Humboldt Universität zu Berlin
Institut für Informatik

Proseminar Kryptografische Algorithmen und Protokolle

Quanten-Kryptografie und Quanten-Computer

Oswald Berthold
<oberthold@informatik.hu-berlin.de>

Berlin, 1. März 2008, v0.11

Inhaltsverzeichnis

1 Über dieses Dokument

Dieses Dokument entstand im Rahmen des Proseminars “Kryptografische Algorithmen und Protokolle” das im Wintersemester 2005/06 am Institut für Informatik der Humboldt Universität zu Berlin abgehalten wurde. Es ist sicher in keiner Weise vollständig oder fehlerfrei. Hinweise zu Fehlern, Kritik und Anregungen sind willkommen. Die Arbeit entstand bei der Erarbeitung eines Referats daher ist der Stil an einigen Stellen stichworthaft und bedarf weiterer Ausarbeitung.

1.1 20080225

Verschiedene Korrekturen auf freundlichen Hinweis von Dr. Ralph Wernsdorf.

2 Einleitung

Definitionen

Quantum Computation and Quantum Information is the study of the information processing tasks that can be accomplished using quantum mechanical systems. [1, S. 1]

Jegliches Rechnen unter Ausnutzung spezifischer quantenmechanischer Effekte: *Verschränkung*, *Superposition* (Parallelität), *Komplementarität* (Unschärfe).

2.1 Motivation

Computing: Besseres Verstehen der Quantenmechanik, Simulation von Quantensystemen.

Kryptografie: Praktischer Nutzen (Nachrichtendienste, Wirtschaft), Ausweitung der klassischen kryptografischen Motivation.

Feynmann: *Physics is like sex: sure, it may give some practical results, but that’s not why we do it.*

2.2 Kurze Geschichte des Quantenrechnens

Was ist überhaupt ein Quant? Diskretes Bauteil der Realität. Physikalische Prozesse und Energieniveaus treten scheinbar quantisiert auf, d.h. sie können nur diskrete Werte annehmen, z.B ein Photon (Quant des Lichts). Ende des 19. und Anfang des 20. Jhdts. häuften sich die Hinweise auf eine solche Quantisierung physikalischer Phänomene. (Max Planck, Welle-Teilchen Dualismus, Stern-Gerlach Experiment).

Beitragende Teilgebiete zur Entwicklung der Idee des “Quantenrechnen”s sind sicher die Quantenmechanik (offensichtlicherweise), die Informatik, die Informationstheorie sowie die Kryptografie. Wegen dieser Diversität hat es erstaunlich lange gedauert bis sich die Idee expliziert etabliert hatte, eigentlich erst zu Beginn der 1980er Jahre. Im folgenden sollen kurz die Schlüsselprobleme innerhalb dieser Teilgebiete angeführt werden.

2.2.1 Physik

- Krise der (klassischen) Physik zu Beginn des 20. Jhdts. deren Höhepunkt in den 1920er Jahren erreicht wurde. Es gab theoretische Voraussagen von *Absurditäten* wie der Ultravioletten Katastrophe, unendliche Energiemengen und in den Atomkern stürzende Elektronen.

- Massgeblich beteiligt an der Entwicklung der physikalischen Quantentheorie waren u.a. Max Planck (1900, Plancksches Wirkungsquantum), Albert Einstein (1905,), Niels Bohr (1913), Louis de Broglie (1924, Materiewellen), Werner Heisenberg (1925, Matrizenmechanik, 1927 Unschärferelation ($\triangle x \triangle p \geq \hbar$)), Erwin Schrödinger (1925, Wellenmechanik), Paul Dirac (1927-1930 "Principles of Quantum Mechanics", Äquivalenz von Matrizen- und Wellen-mechanik, Bra Ket Notation, $QM \cup SRT$), Wolfgang Pauli (Spin, Ausschliessungsprinzip), Max Born (statist. Interpret. der Wellenfunktion), John v. Neumann (mathematische Fundierung der Quantenmechanik im Hilbert Raum).

- Aussagen der Quantentheorie werden meist als gegenintuitiv aufgenommen da sie nicht unseren Wahrnehmungen auf makrospkopischer Ebene entsprechen. (z.B. die gleichzeitige Überlagerung von (Quanten)-Zuständen eines Objekts).

- Kopenhagener Deutung: Diese in der Hauptsache von N. Bohr und W. Heisenberg formulierte Interpretation der Quantentheorie teilt die quantenmechanischen Vorgänge in die *unitäre* Entwicklung der Wellenfunktion nach der Schrödingergleichung und den unumkehrbaren Vorgang der Messung. Realität muss nicht notwendigerweise als quantisiert betrachtet werden aber die Wahrnehmung (Messung) quantisiert diese. Letztlich kann sich die Physik aber nur mit den messbaren Grössen beschäftigen. Eine andere Interpretation ist die Viele-Welten Theorie.

- zum ersten Mal gelang es um 1970 ein einzelnes Quantensystem komplett zu kontrollieren.

- Um 1980 wurde die Idee der superluminalen Informationsübertragung formuliert, die den Aussagen der Relativitätstheorie scheinbar widerspricht (Quantenteleportation). Der Ausweg in diesem Sinne ist die Erklärung dass z.B. ein 2-Qubit System an 4 verschiedenen Basen gemessen werden kann, diese müssen bekannt sein auf Empfängerseite und genau diese klassische Information muss auch übertragen werden, allerdings ist diese Kommunikation wieder durch die Lichtgeschwindigkeit begrenzt.

2.2.2 Informatik

- Die Arbeit von Alan Turing und Anderen (Abstraktes Maschinenkonzept, Klasse der auf physikalischen Geräten berechenbaren Algorithmen / Funktionen), J. v. Neumann und Andere (elektronische Realisierung), Erfindung des Transistors 1947 durch Bardeen, Brattain, und Shockley.

- Starke Church-Turing These [1, S. 5]

- Die ersten asymmetrischen Kryptoverfahren wurden im 20. Jahrhundert entwickelt. Dadurch erhoehte sich die praktische Bedeutung von Primzahltests wesentlich. Die Problemstellung heisst PRIMES. Der einfachste deterministische solche Test ist die Probedivision, das Durchprobieren aller Zahlen zwischen 2 und $\sqrt{n}$ mit n als Primzahlkandidat. Agrawal, Kayal und Saxena konnten 2002 mit einem deterministischen Algorithmus polynomialer Laufzeit zeigen, dass PRIMES in P liegt.

- Die Sicherheit asymmetrischer Verschlüsselungsverfahren steht im Zusammenhang mit Faktorisierungsverfahren, genauer beruht sie darauf, dass die bekannten Verfahren zur Faktorisierung sehr grosser Zahlen, z.B. in der Grössenordnung von 300 Dezimalstellen nicht effizient genug sind, also $N = p \cdot q$ mit $p, q \in \mathbb{P}$ als Teil des öffentlichen Schlüssels praktisch nicht faktorisierbar ist.

- Als scheinbar erster betrachtete Paul Benioff ca. 1980 die Beziehung zwischen Rechnen und Quantenmechanik. Er fragte nicht nach Komplexität aber zeigte, dass umkehrbare unitäre Evolution genügt um eine Turingmaschine auf Quantengrundlage zu realisieren.

- R. Feynmann überlegte 1982,1986 ob Quantenmechanik als Grundlage des Rechnens mächtiger sein könnte als eine Turingmaschine, vor allem im Zusammenhang mit der Komplexität der Simulation quantenmechanischer Systeme.

- David Deutsch stellte 1985 als erster explizit die entscheidende Frage ob Quantenrechner mächtiger sein könnten als klassische Computer und definierte die Quantenturingmaschine und Quantenschaltkreise.

- Ein offenes Problem ist, ob der Universelle Quanten Computer tatsächlich ein beliebiges physikalisches System effizient simulieren kann.
- Peter Shor's Algorithmus (1994, 1995, s.u.): Primfaktorisierung und diskreter Logarithmus. Problem: Es ist nicht bewiesen dass Primfaktorisierung nicht effizient auf einem klassischen Computer lösbar ist. Grover's Suchalgorithmus, s.u.

2.2.3 Informationstheorie

- Claude Shannon 1948: *Mathematische Theorie der Kommunikation* mit zwei Schlüsselsätzen: Noiseless Channel Coding Satz (Speichern) und Noisy Channel Coding Satz (Übertragung).
- Ben Schumacher 1995: Entwickelt analog eine Quanteninformationstheorie bei deren Erarbeitung das Qubit entstand. Allerdings gibt es (noch) kein Analogon zum Noisy Channel Coding Theorem.
- Führte zur Entwicklung der Quantenfehlerkorrektur und z.B. des Superdense Coding (2 klassische Bits werden in ein Qubit gepackt und übertragen) was hier aber nicht weiter betrachtet werden wird.
- Experimentelle Ergebnisse zum verteilten Quantenrechnen, allerdings noch mit vielen Restriktionen und wenigen praktischen Anwendungen.

2.2.4 Kryptografie

In der Kryptografie sind im Zusammenhang mit den Möglichkeit des Quantencomputing zwei Ideen besonders wichtig.

- Die Schlüsselübertragung oder Quantum Key Distribution. Mit verschränkten Teilchen ist es möglich einen Schlüssel für symmetrische Verschlüsselung sicher zu übertragen. Dazu später noch mehr.
- Es können u.a. RSA-Schlüssel geknackt werden, wenn sich die Primfaktorisierung mit einem Quantenalgorithmus effizient lösen lässt [3].

3 Quantencomputer

Hilbert Space is a big Space.

3.1 Hilbert-Raum, Basisvektoren

Der Hilbert-Raum kann als Quantenmechanische Erweiterung des klassischen Phasenraumes betrachtet werden.

Er ist ein n-dimensionaler komplexer Vektorraum der ein n-elementiges physikalisches System vollständig beschreibt, d.h. ein Element des Raumes, ein *Zustandvektor* beschreibt das System zu einem Zeitpunkt t.

Die Hamilton-Funktion der Quantenmechanik gibt eine Masszahl der Gesamtenergie eines Systems.

Beispiel: Wir betrachten ein System mit n-Komponenten:

Klassische Physik benötigt trivialerweise n Bit um ein n-Bit System zu beschreiben, die Quantenphysik benötigt aber 2^n komplexe Zahlen, also der Zustand ist ein Punkt in einem 2^n-dimensionalen Vektorraum, der Zustandsvektor, der als

$$\sum_{i=0}^{2^n-1} a_i |S_i\rangle$$

geschrieben werden kann, wobei a_i eine komplexe Wahrscheinlichkeitsamplitude mit $\sum_i |a_i|^2 = 1$ und jedes $|S_i\rangle$ Basisvektor des Hilbertraumes. Für jede der 2^n klassischen Konfigurationen der Bits gibt es einen Basisvektor z.B. $|0010...1\rangle$. Dieses exponentielle Wachstum in der Grösse des System ist der Grund für die Probleme bei der Simulation von Quantensystemen auf klassischen Rechnern.

3.2 Qubit

Ein Qubit (Quantenbit) ist ein Quantensystem mit zwei möglichen Zuständen die sich in Überlagerung (Superposition) befinden können. Das Qubit als mathematisches Objekt ist unabhängig von einer physikalischen Realisierung.

1-Qubit System

Ein Qubit ist die Linearkombination

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2 \quad \alpha, \beta \in \mathbb{C}$$

mit $|\psi\rangle \in V \subseteq \mathbb{C}^2$ und $B = \{|0\rangle, |1\rangle\}$ eine orthonormale Basis des Vektorraums. Die Basisvektoren lassen sich auch schreiben als $|0\rangle = \binom{1}{0}$ und $|1\rangle = \binom{0}{1}$. Eine *Messung* ergibt immer $|0\rangle$ oder $|1\rangle$ mit $P(|0\rangle) = |\alpha|^2$, $P(|1\rangle) = |\beta|^2$ und $|\alpha|^2 + |\beta|^2 = 1$ wie oben (Hilbertraum) schon kurz beschrieben. α und β heissen *Wahrscheinlichkeitsamplituden* und können nicht direkt ermittelt werden.

Wenn $|\psi\rangle = (a_1, a_2, ..., a_n)^T$ dann ist $\langle\psi| = (\overline{a_1}, ..., \overline{a_n})$ mit $\overline{a_i}$ = komplex konjugiert a_i.

Beispiel:

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = |+\rangle$$

Dieses Qubit ergibt bei Messung in der Hälfte der Fälle $|0\rangle$ und sonst $|1\rangle$.

$|+\rangle$ stellt zusammen mit $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ eine weitere Basis des Vektorraums dar und es kann von einer Basis in die andere übergegangen werden.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$$

Physikalischen Realisierungen von Qubits: Jedes physikalischen System das zwei unterscheidbare Zustände annehmen kann z.B. Polarisierung eines Photons, Ausrichtung der Kernspins in einem uniformen Magnetfeld, 2 Zustände des Elektronenorbits.

Durch die Darstellung von α, β durch Winkel und Betrag und Anwendung der Euler'schen Formel ergibt sich eine weitere Darstellung eines Qubit,

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right), \theta, \varphi, \gamma \in \mathbb{R}$$

Der Term vor der Klammer kann aus physikalischen Gründen weggelassen werden. Dann definieren θ und φ einen Punkt auf einer 3-dimensionalen Einheitskugel, der Blochspähre.

2-Qubit System

Im Fall eines 2-Qubit Systems ist die Basis

$$B_2 = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

wobei $|00\rangle = (1,0,0,0)^T$, $|01\rangle = (0,1,0,0)^T$, $|10\rangle = (0,0,1,0)^T$, $|11\rangle = (0,0,0,1)^T$

Ein Zustandsvektor der 2 Qubits beschreibt ist dann

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

d.h. die Wahrscheinlichkeit $|x\rangle$ zu messen beträgt $|\alpha_x|^2$ und es muss wieder die Normalisierungsbedingung gelten: $\sum_{x\in\{0,1\}^2}|\alpha_x|^2 = 1$.

Interessant wird es wenn nur eines der beiden Qubits gemessen wird, z.B. das erste. Die Wahrscheinlichkeit dass das erste Qubit 0 ist, ist dann $P(|00\rangle) + P(|01\rangle) = |\alpha_{00}|^2 + |\alpha_{01}|^2$ also ist der Zustand nach der Messung

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

wobei der Nenner für die Renormalisierung der Wahrscheinlichkeitsamplituden α_{00}, α_{01} sorgt.

Ein wichtiger 2-Qubit Zustand in diesem Zusammenhang ist der *Bell*-Zustand oder das EPR-Paar,

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Wenn das erste Qubit gemessen wird und mit Wahrscheinlichkeit $\frac{1}{2}$ 0 sowie mit Wahrscheinlichkeitt $\frac{1}{2}$ 1 ergibt ist der Post-Messungs Zustand $|\varphi'\rangle = |00\rangle$ respektive $|\varphi'\rangle = |11\rangle$. Das heisst eine Messung des zweiten Qubits gibt immer das gleiche Ergebnis wie die Messung des ersten Qubits. Die Messausgange sind korreliert. Es gibt noch 3 weitere Bellzustände, mehr dazu weiter unten denn die Bellzustände sind notwendig für die Erklärung der Quantenteleportation (und des Superdense Coding).

3.3 Quantenschaltkreise

Quantenschaltkreise führen Änderungen an den Quantenzuständen, also den Qubits, aus. Sie können als unitäre Transformationen behandelt werden. Der unitäre Charakter und die daraus folgende Reversibilität ergeben sich aus den Gesetzen der Quantenmechanik (Schrödingergleichung, wie oben schon erwähnt).

Eine Matrix A mit komplexen Elementen ist unitär genau dann wenn ihre komplex-konjugierte und Transponierte gleich ihrer Inversen ist, also $(A^*)^T = A^{-1}$ oder $A(A^*)^T = (A^*)^T A = I$.

1-Qubit Gatter
auch Operationen.
Klassisch ist das einzige nichttriviale 1-Bit Gatter das NOT Gatter mit

$$0 \to 1$$
$$1 \to 0$$

Für ein Quanten NOT Gatter würde das bedeuten

$$|0\rangle \to |1\rangle$$
$$|1\rangle \to |0\rangle$$

Was passiert im Fall einer Superposition? Da sich die Operation linear verhält wird ein Zustand

$$|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$$

zu

$$|\psi_2\rangle = \alpha|1\rangle + \beta|0\rangle$$

Die Matrixdarstellung lässt sich so interpretieren dass jede Zeile für einen bestimmten Eingangsbasisvektor die Koeffizienten für die Ausgangsbasisvektoren angibt, also verbos notiert am Beispiel von NOT

	$\|0\rangle$	$\|1\rangle$
$\|0\rangle$	0	1
$\|1\rangle$	1	0

Andere 1-Qubit Quantengatter

- X,Y,Z-Gatter wobei das X-Gate gleich dem NOT-Gate ist. Die Matrixdarstellung der NOT-Operation auf einem Qubit ist

  $$X = NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

  X,

  $$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

  sind die sog. Pauli-Matrizen.

- H-Gatter, Hadamard
  auch $\sqrt{NOT}$ mit der Matrixdarstellung

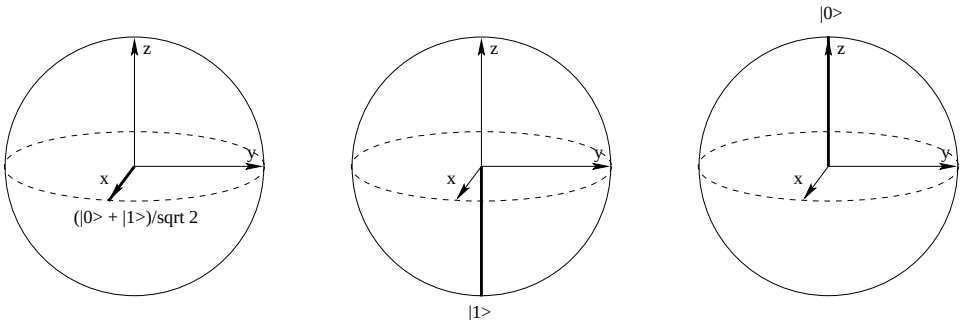
  $$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Beispiel zur Anwendung der Hadamard Operation auf ein Qubit

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} =$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{|0\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}}$$

Beispiel Veranschaulichung auf der Bloch-Sphäre: H angewandt auf $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ ergibt eine Rotation um 90°um die y-Achse, dann 180°um der x-Achse.



Es stellt sich die Frage ob es Einschränkungen gibt welche Matrizen gültige 1-Qubit Operationen darstellen. Die Einschränkung ist genau die Unitariätseinschränkung, die sicherstellt dass die Summe der Quadrate der Beträge der Wahrscheinlichkeitsamplituden nach dem Anwenden des Gates 1 ist. D.h. es gibt (unendlich) viele nicht-triviale 1-Qubit Gatter.

Es gibt eine allgemeine dekomponierte Darstellung aller unitären 2×2 Matrixen (ein Produkt von Rotationen) auf die hier aber nicht näher eingehen werde.

Multi-Qubit Gatter

auch Transformationen.

Es gibt keine Quantengatter die direkt den klassischen AND, OR, XOR Verknüpfungen entsprechen da diese nicht eindeutig umkehrbar sind. Allerdings lässt sich zeigen dass zu jedem klassischen Schaltkreis ein äquivalenter umkehrbarer Schaltkreis konstruiert werden kann.

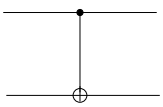
- CNOT, wird an anderer Stelle auch XOR genannt, allerdings entpsricht es nicht einem klassischen XOR mit 2 Eingängen und einem Ausgang

  Das CNOT Gatter hat zwei Eingänge, den Controleingang und den Targeteingang. Wenn das Controlqubit auf $|0\rangle$ gesetzt ist passiert mit dem Targetqubit nichts, wenn das Controlqubit auf $|1\rangle$ gesetzt ist wird das Targetqubit invertiert was einer Addition modulo 2 bzw. der XOR Operation entspricht.

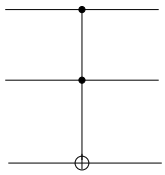
  Die Matrixdarstellung ist

$$U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

  das Schaltbild ist



- Das Toffoli Gatter besitzt drei Eingänge und drei Ausgänge. Der dritte Eingang wird genau dann invertiert wenn die Eingänge 1 und 2 beide $|1\rangle$ sind. Das Schaltbild ist



Die Matrixdarstellung ist

$$U_{Tof} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

- Das Fredkin Gatter vertauscht die Eingänge 1 und 2 wenn der dritte Eingang $|1\rangle$ ist. Die Matrixdarstellung ist

$$U_{Fre} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

CNOT und alle 1-Qubit-Gates sind vollständig um universelle Menge an Quantengates zu realisieren entsprechend klassischen NAND, NOR Gates. Mit Toffoli oder Fredkin Gatter die es als klassische und als Quantenschaltkreise gibt lässen sich alle klassischen Schaltkreise simulieren.

Einige Beispiele für einfache Quantenschaltkreise

- Beispiel: (aus [3, S. 6,7])

  Wir betrachten folgende Wahrheitstabelle

$$\begin{array}{lcl} |00\rangle & \rightarrow & |00\rangle \\ |01\rangle & \rightarrow & |01\rangle \\ |10\rangle & \rightarrow & \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle) \\ |11\rangle & \rightarrow & \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle) \end{array}$$

  Bemerkung: Nicht jede Wahrheitstabelle korrespondiert mit einem gültigen Quantengatter da die durch die Wahrheitstabelle angegebene Transformation nicht unitär ist.

  Die Matrixdarstellung derselben Transformation. Wie oben schon kurz beschrieben entsprechen die Zeilen Eingabevektoren, die Spalten den Anteilen der Ausgabevektoren bei entsprechendem Eingangsvektor, also gibt das Element (i, j) den Koeffizienten des j-ten Basisvektors in der Ausgabe an.

$$\begin{array}{c|cccc} & |00\rangle & |01\rangle & |10\rangle & |11\rangle \\ |00\rangle & 1 & 0 & 0 & 0 \\ |01\rangle & 0 & 1 & 0 & 0 \\ |10\rangle & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ |11\rangle & 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{array}$$

Die Matrix ist unitär da sie gleich ihrer komplex Konjugiert-Transponierten ist.

Ist die Maschine in der folgenden Superposition von Zuständen,

$$\frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

und wird die obige Transformation angewendet ergibt sich am Ausgang

$$\frac{1}{2}(|10\rangle + |11\rangle) - \frac{1}{2}(|10\rangle - |11\rangle) = |11\rangle$$

da sich die Wahrscheinlichkeitsamplituden von $|10\rangle$ auslöschen. Wird $-$ mit $+$ im Ausgangszustand vertauscht ergibt sich entsprechend $|10\rangle$.

- Ein Schaltkreis um Qubits zu vertauschen: 3 in Serie gechaltete CNOTs führen eine Swapping Operation aus.

  $$|a, b\rangle \rightarrow |a, a \otimes b\rangle \rightarrow |a \otimes (a \otimes b), a \otimes b\rangle = |b, a \otimes b\rangle \rightarrow |b, (a \otimes b) \otimes a\rangle = |b, a\rangle$$

  Das Fredkin Gatter ist demnach ein Controlled SWAP Gatter.

- Messung: konvertiert einzelnes Qubit $|\psi\rangle$ in ein klassisches probabilistisches Bit M.

- Kopieren eines Qubit

  Ist es möglich eine Kopie eines unbkannten Quantenzustandes anzulegen?

  Diese Fragestellung führte zum **No Cloning Satz**

  Klassisch funktioniert dies mittels einem CNOT Gatter. Der Controleingang x ist unbekannt, das Bit dass wir kopieren wollen. Der Targeteingang ist immer 0. An den Ausgängen liegen 2 Bits an mit zu x identischem Zustand.

  Angewandt auf Qubits ergibt sich folgenden Situation:

  $|\psi\rangle = a||0\rangle + b|1\rangle$ sei das Qubit das wir mit einem CNOT Gatter kopieren wollen. Der Eingangszustand ist demnach

  $$[a|0\rangle + b|1\rangle]\,|0\rangle = a|00\rangle + b|10\rangle$$

  was am Ausgang rechnerisch

  $$a|00\rangle + b|11\rangle$$

  ergibt. Ist das eine Kopie von $|\psi\rangle$, also $|\psi\rangle|\psi\rangle$?

  Wenn $|\psi\rangle = |0\rangle$ oder $|\psi\rangle = |1\rangle$ ist das der Fall. Wenn sich aber $|\psi\rangle$ in Superposition befindet ist

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$

Es ist also mit diesem Schaltkreis nicht möglich ein Qubit zu kopieren, ausser entspricht gerade einem klassischen Informationsbit.

Im verallgemeinerten Beweis wird von einer allgemeinen unitären Transformation statt CNOT ausgegangen und damit gezeigt dass sich mit keiner unitären Transformation ein Qubit dass sich in Superposition befindent kopieren lässt.

3.4 Algorithmen

In Bezug auf Algorithmen für Quantencomputer stellen sich u.a. folgende Fragen: Welche Klasse von Berechnungen kann auf Quantenschaltkreisen ausgeführt werden? Wie verhält sich diese Klasse zur Klasse der Berechnungen die auf klassischen Schaltkreisen ausgeführt werden können? Gibt es Aufgaben die ein Quantencomputer schneller lösen kann als ein klassischer?

Die Antwort auf die zweite Frage ist klar. Ein Quantenrechner kann einen beliebigen klassischen Rechner simulieren. Das grundsätzliche Argument lautet so, dass die Quantenmechanik jeden physikalischen Vorgang erklären kann, so auch klassische logische Schaltkreise. Wir wissen aber sogar schon dass jeder klassische Schaltkreis durch einen äquivalenten umkehrbaren (klassischen) Schaltkreis ersetzt werden bei Verwendung von Toffoli- oder Fredkin Gates. Diese gibt es als klassische und als Quanten-Schaltkreise. Nehmen wir als Beispiel das Toffoli Gate. a, b, c seien die Eingänge, a', b', c' die Ausgänge des Gatters. Sind $a = b = 1$ wird c invertiert, a und b gehen unverändert durch. Mit $c = 1$ und a, b beliebig ergibt sich NAND, mit $a = 1, c = 0$ FANOUT wobei das Bit auf Eingang b verdoppelt wird. Das widerspricht nicht dem No-Cloning Satz weil es um klassische Informationsbits geht.

Zufallsbits (Nichtdeterminismus) lassen sich mit einer einfachen Quantenschaltung (Hadamard) erzeugen.

$$|0\rangle \rightarrow_H (|0\rangle + |1\rangle)/\sqrt{2}$$

Eine weitere wichtige Besonderheit, die Parallelität von Quanten-Rechnern bzw. Algorithmen möchte ich anhand von Deutsch's Algorithmus vorstellen. Das Prinzip der Parallelität ist die Möglichkeit einer Quantenschaltung durch Superposition eine Funktion in einem Schritt an mehreren Stellen gleichzeitig auszuwerten. Die Schwierigkeit dabei ist es Information über mehr als eine dieser Auswertungen aus dem Prozess zu extrahieren, da sich bei einer Messung die Superposition auf ein klassisches Bit reduziert, also nichts gewonnen wurde.

- **Deutsch's Algorithmus (Deutsch-Josza Algorithmus)**
  Dieser Algorithmus ist ein Beispiel für einen tatsächlichen Geschwindigkeitsvorteil eines Quantenrechners. Es sei $f(x) : \{0, 1\} \rightarrow \{0, 1\}$. Im vereinfachten Fall ist die Eingabe ein Qubit im Zustand $|0\rangle$ und ein Qubit im Zustand $|1\rangle$.

  $$|\psi_0\rangle = |01\rangle$$

  Beide Qubits werden Hadamard-transformiert mit dem Ergebnis

  $$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

  Wir betrachten eine unitäre Transformation U_f als eine Blackbox mit den Eigenschaften: 2 Eingänge x, y und den Ausgängen $x, y \oplus f(x)$. Wird U_f angewandt auf einen Zustand $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ erhalten wir den Zustand $(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$

Durchläuft $|\psi_1\rangle$ nun diese Transformation erhalten wir

$$|\psi_2\rangle = \begin{cases} \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & f(0)=f(1)=0 \\ \left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & f(0)=0\neq f(1)=1 \\ \left[\frac{-|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & f(0)=1\neq f(1)=0 \\ \left[\frac{-|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & f(0)=f(1)=1 \end{cases}$$

Ein Hadamard Gatter angewandt auf das erste Qubit ergibt nun

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & f(0)=f(1) \\ \pm|1\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] & f(0)\neq f(1) \end{cases}$$

Da $f(0)\oplus f(1)=0$ wenn $f(0)=f(1)$ und sonst 1 kann das Ergebnis noch zu

$$|\psi_3\rangle = \pm|f(0)\oplus f(1)\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Jetzt kann durch Messen des ersten Qubits eine globale Eigenschaft, $f(0)\oplus f(1)$, ermittelt werden mit nur einer Auswertung von f. Dies ist möglich durch die Interferenz der beiden Alternativen. Klassisch müsste f auf jeden Fall zwei mal ausgewertet werden.

Deutsch's Algorithmus ist eine Vereinfachung eines allgemeineren Algorithmus, dem Deutsch-Josza Algorithmus der Deutsch's Problem löst: Alice schickt eine Zahl $x \in [0...2^n-1]$ an Bob. Bob wertet eine Funktion f an der Stelle x aus mit Ergebnis 0 oder 1, das er wieder Alice mitteilt. Bob's Funktion muss entweder konstant sein oder gleich 1 für genau die Hälfte aller x und 0 für die andere Hälfte. Alice's Aufgabe ist es nun herauszufinden welche Art von Funktion Bob verwendet.

Klassisch muss Alice Bob im schlechtesten Fall $2^n/2+1$ x auswerten lassen. Können die beiden Qubits austauschen und berechnet Bob seine Funktion mittels unitärer Transformationen kann Alice in einem Schritt ihre Aufgabe lösen. Deutsch-Josza ist zudem im Gegensatz zu fast allen Quantenalgorithmen deterministisch.

Ich werde hier aber nicht weiter auf Deutsch-Josza eingehen, sondern noch einen anderen wichtigen Quantenalgorithmus vorstellen,

- **Grover's Algorithmus**
  Grover's Algorithmus ist eine Methode eine unsortierte Datenbank mit N Einträgen zu durchsuchen. Klassisch deterministisch benötigt diese Aufgabe im schlechtesten Fall $O(N-1)$ Versuche um den gesuchten Eintrag zu finden, ein probabilistischer Algorithmus benötigt immer noch $O(N/2)$ Versuche im Durchschnitt. Grover's Algorithmus ermöglicht eine Beschleunigung auf $O(\sqrt{N})$

  Der Algorithmus ist probabilistisch. Um die Wahrscheinlichkeit des richtigen Treffers zu erhöhen muss der Algorithmus mehrmals laufen.

  Genauer gesagt ist die Funktion dieses Algorithmus das Invertieren einer Funktion. Gibt es eine auf einem Quantencomputer berechenbare Funktion $y=f(x)$, erlaubt es der Algorithmus x bei gegebenem y zu berechnen. Für das Suchproblem wird die Funktion so definiert, dass sie einen bestimmten Wert y ausgibt falls x dem Suchkriterium genügt und einen anderen konstanten Wert für alle übrigen x.

  Es folgt die Darstellung des Algorithmus für den einfachen Fall in dem nach einem einzelnen x gesucht wird. Für die Fälle dass es mehrere x gibt oder die Trefferanzahl genau bekannt ist gibt es weitere Optimierungen.

  – Wir haben eine unsortierte Datenbank mit N Einträgen. Die Eingabe ist ein N-dimensionaler Zustandsraum H in Form von $log_2 N$ Qubits.

– Die Einträge seien durchnummeriert von $0, 1, \ldots, (N-1)$. Wir wählen eine Beobachtbare Ω mit N verschiedenen Eigenwerten die alle bekannt sind und jeder der Eigenzustände in Ω kodiert einen Eintrag in der Datenbank.

$$\{|0\rangle, |1\rangle, ..., |N-1\rangle\}$$

die entsprechenden Eigenwerte sind dann

$$\{\lambda_0, \lambda_1, ..., \lambda_{N-1}\}$$

– Es gibt einen unitären Operator U_ω als Blackbox der die Einträge entsprechend dem Suchkriterium vergleicht. Dieser Operator soll den Effekt haben:

$$U_\omega|\omega\rangle = -|\omega\rangle$$

$$U_\omega|x\rangle = |x\rangle \text{ für alle } x \neq \omega$$

Wir suchen nun $|\omega\rangle$ oder ω für das U_ω besonders wirkt.

Der Alogrithmus läuft wie folgt ab:

– System wird initialisiert mit dem Zustand $|s\rangle = \frac{1}{\sqrt{2}} \sum_x |x\rangle$

– Die Grover Iteration wird $r(N)$ mal durchgeführt. Definition von $r(N)$ folgt unten

1. Anwenden des Operators U_ω
2. Anwenden des Operators $U_s = 2|s\rangle\langle s| - I$, I ist die Identitätsmatrix.

– Ausführen der Messung Ω. Das Resultat davon ist λ_ω aus dem sich ω ermitteln lässt.

Zur Veranschaulichung: $|\omega\rangle$ und $|s\rangle$ spannen eine Hyperebene auf. $|\omega^x\rangle$ sei ein auf dieser Ebene zu $|\omega\rangle$ orthogonaler Vektor. Die Ähnlichkeit zwischen $|\omega\rangle$ und $|s\rangle$ ist

$$\langle\omega|s\rangle = \frac{1}{\sqrt{N}}$$

Geometrisch bedeutet das, es gibt einen Winkel $(\pi/2 - \theta)$ zwischen $|\omega\rangle$ und $|s\rangle$ mit

$$cos\left(\frac{\pi}{2} - \theta\right) = \frac{1}{\sqrt{N}}$$

und

$$\sin\theta = \frac{1}{\sqrt{N}}$$

Der Operator U_ω ist eine Reflexion an der Hyperebene orthogonal zu $|\omega\rangle$, also für Vektoren in der Hyperebene die von $|\omega\rangle$ und $|s\rangle$ aufgespannt wird eine Reflexion an $|\omega^x\rangle$. U_s bedeutet eine Reflexion an der Geraden durch $|s\rangle$. Der Zustandsvektor bleibt also nach jeder Transformation $U_s U_\omega$ auf der Hyperebene und wird in jedem Grover-Schritt um 2θ Richtung $|\omega\rangle$ rotiert. Wenn der Zustandsvektor $|\omega\rangle$ am nächsten kommt wird abgebrochen. Aus θ lässt sich die Anzahl r von Iterationen berechnen. r muss jedoch ganzzahlig sein und ergibt sich als $r \approx \frac{\pi}{4}\sqrt{N}$. Die Wahrscheinlichkeit für eine falsche Antwort wird zu $O(1/N)$.

3.4.1 Komplexität

Relevante Komplexitätsklassen und Begriffe

- P - bezeichnet die Klasse der Entscheidungsprobleme, die durch ein Programm M auf einer deterministischen Turingmaschine in polynomialer Zeit "gelöst" werden können.
- NP - sind alle Entscheidungsprobleme die von einem Programm M auf einer nicht-deterministischen TM in polynomialer Zeit gelöst werden können. Daraus ergibt sich $P \subseteq NP$, da jede deterministische TM von einer nichtdeterministschen TM simuliert werden kann. Umgekehrt hat die Lösung eines Problem $\Pi \in NP$ durch eine deterministische Maschine im schlechtesten Fall die Zeitkomplexität $O(2^{p(n)})$ [9].
- $PSPACE$ - Lösbar von einer deterministischen TM mit polynomialer Platzbeschränkung und keinerlei Zeitbeschränkung. Es gilt $PSPACE = NPSPACE$.
- BPP - Probabilistische, polynomial zeitbeschränkte Algorithmen mit Beschränkung der Fehlerwahrscheinlichkeit z.B. $\leq \frac{1}{4}$
- BQP - polynomial laufzeitbeschränkte Quantenalgorithmen mit Beschränkung der Fehlerwahrscheinlichkeit z.B. $\leq \frac{1}{4}$
- NP-Vollständigkeit - ist eine Eigenschaft von bestimmten Problemen in NP. Das sind die "schwersten" Probleme in dieser Klasse in dem Sinn, dass alle anderen Probleme in NP von einem deterministischen Programm in Polynomialzeit auf ein NP-vollständiges Problem *reduziert* werden können. Für Optimierungsprobleme und Suchprobleme lassen sich korrespondierende Entscheidungsprobleme finden, siehe [9], [10].

Die grosse Frage ist wo BQP angesiedelt ist und ob z.B. NP in BQP enthalten ist.

BQP enthält P und ist in $PSPACE$ enthalten. Der Beweis einer höheren Leistungsfähigkeit von Quantencomputern gegenüber klassischen Computern würde $P \neq PSPACE$ implizieren. Dieser ist bis jetzt noch nicht gelungen.

Für die Probleme *Faktorisierung* und *diskreter Logarithmus* ist auf klassischen Computern kein Lösungsalgorithmus mit polynomialer Laufzeit bekannt, was, wie schon erwähnt, ein wesentlicher Faktor im Zusammenhang mit asymmetrischen kryptografischen Verfahren ist.
Die Ausnutzung der Quantenparallelität zum simplen Durchsuchen des Lösungsraumes eines NP Problems führt auch nicht zu einem optimalen Ergebnis trotz immerhin quadratischer Beschleunigung durch Grover's Algorithmus.

Die Operationen im Standardmodell des Quantencomputers sind Matrixmultiplikationen, also lineare Operationen. Könnte ein Quantenrechner mit nichtlinearen Operationen konstruiert werden, liessen sich damit NP-vollständige Probleme effizient lösen (Abrams, Lloyd 1998).

Bei Quanten Gatter-Arrays: Für jede Eingabelänge muss ein neues Gatter entworfen werden. Dabei darf keine Information im Entwurf "versteckt" werden, d.h. der Entwurf als ganzes muss durch eine zeitlich polynomial beschränkte (klassische) Berechnung entstehen und die Einträge in den unitären Matrizen welche die Gatter beschreiben müssen berechenbare Zahlen sein (analog der Komplexitätsklasse für Analog Computer).

3.5 Physikalische Realisierung

Die physikalische Konstruktion von Quantenrechnern zeigt sich wie der Entwurf von Quantenalgorithmen als Herausforderung.

Die vier grundsätzlichen Aufgaben die dabei gelöst werden müssen sind

1. Die Repräsentation von Qubits.
2. Die Durchführbarkeit und Kontrollierbarkeit von unitären Evolutionen
3. Initialisierung
4. Messbarkeit

Bei vielen Ansätzen können diese Ziele nur teilweise erreicht werden. Kernspin z.B. eignet sich gut zur Qubitrepräsentation lässt sich aber wegen der minimalen Kopplung mit der makroskopischen Welt sehr schwer messen.

Diese Beobachtung der gegenseitigen Ausschliessung der gewünschten Eigenschaften lässt sich ausweiten: Ein Quantencomputer muss gut isoliert von der Umgebung sein und zugleich müssen sich Qubits messen lassen. D.h. es gibt viele Tradeoffs in der Konstruktion und die Grundfrage ändert sich von *wie* lässt sich ein Quantencomputer realisieren auf *wie gut* lässt sich ein Quantencomputer realisieren.

Grösstes Problem (im Zusammenhang mit der Skalierung der Systeme) ist die Dekohärenz, verursacht durch Quantenrauschen, das bei der Interaktion des Quantensystems mit der Umgebung entsteht und die den unitären Charakter der Transformationen stört. Die grösste mögliche Länge einer Quantenberechnung auf einem bestimmten Quantencomputer ergibt sich aus dem Quotienten $\frac{\tau_Q}{\tau_{op}}$ mit τ_Q als die Zeit über die das Quantensystem koherent bleibt und τ_{op} als die Zeit die zur Berechnung elementarer unitärer Transformationen benötigt wird.

An dieser Stelle sei kurz der Quanten-Watchdog-Effekt angeführt: Eine Berechnung wird durch reversible Schritte in einen vorhersagbaren Zustand gebracht, dann wird gemessen. Wenn die Messung abweicht gab es einen Fehler, sonst wird Berechnung stabilisiert.

Zur Realisierung von Quantencomputern verwendete Ansätze

- **Heteropolymere:** Bilden lineare Felder von Atomen. Die Energieniveaus der einzelnen Atome im Polymer sind leicht unterschiedlich wegen magnetischer Wechselwirkungen und können deswegen mit unterschiedlich langen Laserpulsen adressiert und manipuliert werden. (1993)
- **Photonenbasierte Systeme** Speicherung von Qubits in Polarisierung oder Spin von Photonen. Gut ausgereifte optische Technologien und viel Erfahrung aus der Experimentalphysik. Messung über Detektierung von Photonen.
- **Ionen-Fallen** Ionen sind geladene Atome. Diese können in elektromagnetischen Feldern isoliert und kontrolliert werden. Qubits können in energetischen Zuständen eines Ions oder Schwingungsabhängigkeiten zwischen zwei Ionen realisiert und mit Lasern manipuliert werden. Jedes Ion wird dabei von einem separaten Laser kontrolliert. Einer der vielversprechenderen Ansätze zum Bau von skalierbaren Quantencomputern. (1995)
- **Molekulare Magneten:** Systeme in denen magnetische Effekte auf 1-Molekülbasis erzeugt werden können.
- **Cavity Quantum Electrodynamics:** Ein Quanten-elektrodynamischer Hohlraum in dem sich einige z.B. Cäsium Atome sowie Laser, Phasendetekoren, Polarisierer und Spiegel befinden. Jeweils ein Kontroll- und ein Ziel-Photon passieren die Röhre und interagieren dabei, am Ausgang wird eine Rotation der Zielphotonen-Polarisierung gemessen. (1995)

- **Quantum-Dot:** Ein Quantum-Dot oder auch Halbleiter-Nanokristall ist ein winziger halbleitender Kristall in der Grössenordnung von ein paar bis ein paar hundert Nanometern. Diese Quantum-Dots beschränken Elektronen, Elektronenabwesenheit (Holes) und gemischte Paare auf Linien (Quantum Wire) oder Flächen (Quantum Well). Die Beschränkung führt zu quantisierten Energielevels in diesen Bereichen. Die Kristalle werden elektrisch manipuliert. Vielversprechend für Festkörper QCs.

- **NMR - Nuclear magnetic Resonance:** Bestimmte Atomkerne besitzen magnetische Eigenschaften. Diese Atome können in einem starken Magnetfeld ausgerichtet und mit elektromagnetischen Feldern (Radiopulsen) manipuliert werden. Ein wichtiger Ansatz zum Bau von Quantenrechnern der sich aber sehr grundsätzlich von anderen Ansätzen unterscheidet. Es wird nicht versucht einzelne isolierte Quantensysteme zu steuern sondern Manipulation und Messung erfolgt an ganzen Ensembles von Quantenregistern, z.B. den Molekülen einer Flüssigkeit wo jedes Molekül ein Register darstellt. NMR ist zudem eine relativ gut beherrschte Technologie.

  Es wurde gezeigt dass NMR-Rechner NP-vollständige Probleme in Polynomialzeit lösen können [8, S. 33]. Das klingt spektakulär ist aber mit starken praktischen Einschränkungen zu geniessen. Prinzipiell ist einsichtig dass ein Quantenrechnner durch Ausnutzung der Quantenparallelität mit einem Problem exponentiell "mitwachsen" kann wenn $n =$ Problemgrösse $=$ Anzahl der Qubits des Quantencomputers. Allerdings zeigt sich in der Praxis die Konstruktion von Quantencomputern, im speziellen NMR Systemen mit einer nicht-trivialen Anzahl von Qubits als immenses, vielleicht unüberwindbares Problem. Zudem steht zur Debatte ob NMR-Computer tatsächlich Quantencomputer in einem strengen Sinn darstellen.

- **Supraleitungs- und SQUID-basierte Quantenrechner:** SQUIDs sind Superconducting Quantum Interference Devices mit denen minimalste (Grössenordnung 1 nanoTesla bis 1 microTesla) magnetische Felder gemessen werden können. Bestimmte Prozesse in biologischen Organismen produzieren z.B. solche Felder.

- **Elektronen auf Helium:** Elektronen über der Oberfläche von flüssigem Helium. Qubitrepräsention über quantisierte Ladungszustände oder Spinzustände. Gute Stabilität.

- **Fulleren basierte Quantencomputer**

- **Kane Computer:** vorgeschlagen von B. E. Kane 1998. Zwischen Quantum-Dot und NMR.

- **Josephson Junctions:** NEC 1999. Josephson Effekt ist die Bewegung von Elektronenpaaren in einem Supraleiter. Elektrisch kontrollierbar. Angelegte Spannung führt zu Quantenoszillationen über den supraleitenden Kanal.

- **Topologischer Quantencomputer:** Anyons, Quasipartikel.

Bemerkungen:
One-Way Qantum Computing: Qubit kodiert auf "Verschränktheit" in Multiqubit Clustern [6].
QuByte 2005 realisiert / 8 Qubit Quantencomputer in Innsbruck

4 Quantenkryptografie

4.1 Schlüsselverteilung

Die Schlüsselverteilung stellt das derzeit wichtigste Verfahren der Quantenkryptografie dar und ist drauf und dran praktische Anwendung ausserhalb der Labors zu finden. Die Schlüsselverteilung macht sich die Quantenteleportation über verschränkte Zustände zunutze. Wir betrachten nochmal kurz die Bellzustände.

4.1.1 Bell-Zustände

Bell-Zustände oder EPR-Paare nach John Bell bzw. Einstein, Podolsky, Rosen werden erzeugt durch einen 2-Qubit Schaltkreis: ein Hadamard Gate und ein CNOT Gate.
Die vollständige Tabelle sieht wie folgt aus:

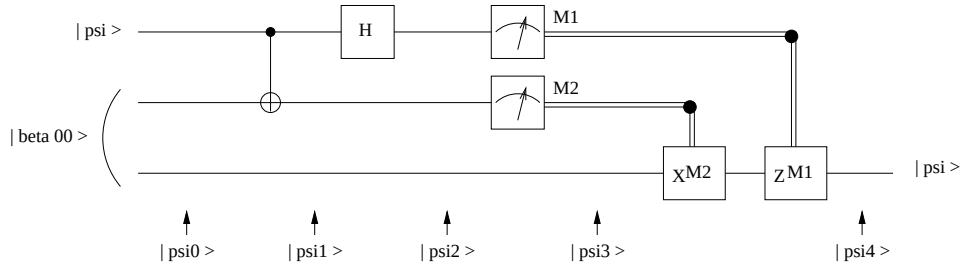
$$\begin{array}{cccc} In & & Out & \\ |00\rangle & \rightarrow & \frac{|00\rangle+|11\rangle}{\sqrt{2}} & \equiv \quad |\beta_{00}\rangle \\ |01\rangle & \rightarrow & \frac{|01\rangle+|10\rangle}{\sqrt{2}} & \equiv \quad |\beta_{01}\rangle \\ |10\rangle & \rightarrow & \frac{|00\rangle-|11\rangle}{\sqrt{2}} & \equiv \quad |\beta_{10}\rangle \\ |11\rangle & \rightarrow & \frac{|01\rangle+|10\rangle}{\sqrt{2}} & \equiv \quad |\beta_{11}\rangle \end{array}$$

Wie weiter oben schon erwähnt gilt für die Bellzustände dass bei Messung des einen Qubits der Zustand des anderen gleichzeitig festgelegt wird.

4.1.2 Quantenteleportation

Quantenteleportation ist ein Verfahren in der Abwesenheit eines Quantenkommunikationskanals Quantenzustände zu übertragen.
Beispielhafter Ablauf nach Methode von Brassard (199x) zur Übertragung eines einzelnen Qubits.

- Alice und Bob teilen sich ein verschränktes Teilchenpaar, also einen Bell-Zustand $\beta_{00} = \frac{(|00\rangle+|11\rangle)}{\sqrt{2}}$.
- Alice will ein Qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ übertragen. (Klassisch ist dies nicht möglich da sie den Zustand von $|\psi\rangle$ nicht bestimmen kann und selbst wenn sie den Zustand kennen würde müsste sie unendlich viel Information übertragen).
- Mit folgendem Quantenschaltkreis ist die Übertragung möglich:



- Alice's Teilchen, das erste Qubit des Bellzustandes $|\beta_{00}\rangle$ interagiert über CNOT mit dem zu übertragenden Qubit $|\psi\rangle$. $|\psi\rangle$ liegt am Kontrolleingang und das erste Qubit des Bell-Zustandes am Targeteingang. Der erste Ausgang, also das unveränderte Kontrollqubit läuft noch durch ein Hadamard-Gatter also ist

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\right]$$

Nach dem CNOT Gate ist

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\right]$$

und nach dem Hadamard Gate

$$|\psi_2\rangle = \frac{1}{2}\left[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right]$$

was sich umschreiben lässt zu

$$|\psi_2\rangle = \frac{1}{2}\left[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\right]$$

- Danach misst Alice beide Qubits. Die vier möglichen Ergebnisse sind $00, 01, 10, 11$. Aus dem letzten Ausdruck oben ergibt sich nun in Abhängigkeit von Alice's Messung als Ergebnis für Bob's Qubit (das zweite Qubit des verschränkten Zustandes) folgende Tabelle

$$\begin{array}{rcll} Alice & & & Bob \\ 00 & \longmapsto & |\psi_3(00)\rangle & \equiv \quad [\alpha|0\rangle + \beta|1\rangle] \\ 01 & \longmapsto & |\psi_3(01)\rangle & \equiv \quad [\alpha|1\rangle + \beta|0\rangle] \\ 10 & \longmapsto & |\psi_3(10)\rangle & \equiv \quad [\alpha|0\rangle - \beta|1\rangle] \\ 11 & \longmapsto & |\psi_3(11)\rangle & \equiv \quad [\alpha|1\rangle - \beta|0\rangle] \end{array}$$

- Bob muss für jede Möglichkeit noch unterschiedliche Transformationen an seinem Qubit durchführen, und zwar

Alice's Ergebnis	Bob's Transformation(en)
00	I
01	X
10	Z
11	ZX

  Es ergibt sich dass Bob Alice's Ergebnis kennen muss, was sie ihm aber nur als klassische Information mitteilen kann.

- Es ist genau dieser Umstand der die superluminale Informationsübertragung bei der Quantenteleportation verhindert! Auch der No-Cloning Satz wird nicht verletzt da das Quellqubit all seine Information verliert und auf einen der beiden Basiszustände reduziert wird.

Nach Ausführen der oben angeführten Prozedur wurde ein Qubit übertragen. Um einen Schlüssel für weitere sichere klassische Kommunikation zw. Alice und Bob zu etablieren muss diese einfach wiederholt ausgeführt werden bis genug Bits vorhanden sind.
Dabei können noch verschiedene Komplikationen auftreten:

- Konkret sind die Teilchen z.B. Photonen deren Polarisation zufällig über vier Zustände moduliert wird (horizontal, vertikal, links-zirkulär, rechts-zirkulär).

- Bob kann zufällig in einer der Basen messen wobei Alice und Bob später vergleichen welche Basen korrekt gewählt waren.

- Rauschen / Noise: Durch Rauschen das mit Teilchen interagiert können sich die Messergebnisse von Alice und Bob unterscheiden bzw. die Basen nicht übereinstimmen. Diese Fehler müssen eliminiert werden. Dazu wird der Bitstring in Blöcke unterteilt und die Parität überprüft. Bei Nichtübereinstimmung wird binäre Suche verwendet um die Diskrepanz zu finden, nach dem Check wird das letzte Bit des Blocks verworfen, dadurch kann die gesamte dazu notwendige Kommunikation öffentlich sein. Prozess kann mit unterschiedlichen Blockgrössen wiederholt werden um weitere Fehler zu finden. Drückt die Fehlerwahrscheinlichkeit unter Schwelle.

- Noise und Angreifer sind ununterscheidbar für A und B. Angreifer kann versuchen Teilchen im Vorbeiflug zu messen.
- Prozedur zum probabilistischen Abgleich der Bitstrings, wobei Messergebnisse beliebig aber fest 0 und 1 zugeordnet werden.

Mögliche Angriffe: Weil praktisch oft Licht-Bursts statt schwierig zu handhabende einzelne Photonen verwendet werden ist es theoretisch möglich einzelne Photonen aus dem Burst zu splitten, bis zur Ansage der richtigen Messbasis aufzubewahren und dann zu messen.

Wegen der Äquivalenz von Angriff und Rauschen ist ein DoS Angriff leicht möglich. Diese Möglichkeit existiert aber auch für viele klassische System und wird ausser acht gelassen. Weiters lädt die Ununterscheidbarkeit gewissermassen zu Angriffsexperimenten ein.
Diese Ideen gehen sogar bis in die 1960er Jahre zurück (Wiesner) und wurden 1984 von Bennett und Brassard wiederaufgefriffen und veröffentlicht.
Erzeugen eines verschränkten Teilchenpaares physikalisch:

Photonen trennen sich mit orthogonalem Spin / Polarisation
Caesium Atom zerfaellt in 2 Photonen

4.2 Shor's Algorithmus

1994 stellte Peter Shor einen Algorithmus bzw. genauer zwei Algorithmen vor zur Faktorisierung von ganzen Zahlen und zur Berechnung des diskreten Logarithmus. Beide Probleme sind wahrscheinlich nicht in P, gelten also für genügend grosse Zahlen mit bekannten Algorithmen als nicht in praktikabler Zeit lösbar und werden genau deshalb, wie wir gesehen haben oft in der Kryptographie eingesetzt.

Faktorisierung ist klar, die eindeutige Zerlegung einer natürlichen Zahl in ein Produkt von Primzahlen. Der schnellste klassische Algorithmus, Lenstra's Number Field Sieve hat in N sub-exponentielle Laufzeit, Shor's Quantenalgorithmus erlaubt es, eine Zahl N mit Laufzeit $O((logN)^3)$ (Quantenalgorithmus) und polynomieller klassischer Nachbearbeitung zu faktorisieren. Damit ist es möglich RSA Schlüssel zu knacken. Der Algorithmus wurde auch an andere asymmetrische Verfahren angepasst. 2001 wurde der Algorithmus in einem IBM Labor zum ersten Mal auf einem 7 Qubit Quantencomputer zur Zerlegung von 15 in 5 und 3 ausgeführt.

Diskreter Logarithmus: Für jede Primzahl p ist die multiplikative Gruppe $(modp)$ zyklisch, also gibt es Erzeuger g sodass $1, g, g^2, ..., g^{p-2}$ alle Restklassen bzgl. $(modp)$ erzeugen. Bei gegebenem p und g ist der *diskrete Logarithmus* einer Zahl x die Zahl r mit $0 \leq r \leq p-1$ und $g^r \equiv x(modp)$. Z.B. Diffie-Hellman Schlüsselaustausch Protokoll.
Ein andere Formulierung: Geg. a, p, p prim, ist es leicht $a^x \mod p$ zu berechnen aber schwierig zu gegebenem y ein x mit $y = a^x \mod p$ zu finden.

Ich will noch grob die Rechenvorschrift erläutern: Der Algorithmus besteht aus einem klassischen- und einem Quanten-Teil. Im klassischen Teil wird das Faktorisierungproblem auf ein Ordnungsproblem reduziert. Der Quantenteil löst das Ordnungsproblem.

- **Klassischer Teil**
  1. Wähle Pseudozufallszahl $a \leq N$.
  2. Berechne $ggt(a, N)$ mit Euklids Algorithmus.
  3. Prüfe ob $ggt(a, N) \neq 1$ sonst Faktor gefunden.
  4. Springe in den Quantenteil und berechne die Ordnung der Funktion

     $$f(x) \equiv a^x modN$$

     also $min(\{r|f(x+r) = f(x)\})$.
  5. Ist r ungerade gehe zu Schritt 1.

6. Ist $a^{a/2} \equiv -1(modN)$ gehe zu Schritt 1.
7. Die Faktoren von N sind $ggt(a^{r/2} \pm 1)$. Fertig.

- **Quantenteil**

1. Initialisiere Eingabe und Ausgabe Register mit jeweils $log_2 N$ Qubit zu

$$N^{-1/2} \sum_{x=0}^{N-1} |x\rangle|0\rangle$$

2. Konstruiere $f(x)$ als Quantenfunktion wende diese auf den Ausgangszustand an

$$N^{-1/2} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle$$

3. Anwenden der Quanten Fourier Transformation (QFT) auf das Eingangsregister. QFT sei definiert durch

$$U_{QFT}|x\rangle = N^{-1/2} \sum_{y=0}^{N-1} e^{2\pi i x y/N}|y\rangle$$

was den Zustand

$$N^{-1} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{2\pi i x y/N}|y\rangle|f(x)\rangle$$

ergibt.

4. Ausführen einer Messung. Diese ergibt ein y im Eingaberegister und $f(x_0)$ im Ausgaberegister. Die Wahrscheinlichkeit ein bestimmtes y zu messen ergibt sich nach Umformen zu

$$N^{-1} \left| \sum_{b}^{N-x_0-1} e^{2\pi i (br+x_0)y/N} \right|$$

Diese Wahrscheinlichkeit wird grösser ja näher $\frac{yr}{N}$ an einer ganzen Zahl ist.

5. Kürzen von $\frac{y}{N}$ sodass sich ein Nenner r' ergibt der ein Kandidat für r ist.
6. Prüfen ob $f(x) = f(x + r')$ gilt. Wenn ja, fertig.
7. Weiterprobieren mit Zahlen in der Umgebung von y und Vielfachen von r'.
8. Gehe zurück zum Schritt 1 des Quantenteils.

4.3 Produkte

Alles bis hier angeführte und noch viel mehr hat zu so handfesten Anwendungen geführt wie Geräten, die mittels Quantenschlüsselübertragung einen symmetrisch verschlüsselten klassischen Kanal herstellen oder Hardwarezufallsgeneratoren. Es lassen sich sicher noch viele weitere Produkte oder Produktklassen sammeln bei denen Quanteneffekte auf irgendeine Art ausgenutzt werden.

- idquantique: http://www.idquantique.com
- MagicQ
- Hardware Zufallszahlengeneratoren (Quantis, Via On-Chip Hardware RNG der thermischen Noise in Halbleiterbauelementen nutzt)
- Entwicklung z.B. NEC, IBM, Fujitsu, Toshiba.
- Demonstration einer Überweisung über Online Banking und quantenverschlüsseltem Kanal.

5 Zusammenfassung

Abschliessend lässt sich folgendes festhalten:

- Das Gebiet des Quantencomputing ist, wie eingangs erwähnt, ziemlich jung und birgt noch einiges an Bewegung und offenen Problemen. Es ist ungeklärt ob Quantenrechner tatsächlich einen für klassische Computer uneinholbaren Geschwindigkeitsvorteil bringen können.
- Es ist zudem unbekannt ob bei der Skalierung von physikalischen Quantenrechnern nicht noch unüberwindbare Schwierigkeiten auftreten.

Literatur

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

[2] Jacobo Torán: *Quantencomputer*. Vorlesungsskript, Theorethische Informatik, Universität Ulm, 2003
http://theorie.informatik.uni-ulm.de/Lehre/SS3/Quantum/Quantum.html

[3] Peter W. Shor: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. arXiv:quant-ph/9508027 v1 30 Aug 1995

[4] Roger Penrose: *Computerdenken*. Spektrum Akad. Verlag, Heidelberg - Berlin, 2002

[5] Anton Zeilinger: *Einsteins Schleier - Die neue Welt der Quantenphysik*. Verlag C.H.Beck, München, 2005

[6] Walther, Resch, Rudolph, Schenck, Weinfurter, Vedral, Aspelmeyer, Zeilinger: *Experimental one-way quantum computing*. Nature Vol 434, 10. März 2005, S. 169-176

[7] Diverse: *Wikipedia*. http://(de|en).wikipedia.org

[8] Zdzislaw Meglicki: *Introduction to Quantum Computing*.
http://beige.ucs.indiana.edu/M743/M743.pdf - 2005

[9] Michael R. Garey, David S. Johnson: *Computers and Intractability*. W. H. Freeman and Company, 1979

[10] http://de.wikipedia.org/wiki: Entscheidungsprobleme, Optimierungsprobleme_und_zugehörige_Entscheidungsprobleme - 20080225