Christian Kollmitzer
Stefan Schauer
Stefan Rass
Benjamin Rainer *Hrsg.*

Quanten-Zufallszahlengenerierung

Theorie und Praxis

Springer Spektrum

Quanten-Zufallszahlengenerierung

Christian Kollmitzer • Stefan Schauer •
Stefan Rass • Benjamin Rainer
Hrsg.

Quanten-Zufallszahlengenerierung

Theorie und Praxis

Springer Spektrum

Hrsg.
Christian Kollmitzer
Security and Communication Technologies
Center for Digital Safety and Security
AIT Austrian Institute of Technology GmbH
Klagenfurt, Österreich

Stefan Rass
LIT Secure and Correct Systems Lab
Johannes Kepler University
Linz, Austria

Institute for Artificial Intelligence and Cybersecurity
University of Klagenfurt
Klagenfurt, Austria

Stefan Schauer
Security and Communication Technologies
Center for Digital Safety and Security
AIT Austrian Institute of Technology GmbH
Klagenfurt, Österreich

Benjamin Rainer
Security and Communication Technologies
Center for Digital Safety and Security
AIT Austrian Institute of Technology GmbH
Klagenfurt, Österreich

Dieses Buch ist eine Übersetzung des Originals in Englisch „Quantum Random Number Generation“ von Christian Kollmitzer, publiziert durch Springer Nature Switzerland AG im Jahr 2020. Die Übersetzung erfolgte mit Hilfe von künstlicher Intelligenz (maschinelle Übersetzung). Eine anschließende Überarbeitung im Satzbetrieb erfolgte vor allem in inhaltlicher Hinsicht, so dass sich das Buch stilistisch anders lesen wird als eine herkömmliche Übersetzung. Springer Nature arbeitet kontinuierlich an der Weiterentwicklung von Werkzeugen für die Produktion von Büchern und an den damit verbundenen Technologien zur Unterstützung der Autoren.

ISBN 978-3-031-54997-7 ISBN 978-3-031-54998-4 (eBook)
https://doi.org/10.1007/978-3-031-54998-4

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über https://portal.dnb.de abrufbar.

Planung/Lektorat: Caroline Strunz
Springer Spektrum ist ein Imprint der eingetragenen Gesellschaft Springer Nature Switzerland AG und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Gewerbestrasse 11, 6330 Cham, Switzerland

Für meine TochterSophie.

—Christian Kollmitzer

Für meine Familie

—Stefan Schauer

Für meine Familie

—Stefan Rass

Für meine Frau Karin und meine Kinder Killian und Zoey.

—Benjamin Rainer

Vorwort

Vom Zufall zur Zufälligkeit. Eine philosophische Einführung.
Das Problem des Zufalls ist vor allem dort virulent, wo Menschen konkret und existenziell betroffen sind. Das bedeutet, dass durch ein Ereignis, sei es positiv oder negativ, dass jemanden aus seiner Routine oder scheinbaren Sicherheit herauswirft, die Frage aufgeworfen wird, ob jemand oder etwas für dieses Ereignis verantwortlich gemacht werden kann.

Diese Frage stellt sich durch eine günstige Fügung. Wie Aristoteles schon zu Beginn der Nikomachischen Ethik sagte, streben alle Menschen nach dem höchsten Gut, nämlich der *eudaimonia* (Aristot. EN 1095a). *Eudaimonia* kann jedoch auf zwei Arten entstehen. Einerseits kann man für sein Glück arbeiten und versuchen, Bedingungen für ein gelingendes Leben zu schaffen. Auf der anderen Seite bleibt das Glück unverfügbar. Man kann es nicht beeinflussen, um es zu erzwingen. Denn nicht nur die Freiheit der anderen, die einem nicht zur Verfügung steht, ist davon betroffen, sondern auch die grundsätzliche Unfähigkeit, alle Ereignisse, die mit dem eigenen Leben zu tun haben, zu beeinflussen.

Glück, auch Pech, löst existenzielle Betroffenheit aus, für die sich der Mensch im Allgemeinen nicht als Ursache identifizieren kann. Wenn man aber glaubt, dass Ereignisse in der Regel Ursachen haben, dann muss man diese Ursachen jenseits der eigenen Einflusssphären suchen. Zunächst werden andere Menschen in Betracht gezogen, die die Menschen in ihrem Umfeld unterstützen oder ihnen schaden. Diese Menschen können für das eigene Glück oder Unglück verantwortlich gemacht werden, weil man vielleicht für ihre Ziele ausgenutzt wurde und deshalb ein Unglück erlitten haben könnte.

Es gibt aber auch Ereignisse, die sich dem menschlichen Einfluss völlig zu entziehen scheinen, weil niemand als Ursache für ein solches Ereignis zu erkennen ist. Religiöse Menschen machen für diese Ereignisse eine göttliche oder transzendente Macht verantwortlich. Für sie ist diese Macht in der Lage, unerklärliche Ereignisse herbeizuführen. Der Zufall als existenziell berührende Erfahrung hat den Charakter eines Schicksals, das keine bloß immanente Ursache hat. Dennoch wird diesem Zu-

fall eine bestimmte Absicht zugeschrieben. Eine göttliche Macht bewirkt, dass jemandem etwas zustößt, weil sie dazu in der Lage ist und zudem eine bestimmte Absicht für ihr Handeln hat.

Nach der klassischen Vier-Ursachen-Theorie, die zwischen der effizienten und der finalen Ursache unterscheidet, ist das Göttliche oder Transzendente nach der skizzierten These über den Zufall der Auslöser eines Ereignisses sowie der Ursprung einer bestimmten Absicht, die der Betroffene für den Empfänger hat. Der Zufall in Form von Glück oder Pech deutet aus religiöser Sicht auf eine übernatürliche Instanz hin, die absichtlich ein Ereignis herbeiführt, das weder vorhersehbar noch antizipierbar ist, um jemanden zu treffen.

In diesem Sinne ist das Transzendente als eine Instanz zu betrachten, die einerseits Macht über Entwicklungen sowohl in der Natur als auch in der menschlichen Geschichte hat und andererseits eigene Absichten und Ziele verfolgt, sofern sie mit der Welt oder den Menschen verbunden ist. Wenn den genannten Ereignissen, die als Zufälle eingestuft werden, ihr letzter Aspekt abgesprochen wird, d. h. der transzendenten Macht ihre Fähigkeit zur Intention abgesprochen wird, dann wird diese Autorität entpersonalisiert. Hinter einem günstigen oder ungünstigen Zufall steht keine Absicht mehr, sondern ein Ereignis, das einem ohne Adressierung zugestoßen ist. Wenn der Zufall so gehandhabt wird, interpretiert man ihn als Schicksal oder Kismet, ein Ereignis, das nicht von einer göttlichen Macht verursacht wurde, sondern das, obwohl es die Geschichte, auch die Geschichte des Einzelnen, unterbrochen hat, keinen Zweck hat. Während man bei einem göttlich verursachten Ereignis eine Adressierung erwartet, trifft ein Schicksalsschlag den Einzelnen ungeplant und ohne die Möglichkeit, darin einen höheren Sinn zu sehen. Ein Mensch ist betroffen, ohne dass es eine mögliche Erklärung dafür gibt, warum gerade dieser Mensch Glück haben darf oder Unglück erleiden muss. Das Schicksal beeinflusst die Geschichte, aber es hat keinen Zweck und ist ohne Teleologie.

Die modernen Naturwissenschaften suchen nach dem Zufall, indem sie ihn als Schicksal verstehen. Dabei folgen sie den methodischen Vorgaben ihrer eigenen Disziplinen, die an der Kausalität als zentrale Kategorie wissenschaftlicher Erklärungsweise festhalten, aber strikt zwischen effektiver und finaler Kausalität unterscheiden. Absichten, Zwecke und Ziele sind als Erklärungsmöglichkeiten für Naturphänomene fast vollständig eliminiert worden. Sieht man vom anthropischen Prinzip ab, das in abgeschwächter Form ex post als Erklärungsprinzip dient, so gilt die finale Kausalität nicht mehr als legitimer Erklärungsweg. Dies beruht auf dem von Pierre-Simon de Laplace überlieferten Diktum, das er Napoleon auf dessen Frage, warum Laplace in seiner „Mécanique Céleste“ konsequent nicht von Gott spreche, geantwortet haben soll. Laplace antwortete: „Je n’avais pas besoin de cette hypothèse-là“. Diese Ablehnung Gottes als Erklärungsmethode für die naturwissenschaftlich erklärbare Natur kann gleichgesetzt werden mit der Beseitigung der Frage nach einem Ziel oder Zweck der Natur, für die Gott bisher als letzte Instanz angesehen wurde. Charles Darwin folgt dieser Auffassung in „On the Origin of Species“ und in „The Descent of Man“ auch für die belebte Natur und konzipierte evolutionäre Naturphänomene auf diese Weise als Entwicklung ohne Absicht.

Mit dem methodischen Ausschluss finaler Möglichkeiten wird es für das Verständnis des Zufalls – selbst wenn man seine existenzielle Bedeutung für den Menschen im Auge behält – notwendig, nicht die finale, sondern ausschließlich die effektive Kausalität heranzuziehen. Der Zufall wird als ein kausales, aber nicht mehr als ein finales Ereignis betrachtet. Für eine wissenschaftliche Theorie bedeutet diese Forderung, dass man den Zufall streng durch effiziente Kausalität erklären kann. Dazu bietet es sich an, ein zufälliges Ereignis so zu setzen, dass ein Kausalnexus, der zur Erklärung eines Ereignisses beitragen soll, auf einen anderen so trifft, dass sich beide an einem Punkt kreuzen und somit etwas Zufälliges geschieht. Eine solche Kreuzung sorgt für ein Überraschungsmoment, da zwar teilweise zwei Kausalbedingungen für das Ereignis angegeben werden können, es aber unmöglich ist, einen Kausalnexus zu finden, der für die Erklärung ausreicht und in dem alle Kausalketten zumindest indirekt miteinander verbunden sind. Es treffen zwei Ereignisse aufeinander, die beide für sich als kausal erklärt werden können (nicht aber das Zusammentreffen der beiden).

Diese Sichtweise des Zufalls zeichnet sich einerseits durch das Fehlen einer finalen Kausalität aus und andererseits durch den Versuch, den Grund des Ereignisses durch effektive Kausalität zu entdecken, ohne eine Struktur kausal verknüpfter Bedingungen, geschweige denn einen geschlossenen Ursachenkomplex zu benennen. Diese Sichtweise auf den Zufall bleibt insofern unbefriedigend, als sich die Frage, warum sich die beteiligten Kausalketten gerade in diesem Moment überschneiden, immer wieder neu stellt. Üblicherweise geht man davon aus, dass es dafür einen Grund geben muss, weil wir den Satz vom (hinreichenden) Grund (nihil est sine ratione sufficiente) für wahr halten. Das bedeutet, dass – ontologisch gesprochen – nichts ohne einen hinreichenden Grund geschehen kann, der das Ereignis hervorruft. Wenn man so denkt, dann wird versucht, die für den Zufall angenommene Unbegründetheit zu verwerfen. Es wird also versucht, nicht die Zufälligkeit des Ereignisses für wahr zu halten, sondern die kausale Gleichförmigkeit aller Naturereignisse zu verteidigen.

Es gibt zwei Möglichkeiten, dieser schwierigen Situation zu entkommen. Erstens kann man versuchen, den Kausalzusammenhang als noch zu finden zu bewerten. Man geht davon aus, dass der Zusammenhang prinzipiell gefunden werden kann, auch wenn dieser Ansatz – aus einem unbekannten Grund – in der Gegenwart nicht als möglich angesehen wird.

Zweitens kann man versuchen, die Unbegründetheit des Zufalls zu begründen. In diesem Fall wird nach Gründen für die Unfähigkeit gesucht, Verbindungen zwischen den Kausalketten zu finden. Man fragt nach Gründen, warum es keine Ursachen gibt, die alle Ereignisse miteinander verbinden. Auf einer Metaebene sollen Gründe gefunden werden, die erklären, warum es keine Ursachen auf der ersten Ebene gibt. Damit wird versucht, die kausale Einheit zu erhalten, auch wenn sie abgeschwächt ist. Das Fehlen der Möglichkeit, ein Ereignis durch Ursachen auf der ersten Ebene zu erklären, wird zugegeben, aber auf der zweiten Ebene wird versucht, Gründe dafür zu finden, dass keine Ursachen gefunden werden können.

Radikaler als die genannten Versuche, die kausale Einheit zu retten und damit den Zufall zu relativieren, ist die Annahme, dass sich für bestimmte Ereignisse

weder kausale Zusammenhänge noch Algorithmen finden lassen. Anstatt Gründe für das Fehlen von Ursachen zu finden, räumt man ein, dass die Tatsache ontologisch behandelt werden muss, dass es Widersprüche im Naturgeschehen gibt, die das Prinzip der hinreichenden Vernunft und eine kausal geschlossene Natur fragwürdig erscheinen lassen.

Es handelt sich nicht um die Annahme, dass die Unfähigkeit zu denken oder das vorübergehende Fehlen einer wissenschaftlichen Erklärung dazu zwingt, von Zufall zu sprechen. Vielmehr geht dieser Begriff des Zufalls davon aus, dass die Wirklichkeit teilweise chaotisch und in diesem Sinne nicht erklärbar ist. Anders als eine Chaostheorie, die trotz der Vervielfachung von kleinen Unterschieden am Anfang zu großen Unterschieden im Ergebnis (nach vielen Iterationen) von einer grundsätzlichen Kausalität des Geschehens ausgeht, beruht der Zufall so gesehen auf einem fundamentalen ontologischen Chaos. Das bedeutet, dass dem Zufall sowohl die finale als auch die globale effiziente Kausalität fehlt. Der Zufall ist zur Zufälligkeit geworden.

Für ein wissenschaftliches Konzept des Zufalls bedeutet eine solche Theorie, an die Grenzen des kausalen Denkens im Allgemeinen zu gelangen. Wenn man über die methodischen Vorgaben von Laplace und Darwin hinausgeht und Endursachen als Erklärungsmöglichkeiten insgesamt ausschließt, stößt man an die Grenzen des Erklärbaren, wenn man den Zufall in den Blick nimmt. Denn neben den nur für eine Dingontologie relevanten Arten der Verursachung (nämlich der materiellen und der formalen Ursache im aristotelischen Sinne) bleibt mit dem Wegfall der Teleologie nur noch die effiziente Verursachung wissenschaftlich relevant. Wenn auch diese in Frage gestellt wird, dann ist das Wagnis, Natur oder Wirklichkeit kausal zu erklären, an seine eigene Grenze gestoßen. Die methodischen Möglichkeiten der Kausalität scheinen sich im Zufall im Sinne der Zufälligkeit zu erschöpfen. Solche Zufälle werden nur entdeckt, ohne die Möglichkeit zu haben, sie zu erklären. Die Naturwissenschaften werden dadurch auf ihre eigenen Voraussetzungen zurückgeworfen.

Vielleicht ist das der Grund, warum die Frage nach Zufall und Zufälligkeit auch oder gerade für die Naturwissenschaften höchst attraktiv ist.

Graz, Österreich — Reinhold Esterbauer
November 2019

Über die Schwierigkeit, einen „richtigen Zufall“ zu erzeugen

Der Begriff „Zufälligkeit“ suggeriert bisweilen den Gedanken an Statistiken, wie Verteilungen und Wahrscheinlichkeiten für bestimmte Ergebnisse, und – vor allem in der Kryptographie – an Unvorhersehbarkeit. Ironischerweise definiert die Statistik eine Zufallsvariable formal als eine messbare Abbildung, die in keiner Weise auf die Unvorhersehbarkeit anspielt (der Begriff „unvorhersehbar“ wird in gebräuchlichen Definitionen von Zufallsvariablen gar nicht verwendet). Zufälligkeit in der Statistik und Zufälligkeit in der Kryptografie sind also von Natur aus verschiedene Dinge, auch wenn letztere eindeutig auf ersterer beruht. In der Kryptografie sind wir in erster Linie an Unabhängigkeit, Gleichverteilung und Unvorhersehbarkeit interessiert. Keine dieser Eigenschaften ist notwendigerweise mit guten statistischen Eigenschaften verbunden, wenn wir nur an Verteilungen denken: Betrachten wir als Beispiel die unendliche Bitfolge 0101010101 … Offensichtlich ist die Verteilung von 0en und 1en in dieser Folge vollkommen gleichmäßig, aber sie ist ebenso offensichtlich vorhersehbar; schlimmer noch, sie ist eindeutig periodisch. Sequenzen, die nicht periodisch sind, sind leicht zu finden (wie die Mantisse einer irrationalen Zahl wie $e, \pi, \sqrt{2}$), sind aber in der Regel für die Kryptografie dennoch nicht brauchbar. Sogenannte Tröpfelalgorithmen ermöglichen die Berechnung einzelner Ziffern für viele solcher Zahlen, ohne dass die gesamte Mantisse bis zur gesuchten Ziffer berechnet werden muss, und wir könnten eine geheim gewählte irrationale Zahl[1] verwenden, um einen Pseudozufallsgenerator zu initialisieren, welcher nur die Ziffern in der Mantisse berechnet. Aber solche Zahlen können schlechte statistische Eigenschaften haben, die es leicht machen, sie aus einer Aufzeichnung vergangener Werte vorherzusagen. Gibt es Sequenzen, die leicht zu berechnen sind, gute statistische Eigenschaften haben und nie periodisch werden? Tatsächlich existieren solche Zahlen, wie etwa die berühmte Champer-

[1] Die Auswahl solcher Zahlen aus den ganzzahligen Parametern ist einfach, da zum Beispiel das Polynom $ax^2 + bx + c$ nur irrationale Wurzeln hat, wenn a, b, c ungerade Zahlen sind; ebenso ist $\sqrt[n]{1+(a/b)^n}$ durch den Satz von Fermat-Wiles für positive ganze Zahlen a, b i.A. irrational für n > 2.

nowne-Konstante, welche durch Verkettung aller natürlichen Zahlen in der Mantisse in aufsteigender Reihenfolge entsteht, d. h.,

$$C := 0.12345678910111213141516 17\ldots$$

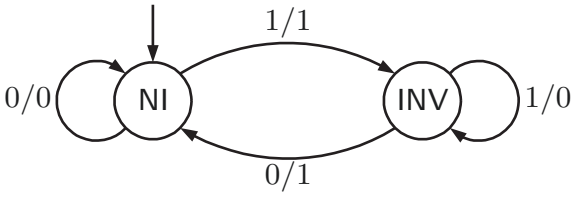
Diese Zahl ist irrational, da in ihr Sequenzen von Nullen (oder anderen Ziffern) beliebiger Länge enthalten sind, so dass es keine feste Periode geben kann. Noch besser: Es lässt sich zeigen, dass es sich um eine *normale Zahl* handelt, was Folgendes bedeutet: Gegeben sei eine zufällige Zeichenkette w über das Alphabet Σ, z. B. $\Sigma = \{0,1,2,\ldots,9\}$. Nehmen wir an, dass die Symbole (Ziffern) in w unabhängig und gleichverteilt über Σ sind, d. h. wir erstellen w, indem wir Symbole mit Zurücklegen aus Σ ziehen und konkatenieren. Dann hat jedes konkrete Wort w eine „natürliche“ Auftretens-Wahrscheinlichkeit von $Pr(w) = |\Sigma|^{-|w|}$, wenn $|w|$ die Länge von w (in Ziffern) bezeichnet. Eine normale Zahl, wie die Champernowne-Konstante, zeichnet sich dadurch aus, dass *jede* zufällige Zeichenkette w in der gesamten Mantisse mit ihrer natürlichen Wahrscheinlichkeit vorkommt (so wie zuvor definiert). Somit hätte C, wie jede andere normale Zahl auch, die perfekten statistischen Eigenschaften: Wenn wir aus ihrer Mantisse Ziffernketten entnehmen zur Erzeugung zufälliger Strings, so erhalten wir Ergebnisse mit perfekten statistischen Eigenschaften. Ein berühmtes Theorem von E. Borel besagt zudem, dass fast alle Zahlen normale Zahlen sind. Obwohl es somit sehr viele normale Zahlen gibt, sind nur wenige explizit bekannt, und die Champernowne-Konstante ist eine von ihnen. Obwohl sie sehr einfach zu berechnen ist und perfekte Eigenschaften hinsichtlich der Verteilung der Zeichenfolgen, gebildet aus ihrer Mantisse, hat, macht ihre triviale Vorhersagbarkeit sie für kryptografische Zwecke unbrauchbar.

Aus diesen (und anderen) Gründen verwenden kryptografische Zufallszahlengeneratoren typischerweise eine Transformationsfunktion f, um neue Zufallswerte aus vergangenen Zufallswerten zu berechnen. Hierfür gibt es verschiedene Konstruktionen wie Pseudozufallszahlengeneratoren (PRNGs) oder Pseudozufallsfunktionen (PRFs) [1], mit für Kryptographie geeigneten Vorhersagbarkeitseigenschaften unter berechenmäßigen Komplexitäts-Annahmen (siehe [3] für einen Überblick). Betrachten wir eine generische Art und Weise, wie ein PRNG auf der Grundlage von Iterationen konstruiert werden kann: Wir wählen eine Funktion f und einen zufälligen Startwert x_0, von dem aus wir eine Folge $x_{n+1} := f(x_n)$ für $n = 0,1, \ldots$ iterieren. Wenn f eine Abbildung zwischen endlichen Mengen ist, wird jede solche Folge notwendigerweise periodisch, und Abschätzungen ab welcher Iteration dies spätestens geschieht, sind bekannt [2]. Können wir das Problem umgehen, indem wir f auf unendlichen Mengen operieren lassen? Genauer gesagt, können wir eine Funktion f verwenden, welche deterministisch ist, aber stochastisch „wirkt“? Auch hier ist die Antwort positiv, da eine chaotische Funktion dies prinzipiell leisten könnte. Warum verwenden wir daher nicht eines der beiden berühmtesten Beispiele wie die logistische Abbildung $f(x) = \lambda \cdot x(1 - x)$ oder die Dreiecks-Funktion $f(x) := \mu \cdot \min\{x, 1 - x\}$, bei denen das tatsächliche Verhalten durch die Wahl von $\lambda > 0$ oder $\mu > 0$ bestimmt wird? Die beiden sind eng mit-

einander verwandt (tatsächlich sind sie topologisch konjugiert), aber die Dreiecks-Funktion hat einige sehr angenehme Eigenschaften:

- Wenn die Iteration mit einem irrationalen Wert x_0 beginnt, wird die resultierende Folge niemals periodisch.
- Die Folge ist sensitiv abhängig von den Anfangsbedingungen, was intuitiv bedeutet, dass jeder beliebig nahe, aber dennoch ungleiche Startwert $x_0' \neq x_0$ dazu führt, dass die resultierende Sequenz beliebig weit von der tatsächlichen Folge abweicht, die von x_0 startet. Dies kann als „Informationsverlust“ bei jedem Schritt verstanden werden, da die Dreiecks-Funktion nicht injektiv ist, da es für jedes Bild mindestens zwei mögliche Urbilder gibt. Somit können wir aus der Beobachtung der Sequenz niemals eindeutig auf den Startwert zurückschließen, was auf den ersten Blick als die gewünschte Eigenschaft erscheint. Es zeigt sich jedoch, dass trotz dieser Tatsache, die gewünschte Wirkung nicht erzielt wird.
- Wenn man von einer irrationalen Zahl x_0 ausgeht und $\mu = 2$ verwendet, ist die Wirkung der Dreiecks-Funktion auf eine irrationale Zahl in Binärform mit den Bits $b_1 b_2 b_3 \ldots$ wie folgt:
  - Verschiebung des Dezimalpunktes um eine Stelle nach rechts.
  - Wenn vor dem Dezimalpunkt eine 1 steht, werden die nachfolgenden Bits invertiert.

Die Wirkung der Dreiecks-Funktion kann somit durch einen einfachen Mealy-Automaten beschrieben werden: Der Zustandsübergang „a/b“ bedeutet, dass der Automat beim Lesen des Symbols „a“, das Symbol „b“ ausgibt. Demnach benötigen wir einen „invertierenden Zustand“ (INV) und einen „nicht-invertierenden“ Zustand (NI), um die Dreiecks-Funktion von einem irrationalen Ausgangspunkt x_0 des Automaten aus zu berechnen:



Analysieren wir nun die Intuition, eine chaotische Funktion ausgehend von einen Startwert wie C zu iterieren, um die Vorteile beider zu vereinen: perfekte statistische Eigenschaften (aufgrund der Normalität von C) mit Unvorhersehbarkeit aufgrund von deterministischem Chaos (aufgrund der Dreiecks-Funktion). Es ist in der Tat eine einfache Aufgabe zu überprüfen, dass der Automat letztlich alle im Startwert enthaltenen Informationen „verbraucht“ (wie wir es aufgrund der sensitiven Abhängigkeit von den Anfangsbedingungen und der Nicht-Injektivität der Dreiecks-Funktion erwarten würden), aber zwei Folgen können dennoch früher oder später in *dieselbe* pseudozufällige Sequenz konvergieren. Genauer gesagt, seien $x_0 \neq x_0'$

zwei Startwerte, die sich von C nur durch eine endliche Anzahl von Ziffern unterscheiden. Das bedeutet, dass der so konstruierte Pseudozufallsgenerator unabhängig vom verwendeten Startwert und einer festen normalen Zahl (C wurde hier willkürlich gewählt) für kryptografische Zwecke keinesfalls nutzbar ist. Intuitiv wird dies deutlich, wenn man sich den Mealy-Automat zur Auswertung der Dreiecks-Funktion genauer ansieht: Die Maschinerie zur Berechnung der Zufallsausgaben ist endlich, aber für die Unvorhersehbarkeit benötigen wir in jeder Ausgabe neue Informationen, die nicht aus vergangenen Beobachtungen gewonnen werden können. Da der irrationale Wert C Teil des Algorithmus ist und nur die Abweichung davon das Geheimnis darstellt, kann von einer deterministischen (endlichen) Maschinerie nicht erwartet werden, dass sie die notwendige Menge an Informationen „erzeugt“, um letztendlich Unvorhersehbarkeit zu erreichen. Das ist es, was J. von Neumann in seinem berühmten Zitat zum Ausdruck bringt:

> „Anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin.“

Als Konsequenz dieser Überlegungen folgt, dass wir Bausteine mit guten statistischen Eigenschaften nicht unreflektiert zu einem kryptografisch sicheren Zufallszahlengenerator (random number generator, RNG) zusammensetzen können; solche Intuitionen können leicht irreführend sein. Die oben skizzierten Ideen dienen nur der Veranschaulichung, zeigen aber im Allgemeinen, dass selbst perfekte statistische Eigenschaften oder scheinbar perfekte Unvorhersehbarkeit (die wir uns von der Chaostheorie erhofft haben, die – anders als ein Großteil der Kryptografie – nicht auf berechenmäßigen Komplexitätsannahmen beruht) zusammengenommen keine guten Ergebnisse für die Kryptografie liefern müssen. Letztendlich sind für Pseudozufallszahlenfolgen (deren Reproduzierbarkeit oft der einzige Grund ist, sie dem echten Zufall vorzuziehen) komplexere Konstruktionen erforderlich und berechenmäßige Komplexität bleibt weiterhin bis heute eine unabdingbare Grundlage hierfür. Eine funktionierende, einfache Konstruktion mit maximaler Periodizität der entstehenden Pseudozufallsfolge ist etwa die AES-Verschlüsselung eines geheimen Zählers, die in einer Zeile C++-ähnlichem Pseudocode implementiert werden könnte: Wenn wir den Zähler mit einem geheimen Wert i_0 initialisieren, erhalten wir die nächste Zufallszahl als

$$\texttt{AES}\big(\texttt{++i,k}\big)$$

wobei k ein weiteres im PRNG gespeichertes Geheimnis ist.

Dies ist in der Tat eine kryptographisch brauchbare Konstruktion, und die Standard-Qualitätsbewertungen für PRNG, die wir später im Buch sehen werden, dass die Ausgabe den Anforderungen kryptographischer Anwendungen entspricht.

Die Sicherheit einer solchen Konstruktion liegt in der Geheimhaltung des Anfangswertes i_0 *und* des geheimen Schlüssels k. Verallgemeinern wir unsere Sichtweise und nennen s den geheimen Startwert, welcher aus einer Zufallsvariable S gewonnen wird. Wie würden wir die „Güte“ des Startwerts quantifizieren? Die Shan-

non-Entropie wird bisweilen als Maßzahl hierfür vorgeschlagen, aber das ist formal nicht gänzlich richtig: „Entropie“ ist zwar ein geeignetes Konzept, jedoch nicht die *Shannon*-Entropie! Da wir das Erraten eines Geheimnisses nicht verhindern können, wie schwierig wäre es dann, *s* zu erraten?

Die Verteilung von *S* sei $\left\{(s_i, p_i = \Pr(S = s_i))\right\}_{i=1}^{n}$ mit $s_i \in \{0,1\}^\ell$ und $p_i \geq 0$, so dass $p_1 + p_2 + \ldots + p_n = 1$. Die *Min-Entropie* von *S* ist definiert als

$$H_\infty(S) = -\log\left[\max_i \left\{\Pr(S = s_i)\right\}\right].$$

Nach dieser Definition haben wir für alle $s : \Pr(S = s) \leq 2^{-H_\infty(S)}$. Wenden wir uns nun der Aufgabe zu, den unbekannten Startwert s_0 zu erraten, was mit der Wahrscheinlichkeit p_0 gelingt: Die durchschnittliche Anzahl *N* von Versuchen, bis wir Erfolg haben, folgt einer geometrischen Verteilung mit dem Parameter p_0, und dessen Mittelwert ist

$$N = \frac{1}{p_0} \geq 2^{H_\infty(S)}.$$

$H_\infty(S)$ liefert also offensichtlich eine untere Schranke für die durchschnittliche Anzahl von Versuchen bis zum Erfolg, so dass $H_\infty(S)$ als Maß für die Schwierigkeit angesehen werden kann, den Startwert zu erraten. Kann die Shannon-Entropie auch hierfür genützt werden? Die Antwort ist im Allgemeinen negativ, wie das folgende Beispiel zeigt:

Sei $0 < q < 1$ ein fester und sehr kleiner Wert, mit welchem wir die Zufallsvariable *S* über der Menge $\{0,1,\ldots,n\}$ definieren wie folgt:

- $S = 0$ tritt mit der Wahrscheinlichkeit $1 - q$ auf,
- $S \in \{1,2,\ldots,n\}$ tritt gleichverteilt mit Wahrscheinlichkeit q/n auf.

Die Min-Entropie ist $H_\infty(S) = -\log(q)$, aber die Shannon-Entropie ist

$$H(S) = -\sum_{i=0}^{n} p_i \cdot \log(p_i) = -(1-q)\cdot\log(1-q) - \sum_{i=1}^{n} \frac{q}{n}\log\left(\frac{q}{n}\right)$$

$$= -(1-q)\cdot\log(1-q) - q\cdot\log\left(\frac{q}{n}\right) \in \Omega(\log n)$$

Offensichtlich gilt $H(S) \to \infty$, wenn wir *n* gegen unendlich streben lassen, während die Min-Entropie für alle *n* konstant bei $\log(q)$ bleibt. Das bedeutet, dass wir eine Zufallsvariable mit *beliebig großer* Shannon-Entropie definieren können, deren Erraten stets einfach ist, da wir nur $S = 0$ als das wahrscheinlichste Ergebnis annehmen dürfen.

Der allgemeine Begriff „Entropie“ kann, ohne weitere Angaben, leicht als Shannon-Entropie fehl-interpretiert werden, obwohl für kryptografische Zwecke,

insbesondere immer dann, wenn von der Qualität der Startwerts für einen Zufallsgenerator gesprochen wird, die *Min-Entropie* gemeint und erforderlich wäre.[2]

Dies führt direkt zu Möglichkeiten, wie Hintertüren in einem RNG implementiert werden können: Angenommen, ein RNG ist (aufgrund mangelnder Sorgfalt) so spezifiziert, dass er einen Startwert mit einer hohen „Entropie“ hat (wobei die Art von Entropie nicht angegeben wird, so dass eine Lesart als „Shannon-Entropie“ denkbar und ggf. sogar wahrscheinlich ist), dann hat die Verwendung eines Startwertes, etwa aus dem oben beschriebenen Zufallsprozess entstammend, verheerende Folgen:

- Die Spezifikation entspricht Anforderungen wie „Zufallsgeneratoren benötigen Startwerte mit mindestens 128 Bit Entropie“.
- aber das Erraten des Startwerts und das Reproduzieren der RNG-Ausgabefolge ist aber dennoch einfach.

Selbst wenn der RNG korrekt mit Seeds von hoher Min-Entropie initialisiert ist, könnte ein anderer Angriff darin bestehen, den kryptographisch korrekten Generator durch einen zu ersetzen, dessen Werte (bei Kenntnis geeigneter Geheimnisse) leicht vorhersagbar sind. Nehmen wir zum Beispiel zwei Generatoren an, die beide auf der AES-Verschlüsselung von Zählern basieren, wobei G_1 einen Startwert und Schlüssel mit hoher Min-Entropie besitzt, während G_2 einen Startwert und Schlüssel mit hoher Shannon-, aber niedriger Min-Entropie hat. In diesem Fall ist die Ausgabe von G_1 praktisch nicht von der Ausgabe von G_2 zu unterscheiden (wie für den AES empirisch überprüft werden kann), so dass ahnungslose Anwender:innen unwissentlich Zufallswerte verwenden, die ein Angreifer leicht erraten und reproduzieren könnte. Jeder kryptografische Schlüssel oder andere Parameter, die auf diese Weise erstellt wurde, ist von Natur aus unsicher, unabhängig davon, wie gut die sonstigen kryptografischen Verfahren ist.

Darüber hinaus muss auch die Bedeutung des Begriffs „hohe Entropie“ genauer geklärt werden: Reicht es aus, etwa 128 Bit Entropie zu verlangen? Wenn wir versuchen, technologischen Steigerungen der Rechenleistung zu entgehen, dann muss „hoch“ als asymptotische Anforderung an die Min-Entropie verstanden werden, welche $H_\infty(S) \in \omega(\log t)$ erfüllen sollte, wobei t der Sicherheitsparameter und ω das Landau-Symbol sind. Unter diesen Umständen gilt für jede Konstante $c > 0$ und für alle hinreichend großen n stets: $H_\infty(S) > c \cdot \log(n)$. Im Weiteren bedeutet dies, dass

$$\Pr\left(S = s\right) \leq 2^{-H_\infty(S)} < 2^{-c \cdot \log(n)} = n^{-c}$$

[2] Dies wird in der Dokumentation von Software oder Geräten nicht immer deutlich gemacht. Mit Stand vom 19. Januar 2020 spricht die Dokumentation von OpenSSL (siehe https://wiki.openssl.org/index.php/Random_Numbers) nur von „Entropie“, ohne ausdrücklich darauf hinzuweisen, dass eigentlich die Min-Entropie gemeint ist. So kann ein:e Benutzer:in stattdessen fälschlicherweise Startwerte mit hoher Shannon-Entropie verwenden, was aufgrund der in diesem Detail ungenauen Dokumentation zwar mit der Spezifikation konform ist, aber dennoch eine unsichere Parametrisierung darstellen würde.