DAS MAGAZIN FÜR FORSCHUNG UND TECHNOLOGIE

Innovate!

AUSGABE SEPTEMBER 2005

Frischer Wind für den Umwelt-schutz

Neue Ideen lösen altbekannte Probleme

Herausgegeben von
EADS, GE, Roche, ThyssenKrupp

Zahlen, wie noch

Die mühsame

Wenn schon zufällig, dann gleich richtig. Online-Casinos und alle
Die Lösung liegt – wieder einmal – in der Natur. Wissenschaftler

✎ Karlhorst Klotz ☐ Zefa, Keno

Kann denn Zufall Sünde sein? Wenn Computer sich daran versuchen, anscheinend schon: „Wer Zufallszahlen mit arithmetischen Methoden erzeugen will, befindet sich im Zustand der Sünde“, verfügte schon 1951 John von Neumann, mit dessen Namen das Konstruktionsprinzip moderner Rechner verknüpft ist. Sein Appell war vergeblich, denn es wird ständig gesündigt im Reich der Rechenknechte.

Seit Computer in immer mehr Lebensbereiche vordringen, sind die Verlockungen der scheinbar unvorhersagbaren Zahlen schier unwiderstehlich. Wer auf „sicheren“ Internetseiten unterwegs ist, führt so manchen Webserver in Versuchung, egal ob er sein Bankkonto inspiziert, ein online bestelltes Buch per Kreditkarten-Code bezahlt oder vertrauliche Angaben in ein Web-Formular eintippt. Denn um den Datentransfer auf dem Weg durchs Internet vor begehrlichen Blicken zu schützen, verschlüsseln die Rechner die Botschaften. Dafür benötigen sie laufend Nachschub an Schlüsseln – unverbrauchtes Zahlenmaterial, das ein Angreifer nicht kennen darf.

Das Dilemma dabei ist: Alles, was Rechner tun, ist berechenbar. Woher sollen sie also Ziffernfolgen nehmen, die ein Hacker nicht ebenso gut berechnen könnte? Jedes Kind kennt das Problem: Der Abzählreim „E-ne, me-ne muh – und raus bist Du!“ funktioniert nur so lange, bis die Kleinen bemerken, dass es immer den neunten in der Reihe trifft. Ein ähnliches Problem haben Programmierer, weil selbst noch so komplizierte Rechenvorschriften nicht verhindern, dass sich die erzeugten Werte irgendwann wiederholen. Ein Rechner kann eben nur endlich viele Zahlen in seinem Speicher darstellen und damit nur so genannte Pseudozufallszahlen erzeugen, die bestenfalls eine Zeitlang zufällig aussehen.

Schon die Rangen auf der Straße wissen sich aber zu helfen: „Raus bist Du noch lange nicht, sag mir erst, wie alt Du bist!“ ergänzen die älteren Kinder und bringen damit einen Zufallsgenerator ins Spiel: Das Alter eines Kindes. Ebenso zapfen Techniker eine äußere Zufallsquelle an, damit nicht vorhersehbar ist, wann ein Computer welchen Schlüssel verwendet. In der Praxis sind die aktuelle Uhrzeit oder Nummer des Programms beliebte Startwerte, mit deren Hilfe Computer die eigentlichen Zufallszahlen bestimmen. Auf dem Schleichweg aus der Sündenfalle lauern jedoch Gefahren: Die vom Netscape-Browser im Jahr 1996 verwendeten Geheimschlüssel ließen sich in wenigen Sekunden brechen, nachdem die zwei Doktoranden Ian Goldberg und David Wagner von der University of California, Berkeley, gezeigt hatten, wie ein Angreifer die vermeintlich unbekannten Ausgangswerte stark eingrenzen oder sogar vom Rechner abrufen kann.

In vielen Anwendungen, beispielsweise wissenschaftlichen Berechnungen, können die sündigen Pseudozufallszahlen dennoch

keine waren – Suche nach dem echten Zufall

Krypto-Anwendungen wären sonst schnell am Ende. verwenden Phänomene aus der Quantenphysik, um den Zufall zu fassen

sehr nützlich sein. Sie sind schnell erzeugt und reproduzierbar, so dass sich die Ergebnisse von Computersimulationen in Forschung und Technik zuverlässig überprüfen lassen. Aus schier unerschöpflichen Füllhörnern („Pseudozufallszahlen-Generatoren") scheinen sie zu kommen: Der „Mersenne Twister" rührt die Zahlen nicht nur besonders gleichmäßig durch, sondern liefert erst nach 2^{19937}-1 Schritten (eine Mersenne-Primzahl mit rund 6.000 Stellen) wieder eine identische Zahlenfolge – die Sonne ist längst erloschen, bevor ein Rechner diesen Zahlenstrom ausschöpfen könnte.

Für sicherheitskritische Anwendungen sind Pseudozufallszahlen dennoch nicht geeignet. Ihr großer Nachteil: Erkennt ein Angreifer einen Abschnitt, kann er alle folgenden Werte voraussagen. Das wäre auch für eine Lotterie katastrophal. Kein Wunder, dass deshalb „echte" Zufallsquellen gefragt sind, um einen neuerlichen Sündenfall zu vermeiden. Aber was ist schon ein wirklicher Zufall? „Das ist ein völlig vager Begriff", warnt Peter Hellekalek von der Universität Salzburg, denn „Zufall entsteht im Auge des Betrachters". Mathematisch sauber definieren lässt sich das Konzept nur für unendlich lange Zahlenreihen. Weisen sie keine Regelmäßigkeiten auf, so lassen sich Folgewerte nie aus vorhergehenden berechnen. Dann kann keine Formel die Abfolge der Zahlen beschreiben, keine kürzere Darstellung ist möglich, als alle Werte aufzuzählen.

In der Natur scheinen einige Phänomene dieses Verhalten zu zeigen. Das Rauschen eines Wasserfalls beispielsweise erzeugt über Mikrofon aufgenommen ein wirres Signal, dessen Verlauf nicht vorhersagbar ist. Obwohl die Physik des Wassers an sich keine Geheimnisse birgt, vereitelt die Unzahl der Tröpfchen jeden Versuch, ihre Position und Geschwindigkeit genau genug zu bestimmen und davon auf das Geräusch zu schließen. Das gilt ähnlich für Elektronikbausteine, in denen Ladungsträger die Rolle der Wasserteilchen übernehmen. Sie geben handliche physikalische Quellen für den Zufall ab. Das thermische Rauschen eines Transistors sorgt beispielsweise seit Februar 2004 bei Lotto Hessen dafür, dass die zehn Gewinnzahlen des Spiels Keno nicht von denen früherer Ziehungen abhängen. Dazu kombiniert im Inneren einer futuristischen Pyramide ein ausfallsicheres Rechnersystem Pseudozufallszahlen mit den vom Transistor abgeleiteten, unvorhersehbaren Werten. Das Ergebnis kann selbst Sergio Montenegro vom Berliner Fraunhofer-Institut für Rechnerarchitektur und Softwaretechnik FIRST nicht prophezeien, der das System gebaut und mit 12 Millionen simulierten Ziehungen getestet hat: „Ich habe bei der Einführung von Keno einmal gespielt, aber nichts gewonnen."

Puristen reicht das Rauschen als Quelle für Zufallszahlen längst nicht aus. Auch wenn chaotische Prozesse in der Natur garantieren, dass schon kleine Veränderungen nach kurzer Zeit gewaltige Wirkungen hervorrufen können und damit Prognosen erschweren, bleiben Zweifel. „Selbst chaotische Phänomene lassen sich deterministisch beschreiben", gibt Harald Weinfurter von der

Für das Keno-Zahlenlotto haben Fraunhofer-Forscher einen Rechner entwickelt, der echte Zufallszahlen erzeugt. Interessant ist sein futuristisches Pyramidendesign.

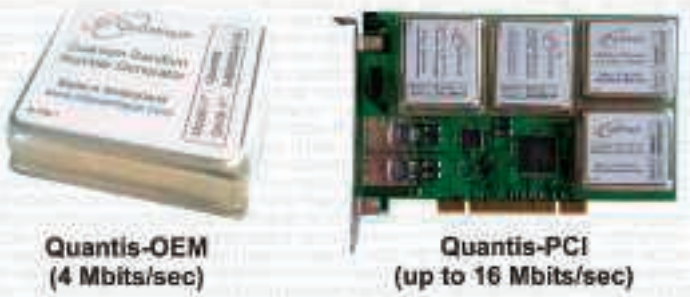
Ludwig-Maximilians-Universität München zu bedenken. „Der quantenmechanische Zufall dagegen ist nicht kontrollierbar, deshalb vertraue ich ihm mehr." Er regiert immer dort, wo es nicht mehr um Massenphänomene, sondern um einzelne Teilchen geht: Dass unter Millionen radioaktiver Atome die Hälfte in einer gewissen Zeit zerfallen, ist bekannt, aber nicht, welches Teilchen dieses Schicksal in welchem Moment erleidet.

Ebenso entscheidet sich an einem halbdurchlässigen Spiegel, ob ein auftreffendes Lichtteilchen ungehindert weiterläuft oder reflektiert wird. Beide Alternativen sind gleich wahrscheinlich, aber nur ein Resultat ist möglich. „Das ist Zufall sozusagen in seiner reinsten Form", meint Weinfurter, „denn welchen Weg das Photon nimmt, hat nichts mit der Vorgeschichte oder anderen Teilchen zu tun, kann also nicht beeinflusst werden". Damit scheinen solche Phänomene ideal geeignet für Anwendungen mit extrem hohem Sicherheitsbedarf, beispielsweise für die Verschlüsselung geheimer Nachrichten. Das einzige beweisbar sichere Krypto-Verfahren beispielsweise arbeitet mit einem Strom von Zahlen, die nur ein einziges Mal benutzt werden (One-Time-Pad). Vom Fenster seines Büros sieht Weinfurter auf einen Turm der Universität München, von dem aus nachts ein Laserstrahl 70.000 Bits pro Sekunde in ein anderes Hochschulgebäude überträgt – unangreifbar dank des aus Quanten-Launen abgeleiteten Zufallsschlüssels.

Dass auch Quantenbits nicht von vorne herein makellos sind, haben Analysen von Peter Hellekalek und seinem Kollegen Stefan Wegenkittl gezeigt. „Wenn man die Werte physikalischer Zufallsgeneratoren zu schnell abfragt, enthalten die Zufallszahlen Korrelationen." Solche Muster würden einem Spion das Handwerk erleichtern. Natürlich lauern handwerkliche Fehler überall: Wer sein Mikrofon auf der Suche nach weißem Rauschen einfach ins Zimmer richtet, muss sich nicht über das fast allgegenwärtige 50-Hertz-Brummen des Stromnetzes wundern. Und jeder physikalische Zufallsgenerator kann wegen technischer Defekte ausfallen.

Entscheidend ist daher die Qualitätskontrolle. Die Genfer Firma id Quantique versucht schon während der Entstehung von Zufallszahlen deren Qualität zu überwachen: Ihr Quantis-System überprüft ständig, ob Lichtquelle und Detektoren richtig arbeiten und ob die Rohdaten innerhalb der erwarteten statistischen Grenzen liegen. Zu den Kunden der ab etwa 1000 Euro erhältlichen Einsteckkarte für PCs gehören nach Auskunft von Geschäftsführer Grégoire Ribordy auch Online-Casinos. Wer mit weniger als vier Millionen Zufallsbits pro Sekunde auskommt, wie sie die PC-Karte in der kleinsten Ausbaustufe liefert, kann solche Zufallszahlen sogar über das Internet beziehen (siehe Kasten).

„Ich sehe nicht, dass die Quantenbits in Kürze andere Zufallszahlen ersetzen", meint Hellekalek. „Diese Verfahren sind viel versprechend, aber noch zu wenig untersucht." Im wissenschaftlichen Neuland wittert sein Kollege Cristian Calude von der Universität in Auckland dagegen sogar Zutaten für den Rechner der Zukunft. „Ein herkömmlicher Computer plus eine Quelle für Quantenzufälle ist jedem normalen Rechner prinzipiell überlegen", argumen-



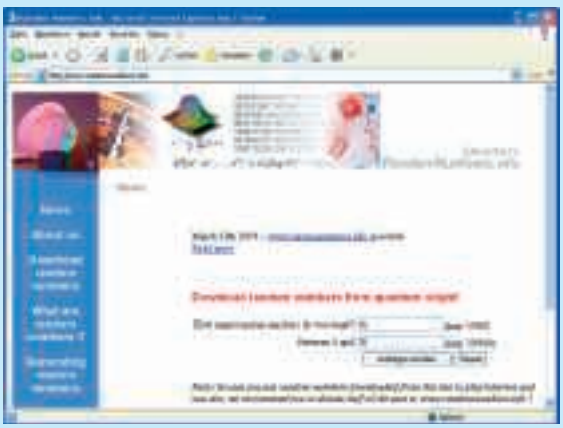
Die Genfer Firma id Quantique bietet eine Steckkarte an, mit der sich in der Ausbaustufe mit vier Modulen 16 Millionen Zufallsbits pro Sekunde erzeugen lassen.

Das Keno-System kombiniert das Rauschen eines Transistors mit einem Pseudozufallszahlen-Generator, um echten Zufall zu erzeugen.

Zufall frei Haus

Wollen Sie Ihrem Glück mit „echten“ Zufallszahlen auf die Sprünge helfen? Also keine im Rechner erzeugten Pseudozufallszahlen (wie in vielen Online-„Quicktipps“), sondern von unvorhersehbaren physikalischen Phänomenen (Quanteneffekte oder Rauschen) abgeleitete Werte? Sie lassen sich bequem und gratis im Internet abrufen. Das Ausgabeformat ist allerdings nicht immer direkt lottoscheintauglich.

- Die Quantenbits der id Quantique (www.randomnumbers.info) rühren von Lichtteilchen her, die an einem halbdurchlässigen Spiegel einen von beiden Wegen nehmen.
- HotBits (www.fourmilab.ch/hotbits/)stammen vom radioaktiven Zerfall. Autodesk-Gründer John Walker misst dazu die Zeitspannen zwischen aufeinander folgenden Zerfällen von Krypton-Atomen.
- www.random.org lauscht auf atmosphärisches Rauschen, wie es im Radio erklingt, wenn es auf einer ungenutzten Frequenz zwischen den Sendern eingestellt ist.
- www.lavarnd.org nutzt im Gegensatz zu seinem Vorgänger „lavarand“ nicht mehr das Bild der in Lavalampen chaotisch aufsteigenden Flüssigkeitsblasen, sondern das Rauschsignal eines Fotosensors, der sich im Dunkeln befindet.



tiert der Mathematiker und Computerwissenschaftler. Der Grund: Traditionelle Computer, so schnell sie auch sein mögen, können nur das errechnen, was der englische Mathematiker Alan Turing schon in den dreißiger Jahren als Limit erkannt hatte. Gewisse Fragestellungen vermögen sie prinzipiell nicht zu lösen, sie kommen bei ihren Berechnungen an kein Ende. Allerdings arbeitet die abstrakte „Turing-Maschine“ ohne Zufallselemente, die – so spekuliert Calude – die Begrenzungen sprengen dürften. „Solche Rechner wären bei manchen Problemen nicht nur schneller, sondern könnten sogar Fragestellungen beantworten, die sich mit herkömmlichen Rechnern nicht lösen lassen.“

Von einem Beweis dieser Aussage ist der Wissenschaftler aus Neuseeland noch weit entfernt. Dass der Zufall nicht nur in der Theorie, sondern manchmal auch im Alltag enorme Probleme elegant lösen hilft, macht er jedoch an seinem Rezept plausibel, eine Überraschungsparty stressfrei zu gestalten: Statt im Vorfeld der großen Mitbring-Fete Dutzende Absprachen mit seinen Gästen zu treffen, empfiehlt Calude, die Wahrscheinlichkeitstheorie für sich arbeiten zu lassen. Der Gastgeber legt dazu auf der Einladung beispielsweise fest: Bitte eine Münze werfen und eine Hauptspeise mitbringen, falls die Vorderseite der Münze oben liegt. Ansonsten noch einmal werfen und eine Vorspeise oder ein Dessert einpacken, je nachdem, ob die Vorder- oder Rückseite der Münze oben liegt. Wenn sich zur Party genügend Gäste einfinden, stehen dann prompt etwa zur Hälfte Hauptspeisen und zu je einem Viertel Vor- und Nachspeisen auf dem Tisch, obwohl der Zufall am Werk war. ■