

den Ablesevorgang zerstört. Das erschwert die Fehlerkorrektur: Auch Qubits können durch Umgebungseinflüsse verfälscht werden. Den Ausweg bietet ein weiteres Phänomen: Zwei Quanten können in einem so genannten verschränkten Zustand existieren. Das heißt: Ändert sich der Zustand des einen, ist auch das zweite Teilchen betroffen. Diese Tatsache lässt sich zur Fehlerkorrektur nutzen.

Andererseits ist es prinzipiell nicht möglich, alle Resultate der parallel abgelaufenen Rechenvorgänge abzulesen. Denn bei der Messung nur eines Ergebnisses wird die Superposition des Qubits zerstört und dieses auf einen Wert festgelegt. Die größte Herausforderung der Wissenschaftler besteht deshalb heute darin, spezielle Rechenalgorithmen zu entwickeln, bei denen sie aus der Kenntnis einzelner Ergebnisse auf andere Resultate schließen können.

Professor Eckhardt Hoenig vom Institut für Physikalische Hochtechnologie in Jena erläutert: „Schon heute liegt eine beträchtliche Zahl raffinierter Algorithmen bereit, mit denen einige auf elektronischen Rechnern nicht zu lösende Rechenaufgaben dann binnen Stunden gelöst werden können.“ Vor allem besonders rechenintensive und wenige Datenzugriffe erfordernde Aufgaben – etwa Fahrplanoptimierungen – seien die Domäne des Quantenrechners, keines-



Skeptischer Forscher: Professor Glaser von der Technischen Universität München sieht noch zahlreiche ungelöste Probleme.

falls Allerweltsaufgaben wie Telefonrechnungen für ganz Europa. Insofern, so Hoenig, werden Quantenrechner ihre elektronischen Kollegen nicht ersetzen, sondern dem „Knacken besonders harter Rechennüsse“ vorbehalten sein. Wie zum Beispiel dem Decodieren geheimer Nachrichten.

Sichere Verschlüsselung

Peter Shor von den Bell Labs fand 1994 ein Verfahren, mit dem ein Quantenrechner Zahlen in ihre Primfaktoren zerlegen kann – und das in einem Bruchteil der Zeit, die ein konventioneller PC benötigt. Das ist von höchster Brisanz: Damit ließen sich heutige Ver-

schlüsselungscodes locker knacken. Trotzdem müssen Geheimdienste nicht um ihre Sicherheit fürchten. Die Quantentheorie liefert die Lösung gleich mit: die Quantenkryptographie.

Sie beruht ebenfalls auf dem Phänomen der Quantenverschränkung. Diese lässt sich dazu nutzen, einen Schlüssel zu generieren, der für sichere Kommunikation zweier Partner sorgt. Den Schlüssel abzufangen bringt einem Angreifer nichts, da er die Nachricht nur gemeinsam mit deren Absender decodieren kann. Der Quantenschlüssel lässt sich auch nicht von dritter Seite kopieren – denn beim Kopiervorgang wird der Schlüssel zerstört.

Wo die Forschung steht

Als Funktionsgrundlage für einen realen Quantencomputer werden heute nicht, wie oben der Einfachheit halber beschrieben, die Flugbahnen von Elektronen genutzt. Steffen Glaser, Professor am Institut für Organische Chemie und Biochemie II der Technischen Universität München, dämpft aufkommende Begeisterung: „Die praktische Realisierung von Quantencomputern steckt noch in den Kinderschuhen und hinkt hinter den theoretischen Möglichkeiten her.“ Insbesondere die Isolierung der Quantensysteme von Umgebungseinflüssen stelle eine Herausforderung dar. Glaser sieht aber eine Reihe interessanter Ansätze, zum Beispiel die Kernspinresonanz, die den Spin – eine Art Drehimpuls – kleinster Teilchen ausnutzt.

Die größten Chancen für künftige Quantencomputer gibt der Jenaer Forscher Hoenig künstlichen, supraleitenden Ringstrukturen, die atomähnliche Eigenschaften haben. Ihr Vorteil: Sie sind leichter zu handhaben als winzige Elektronen und lassen sich, so hat es den Anschein, besser zu größeren Systemen mit einigen Hundert Qubits zusammensetzen.

Matthias Matting m.matting@vhb.de

Links

- Das „Centre for Quantum Computation“
- > www.qubit.org
- Deutschsprachiger Aufsatz zum Thema
- > www.quantencomputer.de
- Forschungsarbeit zur Quantenkryptographie
- > www.quantum.univie.ac.at/research/crypto/

Foto: S. Sahmy/ehm

E-Müll? Zur Kasse, bitte!

>>> ESTHER DYSON über die einfachste Methode, mit Spam fertig zu werden: Die Absender zahlen dafür.

Die US-Regierung denkt derzeit über verschiedene Wege nach, wie mit „Spam“ umzugehen sei – mit E-Mails, meist werblichen Inhalts, die der User ungebeten erhält. (Spam ist übrigens der Name einer Dosenfleischmarke – die von uns Amerikanern mit „wenig nahrhaft“ gleichgesetzt wird.)

Auf juristisch-staatlichem Weg lässt sich das Spam-Problem sicher nicht lösen: aus Gründen der Meinungsfreiheit; weil es schwierig ist, Spam zu erkennen; und weil Spammer ihre Mails ganz leicht außerhalb der Reichweite des Arms des Gesetzes absetzen können. Es gibt eine Reihe technischer Tricks, mit denen Internet Service Provider schon heute Spam abfangen, bevor sie zum User durchdringen. Und Systemadministratoren finden unter <http://mail-abuse.org/rbl> ein „schwarzes Loch“, in das sie Spam von bestimmten, von ihnen in einer Liste verzeichneten Absendern auf Nimmerwiedersehen umleiten lassen können.

Ich aber finde, man sollte es jedem Einzelnen überlassen, ob er Spam bekommen möchte oder nicht. Verschiedene User haben verschiedene Ansichten: Vielleicht findet es der eine oder andere ganz hilfreich, unverlangt Informationen zu bekommen über Schlankheitskuren, den schnellen Weg zum Reichtum oder ein paar Zentimeter mehr an entscheidenden Stellen.

In naher Zukunft werden wir Software haben, die uns bei unserer Entscheidung unterstützt. Zum Beispiel ließen sich Mails von Absendern blockieren, die nicht in Ihrem Mail-Verzeichnis stehen. Natürlich würde solch eine rigide Einstellung auch verhindern, dass Sie Ihren Kreis an Geschäftspart-

Foto: B. Auers



Esther Dyson ist Herausgeberin des Technologie-Newsletters „Release 1.0“, Bestsellerautorin und war früher Vorsitzende der Domain-Verwaltung ICANN. Seit mehr als zwei Jahrzehnten gilt die Amerikanerin als Vordenkerin der IT-Szene. Foto: B. Auers

nern und Freunden erweitern. Aber das lässt sich verfeinern: Die erste Mail des unbekanntes Absenders wird durchgelassen, und Sie müssen mit Ja oder Nein antworten, ob Sie noch weitere Mails wollen. Später können Sie immer noch Ihre Meinung ändern.

Andere Variante: Ihre Software fragt beim Absender nach einem „Begläubigungsschreiben“. Ein Händler könnte so die Gültigkeit der Kreditkarte überprüfen, und Eltern könnten die Mail-Partner ihrer Kinder auf deren Schulkameraden und Freunde beschränken. Microsofts Projekt Hailstorm geht mit der integrierten „Passport“-Funktion in diese Richtung. Trotzdem: Filter schmecken nach staatlicher Kontrolle.

Die beste Lösung wäre doch, wenn der Empfänger für das Lesen von Spam-Mails bezahlt würde. Mal angenommen, meine Grundgebühr für das Empfangen einer Mail beträgt einen Dollar. Wenn mir gefällt, was Sie mir

geschickt haben, verzichte ich auf die Gebühr. Wenn nicht, zahlen Sie, ich blocke weitere Mails und erhöhe die Gebühr auf zehn Dollar. Dann liegt es an Ihnen, zu entscheiden, ob ich Ihnen beim nächsten Mal so viel wert bin. Wenn es Geld kostet, Spam zu versenden, dann wird es weniger davon geben. Spammer werden schnell lernen, welcher Adressat Spam nur akzeptiert, um das Geld zu kassieren.

Das kann im Übrigen zu recht netten Begebenheiten führen: Sie müssten ausdrücklich sagen, dass Sie von der Person, die Sie erst kürzlich auf der Party kennen gelernt haben, keine Mails haben wollen. Politiker müssten Sie durch den Inhalt ihrer elektronischen Werbebotschaft überzeugen, auf Ihre Mail-Gebühr zu verzichten. Vielleicht stecken Sie aber auch einmal in der Zwickmühle: Sollen Sie Ihrem Ex-Partner 100 Dollar für seine letzte Bitte um Versöhnung abknöpfen?

Wie sich herkömmliche Computer und Quantenrechner unterscheiden e-Business



Der klassische Computer arbeitet wie schon Rechenmeister Adam Riese: Wenn an einer Eingabe (hier zweimal die „1“) eine mathematische Operation durchgeführt wird, ist das Ergebnis eindeutig und ändert sich durchs Ablesen nicht.



Der Quantencomputer beruht darauf, dass die Eingabe-Bits nicht nur entweder „1“ oder „0“ sind, sondern auch beide Zustände gleichzeitig annehmen können. Die Rechenoperation wirkt auf alle „Bit-Varianten“ und erzeugt mehrere Ergebnisse. Diese werden allerdings durch den Ablesevorgang zerstört.