Quantencomputer

Vortrag

von Johannes Vrana

Tutorial Halbleiterphysik SS 2002

Inhalt

I Klassischer Computer

1. Nichtreversibler Computer

Klassische nichtreversible Compter (besser: jede z. Z. erhältliche digitale Schaltung) bestehen aus Gattern bei denen man nach einer Operation den Anfangszustand nicht mehr herausfinden kann. Man kann z.B. jede digitale binäre Schaltung (also auch Computer) aus NAND's aufbauen. Dieses Bauelement ist universell, d.h. man kann damit jedes andere Gatter (XOR, ...) ersetzen.

$$(a, b) \rightarrow \neg(a \wedge b)$$

Da durch dieses Gatter Information gelöscht wird, muss man mindestens $W = kT\ln 2$ aufbringen, um diese Information zu löschen. Diese Energie (ca. 10^{-14} J) ist zwar sehr gering im Vergleich zur Verlustwärme heutiger Prozessoren (ca. 10^{-8} J), aber auch dieser Effekt wird immer wichtiger.

2. Reversibler Computer

Es ist aber auch möglich, jede Schaltung aus reversiblen Schaltelementen aufzubauen, d.h., man kann damit jede Berechnung durchführen, nur die alten Algorithmen sind dafür nicht geeignet. Jede solche Schaltung

kann z.B. aus den universellen Toffoli-Gattern aufgebaut werden.

$$(a, b, c) \rightarrow (a, b, c \oplus a \wedge b)$$

Es handelt sich hierbei also um ein NAND-Gatter wenn c=1 ist. Wie man sieht, werden die Bauelemente größer und man braucht mehr Leitungen, die auch ziemlich viel nicht benötigte Information übertragen müssen.

3. Geschwindigkeit von Algorithmen

Um die Geschwindigkeit verschiedener Algorithmen A zu klassifizieren ist es sinnvoll, einen Zusammenhang zwischen der Länge der Eingangsgröße und der maximal dafür benötigten Rechenschritte herzustellen. Beispiel:

$$T(N) = N^2$$

Um einen N-bit Input zu verarbeiten braucht man also maximal $T_A(N)$ Rechenschritte. Wenn

$$T_A(N) \leq Poly(N)$$

ist spricht man von einem polynomiellen Algorithmus. Ansonsten von nichtpolynomiell oder leider auch oft von exponentiell. $N^{\log N}$ ist z.B. nichtpolynomiell, aber eben nicht exponentiell. Daher wird der Begriff oft etwas falsch gebraucht.

II Quantencomputer

1. Einführung

Ein QC operiert nicht wie ein klassischer Computer mit Bits (also 0 und 1), sondern mit quantenmechanischen Zweizustandssystemen, Qubit genannt. Das Qubit $|\psi\rangle$ lässt sich folgendermassen darstellen:

$$|\psi\rangle = a|0\rangle + b|1\rangle \qquad |a|^2 + |b|^2 = 1$$

wobei $|0\rangle$, $|1\rangle$ eine orthonormale Basis bilden.
Bei einer beliebigen Messung wird $|\psi\rangle$ auf die Basis der Messung projiziert. Wenn man z.B. einen Spin in z-Richtung misst erhält man mit der Wahrscheinlichkeit $|a|^2$ den Zustand $|\uparrow\rangle$ sonst $|\downarrow\rangle$. In Messung in x-Richtung projiziert man dagegen den Zustand auf die Basis

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) \qquad |\leftarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle)$$

Der Quantenzustand von N verschränkten Qubits kann man als Vektor in 2^N Dimensionen ausdrücken. Also

$$|\psi\rangle = \sum_{i=0}^{2^N-1} a_i|i\rangle$$

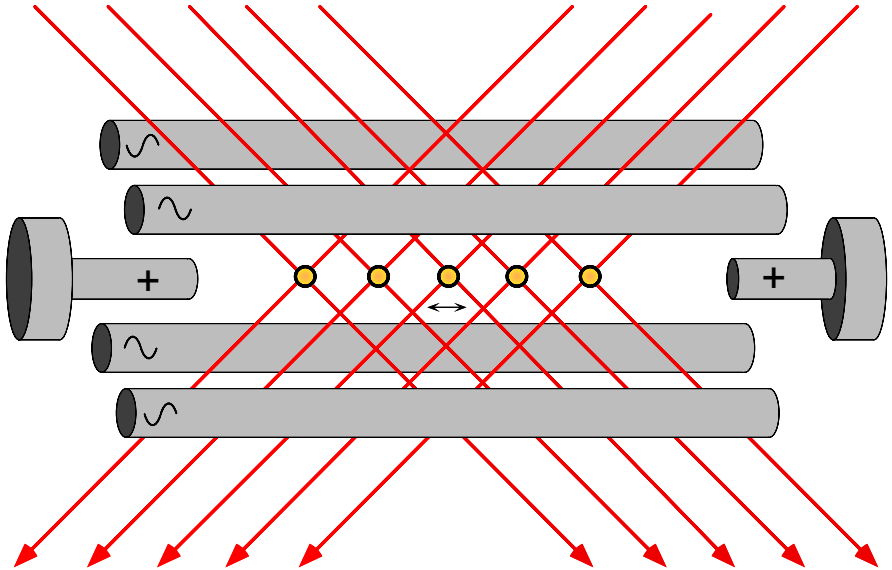
Um einen Algorithmus zu starten müssen zuerst alle Qubits in einen definierten Anfangszustand gebracht werden (z.B.: $|(i = 0)\rangle$). Danach kommt die eigentliche „Rechnung“ - eine unitäre Transformation U, die man auf alle Qubits anwendet. Diese kann aber auch aus mehreren Standardquantengattern zusammengebaut sein, die nur auf einzelne Qubits wirken (z.B. die Hadamard-Transformation). Um Transformationen auf einzelne Qubit-Paare wirken zu lassen muss dazu die WW zu allen anderen ausgeschalten werden. Zum Schluss misst man den Zustand aller Qubits in dem man sie auf die Basis projiziert. Bis zu diesem Zeitpunkt ist jede Operation reversibel. Dies ist dann auch schon das Ergebnis des Algorithmus - eine klassische Information mit höchstens N Bit. Jede Initialisierung oder Transformation ist im Endeffekt auch eine Messung.

Was braucht man also um einen QC zu realisieren?
1. Quantenmechanische Zweizustandssysteme (Qubits)
2. Wechselwirkung zwischen den Qubits (Verschränkung)
3. Messmöglichkeiten

Das Ergebnis des Quantencomputers unterliegt aber einer Wahrscheinlichkeitsverteilung, d.h. man muss auf jeden Fall öfter rechnen, da das Ergebnis falsch sein kann. Bei den meisten Quantenalgorithmen ist es aber einfach das Ergebnis klassisch zu verifizieren (z.B. Primfaktorzerlegung), nur die Berechnung davor geht klassisch schwer.

2. Realisierte Quantencomputer

a) Paul Ionenfalle



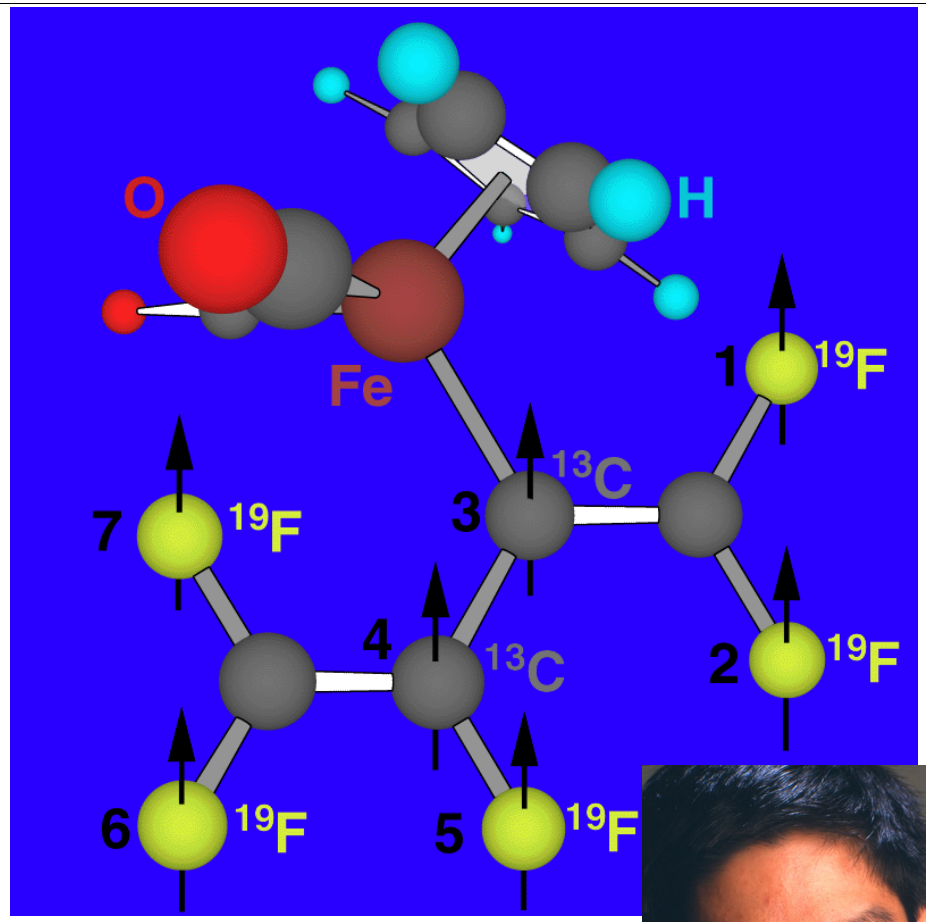
Es werden einige Ionen in eine Paulfalle gesperrt. Als QM Zweizustandssystem nimmt man hier verschiedene Atomniveaus. Zum einen den Grundzustand $|0\rangle$ und zum anderen einen langlebigen metastabilen angeregten Zustand $|1\rangle$.
Die Ionen sind so gut voneinander getrennt, dass spontane Rekombination kein dominanter Effekt ist.
Auslesen kann man durch einfaches Anregen der Ionen mit einem Laser (jedes Ion kann einzeln beleuchtet werden). Nur solche im Grundzustand werden das Licht absorbieren und reemittieren. Damit hat man schon unterschieden, ob sich das Ion in $|0\rangle$ oder in $|1\rangle$ befindet.
Durch Laserlicht mit der Frequenz ω werden Rabi-Oszillationen zwischen $|0\rangle$ und $|1\rangle$ angeregt. Durch exaktes Timing des Laserpulses und Wahl der richtigen Phase ist es möglich, jede unitäre Transformation durchzuführen.
Eine Interaktion der einzelnen Ionen ist durch deren Coulombabstoßung gegeben.
Ein kleiner Nachteil: Durch die sehr tiefen Temperaturen ist es nicht möglich hohe Arbeitsgeschwindigkeiten zu erreichen (Energie-Zeit-Unschärfe) => nur ca. 100kHz möglich.

b) NMR (Nuclear Magneto Resonance)

NMR-Quantencomputer halten zur Zeit den Qubit-Rekord von **7** !!! Dieser Rekord wurde Ende 2001 bei IBM mit nebenstehendem Molekül verwirklicht. Mit dieser QC-Suppe ist es tatsächlich gelungen, 15 zu faktorisieren. Die Mehrzahl der Moleküle hat sich für 3 x 5 entschieden.

Kurz zum Prinzip: Durch ein anliegendes magnetisches Feld werden die atomaren Spins in $|\uparrow\rangle$ und $|\downarrow\rangle$ aufgespalten. Da die Relaxationszeit ziemlich lang ist, können Qubits für einige Zeit gespeichert werden.

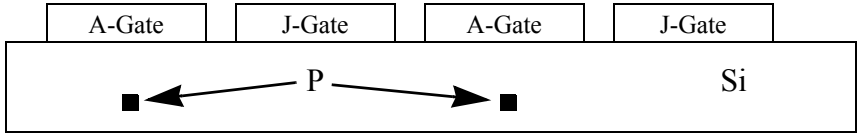
Durch ein gepulstes rotierendes Magnetfeld können Rabi-Oszillationen auf die Spins induziert werden (nur auf die in Resonanz), wodurch sämtliche unitären Transformationen angewendet werden können.



Die Kopplung der Qubits geschieht hier durch Dipol-Dipol-WW.

Da dieser QC sehr heiss ist, (wegen NMR) ist die Streuung der Ergebnisse sehr hoch. Dieses kann aber leicht durch eine hohe Anzahl an Molekülen ausgeglichen werden (ca. 10^{23}). Es dürfte aber auch sehr schwer sein Moleküle mit mehr als 50 Qubits zu finden.

3. Quantencomputer in Halbleitern



a) Donatoren in Silizium

Die zwei bisher gezeigten QC brauchen experimentell relativ komplizierte Aufbauten und sind relativ groß. Wer kann sich schon vorstellen eine Ionenfalle in seinen Computer einzubauen um einen QC-Coprozessor zu haben. Ganz abgesehen von den Lasern, ... Auch muss alles noch angeschlossen sein. Daher liegt es auf der Hand die Quantencomputer auf Chips unterzubringen, incl. der Mess-, Steuer-, und Auswertelektronik. Wie kann man also einen QC in Silizium realisieren?
Als Zweizustandssystem kann man den Spin in Donatoratomen nehmen (=> globales äusseres Magnetfeld). Da zwei solche Spins mit dem selben Elektron wechselwirken können, ist damit auch die Wechselwirkung der Qubits gegeben. Diese Wechselwirkung kann auch einzeln ausgeschalten werden, indem man in den Bereich zwischen zwei Donatoratomen immer eine Gateelektrode (J-Gate) anbringt. Um die Resonanzfrequenz zu beeinflussen, mit der die Spins im Magnetfeld umklappen, muss man noch sogenannte A-Gates über den Donatoratomen anbringen.
Also hat man schon alles was man braucht.
Da die Spins aber nicht mit dem restlichen Material wechselwirken sollen (sonst Dekohärenz) braucht man ein Material mit stabilen Spin 0 Isotopen. Damit kommen III-V Halbleiter nicht mehr in Frage. Aber dafür *Si* mit ^{31}P Donatoratomen. Da hier die Koheränzzeit sehr gut ist (einige tausend Sekunden bei T=1,5K) wäre das fast der ideale QC.
ABER: Der Herstellungsprozess ist sehr schwer - die Donatoratome müssen sehr regelmäßig (nicht zufällig verteilt !!!- für wenige Qubits evtl. nicht nötig) und immer in der gleichen Tiefe liegen und auch die Gateelektroden müssen immer über/zwischen den Donatoratomen sein, d.h. sie dürfen etwa 10µm groß sein. Das ganze ist dementsprechend mit herkömmlicher Lithographie fast nicht zu schaffen.

b) Quantendots

Wenn sich schon herkömmliches Si theoretisch eignet warum nicht auch moderne niedrigdimensionale Systeme - z.B. Quantenpunkte (Quantendots).
Auch hier kann man sich den Spin zunutze machen, aber den von einem Leitungselektron, das in einem Einelektronquantenpunkt eingefangen ist. Die Tunnelbarriere zwischen den Quantendots kann auch hier durch Gateelektroden geregelt werden.
Eine weitere Möglichkeit müsste die Nutzung der Exzitonzustände in Quntendots sein.
Auch hier dürfte die Herstellung der Struktur relativ schwierig werden. Die Quantenpunkte müssen regelmässig angeordnet sein und die Gateelektroden über/zwischen diesen angebracht werden.

c) Quantenhalleffekt

Ein anderer interessanter Ansatz ist es den Quantenhalleffekt auszunützen. In ein zweidimensionales System wird dazu noch eine Kette von Spin 1/2 Kernen implantiert. Zwischen den Leitungselektronen und dem Kernspin besteht die Hyperfein-WW. Um die Kernspins zu kontrollieren wären Elektromagnetische Pulse im Bereich der NMR-Frequenz gut. Aber wie kann man die Kernspins wirklich einzeln kontrollieren? Man könnte verschiedene Kerne hernehmen aber ob man da genügend findet? Es gibt noch ein paar andere Vorschläge, die aber noch näher ausgearbeitet werden müssen.

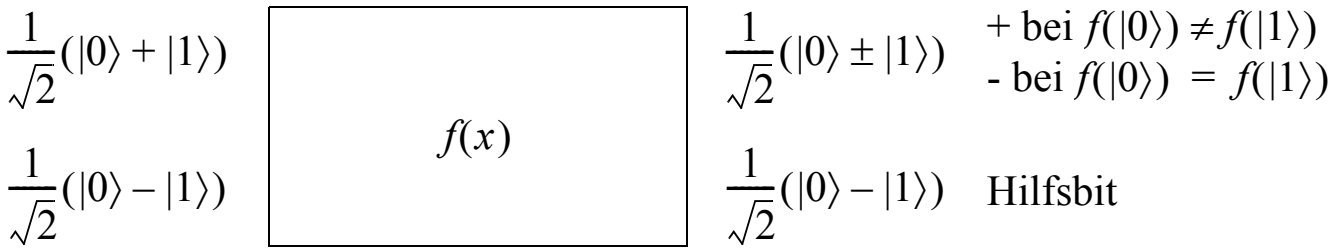
Diese Ansätze sind ein recht deutliches Beispiel, dass es sehr viele Ideen aus den verschiedensten Gebieten der Physik gibt. Das macht QC besonders interessant - und mal sehen was sich durchsetzt.

4. Algorithmus von Deutsch (1985)

Nehmen wir an dass es eine Rechnung mit 1 Bit Input und Output gibt die sehr lange dauert. Wir wissen aber nicht was der Computer macht, d.h. es gibt diese vier Zuweisungsmöglichkeiten:

$$f(0) = 1$$
$$f(0) = 0$$
$$f(1) = 1$$
$$f(1) = 0$$

Um festzustellen ob $f(0) = f(1)$, oder $f(0) \neq f(1)$, (man will ja wissen was die Schaltung macht) muss man mit einem klassischen Computer $f(0)$ und $f(1)$ berechnen. Also 2^N (hier N=1) Rechenschritte durchführen. Jetzt nimmt man für dieses Problem einen QC und kann diese Entscheidung in EINEM Rechenschritt durchführen. Also nur N Rechenschritte. Man braucht aber 2 Qubits, da es sich um einen reversiblen Schaltkreis handelt. Eines der beiden Qubits ist aber nur ein Hilfsbit. Um die gewünschte Information zu erhalten, muss das Input Qubit eine Superposition sein, d.h. der QC ist hier schneller.



5. Weitere Quantenalgorithmen

a) Faktorisierung nach Shor

Die Faktorisierung einer Zahl ist besonders interessant, da die klassische Public-Key Verschlüsselung darauf beruht, dass es heute sehr schwer ist eine große Zahl in ihre zwei Primfaktoren zu zerlegen (sie wurde durch Multiplikation dieser beiden errechnet). Für eine 512bit Zahl braucht man z.Z. mit großen Rechnerclustern einige Monate!!! Der Zeitverbrauch des z.Z. schnellesten Algorithmus ist:

$$T(N) \cong e^{O\left((\ln N)^{\frac{1}{3}}(\ln\ln N)^{\frac{2}{3}}\right)}$$

Die Zeit wächst also exponentiell mit der Länge der Eingabe.
Shor hat 1994 einen Quantenalgorithmus vorgestellt und damit das erste Mal den Sinn von QC gezeigt. Mit seinem Algorithmus lässt sich dieses Problem in folgender Zeit lösen:

$$T(N) = O((\ln N)^2(\ln\ln N)(\ln\ln\ln N))$$

Der Zeitverbrauch wächst also nur polynomiell. Für diese Arbeit erhielt Shor 1998 den Nevanlinna-Preis.

b) Quanten Fourier Transformation (QFT)

Fouriertransformationen sind sehr häufige Operationen, die ein Computer durchführen muss. Der Zeitverbrauch ist aber mit:

$$T(N) = O(N^2)$$

nicht gerade gering. Eine leichte Verbesserung bringt die FFT (Fast Fourier Transformation). Diese setzen aber eine Eingabezahl der Länge 2^n Bit vorraus. Der Computer braucht aber immer noch

$$T(N) = O(N \ln N)$$

Berechnungsschritte.
Also - was ist wenn man einen QC verwenden könnte? Dieser kann das ganze in

$$T(N) = O((\ln N)^2)$$

lösen. Aber damit nicht genug. Coppersmith hat 1994 die schnelle approximative QFT vorgstellt. Wenn man

$$T(N) = O(\ln N \ln \ln N)$$

sich also auf eine gewisse feste Fehlergenauigkeit einlassen kann ist dies der schnellste Weg zum Erfolg!

c) Quanten Suchalgorithmus

Der Suchalgorithmus von Grover (1996) ist ein Beispiel dafür, dass nicht alles exponentiell schneller ist. Eine normale Suche dauert

$$T(N) = O(N)$$

Mit einem QC ist zwar eine Beschleunigung zu erreichen, aber eben nur auf:

$$T(N) = O(\sqrt{N})$$

Das besonders interessante daran ist, dass der Algorithmus optimal ist, d.h. es gibt keinen, der schneller ist. Der Beweis, dass Suchanfragen diese Zeit minimal brauchen, wurde interessanterweise schon 1994 veröffentlicht.

6. Zukunft und zukünftige Aufgaben der QC

Man sieht also, dass QC viel können aber die vielversprochene exponentielle Beschleunigung oft nicht erreichen können. Desweiteren gibt es noch keinen Beweis dafür, dass es keine klassischen Algorithmen gibt, die die Berechnungen nicht genauso schnell durchführen können. Es wird zwar angenommen dass es diesen Beweis gibt, er existiert aber noch nicht.

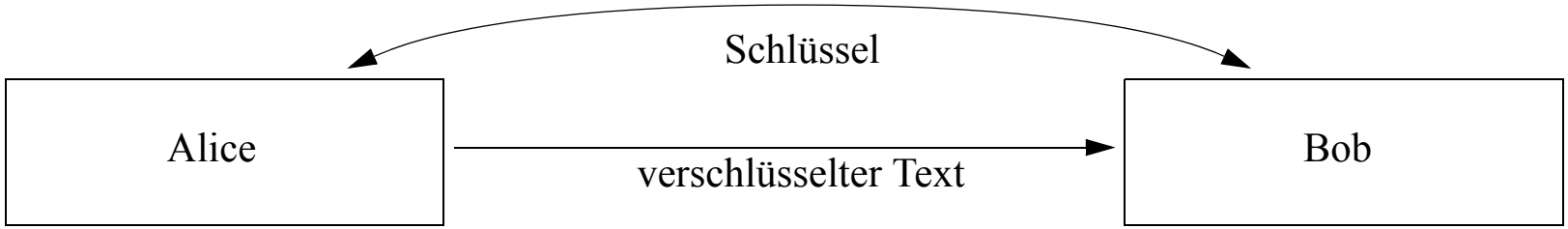
Ausserdem brauchen fehlertolerante Quantenalgorithmen eine Fehlerkorrektur. Diese existiert, braucht aber sehr viele Qubits. Um z.B. eine 430 bit Zahl zu faktorisieren braucht man nach Preskill ca. 10^6 Qubits. Um mit dieser Menge überhaupt Berechnungen durchführen zu können muss man auf jeden Fall jedes Qubit ausmessen können, d.h. es sind sehr viele Leitungen nötig. Diese sind nur dann zu realisieren wenn die restliche Elektronik auf dem selben Baustein untergebracht ist. Dies ist für mich eindeutig der größte Vorteil von Quantencomputern in Halbleitern.

Was gibt es noch für Vorstellungen was ein QC berechnen könnte?
1. Es gibt sicher einige Berechnungen die „nur“ eine ähnliche Beschleunigung erfahren wie die Quantensuche - aber auch das wäre schon viel wert.
2. Es könnte mit Quantencomputern gut möglich sein, Quantensysteme zu simulieren. Das war auch 1982 der Auslöser für Feynman sich mit QCs zu beschäftigen. Auf ihn gehen auch einige grundlegende Ideen zurück.
3. Mal sehen was es sonst noch gibt ...

ABER: Es gibt sicher auch einige Aufgaben, die ein QC nicht schneller als ein klassischer Computer durchführen kann, bzw. sogar langsamer.

III Quantenkryptographie (B92)

1. Klassische Privat Key Kryptographie:



Alice hat eine Nachricht die an Bob geschickt werden soll ohne dass dabei Eve den Inhalt erfährt, d.h., die Nachricht muss verschlüsselt werden.

Alice addiert (Algorithmus E) also auf ihren Text P einen zufälligen Schlüssel K von der gleichen Länge wie P und erhält den verschlüsselten Text C (für einen 2MB Text braucht man einen 2MB Schlüssel)

.

$$c_i = p_i + k_i (mod(N))$$

Also: (ein Beispiel)

Eingabe	B								9								2							
in Bits	0	1	0	0	0	0	1	0	0	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0
Schlüssel	1	0	1	1	0	1	1	1	1	0	0	1	0	0	1	1	0	0	0	0	1	0	0	1
verschlüsselter Text	1	1	1	1	0	1	0	1	1	0	1	0	1	0	1	0	0	0	1	1	1	0	1	1
	õ								ª								;							

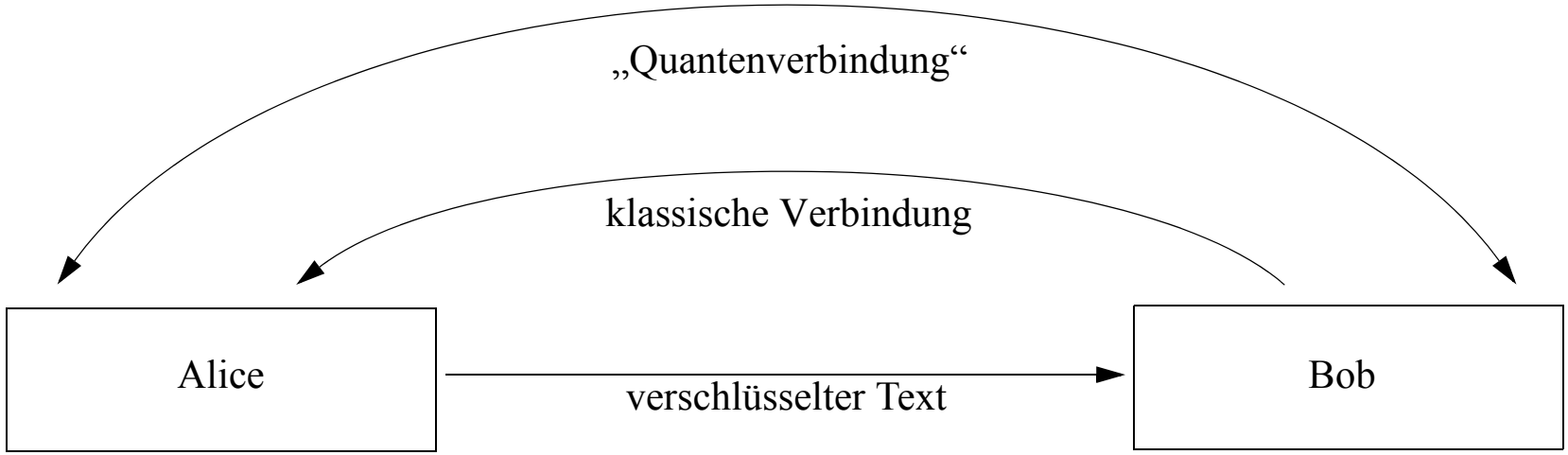
Um diesen Text wieder zu entschlüsseln muss Bob einfach den Schlüssel wieder vom Text abziehen.

Wenn Eve nur die verschlüsselte Nachricht abfängt kann sie also den Text nicht entziffern. Sollte aber auch der Schlüssel bekannt sein dürfte es ein leichtes sein auch den Algorithmus zu erraten. (Eve ist schließlich sehr intelligent)

Daher darf der Schlüssel nur einmal verwendet werden und muss sicher von A zu B gelangen ohne dass Eve diesen in Erfahrung bringen kann. Das ganze wird auch „One-Time-Pad-Verfahren“ genannt.

Und wie kann ich das erreichen? Mit **Quantenkryptographie,** oder besser **QKD** (Quantum Key Distribution) !!!

2. Das Quantenkryptographieverfahren B92



Als erstes generieren Alice und Bob je einen eigenen Schlüssel, der deutlich länger ist als die Nachricht.

A generiert aus seinem Schlüssel einen quantenmechanischen Zustand mit:

$$0 = |\uparrow\rangle \qquad 1 = |\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$$

und schickt diesen zu Bob. Bob seinerseits entscheidet mit seinem Schlüssel wie er den Zustand misst.

Mit folgender Zuweisung (d.h. entweder in z oder in x-Richtung):

$$0 = P_{|\leftarrow\rangle} \qquad 1 = P_{|\downarrow\rangle}$$

B kann also nur dann etwas messen. wenn der Schlüssel von A und B an dieser Stelle übereinstimmt. Und auch dann nur mit 50%. Wenn er eine Schlüsselstelle akzeptiert hat teilt er dies A über eine klassische Verbindung mit. Damit bauen sich A und B langsam aber sicher einen gemeinsamen sicheren Schlüssel zusammen.

Warum kann aber Eve dies nicht auch belauschen?
Beispiel: (Eve versucht im System $|\uparrow\rangle$, $|\downarrow\rangle$ zu messen):

A präpariert	Erfolgswahrscheinlichkeit für $\|\uparrow\rangle$	Zustand nach der Messung von E	Messung von B	Akzeptanzwahrscheinlichkeit	normale Akzeptanzwahrscheinlichkeit
$\|\uparrow\rangle$	1	$\|\uparrow\rangle$	$P_{\|\leftarrow\rangle}$	0,5	0,5
$\|\uparrow\rangle$	1	$\|\uparrow\rangle$	$P_{\|\downarrow\rangle}$	0	0
$\|\rightarrow\rangle$	0,5	$\|\uparrow\rangle$	$P_{\|\leftarrow\rangle}$	0,5	0
		$\|\downarrow\rangle$	$P_{\|\leftarrow\rangle}$	0,5	0
$\|\rightarrow\rangle$	0,5	$\|\uparrow\rangle$	$P_{\|\downarrow\rangle}$	0	0,5
		$\|\downarrow\rangle$	$P_{\|\downarrow\rangle}$	1	0,5

Eve erhält nur dann eine Information über den Zustand von A, wenn der Zustand nach E's Messung $|\downarrow\rangle$ ist. Dann hat nämlich A $|\rightarrow\rangle$ präpariert. Wenn dagegen der Zustand $|\downarrow\rangle$ ist, kann sich E nicht sicher sein ob A 0 oder 1 gewählt hat. Eve erhöht aber mit der Messung die Akzeptanzwahrscheinlichkeit, was A und B merken können. Ausserdem wird die entschlüsselte Nachricht für Bob keinen Sinn ergeben, da er an vielen akzeptierten Stellen nicht den gleichen Schlüssel wie Alice verwendet hat. Die Messmöglichkeit $|\rightarrow\rangle$, $|\leftarrow\rangle$ ist analog zu behandeln. Eve bringt es also auch nichts die klassische Leitung zu überwachen.

Was aber wenn E drei Quanten zur Verfügung hat? Nr.1 für eine Messung in $|\uparrow\rangle$, $|\downarrow\rangle$, Nr.2 in $|\rightarrow\rangle$, $|\leftarrow\rangle$ und Nr.3 für B (also NICHT verändert). Dann weiss E den Schlüssel von A, kann mit Hilfe der klassischen Leitung ermitteln auf welche Schlüsselelemente sich A und B geeinigt haben und ausserdem haben A und B keine Ahnung, dass E lauscht.

=> Jeder Lauschversuch nützt Eve nichts wenn immer nur EIN Quant versendet wird.

3. Eine mögliche Umsetzung und einige Probleme

Die offensichtlichste Umsetzungsmöglichkeit für QKD dürfte ein Quantenkanal mit einzelnen polarisierten Photonen sein, z.B. kann man die Photonen vertikal linear, bzw. rechtshändig zirkular polarisieren und horizontal linear, bzw. linkshändig zirkular polarisiert auslesen.

Dabei kommt aber auch schon das erste Problem auf - die einzelnen Photonen. Bei Verwendung eines gepulsten Lasers erhält man nur bei jedem 10ten Puls ein Photon, damit die Wahrscheinlichkeit für einen Puls mit mehr als einem Photon nur max. 1% ist. Mit Quantenpunkten könnte man hier sicher eine deutlich höhere Effizienz erreichen.

Desweiteren braucht man auch Ein-Photon-Detektoren. Diese gibt es für die Wellenlängen 600-800nm mit einer hohen Erkennungswahrscheinlichkeit (< 90%) und mit niedrigen Rauschraten.

Bei dieser Wellenlänge ist aber die Dämpfung der Glasfasern sehr hoch. Am besten wäre hier eine Wellenlänge von 1,3µm oder noch besser 1,55µm. Dafür bräuchte man aber auch gute Emitter/Detektoren.

4. Ein kommerziell erhältliches System

ID Quantique bietet mittlerweile ein kommerzielles System für 100.000 Euro an. Nur die Datenraten sind noch nicht besonders hoch. Auf 10km 4000bits/s, 20km 1500bit/s, und auf 50 km nur noch 100bit/s.

URL: http://www.idquantique.com/qkd.html

Literaturverzeichnis

[1] P. Vogl, Quantenmechanik 2, http://www.wsi.tum.de/T33/Teaching/Lectures/WS01-02/ws01_02.htm (2001)
[2] F. Bornemann, Quantencomputer, http://www-m3.mathematik.tu-muenchen.de/m3/teaching/QCOMP0102/index.html (2001)
[3] J. Preskill, Quantum Computation, http://theory.caltech.edu/~preskill/ph229/ (2000)
[4] J. Preskill, Reliable Quantum Computers, CALT-68-2112 (1997)
[5] D.G. Cory, A.F. Fahmy, T.F. Havel, Ensemble quantum coumputing by NMR spctroscopy, *Proc. Natl. Acad. Sci*. **94**, 1634-1639 (1997)
[6] B.E. Kane, A silicon-based nuclear spin quantum Computer, *Nature* **393**, 133-137 (1998)
[7] D. Loss, D.P. DiVincenzo, Quantum computation with quantum dots, *Phys. Rev. A* **57**, 120-126 (1998)
[8] V. Privman, I.D. Vagner, G. Kventsel, Quantum computation in quantum-Hall systems, *Phys. Letters A* **239**, 141-146 (1998)
[9] R.J. Hughes, et al., Quantum Cryptography, LA-UR-95-806 (1995)