JUST DO IT
HÖHERE ABTEILUNG FÜR
INFORMATIONSTECHNOLOGIE

tgm
Die Schule der Technik

Systemtechnik - Ausarbeitung

Quantencomputing

Systemtechnik
5BHITT 2015/16

Klaus Ableitinger
Sebastian Steinkellner

Version 0.1
Begonnen am 26. MÃď rz 2016
Beendet am 1. April 2016

Note:
Betreuer: Mi. Borko & Ma. Schabel

Inhaltsverzeichnis

1 Grundlagen

1.1 Qubit

1.1.1 Schrödinger

Schrödingers Katze ist die berühmteste Veranschaulichung eines grundlegenden Phänomens der Quantenmechanik. Genaugenommen ist es ein Versuchsaufbau, anhand dessen sich verschiedene Begriffe der Quantenmechanik leicht erklären lassen. Der Versuchsaufbau sieht folgendermaßen aus:

In einer Kiste befinden sich eine Katze und eine Ampulle mit einer giftigen Substanz. Mit einer exakten Wahrscheinlichkeit von 50% ist die Ampulle offen und die Katze bereits tot, mit einer genau gleich großen Wahrscheinlichkeit ist aber die Ampulle immer noch verschlossen und die Katze am Leben. Da wir nur die Außenseite der Kiste sehen und sie Schall und Geruchsdicht ist, können wir nicht genau sagen, in welchem Zustand die Katze sich befindet. Es könnte also behauptet werden, dass sie gleichzeitig tot und lebendig ist.

Den Umstand, dass 2 (oft gegensätzliche) Zustände zeitgleich wahr sind, wird in der Quantenmechanik als Superposition bezeichnet. Eine Voraussetzung für das erreichen einer Superposition ist die vollkommene Abschottung von der Außenwelt.

Wenn nun die Kiste geöffnet wird und der Betrachter einen Blick ins innere der Kiste wirft, so erkennt er ziemlich schnell, ob die Katze tot oder lebendig ist. Einer der beiden Zustände ist durch diese sogenannte Messung verloren gegangen.

1.1.2 Definition

Per Definition werden die Zustände eines Quantenbits in der Form $\alpha * |0\rangle + \beta * |1\rangle$ angeschrieben. α und β werden "Amplituden" genannt, sind komplexe Zahlen, stellen einen Anteil am Gesamtzustand dar und sind durch die Formel $|\alpha|^2 + |\beta|^2 = 1$ voneinander abhängig.

Dank der folgenden Umrechnung kann ein Qubit auch als Vektor geschrieben werden.

$\alpha|0\rangle + \beta|1\rangle = \alpha\binom{1}{0} + \beta\binom{0}{1} = \binom{\alpha}{\beta}$

1.1.3 Messung

Anders als ein klassisches Bit, kann ein Qubit nicht gelesen, sondern muss gemessen werden, wobei die Superposition zerstört wird.

Die Messung erfolgt je nach Ausführung des Quantenbits, da es auf mehrere Arten realisiert werden kann. Wenn Licht eine Rolle spielt, kann die Lichtstärke gemessen werden, wobei diese Art von Qubits nur kürzer als 1 Minuten gespeichert werden können. Kernspinquantenbits können durch Messung der Magnetfelder, Ionenfallen mithilfe eines Lasers ausgelesen werden (siehe 2.2).

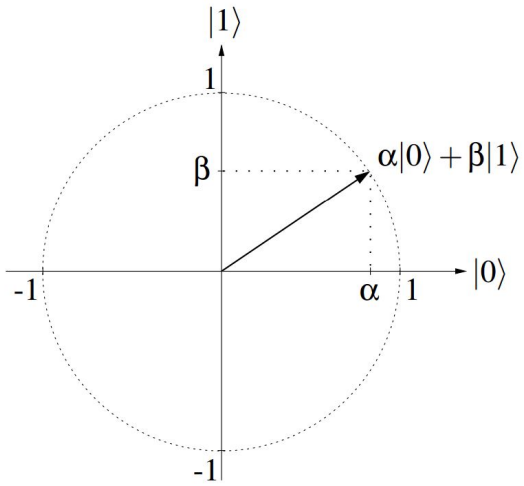

Abbildung 1: Die Superposition als Vektor

1.1.4 Zustände

Bei der Messung eines Quantenbits im Zustand $\alpha|0\rangle+\beta|1\rangle$ wird die Superposition zerstört, wodurch das Quantenbit mit der Wahrscheinlichkeit $|\alpha|^2$ den Zustand $|0\rangle$ und mit der Wahrscheinlichkeit $|\beta|^2$ den Zustand $|1\rangle$ annimmt.

1.1.5 Verschränkung

2 verschränkte Qubits haben die besondere Eigenschaften, dass sie sich unabhäng von der Distanz im genau gleichen Zustand befinden. Bei der Messung des einen Qubits wird die Superpositon beider Qubits zerstört und sie nehmen den selben Wert an, der dann auch beim anderen Qubit gemessen werden kann.

1.1.6 (De)Kohärenz

Kohärenz bedeutet zusammenhängend. Dekohärenz ist ein Phänomen der Quantenphysik, das Kohärenzeigenschaften von Systemen kurzzeitig außer Kraft setzt. Dekohärenzeffekte treten auf, wenn ein geschlossenes System geöffnet wird und mit der Umwelt in Wechselwirkung treten kann, wobei die Zustände beider Systeme irreversibel verändert werden. Im Beispiel mit der Katze, wäre es eine tote oder lebende Katze, und der Betrachter, der nun weiß, ob die Katze tot oder lebendig ist.

1.2 Register

1.2.1 Definition

Ein Quantenregister besteht aus einer Reihe von 2 bis n Qubits und wird angeschrieben als $R = |x_1\rangle|x_0\rangle$ Zur Erklärung ist allerdings eine Beschränkung auf das Minumum von 2 Bits sinnvoll.

1.2.2 Berechnung

Die Berechnung des Zustands eines Quantenregisters mit 2 Bit sieht folgendermaßen aus:

- $|x_0\rangle = \gamma|0\rangle + \gamma_1\rangle, |x_1\rangle = \beta|0\rangle + \beta|1\rangle$
- $R = |x_1\rangle|x_0\rangle$

$= (\beta_0|0\rangle + \beta_1|1\rangle)(\gamma_0|0\rangle + \gamma_1|1\rangle)$

$= \beta_0\gamma_0|0\rangle|0\rangle + \beta_0\gamma_1|0\rangle|1\rangle + \beta_1\gamma_0|1\rangle|0\rangle + \beta_1\gamma_1|1\rangle|1\rangle$

Zur Übersichtlichkeit wird angenommen, dass

- $\alpha_{i,j} = \beta_i\gamma_j$ und
- $|x_1\rangle|x_0\rangle = |x_1x_0\rangle$

sowie die Ziffern vom binären ins dezimale Zahlensystem umgerechnet, wodurch folgende Schreibweise zustande kommt:

$R = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle$

1.2.3 Zustände

per Definition kann sich ein Quantenregister in Zuständen der Form

$$R = \sum_{i=0}^{2^n-1} \alpha_1|i\rangle$$

befinden, wobei die Einschränkung der einzelnen Qubits nicht vergessen werden darf, die für ein Register auf folgende Art erweitert werden kann:

$$\sum_{i=0}^{2^n-1} |\alpha|^2 = 1$$

1.2.4 Begriffe "lokal" und "unitär"

Unitär bedeutet soviel wie Umkehrbar. Eine uniätre Operation kann also rückgängig gemacht werden. Die Voraussetzung dafür ist, dass es nur eine Möglichkeit gibt, auf den Endzustand der Operation zu kommen. Wenn ein Endzustand von 2 verschiedenen Anfangszuständen erreicht werden kann, so ist nicht eindeutig, welcher Zustand der Ausgangszustand war und die Operation ist nicht unitär.

Rechenoperationen können auf einzelne Bits oder ganze Register ausgeführt werden. Da allerdings eine Rechenoperation auf ein ganzes Register auszuführen sehr schnell ziemlich kompliziert werden kann, wird die Operation auf jedes Bit einzeln ausgeführt, wobei das gleiche Gesamtergebnis entsteht. Lokal ist eine Registertransformation, wenn daran für jede Operation konstant viele Qubits beteiligt sind.

2 Hardware

2.1 Gatter & Transformationen

2.1.1 Hadamardtransformation

Definiert ist die Hadamard-Transformation als Matrix $H = 1/\sqrt{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

Um die Hadamard-Matrix verwenden zu können, muss das Qubit mithilfe der unitären Matrix $A = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ folgendermaßen umgerechnet werden: $\binom{\alpha'}{\beta'} = A\binom{\alpha}{\beta} = \binom{a\alpha+b\beta}{c\alpha+d\beta}$

2.1.2 CNOT

Ein CNOT (Controlled Not) hat 2 Eingänge und 2 Ausgänge, wobei der zweite Ausgang den invertierten Wert von 1 ausgibt wird, wenn der erste Eingang auf 1 gesetzt ist und ansonsten das Signal des Eingangs einfach durchleitet.

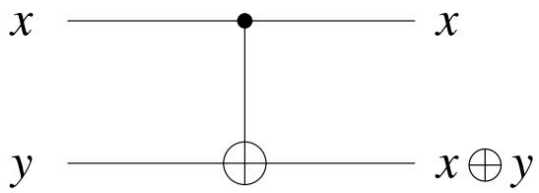

Abbildung 2: CNOT-Gatter

2.2 Architektur

2.2.1 Anforderungen

Definition von David Deutsch 1985: Ein Quantencomputer besteht aus einer Reihe von Quantenbits,

1. die in einen Anfangszustand versetzt werden können,
2. die Information robust speichern,
3. auf die (universelle) Quantengatter anwendbar sind und
4. die gemessen werden können.

2.2.2 Photonen

Die Physiker Ludwig Mach und Ludwig Zehnder entwickelten unabhängig voneinander beide den selben Versuchsaufbau, der heutzutage Mach-Zender-Inferometer genannt wird. Er besteht aus 4 Spiegeln (wovon 2 halbdurchlässig sind), 2 Messgeräten und einem Streifen Papier.

Wenn ein Lichtstrahl in den Aufbau geschickt wird, so wird er über den ersten Spiegel, der halbdurchlässig ist, geteilt in eine gerade und eine um 90° abgelenkte Bahn gelenkt. Nach einem gewissen Abstand befindet sich auf jeder Bahn einer der "normalenSSpiegel, wodurch das Licht jeweils um 90° gelenkt wird und sich die beiden dann an einer Stelle kreuzen, an der der zweite halbdurchlässige Spiegel montiert wird. In eine Bahn wird ein Blatt Papier gehalten. Durch den halbdurchlässigen Spiegel kommt bei beiden Messgeräten gleich viel Licht an. Wird das Blatt Papier entfernt, so kommt es auf einer Bahn zu destruktiven Überlagerungen der Lichtstrahlen zwischen dem letzten Spiegel und dem Messgerät, wodurch bei diesem kein Licht ankommt.

Wenn anstelle eines Lichtstrahles nur einzelne Photonen verwendet werden, zeigt sich der selbe Effekt, obwohl eigentlich keines der Photonen wissen kann, ob der Papierstreifen im Weg ist oder nicht. Und hier kommt wieder die Quantenphysik als Erklärung zum einsatz, da ein Teilchen, wie wir schon wissen, solange es nicht beobachtet wird, in mehreren Zuständen gleichzeitig sein kann. Es kann sich also auf beiden Bahnen gleichzeitig bewegen, bis es gemessen wird, wodurch die Superposition zerstört wird und es nur bei einem Messgerät ankommen kann.

2.2.3 Kernspinresonanz

Kernspinresonanz ist der Name für einen phyiskalischen Effekt der in Form von Wechselwirkung zwischen Atomkernen und Magnetfeldern auftritt. Der Spin eines Moleküls kann durch Magnetfelder ausgerichtet werden, was ausgenutzt wird, um Quantenbits abzubilden und zu speichern. Durch unterschiedliche chemische Eigenschaften der Umgebung kann jedes Bit einzeln angesprochen werden. Mithilfe eines Hauptmagnetfeldes können die Zustande definiert werden, zum Beispiel als: $gleicheAusrichtung = |0\rangle, imrechtenWinkel = |1\rangle$;

2.2.4 Ionenfallen

Ionenfallen sind dazu da, um elektrisch geladene Moleküle oder Atome durch Magnetfelder an ein und der selben Position zu halten, wodurch mit einem gefangenen Ion bis zu 2 Quantenbits abgebildet werden können. Die Abstände zwischen mehreren Ionen liegen im Mikrometerbereich, können durch einen Laser einzeln adressiert werden, aber müssen temperaturmäßig nahe dem absoluten Nullpunkt gehalten werden um sich nicht gegenseitig abzustoßen.

2.3 Umsetzung

2.3.1 D-Wave Systems

D-Wave Systems ist ein 1999 gegründetes amerikanischen Unternehmen, dass seit Jahren damit wirbt, den ersten und einzig wahren Quantencomputer herzustellen. D-Wave Systems hat bereits Geräte an Lockheed-Martin, Google, NASA und die Kalifornische Universität verkauft.

Kritiker sind der Meinung, dass ein echter Quantencomputer erst in vielen Jahren möglich sein wird, falls überhaupt. Ein Google-Test 2014 hat ergeben, dass keine Geschwindigkeitsverbesserung festgestellt werden konnte. Anfang Dezember 2015 scheint durch eine weitere Google-Testreihe allerdings das Gegenteil bewiesen worden zu sein. In einem Test mit großen Bitmengen wurden laut Google Entwicklungsleiter Hartmut Neven eine Reihe herkömmlicher Großrechner zeitmäßig um Längen übertrumpft. [17] [18]

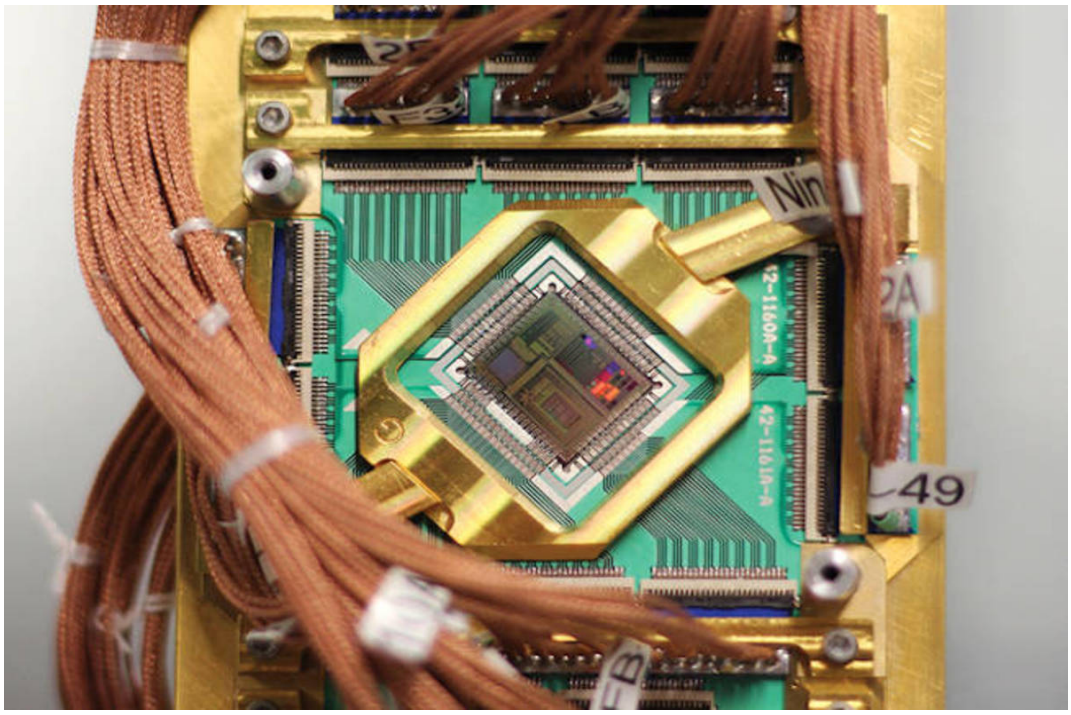

Abbildung 3: D-Wave Systems' Quantenprozessor

Arbeitsweise
Eine Forschungsarbeit an der ETH Zürich hat ergeben, dass der Quantencomputer von D-Wave Systems eigentlich eine Ein-Zweck-Maschine ist, für die ein Problem erst in ein passendes Format, bestehend aus einer großen Anzahl Variablen, gebracht werden muss, damit sie dann in relativ kurzer Zeit ein Optimum ermitteln kann. Sie hat aber weder etwas mit richtigen Quantenrechnern noch mit herkömmlichen Allzweckcomputern zu tun. [19] [20]

Die Arbeitsweise wird auf der offiziellen Webseite von D-Wave Systems erklärt, wobei die Optimierung durch "quantum annealing" (direkt übersetzt: Quanten glühen) als die einzige Art des Quantencomputing dargestellt wird. [21] Desweiteren findet sich auf der offiziellen Webseite eine Auflistung von Anwendungsgebieten, wobei die meisten als Mustererkennung oder Vorraussagen kategorisiert werden können. [22]

Der Prozessor wird um rechnen zu können auf 15°Kelvin gehalten, also knapp über dem absoluten Nullpunkt. Um diese Temperatur zu erreichen, ist der Prozessor in einem stark isolierten und magnetisch abgeschirmten Kasten verbaut.

Kunden

Lockheed-Martin ist vor allem in der Luft- und Raumfahrt tätig. Funktionierende Quantencomputer wären zur Angriffserkennung sowie zur Kommunikation quer durchs Weltall praktisch.

Google ist eine der größten Suchmaschinen der Welt. Bei Suchmaschinen ist das Finden einer optimal zur Eingabe passenden Lösung essentiell. Daher kann Google den D-Wave Quantencomputer auch sehr gut verwenden.

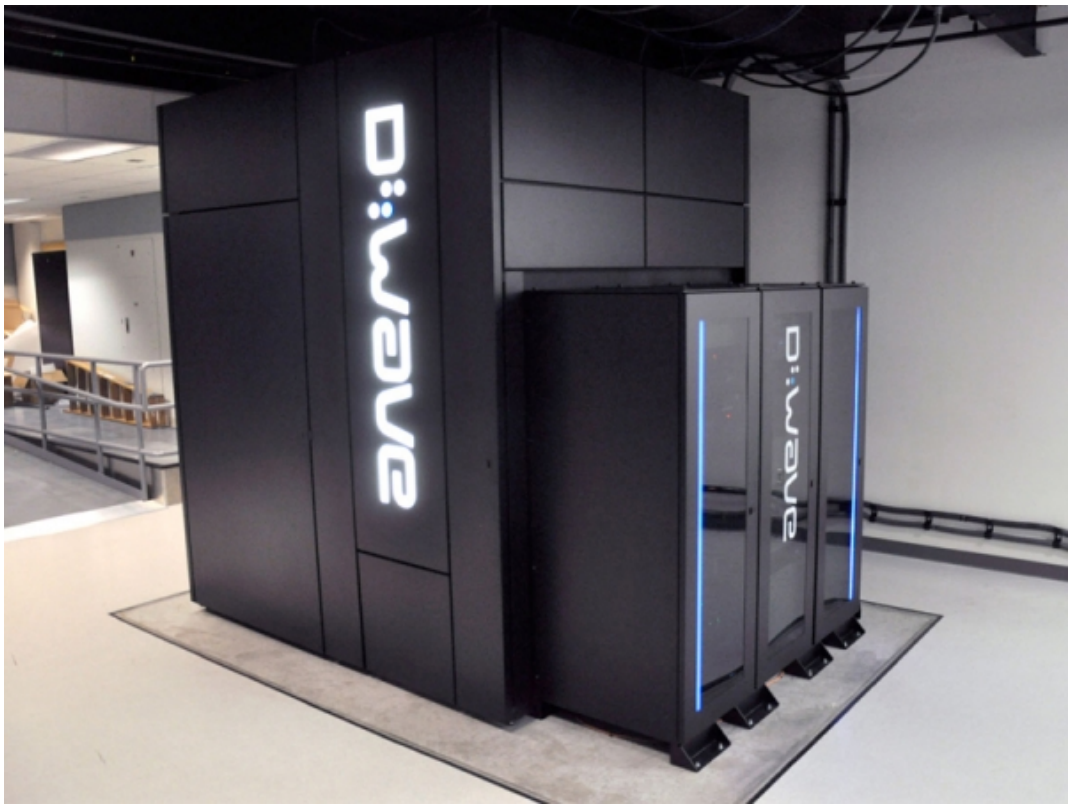

Abbildung 4: D-Wave Systems' Quanten Computer

NASA (ausgesprochen "National Aeronautics and Space Administration") ist ein weltweit bekanntes Weltraumunternehmen. Hier steht natürlich die Datenübertragung in das und aus dem Weltall im Vordergrund, aber auch einfache künstliche Intelligenzen für Alleinflüge unbemannter Raumsonden über Jahrzehnte hinweg.

Die Kalifornische Universität wird sich vorraussichtlich eher auf Wettervorraussagungen und die Erforschung der Quantenphysik selbst spezielisieren.

3 Interkommunikation

3.1 Quantennetzwerke/Kanäle

3.1.1 Klassische vs. Quanten-Kommunikationskanäle

Zu den klassischen Kommunikationskanälen gehören eindeutig Kabel mit 1-n elektrisch leitenden Drähten, über die durch an- und ausschalten einzelne Bits übertragen werden können. Dieser Kommunikationsweg muss nach einer gewissen maximalen Strecke verstärkt werden, was zu verzögerungen führt.

Heutzutage zu klassichen Kommunikationskanälen, aber auch für die Übertragung von Qubits verwendbar, sind Glasfaserkabel. Im Klassischen Sinne wird Licht an und aus-geschalten, für Quantenkommunikation werden einzelne Qubits in form von Photonen übertragen.

Wenn von Quantenkommunikationskanälen gesprochen wird, wird aber meist Verschränkung zwischen 2 Qubits gemeint. Dabei wird unterschieden zwischen rauschfreien und verrauschten Kanälen unterscheiden, wobei sich durch mehrfache Übertragungen mit klassischer Zusatzinformation aus einem verrauschten Kanal Stück für Stück ein rauschfreier Kanal machen lässt.

3.1.2 Photonzählung

Bei der Photonzälung werden zwischen 2 Standorten mit Sichtkontakt einzelne Photonen vom Sender ausgeschickt und vom Empfänger gezählt. Falls kein direkter Sichtkontakt besteht, können die Übertragungen auch über Glasfaserkabel erfolgen.

Praktisch getestet wurde es von Harald Weinfurter im Jahr 2007 mit einer Strecke von 144 km, wofür große Teleskope verwendet werden mussten.

3.2 Quantenteleportation

Bei der Quantenteleportation sind 2 Qubits in Form von Atomen an verschiedenen Orten durch Verschränkung verbunden. Bei einer Messung des Bits auf der "Sender"-Seite wird die Superposition zerstört und beide Qubits nehmen zeitgleich den gleichen Zustand an. Da der Empfänger aber nicht wissen kann, wann der Sender das Bit betrachtet hat, muss über einen herkömmlichen Kanal ein Signal gesendet werden, dass den Empfänger imformiert, dass er sich das Qubit gefahrlos ansehen kann, ohne den Zustand zu verändern. Der zweite Grund für die Notwendigkeit der Übertragung eines Herkömmlichen Bits ist der, dass das Qubit beim Empfänger entweder durch Vertauschung mithilfe der Matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ oder Transformation mithilfe der Matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ gemappt werden muss.

Um allerdings 2 verschränkte Qubits an verschiedene Orte zu bringen, muss entweder ein Quantenkanal bestehen oder schon im Vorfeld eines der verschränkten Qubits vom Sender zum Empfänger oder vom Empfänger zum Sender gebracht werden.

Da die Übertragung des herkömmlichen Bits nicht zeitgleich möglich ist, stellt sich die Frage, in welcher Form eine Quantenteleportation dann schneller ist. Die Antwort hängt mit Quantenregistern zusammen, da auch für ein komplettes Register nur ein einziges herkömmliches Bit übertragen

werden muss.

4 Quantenkryptographie

4.1 One-Time-Pad

Das One-Time-Pad ein symmetrisches Verschlüsselungsverfahren und funktioniert über einen Schlüssel welcher folgende Eigenschaften erfüllen muss: [11]

- er ist mindestens so lang wie die Nachricht
- er ist gleichverteilt zufällig gewählt
- er muss geheim bleiben
- er darf nicht wiederverwendet werden, auch nicht teilweise

Damit erfüllt ein One-Time-Pad Kerckhoffs' Prinzip, welches besagt, dass die Sicherheit eines Kryptosystems nicht von der Geheimhaltung des Verschlüsselungsalgorithmus abhängen darf, sondern lediglich von der Geheimhaltung des Schlüssels.[11]

Es erfüllt daher folgende Kriterien:

- Es gibt genauso viele Schlüssel wie mögliche Chiffate
- Zu jedem Klartext-Chiffrat-Paar gibt es genau einen Schlüssel, der auf den Klartext angewendet das Chiffrat ergibt

Dies bedeuted, dass eine mit einem One-Time-Pad Verschlüsselte Nachricht auch mit beliebig hoher Rechenleistung nicht entschlüsselt werden kann, [2] da auch statistische Methoden, welche bei anderen Verschlüsselungsmethoden dazu verwendet werden können, um die Nachricht zu dechiffrieren, bei einem One-Time-Pad nicht funktionieren.

Beim One-Time-Pad handelt es sich also quasi um ein 'perfektes' Verschlüsselungssystem. Das größte Problem des One-Time-Pads ist es allerdings, den geheimen Schlüssel an beide Parteien zu übertragen, ohne, dass dieser abgefangen wird.

4.2 Quanten-Schlüsselaustausch

Als Quanten-Schlüsselaustausch bezeichnet man Verfahren der Quanteninformatik, die Eigenschaften der Quantenmechanik nutzen, um zwei Parteien eine gemeinsame Zufallszahl zur Verfügung zu stellen. Dies löst nun das größte Problem des One-Time-Pad, nämlich die sichere Übertragung des Schlüssels. Der Quanten-Schlüsselaustausch hat grundlegend nichts mit Quantencomputern zu tun und benötigt auch keinen um durchgeführt zu werden. Erste Theorien wurden bereits 1984 aufgestellt und 2004 ein erster Banktransfer über einen durch einen Quanten-Schlüsselaustausch erstellten Schlüssel getätigt. [3]

Der Quanten-Schlüsselaustausch funktioniert durch das "No-Cloning-Theorem" nach dem Prinzip, einen Angreifer (Man in the Middle) bei der Schlüsselgenerierung zu erkennen, da eine Messung eines quantenmechanischen Zustandes, immer den Wert verändert.

4.2.1 Funktionsweise

Die Informationen werden mittels Photonen übertragen. Photonen können horizontal oder vertikal polarisiert sein (– oder |). Ein horizontal polarisiertes Photon wird von einem vertikalen Filter reflektiert, durch einen horizontalen durchgelassen. Außerdem können Photonen verschiedenartig diagonal polarisiert sein (/, "rechtsdiagonal", oder \, "linksdiagonal"). Diese werden wieder von ihren respektiven Filtern reflektiert, oder durchgelassen. Daraus ergeben sich nun 2 Basen, die +-Basis (- und |) und die ×-Basis (/ und \). Jede Polarisation einer Basis bekommt nun einen anderen binären Wert zugewiesen, wobei die Wahl dabei irrelevant ist, sie muss nur bei beiden Parteien gleich sein.

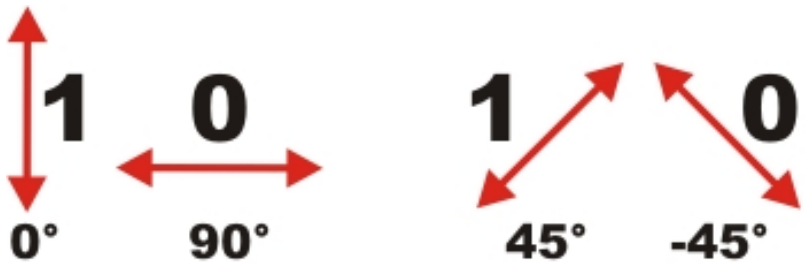

Abbildung 5: Messbasis + (links) und Messbasis × (rechts) [5]

Nun beginnt der Sender der Nachricht (Alice), einzelne Photonen an den Empfänger (Bob) zu verschicken. Beide wählen dabei komplett zufällig, mit gleich großer Wahrscheinlichkeit eine Basis aus. Alice wählt nun weiters, wieder komplett zufällig und gleichverteilt eine Polarisation aus der ausgewählten Basis und sendet so ein Photon an Bob.

Bob wählt nun auch komplett zufällig und gleichverteilt eine Messbasis aus. Wenn Bob nun zufällig die gleiche Basis wie Alice verwendet hat, bekommt dieser ein gültiges Ergebnis (also 0 oder 1), wenn er allerdings eine andere Basis verwendet hat wird das gesendete Photon zu 50% reflektiert oder durchgelassen, ergibt also zu 50% 0 oder 1, diese Messung ist nicht brauchbar und wird später verworfen.

Nachdem Alice genügend Photonen an Bob geschickt hat, müssen beide Parteien noch bestimmen, welche Messwerte für den Schlüssel verwendet werden sollen. Dafür machen Alice und Bob die Wahl ihrer Messbasis öffentlich, jedoch nicht welche Polarisation gesendet bzw. empfangen wurde. Sie veröffentlichen also beide eine Liste mit denen von ihnen gewählten Basen (+ oder ×). Schlussendlich vergleichen beide nun diese Listen, wenn sie bei einer Übertragung die gleiche Basis verwendet haben wird der Wert für den Schlüssel verwendet, ansonsten einfach verworfen. Dadurch werden also ungefähr 50% der gesendeten bits für die Schlüsselgenerierung verwendet.

Photon	Basis	Bit
1	+	**1**
2	×	1
3	+	**0**
4	+	1
5	×	**1**
6	+	**0**
7	×	**0**
8	×	1

Tabelle 1: Beispielübertragung Alice

Photon	Basis	Bit
1	+	**1**
2	+	0
3	+	**0**
4	×	1
5	×	**1**
6	+	**0**
7	×	**0**
8	+	0

Tabelle 2: Beispielmessungen Bob

In diesem Beispiel sind die **Fett** hervorgehoben Basen gleich, also wäre der generierte Schlüssel von Alice und Bob 10100; jeweils Photon 1, 3, 5, 6, 7 werden verwendet, die anderen werden verworfen.

4.2.2 Abhörsicherheit

Bei dem obigen Verfahren ist es nun auch möglich Abhörsicherheit zu garantieren, sodass eine dritte Person (Eve) sich nich zwischen die Kommunikation schalten und den Schlüsselaustausch abfangen kann.

Um zu versuchen die Kommunikation abzufangen kann Eve sich zwischen Bob und Alice schalten. Allerdings muss Eve, genauso wie Bob zuerst das gesendete Photon messen und wählt dafür eine zufällige Basis. Eve muss allerdings sofort wieder ein neues Photon an Bob senden, in 50% der Fälle wählt Eve zur Messung jedoch die falsche Basis und sendet dadurch ein falsches bit an Bob. Diesen durch Eve verursachten Fehler können Alice und Bob nun bemerken, wenn sie die gleiche Basis gewählt haben, da sie bei gleicher Wahl immer eindeutige Ergebnisse erhalten sollten. Außerdem kann Eve so nie den kompletten Schlüssel bekommen, da sie das bit an einer Stelle bei der sie eine falsche Basis verwendet hat, nicht herausfinden kann.

Basis Alice/Bob	Basis Eve	Empfang Bob	Übereinstimmung Alice und Bob
+ +	+	Eindeutig	100%
+ +	×	Zufall	50%
× ×	+	Eindeutig	50%
× ×	×	Zufall	100%

Tabelle 3: Möglichkeiten der Übertragung mit Eve als Man-in-the-Middle [5]

Insgesamt gibt es, wenn Alice und Bob die gleiche Basis gewählt haben, in 25% der Fällen falsche Messergebnisse. Um Eve also zu entdecken müssen Bob und Alice nach der erfolgreichen Übertragung einen Abgleich von einigen (nicht allen!) Werten, bei denen sie die gleiche Basis verwendet haben durchführen, gibt es dort über 25% Diskrepanz zwischen den Werten, ist sehr Wahrscheinlich ein Man-in-the-Middle Angriff durchgeführt worden.

4.3 Post-Quanten-Kryptographie

Ein besonderer Teil der Quantenkryptographie stellt die Post-Quanten-Kryptographie dar. Diese behandelt sich mit der Tatsache, dass alle modernen asymmetrischen Verschlüsselungsverfahren durch die Entwicklung eines Quantencomputers unbrauchbar werden.

Die Sicherheit der momentanen Verschlüsselungsverfahren basiert auf den 3 komplizierten mathematischen Problemen:

- Faktorisierungsproblem
- Diskreter-Logarithmus Problem
- Elliptic Curve Cryptography Problem

Die obigen Probleme können durch einen Quantencomputer mit Shor's Algorithms innerhalb kürzester Zeit gelöst werden. (siehe 5.3).

Damit also momentane Kommunikation auch in Zukunft nicht entschlüsselt werden kann, benötigt man auch jetzt schon Verschlüsselungsverfahren, welche auch Quantencomputer nicht knacken können. [14]

4.3.1 Post-Quanten-Verschlüsselungsalgorithmen

Die aktuelle Post-Quanten-Kryptographie Forschung fokussiert sich auf 6 Bereiche: [14]

- **Lattice-based cryptography**
- **Multivariate cryptography**
- **Hash-based cryptography**
- **Code-based cryptography**
- **Supersingular elliptic curve isogeny cryptography**
- **Symmetric key quantum resistance**

4.3.2 Symmetrische Schlüssel Resistenz

Symmetrische Schlüssel mit ausreichender Länge, sind bereits heute immun gegen Angriffe von Quantencomputern. [4] Zwar können Quantencomputer auch effektivere Brute-Force Angriffe auf einen symmetrischen Schlüssel durchführen, allerdings wird dieser nicht exponentiell schneller, wie bei der asymmetrischen Verschlüsselung. Darum reicht es einfach, die Schlüssellange zu erhöhen.

5 Quantenalgorithmik

5.1 Besonderheiten und Unterschiede zu "klassischer" Algorithmik

Ein "klassischer" (nicht quanten) Algorithmus ist eine endliche Sequenz von Maschineninstruktionen, wo jede Instruktion auf einem klassischen Computer ausgeführt wird. Ähnlich sind Quantenalgorithmen eine endliche Sequenz von Quanteninstruktionen, welche auf einem Quantencomputer ausgeführt werden. Jedoch kann ein Quantencomputer auch klassische Algorithmen ausführen. [15]

Die Besonderheiten von Quantenalgorithmen liegen in der Verwendung von Qubits (siehe **??**), welche quantenmechnische Prinzipien wie die Quantenteleportation und die Superposition verwenden. Zwar gibt es bereits einige entwickelte Quantenalgorithmen, allerdings ist dieses Gebiet noch nicht sehr gut erforscht.

5.2 Quantenalgorithmik Übersicht

5.2.1 Deutsch-Josza Algorithmus

Dieser Algorithmus kann zum Lösen sogenannter Blackbox-Probleme verwendet werden, für die normale Computer exponentiell viele Zugriffe, ein Quantencomputer allerdings nur einen bräuchte. Hierbei wird z.B. das Ergebnis einer Funktion f darauf überprüft, ob alle Eingaben konstant 0 als Ergebnis liefern, oder ob beispielsweise die eine Hälfte 0 und die andere Hälfte 1 liefert. [15]

5.2.2 Simons's Algorithmus

Dieser Algorithmus dient auch zur exponentiell schnelleren Lösung von Blackbox-Problemen und war Vorbild für Shor's Algorithmus. [15]

5.2.3 Quanten Phasen Näherungs-Algorithmus

Aus der englischen Wikipedia: [15]

> *The quantum phase estimation algorithm is used to determine the eigenphase of an eigenvector of a unitary gate given a quantum state proportional to the eigenvector and access to the gate.*

Der Algorithmus wird außerdem oft als Unterfunktion in anderen Quantenalgorithmen verwendet.

5.3 Shor's Algorithmus

Shor's Algorithmus ist ein Quantenmechanischer Algorithmus aus dem mathematischen Gebiet der Zahlentheorie. Er dient dabei zur Ermittlung eines nicht trivialen Teilers und zählt damit zu den Faktorisierungsalgorithmen. Für die Faktorisierung einer Zahl n benötigt ein Quantencomputer mindestens $\log n$ Qubits.

Shor's Algorithmus hat folgende Eigenschaften: [12]

- Eingabe: zusammengesetzte Zahl n
- Ausgabe: ein nicht trivialer Faktor von n
- Laufzeit: $O((\log n)^3)$ Gatteroperationen

Shor's Algorithmus läuft also in polynomieller Zeit und ist dem besten bis jetzt bekannten klassischen Faktorisierungsalgorithmus, dem Zahlkörpersieb, welches mit sub-exponentieller Zeit läuft weit überlegen. Der Zahlenkörpersieb Algorithmus hat eine ungefähre Laufzeit von $O(e^{1.9(\log n)^{1/3}(\log\log n)^{2/3}})$. [6]

Shor's Algorithmus kann man Grundlegend in 2 Teile teilen: einen Klassischen- und einen Quantenteil. Der Klassische Teil wird zur Reduzierung des Problems verwendet, der Quantenteil dient dann zu effektiven Lösung des Restproblems.

5.4 Grover's Algorithmus

Grover's Algorithmus ist ein Quantenalgorithmus zur Suche in einer unsortierten Datenbank mit N Einträgen. Er löst dabei das Problem mit $O(\sqrt{N})$ Schritten und $O(\log N)$ Speicherbedarf.

Die prinzipiell schnellstmögliche Suche in einer unsortierten Datenbank auf einem klassischen Computer, die Linearsuche benötigt dabei $O(N)$ Rechenschritte. Durch Grover's Algorithmus ergibt sich eine beträchtliche quadratische Beschleunigung gegenüber der Linearsuche.

5.5 Quanten Programmierung

Es gibt bereits einige Quantenprogrammierprachen, welche bereits zum Ausdruck von Quantenalgorithmen verwendet werden können. Diese können grob in 2 Gruppen von Quantenprogrammiersprachen eingeteilt werden: Imperative und Funktionale.

Die 2 bekanntesten der ersten Gruppe sind QCL [7] und LanQ [8].

5.5.1 QCL - Quantum computing language

QCL ist eine Erweiterung von C; Die Syntax ist identisch mit der von C, mit einigen Quantenmechnanischen Erweiterungen. Außerdem kann "klassischer" und quanten - Code in einem Programm zusammen verwendet werden.

Der grundlegendste quanten-Datentyp in QCL ist das qureg (Quanten Register). Es ist quasi ein Array von qubits: [10]

```
1 qureg x1[2]; // 2-qubit quantum register x1
  qureg x2[2]; // 2-qubit quantum register x2
  H(x1);       // Hadamard operation on x1
  H(x2[1]);    // Hadamard operation on the first qubit of the register x2
```

Außerdem kann, da die Quantenoperationen nur simuliert werden, der Status des Programms abgerufen werden: [10]

```
qcl> dump
: STATE: 4 / 32 qubits allocated, 28 / 32 qubits free
0.35355 |0> + 0.35355 |1> + 0.35355 |2> + 0.35355 |3>
+ 0.35355 |8> + 0.35355 |9> + 0.35355 |10> + 0.35355 |11>
```

Eine der wichtigsten Funktionen der Sprache ist die Möglichkeit Operationen und Funktionen zu definieren, mit denen Quanteninformation manipuliert werden können. Zum Beispiel: [10]

```
operator diffuse (qureg q) {
    H(q);                   // Hadamard Transform
    Not(q);                 // Invert q
    CPhase(pi, q);          // Rotate if q=1111..
    !Not(q);                // undo inversion
    !H(q);                  // undo Hadamard Transform
}
```

Literatur

[1] Gilbert Brands, *Einführung in die Quanteninformatik: Quantenkryptografie, Teleportation und Quantencomputing*, 2011, ISBN 9783642206474.

[2] Johannes A. Buchmann, *Introduction to Cryptography*, 2001, 4. edition

[3] Anton Zeilinger, *Bank Transfer via Quantum Cryptography Based on Entangled Photons*, 2004, online: `https://web.archive.org/web/20150211032846/http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf`; zuletzt abgerufen 28. März 2016.

[4] U.S. Department of Commerce, *Quantum Resistant Public Key Cryptography: A Survey*, 2013, online: `http://www.nist.gov/manuscript-publication-search.cfm?pub_id=901595`; zuletzt abgerufen 31. März 2016.

[5] Artikel mit Interaktiven Experimenten zu *Quanten Schlüsselaustausch*, `http://www.didaktik.physik.uni-erlangen.de/quantumlab/`; zuletzt abgerufen 28. März 2016.

[6] Eric Weisstein, *Number Field Sieve* (dt. Zahlenkörpersieb), 2016, online: `http://mathworld.wolfram.com/NumberFieldSieve.html`; zuletzt abgerufen 31. März 2016.

[7] *QCL - A Programming Language for Quantum Computers*, online: `http://tph.tuwien.ac.at/~oemer/qcl.html`; zuletzt abgerufen 31. März 2016.

[8] *LanQ – a quantum imperative programming language*, online: `http://lanq.sourceforge.net` zuletzt abgerufen 31. März 2016.

[9] You-Tube Video über Basics von Quantencomputern, `https://www.youtube.com/watch?v=JhHMJCUmq28`; zuletzt abgerufen 28. März 2016.

[10] Wikipediaartiekl zu *Quantenprogrammierung*, `https://en.wikipedia.org/wiki/Quantum_programming#cite_note-2`, zuletzt abgerufen 31. März 2016.

[11] Wikipediaartikel zu *One-Time-Pad*, `https://de.wikipedia.org/wiki/One-Time-Pad`; zuletzt abgerufen 28. März 2016.

[12] Wikipediartikel zu *Shor's Algorithmus* `https://de.wikipedia.org/wiki/Shor-Algorithmus`; zuletzt abgerufen 31. März 2016.

[13] Wikipediaartikel zu *Grover's Algorithmus* `https://de.wikipedia.org/wiki/Grover-Algorithmus`; zuletzt abgerufen 31. März 2016.

[14] Wikipediaartikel zu *Post-Quanten-Kryptographie*, `https://de.wikipedia.org/wiki/Post-Quanten-Kryptographie`; zuletzt abgerufen 28. März 2016.

[15] Wikipediaartikel zu *Quantenalgorithmen*, `https://en.wikipedia.org/wiki/Quantum_algorithm`; zuletzt abgerufen 28. März 2016.

[16] Buch *Quantum Computing Verstehen* Matthias Homeister 2. Auflage, 2008 ISBN 978-3-8348-0436-5 online: `http://catalogplus.tuwien.ac.at/primo_library/libweb/action/display.do?tabs=detailsTab&doc=UTW_aleph_acc000449741` zuletzt aufgerufen: 19.11.2015

[17] online: https://www.wired.de/collection/latest/der-quantencomputer-d-wave-scheint-zu-fun zuletzt aufgerufen: 29.03.2016

[18] online: http://venturebeat.com/2015/12/08/google-says-its-quantum-computer-is-more-than- zuletzt aufgerufen: 29.03.2016

[19] online: http://www.spektrum.de/news/daempfer-fuer-den-d-wave-quantencomputer/1296152 zuletzt aufgerufen: 29.03.2016

[20] online: http://motherboard.vice.com/read/google-claims-its-d-wave-quantum-computer-is-th zuletzt aufgerufen: 29.03.2016

[21] online: http://www.dwavesys.com/quantum-computing zuletzt aufgerufen: 29.03.2016

[22] online: http://www.dwavesys.com/quantum-computing/industries zuletzt aufgerufen: 29.03.2016

[23] Piled Higher and Deeper (PHD Comics), 2013, *Quantum Computers Animated* online: https://www.youtube.com/watch?v=T2DXrs0OpHU zuletzt aufgerufen: 29.03.2016

Abbildungsverzeichnis

Tabellenverzeichnis