Quanteninformationsverarbeitung - Prüfstein für IT-Sicherheit

Article · January 2004

CITATIONS
0

READS
310

2 authors:

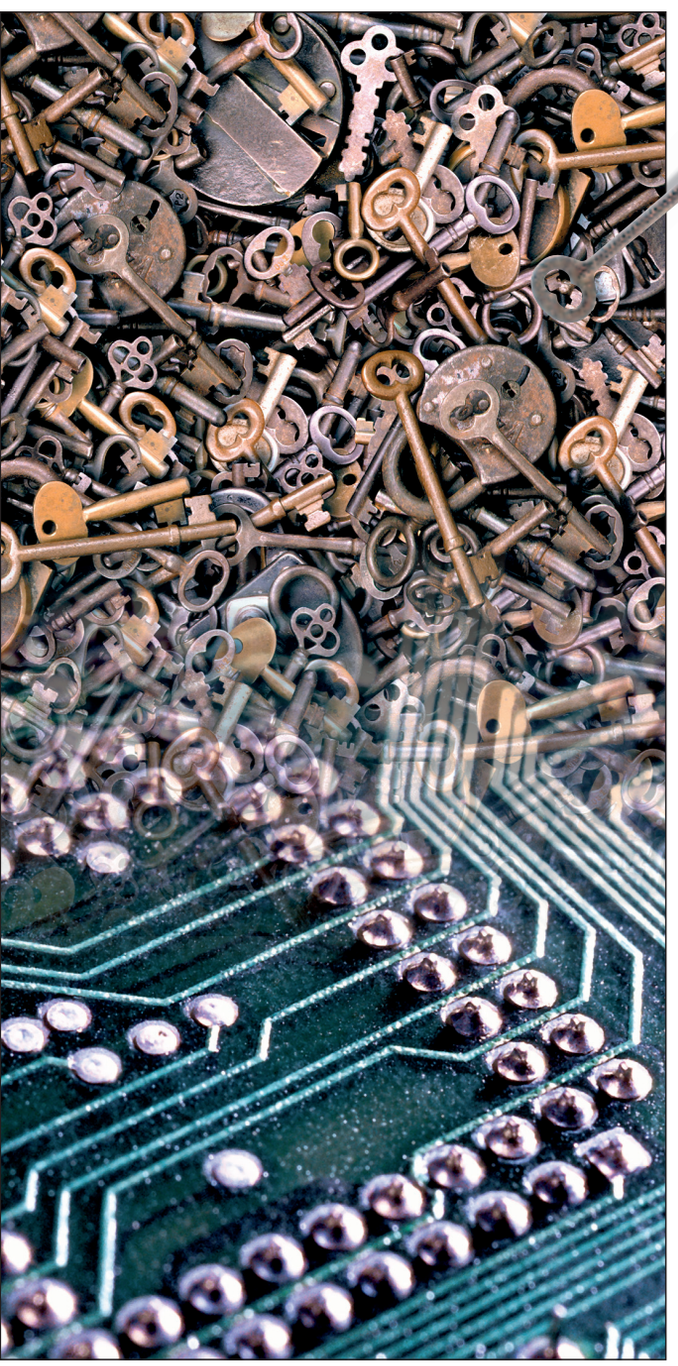
G. Alber
Technische Universität Darmstadt
178 PUBLICATIONS **3,742** CITATIONS
SEE PROFILE

Thomas Walther
Technische Universität Darmstadt
171 PUBLICATIONS **1,968** CITATIONS
SEE PROFILE

Quanteninformationsverarbeitung – Prüfstein für IT-Sicherheit

Prof. Dr. Gernot Alber, Prof. Dr. Thomas Walther

Relativitätstheorie und Quantentheorie sind die beiden großen theoretischen Gebäude der Physik des 20. Jahrhunderts. Während die Relativitätstheorie trotz all ihrer revolutionären Betrachtungsweisen, vor allem was die Struktur von Raum und Zeit anbelangt, als eine Krönung der klassischen Physik des 19. Jahrhunderts angesehen werden kann, vollzieht die Quantentheorie einen radikalen Bruch mit zahlreichen, aus dem Alltag wohlvertrauten Konzepten der klassischen Physik, die auch der Relativitätstheorie zugrunde liegen. Dies betrifft vor allem das Realitätskonzept und das Lokalitätsprinzip, nach dem physikalische Wirkungen lokal beschränkt sind und sich nicht schneller als mit der Lichtgeschwindigkeit des Vakuums ausbreiten können. Die aus den quantentheoretischen Umwälzungen resultierenden Probleme haben die Physiker immer wieder beschäftigt und fasziniert. Einen Durchbruch in der quantitativen Erfassung des Unterschiedes zwischen klassischer Physik und Quantentheorie stellen die 1964 von John Bell [1] entdeckten Ungleichungen dar, denen statistische Korrelationen im Rahmen einer lokalen, klassischen Theorie unterliegen und die durch die Quantentheorie verletzt werden können.



In der ausgehenden Dekade des 20. Jahrhunderts hat sich ein signifikanter Wandel in der Einstellung der Physiker zu den Grundlagen der Quantentheorie vollzogen. Anstatt sich über Unterschiede zur klassischen Physik, auf deren Gesetzen ein Großteil unserer heutigen Technologie basiert, zu wundern, ging man dazu über, charakteristische Quantenphänomene gezielt für praktische Zwecke auszunützen [2]. Diese Entwicklungen stellen daher erste Schritte hin zu einer neuen Quantentechnologie dar. Begünstigt wurde diese Entwicklung vor allem auch durch rasante Fortschritte in der Experimentalphysik [3], die es heute z.B. ermöglichen, einzelne Atome oder Ionen in Fallen zu speichern und deren Quantenzustände zu manipulieren oder Quantenphänomene von Lichtteilchen, also Photonen, über makroskopische Distanzen von einigen Kilometern zu kontrollieren. Zwei Entwicklungen dieser derzeit so rasch fortschreitenden Physik der Quanteninformationsverarbeitung sind dabei besonders hervorzuheben, nämlich der Quantencomputer [4] und die Quantenkryptografie [5].

In den 80er Jahren überlegte der amerikanische Physiker Feynman, ob es möglich sei, Quantensysteme mit herkömmlichen Computern zu simulieren. Er gelangte schnell zur Überzeugung, dass dies unmöglich sei. Er schloss allerdings, dass ein Quantencomputer [2,5] – also ein Rechner, basierend auf den Grundprinzipien der Quantentheorie – , dazu in der Lage sein müsste. Die Idee des Quantencomputers war geboren. Wie in der Folgezeit Forscher wie zum Beispiel P. Shor [6], zeigten, kann der Quantencomputer jedoch weitaus mehr. Die Grundprinzipien der Quantentheorie erlauben es, Rechenprozesse in einer Art und Weise zu parallelisieren, wie es mit her-

Quantum Information Processing – Touchstone for IT-Security

Quantum theory has had an enormous impact on Modern Physics. At first sight many of its basic concepts are counter intuitive from the point of view of our daily experience. Nevertheless recent progress in experimental techniques has not only enabled us to test many of these novel counter intuitive aspects of quantum theory but has also inspired new developments which exploit these very aspects for practical purposes. Though this newly emerging research area of quantum information processing constitutes an enormous threat for the IT-security of classical systems, it also provides new ideas for information theoretically secure communication based on quantum systems. In this contribution we explain basic aspects and topical developments of this rapidly evolving research area.

kömmlichen klassischen Methoden nicht möglich ist. Ein Quantencomputer kann z.B. dazu benützt werden, um in polynomial kurzer Zeit große Zahlen in Primfaktoren zu zerlegen. Diese Tatsache stellt für die Sicherheit weitverbreiteter kryptografischer Verfahren [7] wie das RSA-Verfahren, dessen Sicherheit auf den rechentechnisch großen Schwierigkeiten bei der Primzahlfaktorisierung beruht, eine ernsthafte Bedrohung dar. Bisher existiert das Konzept des Quantencomputers zwar nur auf dem Papier, wichtige erste Schritte in Richtung hin auf seine experimentelle Realisierung sind jedoch schon getan. Eine Hauptschwierigkeit bei der Realisierung von Quantencomputern, die noch überwunden werden muss, ist die Tatsache, dass Quantenzustände durch Messungen oder unkontrollierbare Umgebungseinflüsse leicht geändert werden können.

Es ist bemerkenswert, dass gerade diese Empfindlichkeit von Quantenzuständen, die auf der einen Seite ein großes Problem bei der Realisierung von Quantencomputern darstellt, auf der anderen Seite dazu verhilft, ein altes, noch offenes kryptografisches Problem zu lösen, nämlich das der Verteilung eines geheimen Zufallsschlüssels zwischen mehreren Parteien. Es ist bekannt, dass die Verschlüsselung von Information mit Hilfe eines bereits vorhandenen, geheimen Zufallsschlüssels informationstheoretisch sichere Kommunikation zwischen mehreren Parteien ermöglicht [7]. Mit klassischen Mitteln kann allerdings nicht garantiert werden, dass ein zwischen mehreren Parteien stattgefundener Austausch eines Zufallsschlüssels nicht auch von unerwünschten Außenstehenden belauscht wird. Die Quantenkryptografie[5], die dieses Schlüsselverteilungsproblem lösen kann und somit informationstheoretische Sicherheit in der Kryptografie garantieren kann, war in den letzten Jahren sehr erfolgreich und stellt innerhalb des jungen Forschungsgebietes der Quanteninformationsverarbeitung das am weitesten fortgeschrittene Teilgebiet dar. Erste Systeme, die quantenkryptografische Grundideen realisieren, werden kommerziell bereits vertrieben.

Ziel dieses Artikels ist es, einen kurzen Einblick in aktuelle theoretische und experimentelle Entwicklungen der Quanteninformationsverarbeitung zu geben.

Quantentheoretische Grundlagen – Verschränkung – lokale, klassische statistische Theorien

Der erste Schritt in Richtung Quantentheorie wurde im Jahre 1900 von M. Planck getan durch sein Postulat, dass Energie zwischen dem elektromagnetischen Feld und seiner Umgebung im thermischen Gleichgewicht in Form von diskreten Energiequanten ausgetauscht wird. Es dauerte allerdings noch weitere 25 Jahre, bis in den Jahren 1925/26 schließlich mit der Formulierung der Grundlagen der modernen Quantentheorie durch W. Heisenberg, E. Schrödinger und P. A. M. Dirac die erste logisch konsistente Beschreibung aller heute bekannten charakteristischen Quantenphänomene gelang. Neben der Diskretheit bestimmter physikalischer Variablen zählen dazu insbesondere der irreduzible Zufallscharakter physikalischer Prozesse und die Quanteninterferenz. Die Art und Weise, wie im Rahmen der modernen Quantentheorie die Verzahnung dieser grundlegenden Quantenphänomene beschrieben wird, hat selbst frühe Pioniere der Quantentheorie wie A. Einstein zunächst befremdet und nachkommende Generationen von Physikern immer wieder erneut zu einer denkerischen Durchdringung der Grundkonzepte der modernen Quantentheorie angeregt.

Bereits E. Schrödinger [8] hat 1935 klar erkannt, dass eines der markantesten Phänomene der Quantentheorie das der Verschränkung zwischen mehreren Quantensystemen ist. Grob gesprochen liegt ein verschränkter Quantenzustand zwischen mehreren physikalischen Systemen dann vor, wenn eine Eigenschaft über alle diese Systeme verteilt ist, ohne in einem der Untersysteme separat vorhanden zu sein. Um dieses vom Standpunkt der klassischen Physik aus betrachtet ungewöhnliche Phänomen zu verstehen, betrachten wir als einfaches Beispiel zwei Spin-1/2 Quanten, d.h. zwei Quantensysteme, deren (innere) Drehimpulskomponenten in beliebigen Raumrichtungen nur zwei Werte annehmen können. Realisierungen solcher Spin-1/2 Systeme sind z.B. Atomkerne mit entsprechenden inneren Drehimpulsen oder Helizitätsfreiheitsgrade von Photonen. Diese beiden Spin-1/2 Quantensysteme werden von einer Quelle in entgegengesetzte Richtungen emittiert und werden anschließend von zwei voneinander weit entfernten Experimentatoren (Alice und Bob) in Bezug auf die Drehimpulswerte in drei verschiedenen Richtungen (A,B,C) analysiert (vgl. mit Abb. 1). Alice und Bob wählen dabei unabhängig

voneinander die Drehimpulsrichtung zufällig. Bei beliebiger Wahl der Drehimpulsrichtung (A, B oder C) beobachte Alice oder Bob daher immer entweder ein Messergebnis 0 entsprechend einem Spinwert von +1/2 oder ein Messergebnis 1 entsprechend einem Spinwert von -1/2. Wir wollen außerdem annehmen, dass die Quelle einen speziellen verschränkten Quantenzustand, einen sog. Singulett-Zustand, mit folgenden wesentlichen Eigenschaften präpariert:

(a) Die Messergebnisse 0 und 1 auf Alices und Bobs Seite sind zufällig und gleichverteilt.

(b) Wann immer Alice und Bob in derselben Richtung messen, messen sie unterschiedliche Werte des Spins. Alices und Bobs Messergebnisse sind also streng korreliert.

(c) Die Eigenschaften (a) und (b) gelten für jede der drei möglichen Richtungen A, B, oder C. Der Quantenzustand der beiden Spin-1/2 Teilchen ist also symmetrisch.

Verschränkte Quantenzustände mit diesen Eigenschaften entstehen bei zahlreichen Fragmentationsprozessen, bei denen z.B. ein Molekül in zwei Atome mit entsprechenden Kernspins zerfällt. Besonders interessant ist nun die Frage, wie sich dieser Quantenzustand bezüglich einer Messung nicht identischer Drehimpulsrichtungen, also komplementärer physikalischer Variablen, verhält. Quantentheoretisch und experimentell findet man, dass gemittelt über alle drei möglichen Richtungen die Messergebnisse auf Alices und Bobs Seite mit Wahrscheinlichkeit 1/2 unterschiedlich sind.

Lässt sich dieser Sachverhalt auch im Rahmen einer klassisch statistischen Theorie verstehen [9]? Wenn eine klassische Beschreibung zutreffend wäre, müsste ein 'Anweisungskatalog' existieren, der bereits beim Verlassen der Quelle das physikalische Verhalten, d.h. das 'Element der Realität', der beiden Teilchen in Bezug auf alle möglichen Messungen von Alice und Bob festlegt. Darüber hinaus kann, wenn Alice und Bob hinreichend weit voneinander entfernt sind und annähernd gleichzeitig ihre Messungen durchführen, aufgrund des Lokalitätsprinzips der klassischen Physik die Richtungswahl von Alice diejenige von Bob nicht beeinflussen und umgekehrt. Konsistent mit den Eigenschaften (a)-(c) des betrachteten Quantenzustandes kann dieser 'Anweisungskatalog' nur aus 8 Einträgen ('Elementen der Realität') bestehen (vgl. mit Tab. 1). Für jeden dieser Einträge lässt sich für jede Richtungswahl von Alice und Bob in einfacher Weise bestimmen, ob die beiden Messergebnisse gleich oder verschieden sind. Für jedes 'Element der Realität' ergibt sich so, dass gemittelt über alle möglichen Richtungen die Wahrscheinlichkeit für die Messung verschiedener Spinwerte auf Alices und Bobs Seite größer als 5/9 ist. Diese Ungleichung, die mögliche klassische Korrelationen in dieser physikalischen Situation einschränkt, ist ein einfaches Beispiel für eine Ungleichung vom Bell'schen Typ [1,9]. Die untere Schranke von 5/9 ist im Widerspruch zur Quantentheorie und zum experimentellen Befund von 1/2. Dieses Beispiel demonstriert in einfacher Weise, dass statistische Korrelationen verschränkter Quantenzustände i.a. nicht durch klassisch stati-

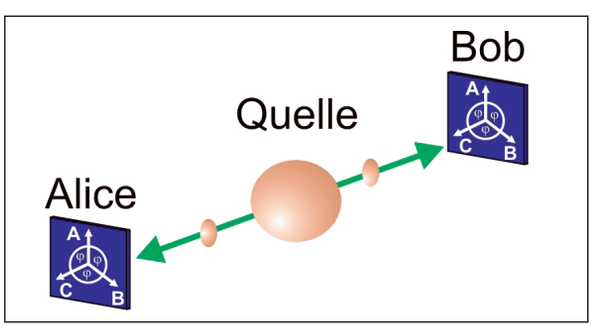


Abb.1: Schematische Darstellung eines Korrelationsexperiments an einem verschränkten Singulett-Zustand zweier Spin-1/2 Quanten: Zwei räumlich weit entfernte Experimentatoren (Alice und Bob) messen die Spins beider Quanten gleichzeitig in je drei unterschiedlichen Richtungen (A, B oder C mit φ=2π/3). Obwohl die Messergebnisse von Alice und Bob zufällig verteilt sind, besteht eine strenge Korrelation zwischen je zwei gleichzeitig gemessenen Spinwerten bei gleicher Richtungswahl von Alice und Bob. Gemittelt über alle Richtungen (A, B und C) sind die Messergebnisse von Alice und Bob mit Wahrscheinlichkeit 1/2 verschieden.

Fig.1: Schematic representation of a correlation experiment involving an entangled singlet-state of two spin-1/2 quantum systems: Two spatially well separated experimenters (Alice and Bob) measure the spins of both systems simultaneously in one of three possible directions (A, B or C with φ=2π/3). Though Alice's and Bob's measurement results are distributed randomly, there is a strict correlation between two simultaneously measured values of the spin provided Alice and Bob choose the same directions. Averaged over all possible direction (A, B or C) the measurement results of Alice and Bob are different with a probability of 1/2.

Tabelle 1: Links: Anweisungskatalog einer klassisch lokal, realistischen Theorie für das Experiment aus Abb. 1: Der Anweisungskatalog besteht aus 8 Elementen der Realität (α,β,...,ξ). Jedes dieser Elemente bestimmt, welches Messergebnis (0 oder 1) Alice und Bob bei jeder möglichen Richtungswahl (A, B oder C) beobachten. Ebenfalls angegeben ist die Wahrscheinlichkeit für die Messung verschiedener Spinwerte für jedes Element der Realität.
Rechts: In 5 von 9 möglichen Richtungen (A, B oder C) beobachten Alice und Bob verschiedene Messwerte beim Vorliegen des Elements der Realität α.

Table 1: Left hand side: Elements of reality of a classical local, realistic theory for the experiment of Fig.1. There are 8 different elements of reality (α,β,...,ξ). Each of these elements determines the measurement results (0 or 1) of Alice and Bob for all possible choices of directions (A, B or C). The probabilities for measuring different spin values are also indicated for each element of reality.
Right hand side: Provided the element of reality α is realized, Alice and Bob measure different spin values in 5 of 9 possible directions.

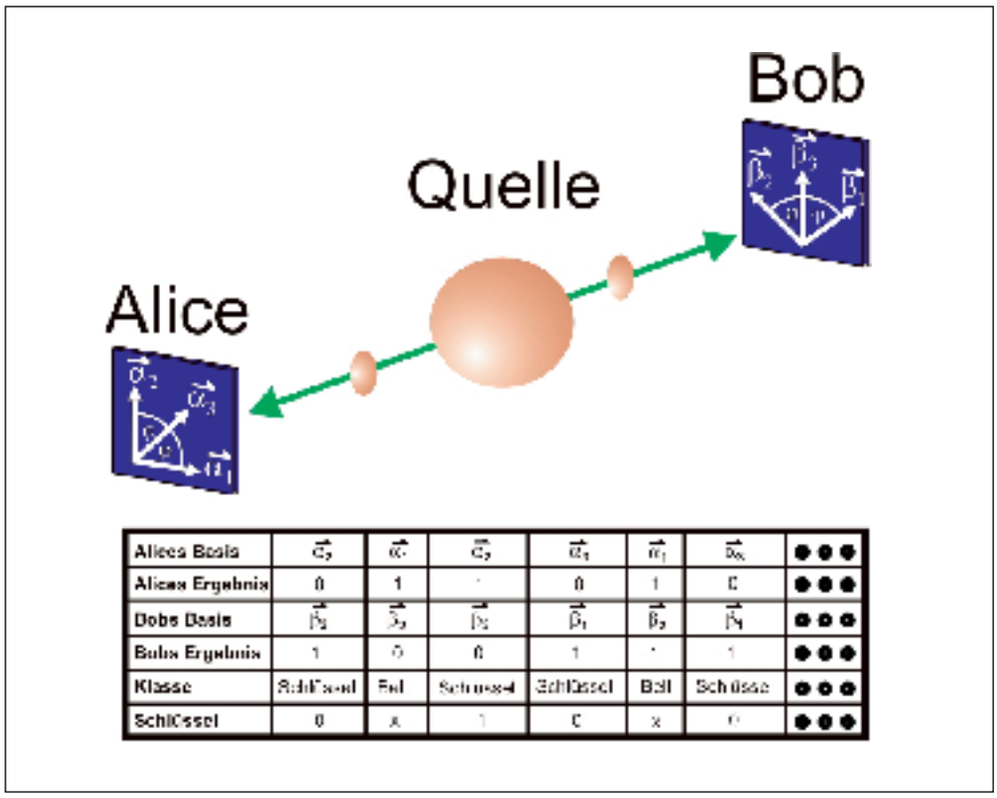
	Anweisungskatalog (Elemente der Realität)						Wahrscheinlichkeit verschiedener Messergebnisse
	Alice			Bob			
	A	B	C	A	B	C	
α	0	0	1	1	1	0	5/9
β	0	1	0	1	0	1	5/9
γ	1	0	0	0	1	1	5/9
δ	1	1	0	0	0	1	5/9
ε	1	0	1	0	1	0	5/9
ζ	0	1	1	1	0	0	5/9
η	1	1	1	0	0	0	1
ξ	0	0	0	1	1	1	1

Richtungswahl		Verschiedene Messergebnisse für Element α
Alice	Bob	
A	A	ja
B	B	ja
C	C	ja
A	B	ja
B	A	ja
A	C	nein
C	A	nein
B	C	nein
C	B	nein

stische Theorien beschrieben werden können. Dies ist auf die unterschiedliche Verzahnung der Begriffe 'Realität' und 'Lokalität' in beiden Theorien zurückzuführen.

Informationstheoretische Sicherheit durch Quantenkryptografie

Die charakteristischen statistischen Korrelationen verschränkter Quantenzustände können praktisch dazu verwendet werden, um geheime Schlüssel abhörsicher zwischen mehreren Parteien auszutauschen. Darüberhinaus bieten verschränkte Quantenzustände die Möglichkeit, Zufallszahlen zu produzieren, deren ideale Zufälligkeit durch ein Naturgesetz garantiert ist. Diese Aspekte lassen sich in einfacher Weise am ersten Quantenprotokoll verdeutlichen, das zum Zwecke eines verschränkungsunterstützten, abhörsicheren Austauschs eines geheimen Zufallszahlenschlüssels von A. Ekert [10] vorgeschlagen wurde. In Abb. 2 sind die wesentlichen Elemente dieses Quantenprotokolls schematisch dargestellt. Zum Zweck des abhörsicheren Schlüsseltausches präpariert eine Quelle eine große Anzahl verschränkter Quantenzustände z.B. von Spin-1/2 Systemen. Von jedem dieser verschränkten Paare wird ein Spin-1/2 System zu Alice und eines zu Bob geschickt. Anschließend messen Alice und Bob die Drehimpulskomponenten jedes Paares, indem sie eine von drei möglichen Richtungen unabhängig voneinander zufällig auswählen. Immer dann, wenn diese zufällig gewählten Richtungen übereinstimmen, sind die Messergebnisse infolge der charakteristischen Eigenschaften der zugrunde liegenden verschränkten Quantenzustände einerseits



Alices Basis						
Alices Ergebnis	0	1		0	1	
Bobs Basis						
Bobs Ergebnis	1	0	0	1		1
Klasse	Schlüssel	Fail	Schlüssel	Schlüssel	Fail	Schlüssel
Schlüssel	0					

Abb.2: Schematische Darstellung des Quantenprotokolls von Ekert [10] zum abhörsicheren Schlüsseltausch: Alice und Bob wählen die Richtungen für ihre Spinmessungen gleichzeitig und zufällig. Bei gleicher Richtungswahl werden die Messergebnisse für den gemeinsamen Zufallsschlüssel verwendet, bei unterschiedlicher Richtungswahl zur Überprüfung der Verletzung der Bellschen Ungleichungen.

Fig2.: Schematic representation of Ekert's quantum protocol [10] for secure key exchange: Alice and Bob choose their directions for spin measurement simultaneously and randomly. If they choose the same directions, they use their measruement results for their common random key. If they choose different directions they can use parts of these data for testing the violation of Bell's inequality.

zufällig verteilt und andererseits streng korreliert. Diese streng korrelierten Zufallszahlen können daher als Zufallsschlüssel für ein kryptografisches Protokoll, ein sog. 'One-time Pad' [7,10], dienen. Die Verschlüsselung einer Nachricht durch einen solchen Zufallsschlüssel erzeugt wieder eine Sequenz von Zufallszahlen, die Alice dann über einen klassischen Kanal wie z. B. ein Telefon an Bob senden kann. Wenn Bob diesen Zufallsschlüssel kennt, kann er diese Nachricht in einfacher Weise entschlüsseln. C. Shannon [12] hat bereits 1949 gezeigt, dass diese Art der Verschlüsselung mittels eines geheimen Zufallsschlüssels informationstheoretisch betrachtet sicher ist.

Vor der Entwicklung der Quantenkryptografie gab es allerdings kein Verfahren, um sicherzustellen, dass ein gemeinsamer Zufallsschlüssel wirklich geheim ist. Durch die Quantenkryptografie ist dieses Schlüsselverteilungsproblem erstmals gelöst worden. Ein möglicher Lauscher, der versucht durch Messung der physikalischen Systeme Information über diesen Zufallsschlüssel zu erhalten, führt durch Messungen an den Spin-1/2 Systemen 'Elemente der Realität' ein und ändert somit die für verschränkte Quantenzustände typischen Quantenkorrelationen. Alice und Bob können daher einen solchen Lauscher dadurch entdecken, dass sie die statistischen Korrelationen der nicht für den Schlüssel verwendeten Messdaten überprüfen. Verletzen diese Korrelationen die Vorhersagen lokaler, klassischer Theorien, so können Alice und Bob sicher sein, dass ihr gemeinsamer Zustand

verschränkt und somit ihr streng korrelierter Zufallsschlüssel geheim ist.

Bei der praktischen Umsetzung dieser neuen Ideen spielen neben diesem Grundprinzip allerdings noch eine Reihe anderer, eigens für diese Zwecke neuentwickelter Methoden eine wesentliche Rolle. Um z.B. Fehler zu beseitigen, die beim Austausch der Quantensysteme zwischen den beiden Parteien auch ohne Anwesenheit eines Lauschers infolge unkontrollierbarer Umgebungseinflüsse auftreten, wurden in den letzten Jahren quantenmechanische Fehlerkorrekturverfahren und Zustandsreinigungsmethoden entwickelt. Mit Hilfe dieser Methoden ist es sogar möglich, einen geheimen Schlüssel in Anwesenheit eines Lauschers zu erzeugen, vorausgesetzt die durch den Lauscher hervorgerufene Fehlerrate ist nicht allzu groß.

Experimentelle Entwicklungen

Viele der Eigenschaften der Quantenmechanik, die unserer Intuition widersprechen, waren zunächst für eine experimentelle Überprüfung unzugänglich. Die Auseinandersetzung zwischen Verfechtern der klassischen Physik und der Quantenmechanik waren auf sogenannte Gedankenexperimente beschränkt – es schien sogar so zu sein, dass Experimente nicht denkbar waren, die es erlaubten, zum Beispiel die oben angesprochenen Korrelationen in verschränkten Systemen zu untersuchen. Diese Situation änderte sich mit der Entdeckung der Bell'schen Ungleichungen 1964 wie oben angedeutet. Jetzt wurden zum ersten Mal zumindest prinzipiell experimentelle Tests möglich.

Wegen der allerdings schwierigen Umsetzung solcher Tests dauerte es 8 Jahre, bis die ersten Experimente auf diesem Gebiet durchgeführt wurden. Die Experimente bestätigten die Voraussagen der Quantenmechanik. Allerdings enthielten diese Experimente einige Lücken, die weitere Tests nötig machten, und in der Folgezeit wurden weitere Tests an sehr unterschiedlichen Systemen durchgeführt; aber auch diese verbesserten Experimente lassen immer noch Lücken in der Argumentation offen. Die Hinweise für die Richtigkeit der quantenmechanischen Sichtweisen sind allerdings erdrückend. Trotzdem muss und wird natürlich weiterhin in diese Richtung geforscht [13]. Für einen lückenlosen experimentellen Beweis müssen sehr komplexe Anforderungen sowohl in prinzipieller als auch technologischer Art erfüllt werden. Es werden zur Zeit verschiedene Ansätze – wie zum Beispiel die Erzeugung von verschränkten Zuständen über die Photodissoziation von Molekülen mit anschliessendem sensitivem Nachweis der Fragmente – verfolgt.

In den letzten Jahren hat sich aber auch der Fokus der Arbeiten von einem Nachweis der Richtigkeit der Quantenphysik auf deren Anwendungen weiterentwickelt. Eine Kombination von Entwicklungen in den letzten Jahren hat dazu beigetragen, das Gebiet der Quanteninformtionsverarbeitung zu einem der interessantesten und schnell wachsendsten Gebiete der modernen Physik werden zu lassen.

Die wohl wichtigste Voraussetzung war die Entwicklung des Lasers, der in den 60er Jahren erfunden wurde und seitdem aus unserem täglichen Leben nicht mehr wegzudenken ist. Man denke nur an seine zahlreichen Anwendungen wie zum Beispiel in der Medizin, aber auch in Barcodelesern, CD-Spielern und so weiter.

Die Erfindung des Lasers war in Hinsicht auf zwei Eigenschaften essentiell für die Entwicklung des Gebietes der Quanteninformationsverarbeitung: (1) Der Laser machte hohe Intensitäten möglich, so dass es gelang, nichtlineare Prozesse in Kristallen hervorzurufen. (2) Durch die hohe Energieschärfe des Laserlichtes ist er ein ideales Hilfsmittel, um die internen Freiheitsgrade eines Atoms sehr genau und präzise zu kontrollieren. Darüber hinaus lassen sich die externen Freiheitsgrade wie die Geschwindigkeit eines Atoms durch den Laser manipulieren. Dies ist möglich, da der Strahlungsdruck des Lichtes eine wenn auch kleine Kraft auf die Atome ausübt. Durch spezielle Techniken können so Atome zum Stillstand gebracht werden und sogar freischwebend in einem Vakuum gefangen werden. Diese Entwicklungen führten letztlich auch zur Bildung von Bose-Einstein Kondensaten, einer völlig neuen Form der Materie und anderen grundlegenden Erkenntnissen [14]. Aber wir wollen zu unserem eigentlichen Thema zurückkommen.

Nicht-lineare Prozesse in speziellen Kristallen können durch Fokussierung des Laserlichtes in diese Kristalle hervorgerufen werden. Normalerweise folgen die Elektronen des Kristalls einem äusseren Feld, wie zum Beispiel einem Lichtstrahl, und führen zu einer Polarisation des Kristalls, die mit der Frequenz des Lichtes variiert. Wird jedoch die Intensität und damit die Feldstärke des eingestrahlten Lichtes sehr hoch, können die Elektronen und damit die Polarisation nicht mehr folgen. Dies führt zum Auftreten von neuen Frequenzen in der Polarisation, vergleichbar mit dem Klirren eines akustischen Verstärkers, dessen Lautstärke zu

hoch geregelt ist. Werden die experimentellen Aufbauten richtig gewählt, kann diese nicht-lineare Komponente der Polarisation zu Licht bei neuen Frequenzen führen. So ist es möglich, mit Hilfe dieses Prozesses ein Lichtteilchen zu vernichten und dafür 2 Photonen mit der je halben Energie zu erzeugen. Man spricht in diesem Fall von einem parametrischen Oszillator. Das Besondere daran ist, dass man die Kristalle so einsetzen kann, dass die beiden entstehenden Lichtteilchen in einem verschränkten Zustand erzeugt werden. Der parametrische Oszillator ist eine ideale Quelle solcher verschränkter Photonen, die – wie wir vorher gesehen haben – in der Quantenkryptografie zum Einsatz kommen. Nicht zuletzt durch diese Entwicklung ist die Quantenkryptografie das am weitesten fortgeschrittene Teilgebiet der Quanteninformationsverarbeitung. Basierend auf diesen parametrischen Oszillatoren sind bereits erste kommerzielle Systeme erhältlich.

Neben diesen ersten Erfolgen gibt es allerdings noch eine Vielzahl interessanter Fragestellungen zu untersuchen: Für die absolut sichere Quantenkryptografie müssen die eingesetzten Lichtquellen einzelne Photonen bzw. Photonenpaare erzeugen. Dies ist im Moment nur bedingt möglich, und ein aktuelles Forschungsgebiet ist die Entwicklung deterministischer Ein-Photonenquellen – also Quellen, die auf Kommando genau ein Photon aussenden. Damit verbunden ist das Streben nach höheren Übertragungsraten der Schlüssel, verbunden mit der Möglichkeit, dies über noch grössere Entfernungen zu tun. Im Moment liegt die praktische Grenze bei einigen 10 km. Weitere Forschungsschwerpunkte sind die sog. 'Privacy Amplification', mit der erreicht werden soll, dass trotz Verlust behafteter Verbindungen zwischen den Parteien ein Austausch der geheimen Schlüssel möglich wird.

Zum Abschluss soll schließlich auch noch kurz auf den experimentellen Stand des Quantencomputers eingegangen werden. Bei den meisten der im Moment diskutierten Ansätze zum Quantencomputer wird die oben bereits erwähnte zweite Möglichkeit des Lasers, nämlich die gezielte Manipulation der internen und externen Freiheitsgrade eines Atoms, dringend notwendig.

Die Basisvoraussetzungen, damit ein System zur Verwirklichung eines Quantencomputers in Betracht kommt, sind (1) das Vorliegen von 2-Niveau Quantensystemen, (2) die Möglichkeit der gezielten Manipulation einzelner dieser Quantensysteme und die Möglichkeit zur Wechselwirkung untereinander sowie (3) die Möglichkeit des Auslesens der Zustände. Durch diese Reihung ist bereits klar, dass dem Laser hierbei eine herausragende Rolle zukommt, da er praktisch in jedem dieser Schritte zum Einsatz kommt.

Gegenwärtig werden eine Vielzahl von möglichen Realisationen eines Quantencomputers diskutiert, auf die im Folgenden kurz eingegangen werden soll. Ein vielversprechendes Quantensystem sind Ionen in Fallen [15]. Dabei werden eine Vielzahl von Ionen wie auf einer Kette aufgereiht in einer sog. linearen Paulfalle festgehalten. Die Abstände zwischen den Ionen sind groß genug, um gezielt einzelne Ionen zu manipulieren, gleichzeitig aber ist es möglich, über Schwingungen der Gesamtheit der Ionenkette auch eine Wechselwirkung zwischen den Ionen hervorzurufen. In diesen Systemen wurden die elementaren Rechenschritte bereits für wenige Ionen demonstriert und das gegenwärtige Ziel ist es, diese Schritte auf eine grössere Anzahl zu erweitern.
Ein weiteres in der Diskussion befindliches System sind neutrale Atome in optischen Gittern. Die optischen Gitter werden durch kreuzende Laserstrahlen erzeugt. Man kann sich diese ähnlich wie Miniatureierkartons vorstellen, in deren Vertiefungen jeweils einzelne Atome sitzen. Durch gezielte Kollisionen zwischen den Atomen können inzwischen Verschränkungen zwischen den Atomen hervorgerufen werden, eine wichtige Voraussetzung für die Verwirklichung eines Quantencomputers [16]. Weitere in der Entwicklung befindliche Systeme sind unter anderem Atome platziert in optischen Resonatoren oder Festkörpersysteme, basierend auf sogenannten Quantenpunkten. Das vielleicht am weitesten fortgeschrittene System sind jedoch Moleküle, eingebettet in Flüssigkeiten, die mittels Kernspinresonanz (NMR) manipuliert werden [4]. Auch hier wurden die elementaren Rechenprozesse durchgeführt, aber es sind darüber hinaus noch weitere wichtige Schritte erfolgreich implementiert worden. So gelang es in diesen NMR basierten Quantensystemen, alle wichtigen bekannten Rechenalgorithmen in der Quanteninformationsverarbeitung durchzuführen, wenn auch mit noch geringem praktischen Nutzen. Unter anderem konnte so die Zahl 15 mit Hilfe des Shor-Algorithmus faktorisiert werden. Dies mag wenig erscheinen, es zeigt jedoch, dass der Quantencomputer Realität werden kann.

Trotz der bemerkenswerten Fortschritte in den letzten Jahren gibt es noch zahlreiche ungelöste Probleme. Der Quantencomputer basiert auf der sehr empfindlichen

Überlagerung von Quantenzuständen. Schon kleinste Umgebungseinflüsse zerstören diese jedoch und machen jegliche Berechnung ungültig. Je grösser ein Quantensystem dabei wird, desto empfindlicher wird es auch gegen diese ungewollten Einflüsse. Ein wichtiges Augenmerk in der Entwicklung liegt also im Versuch, diese Quantensysteme gegen Umwelteinflüsse zu schützen bzw. Mechanismen zu finden, um die Zerstörung der Quanteninformation auszugleichen. Auf der anderen Seite wird natürlich auch nach alternativen Systemen gesucht, und so ist es durchaus denkbar, dass das System der Wahl schließlich völlig anders aussehen wird.

Ausblick

Sowohl theoretisch als auch experimentell macht die Quanteninformationsverarbeitung seit Jahren rasante Fortschritte. Gerade dieses Gebiet der Physik profitiert sehr stark und unmittelbar von dem Wechselspiel zwischen Theorie und Experiment. Wir verstehen es heute dank raffinierter experimenteller Methoden, so gut wie nie zuvor Quantensysteme zu kontrollieren und zu manipulieren. Einzelne Teile eines Quantencomputers sind implementiert und Physiker arbeiten fieberhaft daran, diese Basiseinheiten zu größeren zusammenzufassen. Neue Verfahren zur Fehlerkorrektur werden eingeführt, so dass man annehmen kann, dass sich in den nächsten Jahrzehnten ein Quantencomputer realisieren lässt. Auf der anderen Seite ist die Quantenkryptografie in Bezug auf die praktische Umsetzung bereits so weit fortgeschritten, dass erste Systeme bereits kommerziell vertrieben werden. Neben diesen beiden Zielsetzungen vermitteln die Experimente und theoretischen Arbeiten zur Quanteninformationsverarbeitung jedoch auch einen faszinierenden Einblick in die Funktionsweise der Quantenwelt, die auf dem besten Wege ist, neben dem Mikrokosmos nunmehr auch den Makrokosmos zu erobern.

Literatur

1. J. S. Bell, Physics 1, 195 (1964).
2. D. Bouwmeester, A. Ekert, A. Zeilinger (eds.): The Physics of Quantum Information (Springer, Berlin, Heidelberg, 2000); G. Alber, T. Beth, M. Horodecki, P. Horodecki, R. Horodecki, M. Rötteler, H. Weinfurter, R. Werner, A. Zeilinger: Quantum Information – An Introduction to Basic Theoretical Concepts and Experiments (Springer, Berlin, Heidelberg, 2001).
3. Physics World, Vol. 11, März 1998.
4. A. Galindo, M. A. Martin-Delgado, Rev. Mod. Phys. 74, 347 (2002).
5. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
6. P. Shor: In Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, 1994, Los Alamitos, California (IEEE Computer Society Press, New York, 1994) p.124.
7. J. A. Buchmann: Introduction to Cryptography (Springer, Berlin, Heidelberg, 2000).
8. E. Schrödinger, Naturwiss. 48, 807 (1935).
9. D. F. Styer: The Strange World of Quantum Mechanics (Cambridge UP, Cambridge, 2000).
10. A. Ekert, Phys. Rev. Lett. 67, 661 (1991).
11. G. S. Vernam, J. Am. Inst. Electr. Eng. 45, 109 (1926).
12. C. E. Shannon, Bell. Syst. Tech. J 28, 656 (1949).
13. siehe z.B. Fry, Walther, in Quantum [Un]speakables, 103, (Springer), Berlin 2002.
14. W. D. Phillips, Rev. Mod. Phys. 70, 721 (1998).
15. D. Leibfried, R. Blatt, C. Monroe, D. Wineland, Rev. Mod. Phys., 75, 281 (2003).
16. O. Mandel, M. Greiner, A. Widera, T. Rom, T. Hänsch, I. Bloch, Nature 425, 937 (2003) .

Institut für Angewandte Physik, Fachbereich Physik, der TU Darmstadt

Das Institut für Angewandte Physik ist eines der drei Institute des Fachbereichs Physik der Technischen Universität Darmstadt.

Der gemeinsame Forschungsschwerpunkt aller Hochschullehrer am Institut für Angewandte Physik ist 'Moderne Optik'. Es stehen Fragen, die die Wechselwirkung von Materie mit Laserstrahlung betreffen, im Mittelpunkt. Zu den Arbeitsschwerpunkten des Instituts zählen insbesondere Quantenoptik, Physik der Quanteninformation, Photonik, ultrakalte Quantengase, Laserphysik, nichtlineare Optik, Halbleiteroptik, optische Informationsverarbeitung, Mikrostrukturforschung, nichtlineare Dynamik, räumlich-zeitliche Strukturbildung und Biophysik.

Die Arbeitsgruppen von Profs. Alber (Theorie), Elsaesser und Walther (Experiment) sind Teil des Darmstädter Zentrums für IT Sicherheit und beschäftigen sich mit den im Artikel diskutierten Fragestellungen der Quantenkryptografie und Quantencomputer sowie mit fundamentalen Fragen der Quantenphysik, aber auch ganz allgemein mit Fragen der Kryptografie.

Ansprechpartner:
Prof. Dr. Gernot Alber

Hochschulstr. 4a
D-64289 Darmstadt
Tel.: +49 61 51 / 16-48 02
Fax: +49 61 51 / 16-32 79

E-mail: gernot.alber@physik.tu-darmstadt.de
Internet: http://www.physik.tu-darmstadt.de/tqp

Prof. Dr. Thomas Walther

Schlossgartenstr. 7
D-64289 Darmstadt
Tel.: +49 61 51 / 16-28 86
Fax: +49 61 51 / 16-45 34

E-mail: thomas.walther@physik.tu-darmstadt.de
Internet: http://www.physik.tu-darmstadt.de/lqo

IT-Sicherheit bei der Gestaltung von IT-Outsourcing

Das Outsourcing von IT-Dienstleistungen erfreut sich insbesondere im Hinblick auf die Nutzung von Einsparpotentialen wachsender Beliebtheit. Unberücksichtigt bleibt mitunter, dass dabei auch sensitive Informationen eines Unternehmens außer Haus gegeben werden. Wichtig ist daher die eindeutige Vereinbarung von Sicherheitszielen und -maßnahmen zwischen Outsourcing-Kunden und -Dienstleistern als auch das Schaffen von geeigneten Kontrollmöglichkeiten, mit denen der Kunde sein IT-Sicherheitsbedürfnis adäquat wahren kann.

Das Verhältnis zwischen Dienstleistungsnehmer und -anbieter hat zwei Facetten. Es lässt sich strukturieren in die Aufgaben des täglichen Betriebs und die Koordination und Steuerung des Dienstleistungsverhältnisses. Auch bei der Wahrnehmung von Aufgaben des täglichen Betriebs kann ein Unternehmen die Kontrolle über wichtige Informationen behalten. Dies kann am Beispiel der Kontrolle wesentlicher administrativer Tätigkeiten erläutert werden. Im Rahmen eines Rechtekonzepts für die Administration ausgelagerter IT-Anwendungen werden z. B. folgende Festlegungen getroffen:

- Der Provider erhält logischen Zugriff auf die installierte Software, jedoch nicht auf die Daten.
- Ein Zugriff auf die Daten durch den Provider ist durch ein geeignetes Zugriffskonzept zu verhindern.
- Die Rechtevergabe für den Provider erfolgt durch den Dienstleistungsnehmer.

Die Kontrolle der Einhaltung dieser Vorgaben basiert auf folgenden Tätigkeiten:

- Systemtechnische Protokollierung aller wesentlichen administrativen Tätigkeiten sowie Weiterleitung der Protokolldaten an den Dienstleistungsnehmer
- Einsatz von Intrustion Detection-Systemen zur Überwachung von Systemaktivitäten und Weiterleitung der Meldungen des IDS-Systems an den Dienstleistungsnehmer
- Regelmäßige Audits des Betriebs unter Einbeziehung der technischen, organisatorischen und personellen Gegebenheiten

Christoph Capellaro
Ernst & Young, München