.6) erläutert werden. In nächsten Kapitel werden endliche Systeme genauer behandelt.

Wir beginnen mit einer Ensemblegröße N pro Anfangszustand. Da Bob für seine Auswertung 3 Messoperatoren $\sigma_{x,y,z}$ mit gleicher Wahrscheinlichkeit nutzt, hat er pro Messoperator $n = \frac{N}{3}$ Qubits zu messen. Da die bedingten Wahrscheinlichkeiten $p_\psi(\mathrm{M}_+^\mathrm{A} \mid \uparrow), \ldots$ binomialverteilt sind, gilt dann nach Gleichung (1.13) beispielsweise

$$P(|h(\mathrm{M}_+^\mathrm{A} \mid \uparrow, n) - p(\mathrm{M}_+^\mathrm{A} \mid \uparrow)| \geq \varepsilon) \leq \frac{3}{\varepsilon^2 N} p(\mathrm{M}_+^\mathrm{A} \mid \uparrow)(1 - p(\mathrm{M}_+^\mathrm{A} \mid \uparrow)) \tag{7.19}$$

sowie entsprechend für die anderen Wahrscheinlichkeiten. Da die bedingten Wahrscheinlichkeiten im Allgemeinen unbekannt sind, schätzen wir $p(\mathrm{M}_+^\mathrm{A} \mid \uparrow)(1 - p(\mathrm{M}_+^\mathrm{A} \mid \uparrow))$ mit dem Maximum $\frac{1}{4}$ ab. Dann gilt

$$P(|h(\mathrm{M}_+^\mathrm{A} \mid \uparrow, n) - p(\mathrm{M}_+^\mathrm{A} \mid \uparrow)| \geq \varepsilon) \leq \frac{3}{4} \frac{1}{\varepsilon^2 N}. \tag{7.20}$$

Wählt man beispielsweise $\varepsilon = 0.01$ als Messgenauigkeit und $P \leq 1\%$ als erlaubte Irrtumswahrscheinlichkeit, so muss $N \approx 10^5$ sein, um die Bedingung (7.20) zu erfüllen.

Für Eve gilt eine ähnliche Abschätzung. Sie hat pro Paar q_0, q_1 jeweils zwei Messoperatoren. Dadurch ist bei ihr die Anzahl k der Messoperatoren größer als bei Bob. Analog zur Abschätzung von Bob erhält man dann

$$P(|h(\mathrm{M}_+^\mathrm{A} \mid \uparrow, n) - p(\mathrm{M}_+^\mathrm{A} \mid \uparrow)| \geq \varepsilon) \leq \frac{k}{2} \frac{1}{\varepsilon^2 N}. \tag{7.21}$$

Eve kann hiermit bei 10^5 Teilchen mit einer zugelassenen Irrtumswahrscheinlichkeit von 1% auf eine Genauigkeit von $\varepsilon'^2 = k/2 \cdot 10^{-3}$ also $\varepsilon' \approx \sqrt{k} \cdot 0,02$ kommen. Bei 25 Messparametern ist die Genauigkeit dann schon um den Faktor 10 geringer, so dass die Genauigkeit der Ergebnisse von Eve bei vielen verschiedenen Messungen deutlich unter der Genauigkeit der Messungen von Bob liegt.

7.5 Alternative Modifikation

Eve kann, wie wir gesehen haben, aus ihren Messergebnissen auf mögliche Anfangszustände $|\psi\rangle$ oder $|\psi\rangle'$ schließen. Daher liegen bei Bekanntgabe von p_0 keine unbekannten

Größen mehr vor und das Protokoll ist unsicher. Die Möglichkeit, p_0 geheim zu halten, lieferte, wie die vorherigen Abschnitte zeigten, kein sicheres Protokoll. Eine weitere Möglichkeit, das Protokoll mit unendlich großen Ensemblen zu modifizieren, wäre, auf ein Gemisch als Anfangszustand zurückzugreifen.

Wir betrachten ein endliches Ensemble der Gestalt

$$\rho = \sum_{k=1}^{n} \lambda_k \left|\psi_k\right\rangle \left\langle\psi_k\right|$$

mit $\sum_{k=1}^{n} \lambda_k = 1$. Da für Bob die bedingten Wahrscheinlichkeiten der Messergebnisse nach Lemma 6.3 bei gleicher Basiswahl unabhängig sind vom konkreten Anfangszustand, ändert sich dadurch für Bob nichts am Protokoll.

Für Eve gilt dies im Allgemeinen nicht. Für sie ergeben sich alle bedingten Wahrscheinlichkeiten als Konvexkombination der Wahrscheinlichkeiten der einzelnen Zustände im Gemisch. Es gilt also im Allgemeinen für alle j

$$p_\psi(\mathrm{M}_\pm^\mathrm{A} \,|\, \mathrm{M}_\pm^\mathrm{E}) = \sum_{k=1}^{n} \lambda_k p_{\psi_k}(\mathrm{M}_\pm^\mathrm{A} \,|\, \mathrm{M}_\pm^\mathrm{E}) \neq p_{\psi_j}(\mathrm{M}_\pm^\mathrm{A} \,|\, \mathrm{M}_\pm^\mathrm{E}).$$

Die resultierende Dichtematrix ρ_A von Alice hat die Gestalt

$$\rho_M = \frac{1}{2} \begin{pmatrix} 1 + \sum_{k=1}^{n} \lambda_k \cos\vartheta_k & a \sum_{k=1}^{n} \lambda_k (\cos\varphi_k - i \sin\varphi_k) \sin\vartheta_k \\ a \sum_{k=1}^{n} \lambda_k (\cos\varphi_k + i \sin\varphi_k) \sin\vartheta_k & 1 - \sum_{k=1}^{n} \lambda_k \cos\vartheta_k \end{pmatrix}$$

und entsprechend für die $\mathrm{N}_\pm^\mathrm{A}$-Messung.

Hiermit ergeben sich die folgenden unbedingten Wahrscheinlichkeiten von Eve

$$\begin{aligned} p(\mathrm{M}_+^\mathrm{E}) &= q_0 \sum_{k=1}^{n} \lambda_k \rho_{k00} + q_1 \sum_{k=1}^{n} \lambda_k \rho_{k11} \\ &= \frac{1}{2}(q_0 + q_1) + \frac{1}{2}(q_0 - q_1) \sum_{k=1}^{n} \lambda_k \cos\vartheta_k \qquad (7.22) \\ p(\mathrm{N}_+^\mathrm{E}) &= \frac{1}{2}(q_0 + q_1) \sum_{k=1}^{n} \lambda_k (\rho_{k00} + \rho_{k11}) + \frac{1}{2}(q_0 - q_1) \sum_{k=1}^{n} \lambda_k (\rho_{k01} + \rho_{k10}) \\ &= (q_0 + q_1) + \frac{1}{2}(q_0 - q_1) a \sum_{k=1}^{n} \lambda_k \sin\vartheta_k \cos\varphi_k \qquad (7.23) \end{aligned}$$

Eve kann hiermit zwar den Zustand ρ_A bestimmen, da für die Entropie jedoch im Allgemeinen

$$S(\rho) = S(\sum_{k=1}^{n} \lambda_k \rho_k) \neq \sum_{k=1}^{n} \lambda_k S(\rho_k)$$

gilt, kann Eve nun nicht mehr aus der Entropie auf die Anfangszustände $|\psi_k\rangle$ schließen. Da außerdem die Winkel ϑ_k und φ_k nicht mehr den Beziehungen 6.20 genügen müssen und die Größen λ_k unbekannt sind, kann sie nicht mehr auf $\cos\vartheta_i, \ldots$ also einen möglichen Anfangszustand schließen.

Dieses macht die Auswertung für Eve schwieriger. Betrachtet man jedoch noch einmal die bedingten Wahrscheinlichkeiten genauer, zum Beispiel

$$\begin{aligned}
&p_\rho(\mathrm{N}_+^{\mathrm{A}} \,|\, \mathrm{N}_+^{\mathrm{E}}) = \\
&= (q_0 p_0 (1 + \sum_{k=1}^{n} \lambda_k \sin\vartheta'_k \cos\varphi'_k)^2 + q_1 p_1 (1 - \sum_{k=1}^{n} \lambda_k \sin\vartheta'_k \cos\varphi'_k)^2 + \\
&\qquad + 2a\sqrt{q_0 q_1}\sqrt{p_0 p_1}(\sum_{k=1}^{n} \lambda_k \cos^2\vartheta'_k + \sin^2\vartheta'_k \sin^2\varphi'_k))/ \\
&/(q_0 (1 + \sum_{k=1}^{n} \lambda_k \sin\vartheta'_k \cos\varphi'_k)^2 + q_1 (1 - \sum_{k=1}^{n} \lambda_k \sin\vartheta'_k \cos\varphi'_k)^2 + \\
&\qquad + 2a\sqrt{q_0 q_1} \sum_{k=1}^{n} \lambda_k (\cos^2\vartheta'_k + \sin^2\vartheta'_k \sin^2\varphi'_k)),
\end{aligned}$$

so erkennt man, dass Eve viele der einzelnen Summanden mit ihren Ergebnissen (7.22) und (7.23) berechnen kann. Die verbleibenden unbekannten Größen sind alle proportional zu $\sum_{k=1}^{n} \lambda_k \sin\varphi'_k$ oder $\sum_{k=1}^{n} \lambda_k \sin\varphi_k$. Damit sind nun effektiv zwei Größen unbekannt, so dass hier vielleicht eine mehrdeutige Lösung, wie sie im vorherigen Abschnitt gesucht wurde, gefunden werden kann. Dieses ist allerdings bisher nicht gelungen.

Eine weitere Möglichkeit wäre eine Kombination aus beiden Vorschlägen. Alice präpariert also ein Ensemble auf Grundlage eines Gemisches und hält die Parameter p_0 und p_1 geheim. Eve kann dann nicht auf den Parameter a schließen und die Menge der unbekannten Größen erhöht sich auf vier. Hierbei stellt sich allerdings die Frage, ob der untersuchte Lauschangriff dann immer noch sinnvoll ist, oder ob nicht ein anderer effektiverer Angriff möglich ist. Dieses wurde jedoch im Rahmen dieser Arbeit nicht untersucht.

8 Endliche Ensemble

Wir betrachten nun den Fall endlicher Ensembles zur Übermittelung des Schlüsselbits. Die Vorgehensweise im Protokoll bleibt prinzipiell die selbe, lediglich die Auswertung der Messergebnisse wird leicht modifiziert. Wie schon angedeutet, wertet Bob seine Messergebnisse jetzt mit Methoden der Testtheorie aus. Dieses Verfahren wird im ersten Abschnitt 8.1 erläutert. Außerdem zeigen wir in Abschnitt 8.2, wie groß man das Ensemble wählen sollte, um eine vorher festgelegte Fehlerwahrscheinlichkeit p_f nicht zu überschreiten. Daraus resultiert dann eine Abschätzung für die Varianz der Entropie und damit eine Abschätzung für den Fehler, den ein Lauscher verursachen darf. Dieses wird in Abschnitt 8.3 behandelt. Abschließend untersuchen wir das Protokoll bei Verwendung endlicher Ensemble auf dessen Sicherheit gegenüber Lauschangriffen mit unscharfen Messungen.

8.1 Schlüsselermittlung

Wir demonstrieren hier nur den Fall des Unterensembles von Bob mit Messergebnis $\uparrow$. Die entsprechenden Resultate für das $\downarrow$-Unterensemble und die X-Messung folgen analog. Außerdem gehen wir vereinfacht davon aus, dass Alice nur ein Ensemble zur Verschlüsselung nutzt, welches sie durch unscharfe Messung von reinen Anfangszuständen präpariert hat. Die im vorherigen Kapitel vorgeschlagenen Modifikationen werden hier also nicht berücksichtigt.

Wir gehen davon aus, dass das entsprechende Unterensemble aus n Qubits besteht. Da nur zwei Messergebnisse (+/-) auftreten und die einzelnen Ergebnisse unabhängig voneinander sind, ist die zugehörige relative Häufigkeit $h(+|\uparrow, n)$ binomialverteilt um den Erwartungswert $p = p(\mathrm{M}^{\mathrm{A}}_{+} \mid \uparrow)$, falls Alice $\mathrm{M}^{\mathrm{A}}_{\pm}$ gemessen hat, oder um $p' = p(\mathrm{N}^{\mathrm{A}}_{+} \mid \uparrow)$ für die $\mathrm{N}^{\mathrm{A}}_{\pm}$-Messung. Ohne Einschränkung gehen wir davon aus, dass $p > p'$ gilt.

Wir testen das Unterensemble auf die Hypothese $\bar{h}(+|\uparrow, n) = p$, wobei $\bar{h}$ den Mittelwert der zu h gehörenden Wahrscheinlichkeitsverteilung darstellt. Dabei nehmen wir die Hypothese an, wenn $h(+|\uparrow, n)$ im Konfidenzintervall

$$\left[p - \frac{p - p'}{2}, 1\right]$$

liegt. Ist $h(+|\uparrow, n) < p - \frac{p-p'}{2}$, so verwerfen wir die Hypothese und nehmen die Gegenhypothese $\bar{h}(+|\uparrow, n) = p'$ an. Erster Fall erntspricht der Präparation von Alice mit $\mathrm{M}^{\mathrm{A}}_{\pm}$, letzteres der Präparation mit $\mathrm{N}^{\mathrm{A}}_{\pm}$.

Gilt $p' < p$, so betrachten wir das Konfidenzintervall $[0, p + \frac{p-p'}{2}]$ und verfahren analog.

Beispiel 8.1. Wir beginnen mit dem Anfangszustand $|\uparrow_y\rangle$ und den Parametern $p_0 = 0.6$, $p_1 = 0.4$. Dann ergibt sich bei Verwendung der Messergebnisse $\uparrow$ das Konfidenzintervall $I_\uparrow = [0.6 - 0.05, 1] = [0.55, 1]$ und bei Verwendung der Ergebnisse $\downarrow$ das Konfidenzintervall $[0, 0.45]$.

Misst Bob nun eine relative Häufigkeit $h(+|\uparrow, n) = 0.57$, so akzeptiert er die Hypothese $\bar{h}(+|\uparrow, n) = 0.6$ und notiert sich das Schlüsselbit 0. Hat er eine relative Häufigkeit von $h(+|\uparrow, n) = 0.51$, so verwirft er die Hypothese und notiert sich das Schlüsselbit 1.

Für den Fall des modifizierten Protokolls, bei dem Bob die Parameter p_0 und p_1 nicht mehr kennt, testet er eine andere Hypothese. Die Verwendung von zwei Ensemblen liefert Bob zwei relative Häufigkeiten $h_a(+|\uparrow, n_a)$ und $h_b(+|\uparrow, n_b)$ mit zugehörigen Erwartungwerten p_a und p_b. Bob testet nun die Hypothese $p_a - p_b = 0$, er testet also, ab sich die entsprechenden bedingten Wahrscheinlichkeiten beim Wechsel des Ensembles verändert haben (Präparation mit $\mathrm{N}^{\mathrm{A}}_{\pm}$) oder nicht (Präparation mit $\mathrm{M}^{\mathrm{A}}_{\pm}$). Allerdings muss ihm Alice hierfür das Konfidenzintervall vorgeben.

8.2 Bestimmung der kritischen Ensemblegröße

Die Bestimmung der kritischen Ensemblegröße, also der Mindestanzahl an Qubits pro Ensemble, die Alice schicken muss, damit Bob bei seiner Schätzung mit höchstens p_f falsch tippt, erfolgt über das Fehlerquantil des entsprechenden Konfidenzintervalls, vgl. Abschnitt 1.4.1. Der zentrale Grenzwertsatz liefert, dass man bei Wahl des Konfidenzintervalls $[p - u_{1-\alpha/2}\sigma(p), p]$ höchstens einen Fehler von der Konfidenzzahl α macht [17].

Wir betrachten wieder den Fall des Unterensembles aus n Qubits mit Messergebnis $\uparrow$ und testen wieder die Hypothese $\bar{h}(+|\uparrow, n) = p$. Hierzu betrachten wir das Konfidenzintervall $[p - \delta, p]$ mit $\delta = \frac{p-p'}{2}$.

Damit Bob nun einen Fehler 1. Art von höchstens p_f macht, muss gelten

$$\delta \leq u_{1-\frac{p_f}{2}}\sigma(p). \tag{8.1}$$

Setzt man $\delta = \frac{p-p'}{2}$ und die Varianz $\sigma^2(p) = \frac{p(1-p)}{n}$ von p ein, so ergibt sich

$$n_1 \geq u^2_{1-\frac{p_f}{2}} \frac{4p(1-p)}{(p-p')^2}. \tag{8.2}$$

Um die kritische Ensemblegröße n_2 für den Fehler 2. Art zu berechnen, geht man entsprechend für die Alternativhypothese vor. Nehmen wir an, wir fordern ebenfalls

$1 - \beta = \alpha' \leq p_f$, so erhält man dementsprechend

$$n_2 \geq u^2_{1-\frac{p_f}{2}} \frac{4p'(1-p')}{(p-p')^2}. \tag{8.3}$$

Die kritische Größe n_c ist dann das Maximum dieser beiden Größen, also

$$n_c = \max\{n_1, n_2\}.$$

Diese Größe hängt also konkret von Alice' Präparationsparametern ab. Da diese jedoch Alice bekannt sind, kann sie stets im Vorfeld des Protokolls die benötigte Qubitanzahl berechnen.

Die Gesamtzahl N des benötigten Ensembles errechnet sich dann näherungsweise mir $N = 6n_c$, da Bob das Ensemble durch seine Auswertung in sechs Unterensemble einteilt.

Setzen wir $p_f = 1\%$, so ist $u_{0.995} = 2.3265$. Hiermit ergeben sich dann beispielsweise die Werte in Tabelle 8.1.

$\varphi(\|\psi\rangle)$	p_0	p_1	n_1	n_2	N
$\pi/2$	0.4	0.6	519	541	3246
$\pi/4$	0.4	0.6	1430	1480	8880
$3\pi/4$	0.4	0.6	296	307	1842
$\pi/2$	0.5	0.6	2165	2143	12990
$\pi/4$	0.5	0.6	5655	5633	3393
$3\pi/4$	0.5	0.6	1191	1170	7146
$\pi/2$	0.2	0.8	38	60	360
$\pi/4$	0.2	0.8	119	173	1038
$3\pi/4$	0.2	0.8	27	42	252

Tabelle 8.1: Beispiele von kritischen Ensemblegrößen bei verschiedenen Parametern p_0, p_1; $\varphi(|\psi\rangle)$ gibt den Winkel φ von $|\psi\rangle$ in der Blochdarstellung an, die entsprechenden übrigen Winkel ergeben sich dann mit (6.21)

Hieran sieht man, dass die notwendige Ensemblegröße stark von den gewählten Parametern abhängt. Alice sollte aber in jedem Fall ein Ensemble von der Größenordnung $10^3 - 10^4$ verwenden.

Um einen ersten Eindruck für die Sicherheit des Protokolls bei Verwendung endlicher Ensemble zu bekommen, führe wir die gleichen Berechnungen für Eve durch. Sie sortiert das abgehöhrte Ensemble in Unterensemble mit Messergebnis $+^E$ und Messergebnis $-^E$ anstelle von $\uparrow$ und $\downarrow$ und vergleicht dann entsprechend ihre relativen

Häufigkeiten $h(+^A|+^E, n)$ mit $p(\mathrm{M}_+^{\mathrm{A}} \,|\, \mathrm{M}_+^{\mathrm{E}})$. Setzt man die entsprechenden Wahrscheinlichkeiten (7.8)für p und (7.11) für p' in obige Gleichung (8.2) ein, ergeben sich für $q_0 = p_0$ und $q_1 = p_1$ die folgenden Werte in Tabelle 8.2 für die kritische Ensemblegröße n_c^E. Desweiteren ist der mittlere Fehler p_E angegeben, mit dem Eve bei ihrer Testmethode falsch liegt, wenn man die kritische Ensemblegröße $_c$ verwendet. Diesen erhält man ebenfalls aus Gleichung (8.2), indem man diese nach $u_{1-\frac{p_f}{2}}$ auflöst und mit den tabellierten Werte von $u_{1-\frac{p_f}{2}}$ vergleicht.

$\varphi(\psi)$	p_0	p_1	n_c	n_c^E	$u_{1-\frac{p_f}{2}}$	p_E
$\pi/2$	0.4	0.6	541	51977	0.23	0.59
$\pi/4$	0.4	0.6	1480	50935	0.34	0.63
$\pi/2$	0.5	0.6	2165	$1.02 \cdot 10^6$	0.10	0.54
$\pi/4$	0.5	0.6	5655	$1.03 \cdot 10^6$	0.17	0.56
$\pi/2$	0.2	0.8	38	446	0.67	0.74
$\pi/4$	0.2	0.8	119	358	0.51	0.69

Tabelle 8.2: Kritische Ensemblegröße n_c^E und mittlerer Fehler bei Verwendung der kritischen Ensemblegröße n_c

Man erkennt, dass Eve im Vergleich zu Bob eine deutlich höhere Enesemblegröße benötigt, um auf den gleichen Fehler zu kommen. Bei Verwendung der kritischen Ensemblegröße n_c macht Eve einen Fehler von über 50%. Somit liefert ihre Auswertung kein sinnvolles Ergebnis.

8.3 Varianz der Entropie

Die Varianz der Entropie berechnet sich mit dem Fortpflanzungsgestz aus den Varianzen von Bobs Messergebnissen der tomographischen Messung. Ist $f(x, y)$ eine Funktion in Abhängigkeit von x und y, wobei x und y eine Varianz von $\sigma^2(x)$ bzw. $\sigma^2(y)$ besitzen, so ist die Varianz von f gegeben durch

$$\sigma^2(f) = \left(\frac{\partial f}{\partial x}\right)^2 \sigma^2(x) + \left(\frac{\partial f}{\partial y}\right)^2 \sigma^2(y) \tag{8.4}$$

In unserem Fall erfolgt die Berechnung in mehreren Schritten. Bob misst das erhaltene endliche Ensemble der Größe $3n$ gleichverteilt mit X, Y und Z. Er hat also pro Projektionsmessung n Qubits gemessen. Die Erwartungswerte der einzelnen Messungen sind

$$\begin{aligned} \mathrm{tr}[\rho X] &= a \sin\vartheta \cos\varphi \\ \mathrm{tr}[\rho Y] &= a \sin\vartheta \sin\varphi \\ \mathrm{tr}[\rho Z] &= \cos\vartheta \end{aligned}$$

Da die Messergebnisse der Projektionsmessungen binomialverteilt sind, ergeben sich jeweils die folgenden Varianzen:

$$\begin{aligned}
\sigma^2(\mathrm{tr}[\rho X]) &= \sigma^2(\mathrm{tr}[\rho\,|\uparrow_x\rangle\,\langle\uparrow_x|]) = \frac{(1+a\sin\vartheta\cos\varphi)(1-a\sin\vartheta\cos\varphi)}{n} \\
\sigma^2(\mathrm{tr}[\rho Y]) &= \sigma^2(\mathrm{tr}[\rho\,|\uparrow_y\rangle\,\langle\uparrow_y|]) = \frac{(1+a\sin\vartheta\sin\varphi)(1-a\sin\vartheta\sin\varphi)}{n} \\
\sigma^2(\mathrm{tr}[\rho Z]) &= \sigma^2(\mathrm{tr}[\rho\,|\uparrow\rangle\,\langle\uparrow|]) = \frac{(1+\cos\vartheta)(1-\cos\vartheta)}{n}.
\end{aligned} \tag{8.5}$$

Die Dichtematrix ρ_B errechnet sich nach Gleichung (1.9) zu

$$\rho_B = \frac{1}{2}\begin{pmatrix} \mathrm{tr}[\rho]+\mathrm{tr}[\rho Z] & \mathrm{tr}[\rho X]-i\,\mathrm{tr}[\rho Y] \\ \mathrm{tr}[\rho X]+i\,\mathrm{tr}[\rho Y] & \mathrm{tr}[\rho]-\mathrm{tr}[\rho Z] \end{pmatrix}.$$

Die Entropie $S(\rho_B)$ ergibt sich dann über die Eigenwerte

$$\lambda_\pm = \frac{1}{2} \pm \frac{1}{2}\sqrt{\mathrm{tr}[\rho X]^2+\mathrm{tr}[\rho Y]^2+\mathrm{tr}[\rho Z]^2} \tag{8.6}$$

zu

$$S(\rho_B) = -\lambda_+\log\lambda_+ - \lambda_-\log\lambda_-.$$

Die Varianz von $\lambda_\pm$ ist

$$\sigma^2(\lambda_\pm) = \frac{\mathrm{tr}[\rho X]^2\sigma^2(\mathrm{tr}[\rho X]) + \mathrm{tr}[\rho Y]^2\sigma^2(\mathrm{tr}[\rho Y]) + \mathrm{tr}[\rho Z]^2\sigma^2(\mathrm{tr}[\rho Z])}{\mathrm{tr}[\rho X]^2+\mathrm{tr}[\rho Y]^2+\mathrm{tr}[\rho Z]^2}. \tag{8.7}$$

Damit folgt dann für die Varianz der Entropie

$$\begin{aligned}
\sigma^2(S(\rho_B)) &= \sigma^2(\lambda_+\log\lambda_+) + \sigma^2(\lambda_-\log\lambda_-) \\
&= (1+\log\lambda_+)^2\sigma^2(\lambda_+) + (1+\log\lambda_-)^2\sigma^2(\lambda_-) \\
&= [(1+\log(\frac{1}{2}+\frac{1}{2}\sqrt{\mathrm{tr}[\rho X]^2+\mathrm{tr}[\rho Y]^2+\mathrm{tr}[\rho Z]^2}))^2 + \\
&\quad + (1+\log(\frac{1}{2}-\frac{1}{2}\sqrt{\mathrm{tr}[\rho X]^2+\mathrm{tr}[\rho Y]^2+\mathrm{tr}[\rho Z]^2}))^2]\cdot \\
&\quad \cdot \frac{\mathrm{tr}[\rho X]^2\sigma^2(\mathrm{tr}[\rho X]) + \mathrm{tr}[\rho Y]^2\sigma^2(\mathrm{tr}[\rho Y]) + \mathrm{tr}[\rho Z]^2\sigma^2(\mathrm{tr}[\rho Z])}{\mathrm{tr}[\rho X]^2+\mathrm{tr}[\rho Y]^2+\mathrm{tr}[\rho Z]^2}.
\end{aligned} \tag{8.8}$$

Für die in Tabelle 8.1 im vorherigen Kapitel verwendeten Parameter ergeben sich damit beispielsweise die folgenden Werte in Tabelle 8.3. Dabei nehmen wir an, dass jeweils $2n_c$ Qubits pro Projektionsoperator gemesen wurden.

Hieran sieht man, dass sich die Varianz der Entropie bei der Verwendung der kritischen Ensemblegröße nur wenig ändert. Sieht man von dem Fall kleiner Ensemblegrößen ab ($2n_c < 1000$), so liegt die Varianz in der Größenordnung von $0.01 - 0.1$.

Diese Varianz addiert sich bei der Ermittlung der Schranke für die erlaubte Entropieänderung zur Entropieänderung durch den Kanal.

$\varphi(\|\psi\rangle)$	p_0	p_1	$2n_c$	$\sigma(S(\rho_B))$
$\pi/2$	0.4	0.6	1082	0.035
$\pi/4$	0.4	0.6	2960	0.088
$3\pi/4$	0.4	0.6	614	0.193
$\pi/2$	0.5	0.6	4330	0.011
$\pi/4$	0.5	0.6	11310	0.059
$3\pi/4$	0.5	0.6	2382	0.122
$\pi/2$	0.2	0.8	120	0.169
$\pi/4$	0.2	0.8	346	0.141
$3\pi/4$	0.2	0.8	82	0.292

Tabelle 8.3: Beispiele zur Berechnung von $\sigma(S(\rho_B))$ bei Verwendung der kritischen Ensemblegrößen aus Tabelle 8.1

8.4 Sicherheit des Protokolls

Wir haben in Abschnitt 8.2 gesehen, dass Eve bei analoger Auswertung zu Bob einen großen Fehler in Kauf nehmen muss. Dadurch kann sie ihren Resultaten nicht vertrauen und erhält somit nur wenig Information über den Schlüssel. Dieses wird nun noch einmal informationstheoretisch über die wechselseitige Information nachgewiesen.

Wir berechnen die wechselseitge Information $H(A:B)$ von Alice und Bob und $H(A:E)$ von Alice und Eve, welche durch die Korrelationen der Messergebnisse gegeben ist. Dabei setzen wir voraus, dass Bob projektiv in der Z-Basis und Eve unscharf mit $\mathrm{M}^{\mathrm{E}}_{\pm}$ misst.

Für $H(A:B) > H(A:E)$ folgt aus Satz 1.12, dass man mit diesem Protokoll unter Verwendung der in Abschnitt 2.1.1 und 2.1.2 erläuterten Methoden der Fehlerkorrektur und Verschwiegenheitsverstärkung einen sicheren Schlüssel erzeugen kann.

Dazu benötigen wir die Darstellung in der Formulierung der entsprechenden Zufallsvariablen. Die Zufallsvariable von Alice ist gegeben durch die Menge $\{M, N\}$, jeweils mit Wahrscheinlichkeit 1/2. Diese besitzt eine Entropie von 1.

Zur Berechnung der wechselseitigen Information von Bob betrachten wir der Einfachheit halber wieder nur das Unterensemble der Qubits mit Messergebnis $\uparrow$. Dieses Unterensemble bestehe aus $n_\uparrow$ Qubits. Das Ensemble der in der z-Basis gemessenen Qubits habe die Größe n. Die Zufallsvariable von Bob ist dann gegeben durch die Menge $\{n_+ | 0 \leq n_+ \leq n_\uparrow\}$, also der Anzahl der Qubits mit Messresultat "+ und $\uparrow$". Um die wechselseitige Information zu berechnen, benötigen wir die Größen $p(M, n_+), p(N, n_+)$ und $p(n_+)$, denn es gilt

$$\begin{aligned} H(A:B) &= H(A) - H(A|B) \\ &= 1 + \sum_{n_+} [p(M, n_+) \log p(M|n_+) + p(N, n_+) \log p(N|n_+)] \end{aligned}$$

$$= 1 + \sum_{n_+} [p(M, n_+) \log \frac{p(M, n_+)}{p(n_+)} + p(N, n_+) \log \frac{p(N, n_+)}{p(n_+)}]. \tag{8.9}$$

Dazu berechnen wir zunächst $p(n_+|n_\uparrow, M)$ und $p(n_\uparrow|M)$ für festes $n_\uparrow$. Hierfür gilt (siehe Anhang)

$$\begin{aligned} p(n_+|n_\uparrow, M) &= \binom{n_\uparrow}{n_+} p(\mathrm{M}_+^{\mathrm{A}\,n_+}\, \mathrm{M}_-^{\mathrm{A}\,n_\uparrow - n_+} |n_\uparrow) \\ &= \binom{n_\uparrow}{n_+} \frac{p_{M+\uparrow}^{n_+} (\rho_{M00} - p_{M+\uparrow})^{n_\uparrow - n_+}}{\rho_{M00}^{n_\uparrow}} \end{aligned} \tag{8.10}$$

mit

$$p_{M\pm\uparrow} = \langle\uparrow|\, \mathrm{M}_\pm^{\mathrm{A}} |\psi\rangle \langle\psi|\, \mathrm{M}_\pm^{\mathrm{A}^\dagger} |\uparrow\rangle .$$

Für $p(n_\uparrow|M)$ ergibt sich

$$p(n_\uparrow|M) = \binom{n}{n_\uparrow} \rho_{M00}^{n_\uparrow} \rho_{M11}^{n-n_\uparrow}. \tag{8.11}$$

Durch Summation über $n_\uparrow$ mit der entsprechenden Wahrscheinlichkeit $p(n_\uparrow|M)$ erhalten wir

$$\begin{aligned} p(n_+|M) &= \sum_{n_\uparrow} p(n_+|n_\uparrow, M) p(n_\uparrow|M) \\ &= \sum_{n_\uparrow} \binom{n_\uparrow}{n_+} \frac{p_{M+\uparrow}^{n_+} p_{M-\uparrow}^{n_\uparrow - n_+}}{\rho_{M00}^{n_\uparrow}} \binom{n}{n_\uparrow} \rho_{M00}^{n_\uparrow} \rho_{M11}^{n-n_\uparrow} \\ &= \sum_{n_\uparrow} \binom{n}{n_\uparrow} \binom{n_\uparrow}{n_+} p_{M+\uparrow}^{n_+} p_{M-\uparrow}^{n_\uparrow - n_+} \rho_{M11}^{n-n_\uparrow}. \end{aligned} \tag{8.12}$$

Hieraus erhält man dann

$$p(n_+, M) = p(n_+|M) p(M) = \frac{1}{2} \sum_{n_\uparrow} \binom{n}{n_\uparrow} \binom{n_\uparrow}{n_+} p_{M+\uparrow}^{n_+} p_{M-\uparrow}^{n_\uparrow - n_+} \rho_{M11}^{n-n_\uparrow}. \tag{8.13}$$

Für $p(n_+, N)$ ergibt sich entsprechend

$$p(n_+, N) = \frac{1}{2} \sum_{n_\uparrow} \binom{n}{n_\uparrow} \binom{n_\uparrow}{n_+} p_{N+\uparrow}^{n_+} p_{N-\uparrow}^{n_\uparrow - n_+} \rho_{N11}^{n-n_\uparrow}. \tag{8.14}$$

mit

$$p_{N\pm\uparrow} = \langle\uparrow|\, \mathrm{N}_\pm^{\mathrm{A}} |\psi\rangle \langle\psi|\, \mathrm{N}_\pm^{\mathrm{A}^\dagger} |\uparrow\rangle .$$

Verwendet man noch $p(n_+) = p(n_+, M) + p(n_+, N)$, so hat man alle erforderlichen Größen zur Berechnung vorliegen. Zusammengefasst ergibt sich also für die wechselseitige Information $H(A : B)$

$$\begin{aligned} H(A:B) &= 1 + \sum_{n_+} [p(n_+, M) \log \frac{p(n_+, M)}{p(n_+)} + p(n_+, N) \log \frac{p(n_+, N)}{p(n_+)}] \\ &= 1 + \sum_{n_+} [p(n_+, M) \log p(n_+, M) + p(n_+, N) \log p(n_+, N) - \\ &\qquad - (p(n_+, M) + p(n_+, N)) \log(p(n_+, M) + p(n_+, N)] \end{aligned}$$

mit obigen Werten aus Gleichung (8.13) und (8.14).

Beispielhaft ergeben sich hiermit die Werte der folgenden Tabelle 8.4. Dabei wurden Ensemble der Größe $n = 100$, $n = 200$ und $n = 500$ betrachtet. Eine Berechnung für höhere Ensemblegrößen war aus rechentechnischen Gründen leider nicht möglich.

$\varphi(\psi)$	p_0	p_1	$H(A:B)_{100}$	$H(A:B)_{200}$	$H(A:B)_{500}$
$\pi/2$	0.6	0.4	0.197	0.348	0.639
$\pi/4$	0.6	0.4	0.162	0.294	0.565
$\pi/2$	0.6	0.5	0.059	0.115	0.233
$\pi/4$	0.6	0.5	0.046	0.091	0.195
$\pi/2$	0.2	0.8	0.805	0.975	$1 - 1.2 \cdot 10^{-5}$
$\pi/4$	0.2	0.8	0.764	0.937	$1 - 9.2 \cdot 10^{-5}$
$\pi/2$	0.4	0.4	0	0	0
$\pi/4$	0.4	0.4	0	0	0

Tabelle 8.4: Beispiele zur Berechnung der wechselseitigen Information $H(A : B)$ unter Verwendung von $n = 100$, $n = 200$ und $n = 500$

Hieran sieht man, dass die wechselseitige Information von den gewählten Parametern p_0, p_1 und von der Ensemblegröße n abhängt. Weiter ist zu erkennen, dass die wechselseitige Information monoton wächst und für große Ensemble gegen 1 geht. Damit haben wir informationstheoretisch gezeigt, dass man mit dem vorgeschlagenen Protokoll bei Wahl geeigneter Parameter die gewünschte Information 0 oder 1 übermitteln kann. Die Effektivität des Protokolls ist dabei von der Wahl der verwendeten Ensemblegrößen abhängig.

Wir betrachten den Fall $p_0 = p_1$ noch einmal gesondert. Dann gilt $p(n_+, M) = p(n_+, N)$, da schon $p_{M\pm\uparrow} = p_{N\pm\uparrow}$ gilt. Damit folgt dann $p(n_+) = 2p(n_+, M)$ und für die wechselseitige Information gilt

$$H(A:B) = 1 + \sum_{n_+} [p(n_+, M) \log p(n_+, M) + p(n_+, N) \log p(n_+, N) - p(n_+) \log(p(n_+)]$$

$$
\begin{aligned}
&= 1 + \sum_{n_+} [2p(n_+, M) \log(p(n_+, M)) - 2p(n_+, M) \log(2p(n_+, M))] \\
&= 1 + \sum_{n_+} p(n_+) [\log(p(n_+, M)) - \log(p(n_+, M)) - \log 2] \\
&= 1 - \sum_{n_+} [p(n_+) \log 2] = 1 - \sum_{n_+} p(n_+) = 0
\end{aligned} \tag{8.15}
$$

Somit haben wir noch einmal bestätigt, dass Bob für $p_0 = p_1$ keine Information über das Ensemble erhält. Das präparierte Ensemble erscheint wie ein totales Gemisch.

Wir betrachten nun die Zufallsvariable von Eve. Da Eve ihre Messergebnisse aus ihren unscharfen Messungen analog zu Bob auswertet, ergibt sich für Eve die gleiche Zufallsvariable. Wir betrachten also wieder $\{n_+ | 0 \leq n_+ \leq n_{+^E}\}$, dieses Mal jedoch für das Unterensemble mit Messergebnis $+^E$ von Eve. Die Berechnungen von oben können somit übernommen werden, es ändern sich lediglich die Wahrscheinlichkeiten $p_{M\pm\uparrow}, p_{N\pm\uparrow}, \ldots$. Es gilt also ebenfalls

$$
H(A:E) = 1 + \sum_{n_+} [p(n_+, M) \log p(n_+, M) + p(n_+, N) \log p(n_+, N) - p(n_+) \log(p(n_+))]
$$

mit den entsprechenden obigen Größen (8.13) und (8.14). Dabei sind die Wahrscheinlichkeiten $p_{M\pm\uparrow}$ und $p_{M\pm\downarrow}$ zu ersetzen durch

$$
\begin{aligned}
p_{M+,+} &= \langle\psi| \, \mathrm{M}_+^{\mathrm{A}\dagger} \, \mathrm{M}_+^{\mathrm{E}} \, \rho_M \, \mathrm{M}_+^{\mathrm{E}\dagger} \, \mathrm{M}_+^{\mathrm{A}} \, |\psi\rangle \\
&= \frac{1}{4}(p_0 q_0 (1 + \cos\vartheta)^2 + p_1 q_1 (1 - \cos\vartheta)^2 + 2a\sqrt{p_0 p_1}\sqrt{q_0 q_1} \sin^2\vartheta) \\
p_{M+,-} &= \frac{1}{4}(p_0 (1 - q_0)(1 + \cos\vartheta)^2 + p_1 (1 - q_1)(1 - \cos\vartheta)^2 + \\
&\qquad + 2a\sqrt{p_0 p_1}\sqrt{(1 - q_0)(1 - q_1)} \sin^2\vartheta) \\
p_{M-,+} &= \frac{1}{4}((1 - p_0) q_0 (1 + \cos\vartheta)^2 + (1 - p_1) q_1 (1 - \cos\vartheta)^2 + \\
&\qquad + 2a\sqrt{(1 - p_0)(1 - p_1)}\sqrt{q_0 q_1} \sin^2\vartheta) \\
p_{M-,-} &= \frac{1}{4}((1 - p_0)(1 - q_0)(1 + \cos\vartheta)^2 + (1 - p_1)(1 - q_1)(1 - \cos\vartheta)^2 + \\
&\qquad + 2a\sqrt{(1 - p_0)(1 - p_1)}\sqrt{(1 - q_0)(1 - q_1)} \sin^2\vartheta)
\end{aligned}
$$

Für $p_{N\pm\uparrow}$ und $p_{N\pm\downarrow}$ gilt entsprechendes, ausgehend von

$$
\begin{aligned}
p_{N+,+} = \frac{1}{8}[&q_0 (1 + \cos\vartheta)(p_0 + p_1 + (p_0 - p_1) a \sin\vartheta \cos\varphi + 2\sqrt{p_0 p_1}\frac{1}{a}\cos\vartheta) + \\
&+ q_1 (1 - \cos\vartheta)(p_0 + p_1 + (p_0 - p_1) a \sin\vartheta \cos\varphi - 2\sqrt{p_0 p_1}\frac{1}{a}\cos\vartheta) + \\
&+ 2a\sqrt{q_0 q_1}((p_0 - p_1)\sin\vartheta\cos\varphi + (p_0 + p_1) a \sin^2\vartheta \cos^2\varphi + 2\sqrt{p_0 p_1}\sin^2\vartheta \sin^2\varphi)]
\end{aligned}
$$

Hiermit ergeben sich dann beispielsweise die Werte der Tabelle 8.5. Dabei legen wir wieder $n = 100$ und $n = 200$ für die Berechnung zugrunde, um diese Werte mit den Ergebnissen von Bob vergleichen zu können. Dabei wählen wir $q_0 = p_0$ und $q_1 = p_1$. Für $n = 100$ geben wir zusätzlich die optimierte wechselseitige Information unter der Bedingung, dass eine Entropieänderung von maximal 0.1 auftritt, an. Die optimierten Parameter q_0, q_1 liegen dann im Bereich $q_0 \approx 0.21$ und $q_1 \approx 0.004$.

$\varphi(\psi)$	p_0	p_1	$H(A:E)_{100}$	$H(A:E)_{opt}$	$H(A:E)_{200}$
$\pi/2$	0.6	0.4	0.003	0.027	0.005
$\pi/4$	0.6	0.4	0.002	0.027	0.005
$\pi/2$	0.6	0.5	0.001	0.008	0.001
$\pi/4$	0.6	0.5	0.001	0.008	0.001
$\pi/2$	0.2	0.8	0.192	0.305	0.330
$\pi/4$	0.2	0.8	0.184	0.233	0.328

Tabelle 8.5: Beispiele zur Berechnung der wechselseitigen Information $H(A:E)$

Auch hier gilt analog zu (8.15), dass für $p_0 = p_1$ stets $H(A:E) = 0$ gilt.

Vergleichen wir nun die Werte der wechselseitigen Information von Alice und Bob mit der von Alice und Eve, so sieht man, dass selbst die optimierte Messung von Eve einen deutlich kleineren Wert liefert. Die Differenzen $\Delta H = H(A:B) - H(A:E)$ und die relative Abweichung von Eve $r = \Delta H / H(A:B)$ in Prozent sind in Tabelle 8.6 augeführt.

$\varphi(\psi)$	p_0	p_1	ΔH_{100}	r_{100}	ΔH_{opt}	r_{opt}	ΔH_{200}	r_{200}
$\pi/2$	0.6	0.4	0.197	99	0.170	86	0.343	98
$\pi/4$	0.6	0.4	0.159	98	0.135	83	0.289	98
$\pi/2$	0.6	0.5	0.058	98	0.051	86	0.114	98
$\pi/4$	0.6	0.5	0.045	97	0.038	82	0.090	98
$\pi/2$	0.2	0.8	0.613	76	0.503	62	0.635	65
$\pi/4$	0.2	0.8	0.579	75	0.531	70	0.608	64

Tabelle 8.6: Differenzen der wechselseitigen Information von $H(A:B)$ und $H(A:E)$ sowie die relativen Abweichungen bezogen auf die wechselseitige Information $H(A:B)$

Man erkennt, dass die relativen Abweichungen sehr groß sind. Auch im optimierten Fall liegt sie deutlich über 50%. Eve weiß also weniger als die Hälfte über den Schlüssel im Vergelich zu Bobs. Für größere Ensemble wird die relative Abweichung kleiner, wie ansatzweise am letzten Beispiel mit den Parametern $p_0 = 0.2, p_1 = 0.8$ zu erkennen ist.

Die Abweichung nimmt monoton ab, da Eve immer mehr Qubits pro Ensemble messen kann. Hierdurch nimmt ihre Streuung der Messergebnisse ab und ab einer bestimmten Ensemblegröße erhält Eve die gleiche Informationsmenge wie Bob.

Im Grenzfall unendlicher Ensemblegröße stimmt die wechselseitige Information von Bob mit der von Eve überein. Allerdings bleibt die Frage offen, ob dieser Fall auch schon bei einer endlichen Ensemblegröße auftritt. Dieses wäre dann eine kritische Größe, welche man nicht überschreiten sollte.

Durch numerische Optimierung, welche im Rahmen dieser Arbeit nicht durchgeführt wurde, lassen sich die Parameter so optimieren, dass einerseits die wechselseitige Information für Bob möglichst groß ist, so dass man auf aufwendige Fehlerkorrekturverfahren verzichten kann, und andererseits die wechselseitige Information für Eve besonders klein ist. Dann erfährt sie nur wenig über den Schlüssel und die Verluste an Schlüsselbits durch Verschwiegenheitsverstärkung können minimiert werden.

Dieses Protokoll ist also bei Verwendung endlicher Ensemble (von passender Größe) sicher gegenüber dem untersuchten Lauschangriff durch unscharfe Messungen.

Betrachtet man die vorgeschlagenen Modifikationen des Protkolls, so kann sich die Sicherheit nur erhöhen, da sich die wechselseitige Information von Bob nach Lemma 6.3 nicht ändert, wenn Alice den Anfangszustand nicht bekannt gibt. Werden die Parameter p_0 und p_1 nicht bekannt gegeben, so muss man die Zufallsvariable von Bob abändern in $\{\Delta n_+ : -n_\uparrow \leq \Delta n_+ \leq n_\uparrow\}$ mit $\Delta n_+ = n_{+,1} - n_{+,2}$, wobei $n_{+,k}$ die Anzahl an Qubits mit Messresultat "+ und ↑" des k-ten Ensembles angibt. Die entsprechenden Rechnungen ergeben sich dann analog. Allerding berücksichtigt die Berechnung der wechselseitigen Information nicht das Unwissen von Eve. Dadurch kann Eve nicht die gesamte für den betrachteten Angriff mögliche wechselseitige Information erhalten. Sie besitzt weniger Information, da sie den Anfangszustand $|\psi\rangle$ mit ihren Messergebnisen nur noch schätzen kann. Dadurch erhöht sich die Varianz der einzelnen Wahrscheinlichkeiten und das Wissen nimmt ab. Sind p_0 und p_1 geheim, so kann Eve kein Konfidenzintervall mehr angeben, sie benötigt also eine neue Angriffsstrategie.

9 Abschließende Bemerkungen

9.1 Bedingungslose Sicherheit

Die Sicherheitsuntersuchungen des Protkolls sind hiermit noch nicht abgeschlossen. Im Rahmen dieser Arbeit wurden jedoch erste Ergebnisse erziehlt.

Es konnte gezeigt werden, dass das Protokoll unter den idealisierten Voraussetzungen unendlich großer Ensemble und Verwendung eines fehlerfreien Quantenkanals uneingeschränkt sicher ist. Der Verzicht auf den fehlerfreien Quantenkanal unter Beibehaltung unendlich großer Ensemble liefert bei Verwendung reiner Zustände als Anfangszustände kein sicheres Protokoll wie in Kapitel 7 dargelegt wurde. Allerdings ist der Fall eines Gemisches als Anfangszustand momentan noch ungeklärt.

Betrachtet man stattdessen endliche Ensemble, so ist das Protokoll zumindest gegenüber Lauschangriffen mit unscharfen Messungen sicher. Allerdings muss man in Kauf nehmen, dass man durch Verschwiegenheitsverstärkung einen Teil des Schlüssel wieder verliert. Dieses wurde in Kapitel 8 gezeigt. Hierbei wurde ebenfalls mit reinen Zuständen begonnen.

Somit bleibt die Frage der bedingungslosen Sicherheit des Protokolls offen. Der Fall des Gemisches als Anfangszustand sowie die Betrachtung der Modifikation in Abschnitt 7.2, bei der die Parameter p_0 und p_1 geheim bleiben, müssen noch genauer untersucht werden. Diese Varianten lassen ein effektiveres Protokoll vermuten, da der untersuchte Lauschangriff hierbei unwirksam ist.

Es ist unklar, wie man die bedingungslose Sicherheit des Protokolls zeigt. Ein naheliegender Ansatz ist, die Sicherheit analog zum BB84-Protokoll zu beweisen. Dazu müsste man ein auf verschränkten Zuständen basierendes Protokoll konstruieren, dass einerseits sicher ist und andererseits nach geeigneter Transformation genau auf das vorgeschlagene Protokoll führt. Dabei gibt es allerdings Schwierigkeiten.

Die Konstruktion der Schlüsselübermittlung mit verschränkten Zuständen stellt kein Problem dar. Man kann ebenso wie im BB8-Protokoll mit Bell-Zuständen $|\phi\rangle^+$ beginnen. Misst Alice ihre Hälfte der Bell-Zustände mit einer unscharfen Messung und Bob seine Hälfte anschließend projektiv, so ergeben sich genau die gleichen Messergebnisse und damit genau der gleiche Schlüssel wie beim eigentlichen Verfahren.

Allerdings wurde im Rahmen dieser Arbeit kein Weg gefunden, den Sicherheitsbeweis zu übertragen. Das Problem dabei besteht darin, dass für Gemische keine Relation zwischen der Verschränkung und der Entropie der reduzierten Dichtematrizen rh_A und ρ_B gefunden wurde.

Ein anderer Ansatz ist der Satz 1.12 von Csiszár und Körner, welcher im vorherigen

Kapitel verwendet wurde. Dadurch wurde gezeigt, dass man mit Projektionsmessungen mehr Informationen über den Schlüssel erhält als mit unscharfen Messungen. Allerdings berücksichtigt die wechselseitige Information nur die Korrelationen der Messergebnisse.

Eine Möglichkeit, wie man bei der Berechnung der wechselseitigen Information fehlendes oder fehlerbehaftetes Wissen berücksichtigen kann, ist die Untersuchung allgemeiner Angriffe. Allerdings treten auch hierbei Schwierigkeiten auf. Im Gegensatz zu den herkömmlichen Protokollen nutzt das untersuchte Protokoll keine einzelnen Qubits zur Schlüsselübertragung sondern Ensemble. Dadurch besitzt Eve die Möglichkeit, sehr viele Hilfssysteme (schwach) an das Ensemble zu koppeln. Ein optimiertes POVM liefert dann das Maximum der erreichberen wechselseitigen Information . Aufgrund der großen Anzahl an Hilfssystemen ist es jedoch sehr schwierig eine solche optimierte Messung zu finden.

Möchte man die vorgeschlagenen Modifikationen untersuchen, so steht man vor dem Problem, dass die präparierte Dichtematrix, welche die Zustände, die über den Quantenkanal übertragen werden, beschreibt, für den Lauscher unbekannt ist. Bei bisherigen Sicherheitsuntersuchungen war diese dem Lauscher stets als bekannt vorausgesetzt. Es müssen also neue Methoden gefunden werden, um die bedingungslose Sicherheit des Protokolls zu zeigen.

9.2 Ausblick

Die in dieser Arbeit vorgestellten Resultate zeigen die Sicherheit des Protokolls gegenüber bestimmten Angriffen. Sollte die bedingungslose Sicherheit gezeigt werden können, öffnet sich eine Reihe weiterer Fragen. Ein bedingunglos sicheres Protokoll ist nur dann sinnvoll, wenn es sich auch experimentell realisieren lässt. Dadurch stellt sich die Frage nach der Realisierbarkeit des Protokolls. Daran anknüpfend muss man zunächst untersuchen, ob das Protokoll auch bei inperfekten Photonenquellen sicher ist. Man sollte also beispielsweise die in Kapitel 3 vorgestellte PNS-Attacke näher untersuchen. Allerdings benötigt man, wie in Abschnitt 8.2 gezeigt wurde, eine sehr große Anzahl an Photonen, um sicher auf den Schlüssel schließen zu können. Dadurch ist es dann eventuell – wie ursprünglich beim SARG-Protokoll – möglich, dass die maximale Reichweite, bei der das Protokoll noch sicher ist, über der maximalen Reichweite momentan bestehender Protokolle liegt. Dieses wäre dann ein wesentlicher Vorteil des untersuchten Protokolls, welcher den Umstand, dass man vergleichsweise viele Qubits zur Schlüsselerzeugung benötigt, ausgleicht.

A Berechnungen

Für die Berechnungen verwenden wir folgende Abkürzungen:

$$\gamma_+ = \sqrt{p_0} + \sqrt{p_1}$$

$$\gamma_- = \sqrt{p_0} - \sqrt{p_1}$$

$$\sqrt{p_-} = \sqrt{(1-p_0)(1-p_1)}$$

sowie entsprechend für Eve

$$\chi_+ = \sqrt{q_0} + \sqrt{q_1}$$

$$\chi_- = \sqrt{q_0} - \sqrt{q_1}$$

$$\sqrt{q_-} = \sqrt{(1-q_0)(1-q_1)}.$$

A.1 Berechnung von ρ_M

$$\rho_M = \frac{1}{2}(\mathrm{M}_+^{\mathrm{A}}\,\rho_A\,\mathrm{M}_+^{\mathrm{A}\dagger} + \mathrm{M}_-^{\mathrm{A}}\,\rho_A\,\mathrm{M}_-^{\mathrm{A}\dagger}) = \frac{1}{2}\begin{pmatrix} 1+\cos\vartheta & ae^{-i\varphi}\sin\vartheta \\ ae^{i\varphi}\sin\vartheta & 1-\cos\vartheta \end{pmatrix}$$

mit

$$\begin{aligned}
\mathrm{M}_+^{\mathrm{A}}\,\rho_A\,\mathrm{M}_+^{\mathrm{A}\dagger} &= \begin{pmatrix} \sqrt{p_0} & 0 \\ 0 & \sqrt{p_1} \end{pmatrix}\begin{pmatrix} 1+\cos\vartheta & e^{-i\varphi}\sin\vartheta \\ e^{i\varphi}\sin\vartheta & 1-\cos\vartheta \end{pmatrix}\begin{pmatrix} \sqrt{p_0} & 0 \\ 0 & \sqrt{p_1} \end{pmatrix} \\
&= \begin{pmatrix} \sqrt{p_0} & 0 \\ 0 & \sqrt{p_1} \end{pmatrix}\begin{pmatrix} \sqrt{p_0}(1+\cos\vartheta) & \sqrt{p_1}e^{-i\varphi}\sin\vartheta \\ \sqrt{p_0}e^{i\varphi}\sin\vartheta & \sqrt{p_1}(1-\cos\vartheta) \end{pmatrix} \\
&= \begin{pmatrix} p_0(1+\cos\vartheta) & \sqrt{p_0p_1}e^{-i\varphi}\sin\vartheta \\ \sqrt{p_0p_1}e^{i\varphi}\sin\vartheta & p_1(1-\cos\vartheta) \end{pmatrix}
\end{aligned}$$

und analog

$$\begin{aligned}
\mathrm{M}_-^{\mathrm{A}}\,\rho_A\,\mathrm{M}_-^{\mathrm{A}\dagger} &= \begin{pmatrix} \sqrt{1-p_0} & 0 \\ 0 & \sqrt{1-p_1} \end{pmatrix}\begin{pmatrix} 1+\cos\vartheta & e^{-i\varphi}\sin\vartheta \\ e^{i\varphi}\sin\vartheta & 1-\cos\vartheta \end{pmatrix}\begin{pmatrix} \sqrt{1-p_0} & 0 \\ 0 & \sqrt{1-p_1} \end{pmatrix} \\
&= \begin{pmatrix} (1-p_0)(1+\cos\vartheta) & \sqrt{(1-p_0)(1-p_1)}e^{-i\varphi}\sin\vartheta \\ \sqrt{(1-p_0)(1-p_1)}e^{i\varphi}\sin\vartheta & (1-p_1)(1-\cos\vartheta) \end{pmatrix}
\end{aligned}$$

Die Berechnung der Dichtemtrix bei $\mathrm{N}_\pm^{\mathrm{A}}$-Messung befindet sich separat am Ende des Anhangs.

A.2 Bedingte Wahrscheinlichkeiten für Eve

A.2.1 Anfangszustand $|\uparrow_y\rangle$

Es gilt

$$p_{|\uparrow_y\rangle}(\mathrm{M}_+^{\mathrm{A}} \,|\, \mathrm{M}_+^{\mathrm{E}}) = \frac{\langle\uparrow_y|\, \mathrm{M}_+^{\mathrm{A}\dagger}\, \mathrm{M}_+^{\mathrm{E}}\, \rho_A\, \mathrm{M}_+^{\mathrm{E}\dagger}\, \mathrm{M}_+^{\mathrm{A}}\, |\uparrow_y\rangle}{\langle\uparrow_y|\, \mathrm{M}_+^{\mathrm{E}}\, \rho_A\, \mathrm{M}_+^{\mathrm{E}\dagger}\, |\uparrow_y\rangle} = \frac{q_0p_0 + q_1p_1 + 2a\sqrt{p_0p_1}\sqrt{q_0q_1}}{q_0 + q_1 + 2a\sqrt{q_0q_1}}$$

nach folgender Rechnung.

$$\begin{aligned}
&\langle\uparrow_y|\, \mathrm{M}_+^{\mathrm{A}\dagger}\, \mathrm{M}_+^{\mathrm{E}}\, \rho_A\, \mathrm{M}_+^{\mathrm{E}\dagger}\, \mathrm{M}_+^{\mathrm{A}}\, |\uparrow_y\rangle = \\
&= \frac{1}{4} \begin{pmatrix} 1, \\ -i \end{pmatrix}^T \begin{pmatrix} \sqrt{p_0} & 0 \\ 0 & \sqrt{p_1} \end{pmatrix} \begin{pmatrix} \sqrt{q_0} & 0 \\ 0 & \sqrt{q_1} \end{pmatrix} \begin{pmatrix} 1 & -ia \\ ia & 1 \end{pmatrix} \begin{pmatrix} \sqrt{q_0} & 0 \\ 0 & \sqrt{q_1} \end{pmatrix} \begin{pmatrix} \sqrt{p_0} & 0 \\ 0 & \sqrt{p_1} \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix} \\
&= \frac{1}{4} \begin{pmatrix} \sqrt{p_0}, \\ -i\sqrt{p_1} \end{pmatrix}^T \begin{pmatrix} \sqrt{q_0} & -ia\sqrt{q_0} \\ ia\sqrt{q_1} & \sqrt{q_1} \end{pmatrix} \begin{pmatrix} \sqrt{q_0} & 0 \\ 0 & \sqrt{q_1} \end{pmatrix} \begin{pmatrix} \sqrt{p_0} \\ i\sqrt{p_1} \end{pmatrix} \\
&= \frac{1}{4} \begin{pmatrix} \sqrt{p_0}, \\ -i\sqrt{p_1} \end{pmatrix}^T \begin{pmatrix} q_0 & -ia\sqrt{q_0q_1} \\ ia\sqrt{q_0q_1} & q_1 \end{pmatrix} \begin{pmatrix} \sqrt{p_0} \\ i\sqrt{p_1} \end{pmatrix} \\
&= \frac{1}{4} \begin{pmatrix} \sqrt{p_0}, \\ -i\sqrt{p_1} \end{pmatrix}^T \begin{pmatrix} q_0\sqrt{p_0} - i^2a\sqrt{p_1}\sqrt{q_0q_1} \\ ia\sqrt{p_0}\sqrt{q_0q_1} + i\sqrt{p_1}q_1 \end{pmatrix} \\
&= \frac{1}{4}[q_0p_0 + a\sqrt{p_0p_1}\sqrt{q_0q_1} + a\sqrt{p_0p_1}\sqrt{q_0q_1} + q_1p_1] \\
&= \frac{1}{4}[q_0p_0 + q_1p_1 + 2a\sqrt{p_0p_1}\sqrt{q_0q_1}]
\end{aligned}$$

$$\begin{aligned}
\langle\uparrow_y|\, \mathrm{M}_+^{\mathrm{E}}\, \rho_A\, \mathrm{M}_+^{\mathrm{E}\dagger}\, |\uparrow_y\rangle &= \frac{1}{4} \begin{pmatrix} 1, & -i \end{pmatrix} \begin{pmatrix} \sqrt{q_0} & 0 \\ 0 & \sqrt{q_1} \end{pmatrix} \begin{pmatrix} 1 & -ia \\ ia & 1 \end{pmatrix} \begin{pmatrix} \sqrt{q_0} & 0 \\ 0 & \sqrt{q_1} \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix} \\
&= \frac{1}{4} \begin{pmatrix} 1, & -i \end{pmatrix} \begin{pmatrix} \sqrt{q_0} & -ia\sqrt{q_0} \\ ia\sqrt{q_1} & \sqrt{q_1} \end{pmatrix} \begin{pmatrix} \sqrt{q_0} & 0 \\ 0 & \sqrt{q_1} \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix} \\
&= \frac{1}{4} \begin{pmatrix} 1, & -i \end{pmatrix} \begin{pmatrix} q_0 & -ia\sqrt{q_0q_1} \\ ia\sqrt{q_0q_1} & q_1 \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix} \\
&= \frac{1}{4} \begin{pmatrix} 1, & -i \end{pmatrix} \begin{pmatrix} q_0 + a\sqrt{q_0q_1} \\ ia\sqrt{q_0q_1} + iq_1 \end{pmatrix} \\
&= \frac{1}{4}[q_0 + q_1 + 2a\sqrt{q_0q_1}]
\end{aligned}$$

Weiter erhält man

$$p_{|\uparrow_y\rangle}(\mathrm{N}_+^{\mathrm{A}} \,|\, \mathrm{N}_+^{\mathrm{E}}) = \frac{\langle\uparrow_y|\, \mathrm{N}_+^{\mathrm{A}\dagger}\, \mathrm{N}_+^{\mathrm{E}}\, \rho_A\, \mathrm{N}_+^{\mathrm{E}\dagger}\, \mathrm{N}_+^{\mathrm{A}}\, |\uparrow_y\rangle}{\langle\uparrow_y|\, \mathrm{N}_+^{\mathrm{E}}\, \rho_A\, \mathrm{N}_+^{\mathrm{E}\dagger}\, |\uparrow_y\rangle} = \frac{q_0p_0 + q_1p_1 + 2a\sqrt{p_0p_1}\sqrt{q_0q_1}}{q_0 + q_1 + 2a\sqrt{q_0q_1}},$$

indem man in obiger Rechnung die Rechenbasis $|\uparrow\rangle, |\downarrow\rangle$ ersetzt durch die Rechenbasis $|\uparrow_x\rangle, |\downarrow_x\rangle$ und benutzt, dass die Darstellung von $\mathrm{M}_+^{\mathrm{A}}, \mathrm{M}_+^{\mathrm{E}}$ in der z-Basis die gleiche ist wie die Darstellung von $\mathrm{N}_+^{\mathrm{A}}, \mathrm{N}_+^{\mathrm{E}}$ in der x-Basis, sowie $|\uparrow_y\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + i\,|\downarrow\rangle) = \frac{1}{\sqrt{2}}(|\uparrow_x\rangle + i\,|\downarrow_x\rangle)$.

Es gilt

$$\begin{aligned} p_{|\uparrow_y\rangle}(\mathrm{N}_+^{\mathrm{A}} \,|\, \mathrm{M}_+^{\mathrm{E}}) &= \frac{\langle\uparrow_y|\, \mathrm{N}_+^{\mathrm{A}\dagger}\, \mathrm{M}_+^{\mathrm{E}}\, \rho_A\, \mathrm{M}_+^{\mathrm{E}\dagger}\, \mathrm{N}_+^{\mathrm{A}}\, |\uparrow_y\rangle}{\langle\uparrow_y|\, \mathrm{M}_+^{\mathrm{E}}\, \rho_A\, \mathrm{M}_+^{\mathrm{E}\dagger}\, |\uparrow_y\rangle} \\ &= \frac{1}{2}\frac{q_0(p_0+p_1) + q_1(p_0+p_1) + 4\sqrt{q_0q_1}\sqrt{p_0p_1}a}{q_0+q_1+2a\sqrt{q_0q_1}} \end{aligned}$$

nach folgender Berechnung des Zählers und Verwendung des obigen Ergebnisses für den Zähler.

$$\begin{aligned} &\langle\uparrow_y|\, \mathrm{N}_+^{\mathrm{A}\dagger}\, \mathrm{M}_+^{\mathrm{E}}\, \rho_A\, \mathrm{M}_+^{\mathrm{E}\dagger}\, \mathrm{N}_+^{\mathrm{A}}\, |\uparrow_y\rangle = \\ &= \frac{1}{4}\frac{1}{4}\begin{pmatrix}1\\-i\end{pmatrix}^T \begin{pmatrix}\gamma_+ & \gamma_-\\ \gamma_- & \gamma_+\end{pmatrix}\begin{pmatrix}\sqrt{q_0} & 0\\ 0 & \sqrt{q_1}\end{pmatrix}\begin{pmatrix}1 & -ia\\ ia & 1\end{pmatrix}\begin{pmatrix}\sqrt{q_0} & 0\\ 0 & \sqrt{q_1}\end{pmatrix}\begin{pmatrix}\gamma_+ & \gamma_-\\ \gamma_- & \gamma_+\end{pmatrix}\begin{pmatrix}1\\ i\end{pmatrix} \\ &= \frac{1}{16}\begin{pmatrix}\gamma_+ - i\gamma_-\\ \gamma_- - i\gamma_+\end{pmatrix}^T \begin{pmatrix}\sqrt{q_0} & -ia\sqrt{q_0}\\ ia\sqrt{q_1} & \sqrt{q_1}\end{pmatrix}\begin{pmatrix}\sqrt{q_0} & 0\\ 0 & \sqrt{q_1}\end{pmatrix}\begin{pmatrix}\gamma_+ + i\gamma_-\\ \gamma_- + i\gamma_+\end{pmatrix} \\ &= \frac{1}{16}\begin{pmatrix}\gamma_+ - i\gamma_-\\ \gamma_- - i\gamma_+\end{pmatrix}^T \begin{pmatrix}q_0 & -ia\sqrt{q_0q_1}\\ ia\sqrt{q_0q_1} & q_1\end{pmatrix}\begin{pmatrix}\gamma_+ + i\gamma_-\\ \gamma_- + i\gamma_+\end{pmatrix} \\ &= \frac{1}{16}\begin{pmatrix}\gamma_+ - i\gamma_-\\ \gamma_- - i\gamma_+\end{pmatrix}^T \begin{pmatrix}q_0(\gamma_+ + i\gamma_-) - ia(\gamma_- + i\gamma_+)\sqrt{q_0q_1}\\ ia(\gamma_+ + i\gamma_-)\sqrt{q_0q_1} + q_1(\gamma_- + i\gamma_+)\end{pmatrix} \\ &= \frac{1}{16}[(q_0(\gamma_+ + i\gamma_-) - ia\sqrt{q_0q_1}(\gamma_- + i\gamma_+))(\gamma_+ - i\gamma_-) + \\ &\qquad + (ia\sqrt{p_0p_1}(\gamma_+ + i\gamma_-) + q_1(\gamma_- + i\gamma_+))(\gamma_- - i\gamma_+)] \\ &= \frac{1}{16}[q_0(\gamma_+^2 + \gamma_-^2) - ia\sqrt{q_0q_1}i(\gamma_+^2 - \gamma_-^2) + ia\sqrt{q_0q_1}i(\gamma_-^2 - \gamma_+^2) + q_1(\gamma_-^2 + \gamma_+^2)] \\ &= \frac{1}{16}[2(p_0+p_1)q_0 + a\sqrt{q_0q_1}(4\sqrt{p_0p_1} + 4\sqrt{p_0p_1}) + 2(p_0+p_1)q_1] \\ &= \frac{1}{8}[q_0(p_0+p_1) + q_1(p_0+p_1) + 4a\sqrt{q_0q_1}\sqrt{p_0p_1}] \end{aligned}$$

Das Ergebnis

$$\begin{aligned} p_{|\uparrow_y\rangle}(\mathrm{M}_+^{\mathrm{A}} \,|\, \mathrm{N}_+^{\mathrm{E}}) &= \frac{\langle\uparrow_y|\, \mathrm{M}_+^{\mathrm{A}\dagger}\, \mathrm{N}_+^{\mathrm{E}}\, \rho_A\, \mathrm{N}_+^{\mathrm{E}\dagger}\, \mathrm{M}_+^{\mathrm{A}}\, |\uparrow_y\rangle}{\langle\uparrow_y|\, \mathrm{N}_+^{\mathrm{E}}\, \rho_A\, \mathrm{N}_+^{\mathrm{E}\dagger}\, |\uparrow_y\rangle} \\ &= \frac{1}{2}\frac{q_0(p_0+p_1) + q_1(p_0+p_1) + 4\sqrt{q_0q_1}\sqrt{p_0p_1}a}{q_0+q_1+2a\sqrt{q_0q_1}} \end{aligned}$$

erhält man wieder mit analoger Rechnung in der x-Basis.

A.2.2 Allgemeiner Anfangszustand

Es gelten folgende Additionstheoreme:

$$2\cos^2\frac{\vartheta}{2} = 1+\cos\vartheta$$

$$2\sin^2\frac{\vartheta}{2} = 1-\cos\vartheta$$

$$2\sin\frac{\vartheta}{2}\cos\frac{\vartheta}{2} = \sin\vartheta$$

Damit ergeben sich dann die folgenden bedingten Wahrscheinlichkeiten:

$$\begin{aligned} p_\psi(\mathrm{M}_+^\mathrm{A}\,|\,\mathrm{M}_+^\mathrm{E}) &= \frac{\langle\psi|\,\mathrm{M}_+^{\mathrm{A}\dagger}\,\mathrm{M}_+^\mathrm{E}\,\rho\,\mathrm{M}_+^{\mathrm{E}\dagger}\,\mathrm{M}_+^\mathrm{A}\,|\psi\rangle}{\langle\psi|\,\mathrm{M}_+^\mathrm{E}\,\tilde\rho\,\mathrm{M}_+^{\mathrm{E}\dagger}\,|\psi\rangle} \\ &= \frac{q_0p_0(1+\cos\vartheta)^2 + q_1p_1(1-\cos\vartheta)^2 + 2\sqrt{q_0q_1}\sqrt{p_0p_1}a\sin^2\vartheta}{q_0(1+\cos\vartheta)^2 + q_1(1-\cos\vartheta)^2 + 2\sqrt{q_0q_1}a\sin^2\vartheta} \end{aligned}$$

mit folgender Berechnung des Zählers

$$\begin{aligned} &\langle\psi|\,\mathrm{M}_+^{\mathrm{A}\dagger}\,\mathrm{M}_+^\mathrm{E}\,\rho\,\mathrm{M}_+^{\mathrm{E}\dagger}\,\mathrm{M}_+^\mathrm{A}\,|\psi\rangle = \\ &= \frac{1}{2}\begin{pmatrix}\cos\frac{\vartheta}{2}\\ e^{-i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix}^T\begin{pmatrix}\sqrt{p_0} & 0\\ 0 & \sqrt{p_1}\end{pmatrix}\begin{pmatrix}\sqrt{q_0} & 0\\ 0 & \sqrt{q_1}\end{pmatrix}\begin{pmatrix}1+\cos\vartheta & ae^{-i\varphi}\sin\vartheta\\ ae^{i\varphi}\sin\vartheta & 1-\cos\vartheta\end{pmatrix}\cdot \\ &\qquad\cdot\begin{pmatrix}\sqrt{q_0} & 0\\ 0 & \sqrt{q_1}\end{pmatrix}\begin{pmatrix}\sqrt{p_0} & 0\\ 0 & \sqrt{p_1}\end{pmatrix}\begin{pmatrix}\cos\frac{\vartheta}{2}\\ e^{i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix}\sqrt{p_0q_0}\cos\frac{\vartheta}{2}\\ \sqrt{p_1q_1}e^{-i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix}^T\begin{pmatrix}1+\cos\vartheta & ae^{-i\varphi}\sin\vartheta\\ ae^{i\varphi}\sin\vartheta & 1-\cos\vartheta\end{pmatrix}\begin{pmatrix}\sqrt{p_0q_0}\cos\frac{\vartheta}{2}\\ \sqrt{p_1q_1}e^{i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix}\sqrt{p_0q_0}\cos\frac{\vartheta}{2}\\ \sqrt{p_1q_1}e^{-i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix}^T\begin{pmatrix}(1+\cos\vartheta)\cos\frac{\vartheta}{2}\sqrt{p_0q_0} + ae^{-i\varphi}e^{i\varphi}\sin\vartheta\sin\frac{\vartheta}{2}\sqrt{p_1q_1}\\ ae^{i\varphi}\sin\vartheta\cos\frac{\vartheta}{2}\sqrt{p_0q_0} + (1-\cos\vartheta)e^{i\varphi}\sin\frac{\vartheta}{2}\sqrt{p_1q_1}\end{pmatrix} \\ &= \frac{1}{2}[(1+\cos\vartheta)(\sqrt{p_0q_0}\cos\frac{\vartheta}{2})^2 + 2a\sin\vartheta\sin\frac{\vartheta}{2}\cos\frac{\vartheta}{2}\sqrt{p_0q_0}\sqrt{p_1q_1} + \\ &\qquad + (1-\cos\vartheta)(\sin\frac{\vartheta}{2}\sqrt{p_1q_1})^2] \\ &= \frac{1}{4}[p_0q_0(1+\cos\vartheta)^2 + 2a\sin^2\vartheta\sqrt{p_0q_0p_1q_1} + (1-\cos\vartheta)^2p_1q_1] \end{aligned}$$

Der Nenner ergibt sich analog, indem man beispielsweise $p_0 = p_1 = 1$ setzt, also

$$\begin{aligned} &\langle\psi|\,\mathrm{M}_+^\mathrm{E}\,\rho\,\mathrm{M}_+^{\mathrm{E}\dagger}\,|\psi\rangle = \\ &= \frac{1}{2}\begin{pmatrix}\cos\frac{\vartheta}{2}\\ e^{-i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix}^T\begin{pmatrix}\sqrt{q_0} & 0\\ 0 & \sqrt{q_1}\end{pmatrix}\begin{pmatrix}1+\cos\vartheta & ae^{-i\varphi}\sin\vartheta\\ ae^{i\varphi}\sin\vartheta & 1-\cos\vartheta\end{pmatrix}\begin{pmatrix}\sqrt{q_0} & 0\\ 0 & \sqrt{q_1}\end{pmatrix}\begin{pmatrix}\cos\frac{\vartheta}{2}\\ e^{i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix} \end{aligned}$$

$$= \frac{1}{2}[(1+\cos\vartheta)(\sqrt{q_0}\cos\frac{\vartheta}{2})^2 + 2a\sin\vartheta\sin\frac{\vartheta}{2}\cos\frac{\vartheta}{2}\sqrt{q_0}\sqrt{q_1} + (1-\cos\vartheta)(\sin\frac{\vartheta}{2}\sqrt{q_1})^2]$$
$$= \frac{1}{4}[q_0(1+\cos\vartheta)^2 + 2a\sin^2\vartheta\sqrt{q_0q_1} + (1-\cos\vartheta)^2 q_1]$$

$$p_\psi(\mathrm{N}_+^{\mathrm{A}} \,|\, \mathrm{M}_+^{\mathrm{E}}) =$$
$$= \frac{q_0(1+a\cos\vartheta)(p_0+p_1+(p_0-p_1)\sin\vartheta\cos\varphi+2\sqrt{p_0p_1}\cos\vartheta)}{2q_0(1+a\cos\vartheta)(1+\cos\vartheta)+2q_1(1-\cos\vartheta)+4\sqrt{q_0q_1}(\sin^2\vartheta\cos^2\varphi+a\sin^2\vartheta\sin^2\varphi)} +$$
$$+ \frac{q_1(1-a\cos\vartheta)(p_0+p_1+(p_0-p_1)\sin\vartheta\cos\varphi-2\sqrt{p_0p_1}\cos\vartheta)}{2q_0(1+a\cos\vartheta)(1+\cos\vartheta)+2q_1(1-\cos\vartheta)+4\sqrt{q_0q_1}(\sin^2\vartheta\cos^2\varphi+a\sin^2\vartheta\sin^2\varphi)} +$$
$$+ \frac{2\sqrt{q_0q_1}((p_0-p_1)\sin\vartheta\cos\varphi+(p_0+p_1)\sin^2\vartheta\cos^2\varphi+2a\sqrt{p_0p_1}\sin^2\vartheta\sin^2\varphi)}{2q_0(1+a\cos\vartheta)(1+\cos\vartheta)+2q_1(1-\cos\vartheta)+4\sqrt{q_0q_1}(\sin^2\vartheta\cos^2\varphi+a\sin^2\vartheta\sin^2\varphi)}$$

mit

$$\langle\psi|\,\mathrm{N}_+^{\mathrm{A}\dagger}\,\mathrm{M}_+^{\mathrm{E}}\,\rho\,\mathrm{M}_+^{\mathrm{E}\dagger}\,\mathrm{N}_+^{\mathrm{A}}\,|\psi\rangle =$$
$$= \frac{1}{8}\begin{pmatrix}\cos\frac{\vartheta}{2}\\ e^{-i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix}^T\begin{pmatrix}\gamma_+ & \gamma_-\\ \gamma_- & \gamma_+\end{pmatrix}\begin{pmatrix}\sqrt{q_0} & 0\\ 0 & \sqrt{q_1}\end{pmatrix}\cdot$$
$$\cdot\begin{pmatrix}1+a\cos\vartheta & (\cos\varphi-ia\sin\varphi)\sin\vartheta\\ (\cos\varphi+ia\sin\varphi)\sin\vartheta & 1-a\cos\vartheta\end{pmatrix}\begin{pmatrix}\gamma_+ & \gamma_-\\ \gamma_- & \gamma_+\end{pmatrix}\begin{pmatrix}\sqrt{p_0} & 0\\ 0 & \sqrt{p_1}\end{pmatrix}\begin{pmatrix}\cos\frac{\vartheta}{2}\\ e^{i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix}$$
$$= \frac{1}{8}\begin{pmatrix}(\gamma_+\cos\frac{\vartheta}{2}+\gamma_-e^{-i\varphi}\sin\frac{\vartheta}{2})\sqrt{q_0}\\ (\gamma_-\cos\frac{\vartheta}{2}+\gamma_+e^{-i\varphi}\sin\frac{\vartheta}{2})\sqrt{q_1}\end{pmatrix}^T\cdot$$
$$\cdot\begin{pmatrix}1+a\cos\vartheta & (\cos\varphi-ia\sin\varphi)\sin\vartheta\\ (\cos\varphi+ia\sin\varphi)\sin\vartheta & 1-a\cos\vartheta\end{pmatrix}\begin{pmatrix}(\gamma_+\cos\frac{\vartheta}{2}+\gamma_-e^{i\varphi}\sin\frac{\vartheta}{2})\sqrt{q_0}\\ (\gamma_-\cos\frac{\vartheta}{2}+\gamma_+e^{i\varphi}\sin\frac{\vartheta}{2})\sqrt{q_1}\end{pmatrix}$$
$$= \frac{1}{8}[(1+a\cos\vartheta)((\gamma_+\cos\frac{\vartheta}{2})^2+(\gamma_-\sin\frac{\vartheta}{2})^2+\gamma_+\gamma_-\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(e^{i\varphi}+e^{-i\varphi}))q_0+$$
$$+(1-a\cos\vartheta)((\gamma_-\cos\frac{\vartheta}{2})^2+(\gamma_+\sin\frac{\vartheta}{2})^2+\gamma_+\gamma_-\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(e^{i\varphi}+e^{-i\varphi}))q_1+$$
$$+(\cos\varphi\sin\vartheta(\gamma_+\gamma_-(\cos^2\frac{\vartheta}{2}+\sin^2\frac{\vartheta}{2})+\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(\gamma_+^2+\gamma_-^2)(e^{i\varphi}+e^{-i\varphi}))+$$
$$+ia\sin\varphi\sin\vartheta\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(\gamma_-^2-\gamma_+^2)(e^{i\varphi}-e^{-i\varphi}))\sqrt{q_0q_1})]$$
$$= \frac{1}{8}[q_0(1+a\cos\vartheta)(p_0+p_1+2\sqrt{p_0p_1}\cos\vartheta+(p_0-p_1)\sin\vartheta\cos\varphi)+$$
$$+q_1(1-a\cos\vartheta)(p_0+p_1-2\sqrt{p_0p_1}\cos\vartheta+(p_0-p_1)\sin\vartheta\cos\varphi)+$$
$$+2\sqrt{q_0q_1}((p_0-p_1)\sin\vartheta\cos\varphi+(p_0+p_1)\sin^2\vartheta\cos^2\varphi+2a\sqrt{p_0p_1}\sin^2\vartheta\sin^2\varphi)]$$

und

$$
\begin{aligned}
&\langle\psi|\,\mathrm{M}_+^{\mathrm{E}}\,\rho\,\mathrm{M}_+^{\mathrm{E}\,\dagger}\,|\psi\rangle = \\
&\quad= \frac{1}{8}[q_0(1+a\cos\vartheta)(2+2\cos\vartheta)+q_1(1-a\cos\vartheta)(2-2\cos\vartheta)+ \\
&\qquad\qquad + 2\sqrt{q_0q_1}(2\sin^2\vartheta\cos^2\varphi+2a\sin^2\vartheta\sin^2\varphi)] \\
&\quad= \frac{1}{4}[q_0(1+a\cos\vartheta)(1+\cos\vartheta)+q_1(1-a\cos\vartheta)(1-\cos\vartheta)+ \\
&\qquad\qquad + 2\sqrt{q_0q_1}(\sin^2\vartheta\cos^2\varphi+a\sin^2\vartheta\sin^2\varphi)]
\end{aligned}
$$

$$
\begin{aligned}
&p_\psi(\mathrm{M}_+^{\mathrm{A}}\,|\,\mathrm{N}_+^{\mathrm{E}}) = \\
&\quad= [q_0(1+a\sin\vartheta\cos\varphi)(p_0+p_1+(p_0-p_1)\cos\vartheta+2\sqrt{p_0p_1}\sin\vartheta\cos\varphi)+ \\
&\qquad + q_1(1-a\sin\vartheta\cos\varphi)(p_0+p_1+(p_0-p_1)\cos\vartheta-2\sqrt{p_0p_1}\sin\vartheta\cos\varphi)+ \\
&\qquad\quad + 2\sqrt{q_0q_1}((p_0-p_1)\cos\vartheta+(p_0+p_1)cos^2\vartheta+2a\sqrt{p_0p_1}\sin^2\vartheta(1-\cos^2\varphi)]/ \\
&\qquad /[2q_0(1+\sin\vartheta\cos\varphi)(1+a\sin\vartheta\cos\varphi)+2q_1(1-\sin\vartheta\cos\varphi)(1-a\sin\vartheta\cos\varphi)+ \\
&\qquad\qquad + 4\sqrt{q_0q_1}(\cos^2\vartheta+a\sin^2\vartheta\sin^2\varphi)]
\end{aligned}
$$

ergibt sich aus

$$
\begin{aligned}
&\langle\psi|\,\mathrm{M}_+^{\mathrm{A}\,\dagger}\,\mathrm{N}_+^{\mathrm{E}}\,\rho\,\mathrm{N}_+^{\mathrm{E}\,\dagger}\,\mathrm{M}_+^{\mathrm{A}}\,|\psi\rangle = \\
&= \frac{1}{8}\begin{pmatrix}\cos\frac{\vartheta}{2}\\ e^{-i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix}^T\begin{pmatrix}\sqrt{p_0}&0\\0&\sqrt{p_1}\end{pmatrix}\begin{pmatrix}\chi_+&\chi_-\\\chi_-&\chi_+\end{pmatrix}\begin{pmatrix}1+\cos\vartheta&ae^{-i\varphi}\sin\vartheta\\ae^{i\varphi}\sin\vartheta&1-\cos\vartheta\end{pmatrix}\cdot \\
&\qquad\qquad\cdot\begin{pmatrix}\chi_+&\chi_-\\\chi_-&\chi_+\end{pmatrix}\begin{pmatrix}\sqrt{p_0}&0\\0&\sqrt{p_1}\end{pmatrix}\begin{pmatrix}\cos\frac{\vartheta}{2}\\ e^{i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix} \\
&= \frac{1}{8}\begin{pmatrix}\sqrt{p_0}\cos\frac{\vartheta}{2}\chi_+ + \sqrt{p_1}e^{-i\varphi}\sin\frac{\vartheta}{2}\chi_-\\ \sqrt{p_0}\cos\frac{\vartheta}{2}\chi_- + \sqrt{p_1}e^{-i\varphi}\sin\frac{\vartheta}{2}\chi_+\end{pmatrix}^T\begin{pmatrix}1+\cos\vartheta&ae^{-i\varphi}\sin\vartheta\\ae^{i\varphi}\sin\vartheta&1-\cos\vartheta\end{pmatrix}\cdot \\
&\qquad\qquad\cdot\begin{pmatrix}\sqrt{p_0}\cos\frac{\vartheta}{2}\chi_+ + \sqrt{p_1}e^{i\varphi}\sin\frac{\vartheta}{2}\chi_-\\ \sqrt{p_0}\cos\frac{\vartheta}{2}\chi_- + \sqrt{p_1}e^{i\varphi}\sin\frac{\vartheta}{2}\chi_+\end{pmatrix} \\
&= \frac{1}{8}[(1+\cos\vartheta)p_0(\cos\frac{\vartheta}{2}\chi_+)^2+p_1(\sin\frac{\vartheta}{2}\chi_-)^2+\sqrt{p_0p_1}\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}\chi_+\chi_-(e^{i\varphi}+e^{-i\varphi})+ \\
&\quad + (1-\cos\vartheta)p_1(\cos\frac{\vartheta}{2}\chi_+)^2+p_0(\sin\frac{\vartheta}{2}\chi_-)^2+\sqrt{p_0p_1}\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}\chi_+\chi_-(e^{i\varphi}+e^{-i\varphi})+ \\
&\quad + ae^{-i\varphi}\sin\vartheta((\sqrt{p_0}\cos\frac{\vartheta}{2}+\sqrt{p_1}\sin\frac{\vartheta}{2})^2\chi_+\chi_-+\sqrt{p_0p_1}\sin\frac{\vartheta}{2}\cos\frac{\vartheta}{2}(\chi_+^2e^{i\varphi}+\chi_-^2e^{-i\varphi}))+ \\
&\quad + ae^{i\varphi}\sin\vartheta(((\sqrt{p_0}\cos\frac{\vartheta}{2}+\sqrt{p_1}\sin\frac{\vartheta}{2})^2\chi_+\chi_-+\sqrt{p_0p_1}\sin\frac{\vartheta}{2}\cos\frac{\vartheta}{2}(\chi_-^2e^{i\varphi}+\chi_+^2e^{-i\varphi}))] \\
&= \frac{1}{8}[q_0(1+a\sin\vartheta\cos\varphi)(p_0+p_1+(p_0-p_1)\cos\vartheta+2\sqrt{p_0p_1}\sin\vartheta\cos\varphi)+ \\
&\qquad + q_1(1-a\sin\vartheta\cos\varphi)(p_0+p_1+(p_0-p_1)\cos\vartheta-2\sqrt{p_0p_1}\sin\vartheta\cos\varphi)+
\end{aligned}
$$

$$+ 2\sqrt{q_0 q_1}((p_0 - p_1)\cos\vartheta + (p_0 + p_1)cos^2\vartheta + 2a\sqrt{p_0 p_1}\sin^2\vartheta\sin^2\varphi]$$

und

$$\langle\psi|\,\mathrm{N}_+^{\mathrm{E}}\,\rho\,\mathrm{N}_+^{\mathrm{E}\,\dagger}\,|\psi\rangle = \frac{1}{4}q_0(1 + a\sin\vartheta\cos\varphi)(1 + \sin\vartheta\cos\varphi) +$$
$$+ q_1(1 - a\sin\vartheta\cos\varphi)(1 - \sin\vartheta\cos\varphi) + 2\sqrt{q_0 q_1}(cos^2\vartheta + a\sin^2\vartheta\sin^2\varphi]$$

$$p_\psi(\mathrm{N}_+^{\mathrm{A}}\,|\,\mathrm{N}_+^{\mathrm{E}}) =$$
$$= \frac{q_0 p_0(1 + \sin\vartheta\cos\varphi)^2 + q_1 p_1(1 - \sin\vartheta\cos\varphi)^2 + 2a\sqrt{q_0 q_1}\sqrt{p_0 p_1}(\cos^2\vartheta + \sin^2\vartheta\sin^2\varphi)}{q_0(1 + \sin\vartheta\cos\varphi)^2 + q_1(1 - \sin\vartheta\cos\varphi)^2 + 2a\sqrt{q_0 q_1}(\cos^2\vartheta + \sin^2\vartheta\sin^2\varphi)}$$

folgt aus

$$\langle\psi|\,\mathrm{N}_+^{\mathrm{A}\,\dagger}\,\mathrm{N}_+^{\mathrm{E}}\,\rho\,\mathrm{N}_+^{\mathrm{E}\,\dagger}\,\mathrm{N}_+^{\mathrm{A}}\,|\psi\rangle =$$
$$= \frac{1}{32}\begin{pmatrix}\cos\frac{\vartheta}{2}\\ e^{-i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix}^T\begin{pmatrix}\gamma_+ & \gamma_-\\ \gamma_- & \gamma_+\end{pmatrix}\begin{pmatrix}\chi_+ & \chi_-\\ \chi_- & \chi_+\end{pmatrix}\cdot$$
$$\cdot\begin{pmatrix}1 + a\cos\vartheta & (\cos\varphi - ia\sin\varphi)\sin\vartheta\\ (\cos\varphi + ia\sin\varphi)\sin\vartheta & 1 - a\cos\vartheta\end{pmatrix}\begin{pmatrix}\gamma_+ & \gamma_-\\ \gamma_- & \gamma_+\end{pmatrix}\begin{pmatrix}\chi_+ & \chi_-\\ \chi_- & \chi_+\end{pmatrix}\begin{pmatrix}\cos\frac{\vartheta}{2}\\ e^{i\varphi}\sin\frac{\vartheta}{2}\end{pmatrix}$$
$$= \frac{1}{32}[(1 + a\cos\vartheta)[\chi_+^2((\gamma_+\cos\frac{\vartheta}{2})^2 + (\gamma_-\sin\frac{\vartheta}{2})^2 + \gamma_+\gamma_-\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(e^{i\varphi} + e^{-i\varphi})) +$$
$$+ \chi_-^2((\gamma_-\cos\frac{\vartheta}{2})^2 + (\gamma_+\sin\frac{\vartheta}{2})^2 + \gamma_+\gamma_-\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(e^{i\varphi} + e^{-i\varphi})) +$$
$$+ \chi_+\chi_-(2\gamma_+\gamma_- + \cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(\gamma_+^{@}e^{i\varphi} + \gamma_- e^{-i\varphi} + \gamma_-^2 e^{i\varphi} + \gamma_+^2 e^{-i\varphi}))]$$
$$+ (1 - a\cos\vartheta)[\chi_-^2((\gamma_-\cos\frac{\vartheta}{2})^2 + (\gamma_+\sin\frac{\vartheta}{2})^2 + \gamma_+\gamma_-\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(e^{i\varphi} + e^{-i\varphi})) +$$
$$+ \chi_+^2((\gamma_+\cos\frac{\vartheta}{2})^2 + (\gamma_-\sin\frac{\vartheta}{2})^2 + \gamma_+\gamma_-\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(e^{i\varphi} + e^{-i\varphi})) +$$
$$+ \chi_+\chi_-(2\gamma_+\gamma_- + \cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(\gamma_-^2 e^{i\varphi} + \gamma_+^2 e^{-i\varphi} + \gamma_+^2 e^{i\varphi} + \gamma_-^2 e^{-i\varphi}))]$$
$$+ \sin\vartheta(\cos\varphi + ia\sin\varphi)$$
$$[\chi_+^2(\gamma_+\gamma_- + \cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(\gamma_-^2 e^{i\varphi} + \gamma_+^2 e^{-i\varphi})) + \chi_-^2(\gamma_+\gamma_- + \cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(\gamma_+^2 e^{i\varphi} + \gamma_-^2 e^{-i\varphi})) +$$
$$+ \chi_+\chi_-[(\gamma_-^2 + \gamma_+^2) + \gamma_+\gamma_-\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(e^{i\varphi} + e^{-i\varphi} + e^{i\varphi} + e^{-i\varphi})]]$$
$$+ \sin\vartheta(\cos\varphi - ia\sin\varphi)$$
$$[\chi_-^2(\gamma_+\gamma_- + \cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(\gamma_-^2 e^{i\varphi} + \gamma_+^2 e^{-i\varphi})) + \chi_+^2(\gamma_+\gamma_- + \cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(\gamma_+^2 e^{i\varphi} + \gamma_-^2 e^{-i\varphi})) +$$
$$+ \chi_+\chi_-(\gamma_-^2 + \gamma_+^2 + \gamma_+\gamma_-\cos\frac{\vartheta}{2}\sin\frac{\vartheta}{2}(e^{i\varphi} + e^{-i\varphi} + e^{i\varphi} + e^{-i\varphi}))]]$$

$$= \frac{1}{4}[q_0 p_0 (1 + \sin\vartheta\cos\varphi)^2 + q_1 p_1 (1 - \sin\vartheta\cos\varphi) + 2\sqrt{q_0 q_1}\sqrt{p_0 p_1}(\cos^2\vartheta + \sin^2\vartheta\sin^2\varphi)]$$

und entsprechend

$$\langle\psi|\,\mathrm{N}_+^{\mathrm{E}}\,\rho\,\mathrm{N}_+^{\mathrm{E}\,\dagger}\,|\psi\rangle = \\ = \frac{1}{4}[q_0(1 + \sin\vartheta\cos\varphi)^2 + q_1(1 - \sin\vartheta\cos\varphi) + 2\sqrt{q_0 q_1}(\cos^2\vartheta + \sin^2\vartheta\sin^2\varphi)]$$

A.3 Berechnung von $p(n_+)$

Um die Wahrscheinlichkeitsverteilung $p(n_+)$ der Zufallsvariable von Bob in Abschnitt 8.4 zu berechnen, benötigen wir die Größen $p(n_+|n_\uparrow, M)$, $p(n_+|n_\uparrow, M)$, $p(n_+|M)$ sowie $p(n_+|N)$. Dabei verwenden wir zur Berechnung die Bezeichnungen $P_\uparrow = |\uparrow\rangle\langle\uparrow|$ und $P_\downarrow = |\downarrow\rangle\langle\downarrow|$. Mit $\sum_\pm^k$ bezeichnen wir die Summe über alle möglichen Reihenfolgen von $+$ und $-$, wobei sich die Anzahlen stets zu k summieren. Es bezeichnet $\sum_\pm^k \mathrm{M}_\pm^{\mathrm{A}}$ also die Summe über alle möglichen Messergebnisse eines Ensembles der Größe k bei unscharfer Messung mit $\mathrm{M}_\pm^{\mathrm{A}}$. Es gilt außerdem $n = n_\uparrow + n_\downarrow$, $n_\uparrow = n_+ + n_-$. Weiter definieren wir

$$p_{M\pm\uparrow} := \langle\uparrow|\,\mathrm{M}_\pm^{\mathrm{A}}\,|\psi\rangle\,\langle\psi|\,\mathrm{M}_\pm^{\mathrm{A}\,\dagger}\,|\uparrow\rangle$$

und entsprechend für $\downarrow$. Hierfür gilt $p_{M-\uparrow} = \rho_{M00} - p_{M+\uparrow}$ und $p_{M-\downarrow} = \rho_{M11} - p_{M+\downarrow}$, wobei ρ_M die Dichtematrix nach unscharfer Messung mit $\mathrm{M}_\pm^{\mathrm{A}}$ darstellt. Damit können wir die erforderlichen Größen berechnen.

$$\begin{aligned}
p(n_+|n_\uparrow, M) &= \binom{n_\uparrow}{n_+} p(\mathrm{M}_+^{\mathrm{A}\otimes n_+}\,\mathrm{M}_-^{\mathrm{A}\otimes(n_\uparrow - n_+)}\,|n_\uparrow) \\
&= \binom{n_\uparrow}{n_+} \frac{\mathrm{tr}[P_\uparrow^{\otimes n_\uparrow} \otimes P_\downarrow^{\otimes n_\downarrow} \cdot \mathrm{M}_+^{\mathrm{A}\otimes n_+} \otimes \mathrm{M}_-^{\mathrm{A}\otimes n_-} \otimes \sum_\pm^{n_\downarrow} \mathrm{M}_\pm^{\mathrm{A}}\,|\psi\rangle\langle\psi|^{\otimes n}]}{\mathrm{tr}[P_\uparrow^{\otimes n_\uparrow} \otimes P_\downarrow^{\otimes n_\downarrow} \cdot \sum_\pm^n \mathrm{M}_\pm^{\mathrm{A}}\,|\psi\rangle\langle\psi|^{\otimes n}]} \\
&= \binom{n_\uparrow}{n_+} \frac{\mathrm{tr}[P_\uparrow^{\otimes n_\uparrow} \cdot \mathrm{M}_+^{\mathrm{A}\otimes n_+} \otimes \mathrm{M}_-^{\mathrm{A}\otimes n_-}\,|\psi\rangle\langle\psi|^{\otimes n_\uparrow}]}{\mathrm{tr}[P_\uparrow^{\otimes n_\uparrow} \cdot \sum_\pm^{n_\uparrow} \mathrm{M}_\pm^{\mathrm{A}}\,|\psi\rangle\langle\psi|^{\otimes n_\uparrow}]} \cdot \frac{\mathrm{tr}[P_\downarrow^{\otimes n_\downarrow} \cdot \sum_\pm^{n_\downarrow} \mathrm{M}_\pm^{\mathrm{A}}\,|\psi\rangle\langle\psi|^{\otimes n_\downarrow}]}{\mathrm{tr}[P_\downarrow^{\otimes n_\downarrow} \cdot \sum_\pm^{n_\downarrow} \mathrm{M}_\pm^{\mathrm{A}}\,|\psi\rangle\langle\psi|^{\otimes n_\downarrow}]} \\
&= \binom{n_\uparrow}{n_+} \frac{\mathrm{tr}[P_\uparrow^{\otimes n_\uparrow} \cdot \mathrm{M}_+^{\mathrm{A}\otimes n_+} \otimes \mathrm{M}_-^{\mathrm{A}\otimes n_-}\,|\psi\rangle\langle\psi|^{\otimes n_\uparrow}]}{\mathrm{tr}[P_\uparrow^{\otimes n_\uparrow} \cdot \sum_\pm^{n_\uparrow} \mathrm{M}_\pm^{\mathrm{A}}\,|\psi\rangle\langle\psi|^{\otimes n_\uparrow}]} \\
&= \binom{n_\uparrow}{n_+} \frac{\mathrm{tr}[P_\uparrow \cdot \mathrm{M}_+^{\mathrm{A}}\,|\psi\rangle\langle\psi|]^{n_+}\,\mathrm{tr}[P_\uparrow \cdot \mathrm{M}_-^{\mathrm{A}}\,|\psi\rangle\langle\psi|]^{n_-}}{\sum_\pm^{n_\uparrow} \mathrm{tr}[P_\uparrow \cdot \mathrm{M}_\pm^{\mathrm{A}}\,|\psi\rangle\langle\psi|^{n_\uparrow}]} \\
&= \binom{n_\uparrow}{n_+} \frac{(\langle\uparrow|\,\mathrm{M}_+^{\mathrm{A}}\,|\psi\rangle\,\langle\psi|\,\mathrm{M}_+^{\mathrm{A}\,\dagger}\,|\uparrow\rangle)^{n_+}(\langle\uparrow|\,\mathrm{M}_-^{\mathrm{A}}\,|\psi\rangle\,\langle\psi|\,\mathrm{M}_-^{\mathrm{A}\,\dagger}\,|\uparrow\rangle)^{n_-}}{\sum_{m_+}\binom{n_\uparrow}{m_+}\,\mathrm{tr}[P_\uparrow \cdot \mathrm{M}_+^{\mathrm{A}}\,|\psi\rangle\langle\psi|]^{m_+}\,\mathrm{tr}[P_\uparrow \cdot \mathrm{M}_-^{\mathrm{A}}\,|\psi\rangle\langle\psi|]^{m_-}} \\
&= \binom{n_\uparrow}{n_+} \frac{p_{M+\uparrow}^{n_+} p_{M-\uparrow}^{n_-}}{\sum_{m_+}\binom{n_\uparrow}{m_+} p_{M+\uparrow}^{m_+} p_{M-\uparrow}^{m_-}}
\end{aligned}$$

$$= \binom{n_\uparrow}{n_+} \frac{p_{M+\uparrow}^{n_+}(\rho_{M00} - p_{M+\uparrow})^{n_-}}{\sum_{m_+} \binom{n_\uparrow}{m_+} p_{M+\uparrow}^{m_+}(\rho_{M00} - p_{M+\uparrow})^{n_\uparrow - m_+}}$$
$$= \binom{n_\uparrow}{n_+} \frac{p_{M+\uparrow}^{n_+}(\rho_{M00} - p_{M+\uparrow})^{n_\uparrow - n_+}}{\rho_{M00}^{n_\uparrow}}$$

Es folgt mit ähnlichen Umformungen

$$\begin{aligned}
p(n_\uparrow|M) &= \sum_{\pm}^{n} \binom{n}{n_\uparrow} \operatorname{tr}[P_\uparrow^{\otimes n_\uparrow} \otimes P_\downarrow^{\otimes n_\downarrow} \cdot \sum_{\pm}^{n} \mathrm{M}_\pm^{\mathrm{A}} |\psi\rangle \langle\psi|^{\otimes n}] \\
&= \sum_{n_+} \binom{n}{n_\uparrow} \binom{n_\uparrow}{n_+} [(\langle\uparrow| \mathrm{M}_+^{\mathrm{A}} |\psi\rangle \langle\psi| \mathrm{M}_+^{\mathrm{A}^\dagger} |\uparrow\rangle)^{n_+} (\langle\uparrow| \mathrm{M}_-^{\mathrm{A}} |\psi\rangle \langle\psi| \mathrm{M}_-^{\mathrm{A}^\dagger} |\uparrow\rangle)^{n_-} + \\
&\quad + (\langle\downarrow| \mathrm{M}_+^{\mathrm{A}} |\psi\rangle \langle\psi| \mathrm{M}_+^{\mathrm{A}^\dagger} |\downarrow\rangle)^{n_+} (\langle\downarrow| \mathrm{M}_-^{\mathrm{A}} |\psi\rangle \langle\psi| \mathrm{M}_-^{\mathrm{A}^\dagger} |\downarrow\rangle)^{n_-}] \\
&= \binom{n}{n_\uparrow} [\sum_{n_+} \binom{n_\uparrow}{n_+} p_{M+\uparrow}^{n_+}(\rho_{M00} - p_{M+\uparrow})^{n_\uparrow - n_+} + \\
&\qquad\qquad + \sum_{n_+} \binom{n_\uparrow}{n_+} p_{M+\downarrow}^{n_+}(\rho_{M11} - p_{M+\downarrow})^{n_\uparrow - n_+}] \\
&= \binom{n}{n_u p} \rho_{M00}^{n_\uparrow} \rho_{M11}^{n - n_\uparrow} \cdot
\end{aligned}$$

A.4 Berechnung von ρ_N

$$\rho_N = \frac{1}{2}(\mathrm{N}_+^{\mathrm{A}}\,\rho_A\,\mathrm{N}_+^{\mathrm{A}\dagger} + \mathrm{N}_-^{\mathrm{A}}\,\rho_A\,\mathrm{N}_-^{\mathrm{A}\dagger}) = \frac{1}{2}\begin{pmatrix} 1+a\cos\vartheta & \sin\vartheta(\cos\varphi - ia\sin\varphi) \\ \sin\vartheta(\cos\varphi + ia\sin\varphi) & 1-a\cos\vartheta \end{pmatrix}$$

mit

$$\begin{aligned}
&\mathrm{N}_+^{\mathrm{A}}\,\rho_A\,\mathrm{N}_+^{\mathrm{A}\dagger} = \\
&= \frac{1}{8}\begin{pmatrix}\gamma_+ & \gamma_- \\ \gamma_- & \gamma_+\end{pmatrix}\begin{pmatrix}1+\cos\vartheta & e^{-i\varphi}\sin\vartheta \\ e^{i\varphi}\sin\vartheta & 1-\cos\vartheta\end{pmatrix}\begin{pmatrix}\gamma_+ & \gamma_- \\ \gamma_- & \gamma_+\end{pmatrix} \\
&= \frac{1}{8}\begin{pmatrix}\gamma_+ & \gamma_- \\ \gamma_- & \gamma_+\end{pmatrix}\begin{pmatrix}\gamma_+(1+\cos\vartheta)+\gamma_- e^{-i\varphi}\sin\vartheta & \gamma_-(1+\cos\vartheta)+\gamma_+ e^{-i\varphi}\sin\vartheta \\ \gamma_-(1-\cos\vartheta)+\gamma_+ e^{i\varphi}\sin\vartheta & \gamma_+(1-\cos\vartheta)+\gamma_- e^{i\varphi}\sin\vartheta\end{pmatrix} \\
&= \frac{1}{8}\begin{pmatrix}\gamma_+^2(1+\cos\vartheta)+\gamma_-^2(1-\cos\vartheta)+\gamma_+\gamma_-\sin\vartheta(e^{-i\varphi}+e^{i\varphi}) & 2\gamma_+\gamma_- + (\gamma_+^2 e^{-i\varphi}+\gamma_-^2 e^{i\varphi})\sin\vartheta \\ 2\gamma_+\gamma_- + (\gamma_-^2 e^{-i\varphi}+\gamma_+^2 e^{i\varphi})\sin\vartheta & \gamma_-^2(1+\cos\vartheta)+\gamma_+^2(1-\cos\vartheta)+\gamma_+\gamma_-\sin\vartheta(e^{i\varphi}+e^{-i\varphi})\end{pmatrix} \\
&= \frac{1}{4}\begin{pmatrix} p_0+p_1+2\sqrt{p_0p_1}\cos\vartheta+(p_0-p_1)\sin\vartheta\cos\varphi & p_0-p_1+(p_0+p_1)\sin\vartheta\cos\varphi-2i\sqrt{p_0p_1}\sin\vartheta\sin\varphi \\ p_0-p_1+(p_0+p_1)\sin\vartheta\cos\varphi+2i\sqrt{p_0p_1}\sin\vartheta\sin\varphi & p_0+p_1-2\sqrt{p_0p_1}\cos\vartheta+(p_0-p_1)\sin\vartheta\cos\varphi\end{pmatrix}
\end{aligned}$$

und analog

$$\begin{aligned}
&\mathrm{N}_-^{\mathrm{A}}\,\rho_A\,\mathrm{N}_-^{\mathrm{A}\dagger} = \\
&\quad= \frac{1}{4}\begin{pmatrix} 2-p_0-p_1+2\sqrt{p-}\cos\vartheta+(p_1-p_0)\sin\vartheta\cos\varphi & p_1-p_0+(2-p_0-p_1)\sin\vartheta\cos\varphi-2i\sqrt{-}\sin\vartheta\sin\varphi \\ p_1-p_0+(2-p_0-p_1)\sin\vartheta\cos\varphi+2i\sqrt{-}\sin\vartheta\sin\varphi & 2-p_0-p_1-2\sqrt{p-}\cos\vartheta+(p_1-p_0)\sin\vartheta\cos\varphi\end{pmatrix}
\end{aligned}$$

Literaturverzeichnis

[1] Norbert Lütkenhaus. Security against eavesdropping in quantum cryptography. *Phys. Rev. A*, 54(1):97, 1996.

[2] id Quantique. A leap for quantum cryptography . http://www.idquantique.com/products/files/clavis-white.pdf.

[3] Miloslav Dusek, Norbert Lutkenhaus, and Martin Hendrych. Quantum cryptography, 2006. quant-ph/0601207.

[4] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal American Institute of Electrical Engineers*, XLV(55):109–115, 1926.

[5] Claude Shannon. Communication theory of secrecy systems. *Bell System Tech. J.*, 28(4):656–715, 1949.

[6] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of International Conference on Computers, Systems and Signal Processing*, December 1984.

[7] Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050, 1999.

[8] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85:441, 2000.

[9] Daniel Gottesman and John Preskill. Secure quantum key distribution using squeezed states. *Physical Review A*, 63:022309, 2001.

[10] Daniel Gottesman and Hoi-Kwong Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory*, 49:457, 2003.

[11] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed state entanglement and quantum error correction. *Physical Review A*, 54:3824, 1996.

[12] Valerio Scarani, Antonio Acin, Gregoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. *Physical Review Letters*, 92:057901, 2004.

[13] J. Audretsch. *Verschränkte Systeme – Die Quantenphysik auf neuen Wegen.* Wiley-VCH, Weinheim, 2005.

[14] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, October 2004.

[15] T. Konrad. *Less is More. On the Theory and Application of Weak and Unsharp Measurements in Quantum Mechanics*. PhD thesis, Universität Konstanz, 2003.

[16] Albrecht Irle. *Wahrscheinlichkeitstheorie und Statistik. Grundlagen – Resultate – Anwendungen*. Wiesbaden: Teubner. , 2005.

[17] L. Fahrmeir, R. Künstler, I. Pigeot, and G Tutz. *Statistik. Der Weg zur Datenanalyse*. Springer Verlag, 2003.

[18] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Info. Theor.*, IT-24:339–348, 1978.

[19] C. H. Bennett and G. Brassard. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working]. *SIGACT News*, 20(4):78–80, 1989.

[20] Charles H. Bennett, Francois Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *J. Cryptol.*, 5(1):3–28, 1992.

[21] W.P. Risk and D.S. Bethune. Quantum Cryptography: Using Autocompensating Fiber-Optic Interferometers. *New Journal of Physics*, 4:41, 2002. http//:www.idquantique.com.

[22] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67km with a plug & play system. *Optics and Photonic News*, pages 26–32, 2002. http//:www.idquantique.com.

[23] M. Martinelli. Time reversal for the polarization state in optical systems. *J. Mod. Opt.*, 39:451–455, 1992.

[24] Eguchi Makoto, Hagiwara Manabu, and Hideki Imai. A quantum key distribution protocol with selecting announced states, robust against photon number splitting attacks, 2006. quant-ph/0603066.

[25] Klaus Jänich. *Funktionentheorie. Eine Einführung, 3. Aufl.* Springer-Lehrbuch. Berlin: Springer., 1991.

[26] Ludger Kaup and Burchard Kaup. *Holomorphic functions of several variables.* De Gruyter Studies in Mathematics, 3. Berlin - New York: Walter de Gruyter. XV, 1983.

[27] J. Preskill. Lecture Notes for Physics 229: Quantum Information and Computation, 1998. http//:www.theory.Caltech.edu/ preskill/ph229.

[28] Dominic Mayers. Unconditional security in quantum cryptography. *JACM*, 3:35, 1998.

[29] Claude Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27(3):379–423,623–656, 1948.