Zufallszahlen und ihre Anwendung

Lars Richter, Georg Gentzen und Hannes Vogel

Humboldt-Universität zu Berlin

Überblick

- Zufallszahlen werden in einer Vielzahl von Industrien verwendet.
- Die Bereitstellung von Zufallszahlen stellt einen eigenen Industriezweig dar.
- Ein alltäglicher Anwendungsfall ist die Verschlüsselung von Webseiten per TLS/SSL.
- Zudem eignen sich Zufallszahlen zur Simulation von komplexen Systemen.

Zufallszahlen in der Industrie

Zufallszahlen sind für die Industrie von nicht zu vernachlässigender Bedeutung. Viele Branchen benötigen Zufallszahlen für ihre Anwendungen, wobei oftmals nicht direkt offensichtlich ist, dass Zufallszahlen eine tragende Rolle spielen. In Abbildung 1 ist grafisch dargestellt, in welchen Bereichen der Industrie Zufallszahlen von hoher Relevanz sind.

Abbildung 1: Zufallszahlen in der Industrie in den Bereichen Glücksspiel, Verschlüsselung und Simulation.

Neben den Nutzern von Zufallszahlen hat sich eine kleine Branche mit dem Ziel der Erzeugung sowie Bereitstellung von Zufallszahlen entwickelt. Grundsätzlich sind hierbei zu unterscheiden zwischen

1. Firmen, die Zufallszahlen-Generatoren entwickeln und vertreiben und
2. Unternehmen, die bereits generierte Zufallszahlen anbieten.

Entwickler

Beispielhafte Unternehmen, die sog. *echte* ZZGs zum Kauf anbieten sind in Tabelle 1 abgebildet.

Silex Insight	ID Quantique SA	Quintessence Labs

Tabelle 1: Representative Entwickler von Zufallszahlen-Generatoren

Alle drei Anbieter vertreiben Computerchips mit denen sich am eigenen PC beliege Mengen an Zufallszahlen erzeugen lassen.

Anbieter

Unter den Firmen, die Zufallszahlen direkt zum Verkauf anbieten, lassen sich zwei Internetanbieter identifizieren. Das Unternehmen RANDOM.ORG, zeichnet sich durch den Verkauf von *echten* Zufallszahlen aus, die durch das Auslesen von atmosphärischem Rauschen erzeugt werden. Der zweite Anbieter, Random Code Generator, generiert hingegen Codes mit einem physikalisch nicht-korrekt zufälligem Algorithmus. Beeindruckend ist jedoch die Vielzahl der weltweit bekannten, agierenden Unternehmenskunden. Abbildung 2 stellt die Kosten für generierte Zufallszahlen gegenüber. Als Vergleich dient hierbei die Firma ID Quantique mit dem kommerziell am günstigsten verfügbaren ZZG.

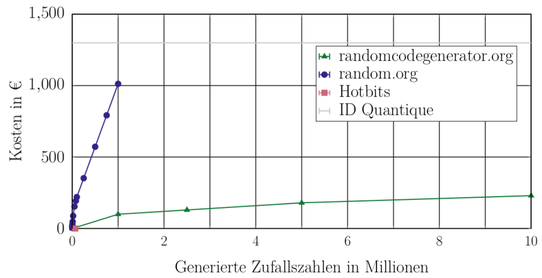

Abbildung 2: Die Kosten von Zufallszahlen.

Post-Quanten-Schlüsselaustausch

Zufallszahlen werden alltäglich für kryptographische Schlüssel u. a. zum verschlüsselten Aufruf von Webseiten oder zur Kommunikation zwischen Smart-Home Geräten verwendet. Eine aktuelle Forschungsfrage ist hierbei, ob sichere elektronische Kommunikation auch möglich ist, wenn Quantencomputer praktisch einsetzbar werden. Diese können fundamentale mathematische Probleme, auf denen derzeitige Schlüsselaustauschverfahren (SAV) basieren, effizient knacken. Tabelle 1 liefert einen Vergleich des Stands der Technik zur einigen potentiellen SAVs, die auch in post-quanten Zeiten (PQ) sicher sein sollen und zu übertragende Datenmengen beim Aufbau von Verbindungen (Handshake).

Schlüssel-austausch	Handshake (bytes) $A \to B$	$A \leftarrow B$	Schlüssel-austausch	Handshake (bytes) $A \to B$	$A \leftarrow B$
NewHope512	67509	1299	NewHope1024	68479	2195
Frodo640	76109	9987	Frodo976	82173	16003
Sidh503	66537	66537	Sidh751	67097	67097
Stand der Technik:			$\text{ECDHE}_{\text{X25519}}$	1403	217

Tabelle 2: Handshake-Größe aktueller Standard zu potenziellen Post-Quanten-Verfahren. Die Verfahren wurden alle mit openssl und AES256-GCM-SHA384 als Ciphersuite simuliert.

Simulationen

Beim **Random Walk** handelt es sich um eine Simulation mithilfe von zufälligen Schrittfolgen. Beispielsweise kann ein physikalisches Teilchen untersucht werden, dass sich nach jedem Zeitschritt in eine zufällige Richtung bewegt (Siehe Abb. 3).

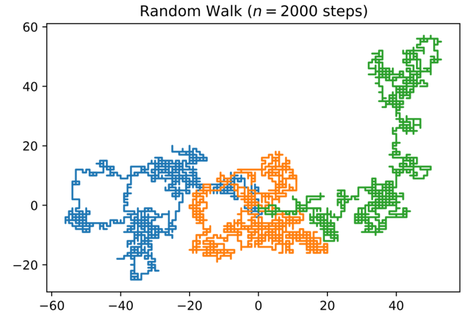

Abbildung 3: Drei verschiedene Random Walks (blau, orange und grün), Simulation nach Subhajit Saha.

Mögliche Anwendungen sind u. a. Diffusionsprozesse, die Ausbreitung von Krankheitserregern oder Gerüchten, Schalltransport in Festkörpern oder der Zahlungsstrom in Wirtschaftssystemen.
Um aufwendige Probleme zu untersuchen, wird die **Monte-Carlo-Simulation** (MCS) genutzt. Dazu werden Zufallsexperimente genutzt, um nach dem Gesetz der großen Zahlen eine Lösung zu ermitteln. Beispielsweise lässt sich die Kreiszahl π durch zufälliges Tippen von Punkten in einem Kästchen ermitteln. Das Verhältnis von Punkten, die im Kästchen und im Kreis liegen zur Gesamtzahl aller Punkte ist eine Näherung für das Verhältnis der Kreisfläche zur Kästchenfläche. Je mehr zufällige Punkte einbezogen werden, desto besser ist die Näherung (Siehe Abb. 4).

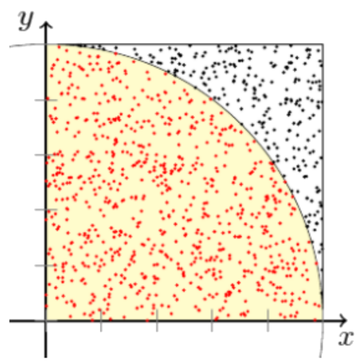

Abbildung 4: Ermittlung von π per MCS [Springob, (CC BY-SA 3.0)].