

Quantum Science and Technology

Christian Kollmitzer
Stefan Schauer
Stefan Rass
Benjamin Rainer *Editors*

Quantum Random Number Generation

Theory and Practice

 Springer

Quantum Science and Technology

Series Editors

Raymond Laflamme, Waterloo, ON, Canada

Gaby Lenhart, Sophia Antipolis, France

Daniel Lidar, Los Angeles, CA, USA

Arno Rauschenbeutel, Vienna University of Technology, Vienna, Austria

Renato Renner, Institut für Theoretische Physik, ETH Zürich, Zürich, Switzerland

Maximilian Schlosshauer, Department of Physics, University of Portland, Portland, OR, USA

Yaakov S. Weinstein, Quantum Information Science Group, The MITRE Corporation, Princeton, NJ, USA

H. M. Wiseman, Brisbane, QLD, Australia

The book series Quantum Science and Technology is dedicated to one of today's most active and rapidly expanding fields of research and development. In particular, the series will be a showcase for the growing number of experimental implementations and practical applications of quantum systems. These will include, but are not restricted to: quantum information processing, quantum computing, and quantum simulation; quantum communication and quantum cryptography; entanglement and other quantum resources; quantum interfaces and hybrid quantum systems; quantum memories and quantum repeaters; measurement-based quantum control and quantum feedback; quantum nanomechanics, quantum optomechanics and quantum transducers; quantum sensing and quantum metrology; as well as quantum effects in biology. Last but not least, the series will include books on the theoretical and mathematical questions relevant to designing and understanding these systems and devices, as well as foundational issues concerning the quantum phenomena themselves. Written and edited by leading experts, the treatments will be designed for graduate students and other researchers already working in, or intending to enter the field of quantum science and technology.

More information about this series at <http://www.springer.com/series/10039>


Christian Kollmitzer · Stefan Schauer ·
Stefan Rass · Benjamin Rainer
Editors


Quantum Random Number Generation

Theory and Practice


 Springer

Editors

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

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

Stefan Rass 
Institute of Applied Informatics
Universität Klagenfurt
Klagenfurt, Austria

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

ISSN 2364-9054 ISSN 2364-9062 (electronic)
Quantum Science and Technology
ISBN 978-3-319-72594-9 ISBN 978-3-319-72596-3 (eBook)
<https://doi.org/10.1007/978-3-319-72596-3>

© Springer Nature Switzerland AG 2020

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Dedicated to Judith and Sophie.
—Christian Kollmitzer

To my family
—Stefan Schauer

To my family
—Stefan Rass

For my wife Karin and children, Killian and Zoey.
—Benjamin Rainer

Foreword

From coincidence to randomness. A philosophical introduction.

The problem of coincidence is virulent especially where humans are affected concretely and existentially. This means that through an occurrence, be it positive or negative, that throws someone out of their routine or seeming confidence, the question gets aroused whether someone or something can be held responsible for this occurrence.

This question arises through a beneficial coincidence. Like Aristotle said already at the beginning of *Nicomachean Ethics*, all humans search for the highest good, namely, *eudaimonia* (Aristot. EN 1095a). However, *eudaimonia* can occur in two ways. On the one hand, one can work for one's happiness and try to create conditions for a successful life. On the other hand, luck stays unavailable. One cannot influence it in order to force it to happen. Because not only the freedom of others, which is not at one's disposal, is affected by it, but also the fundamental inability to influence all the events that have to do with one's own life.

Luck, including bad luck, make someone feel existential concern, which people generally cannot identify themselves as causes for. But if you believe that events usually have causes for happening, then these causes have to be looked for beyond the spheres of one's own influence. At first, other people, who support or harm those around them, are considered. These people can be held responsible for one's good or bad luck, because one may have been exploited for their goals and therefore could have suffered misfortunes.

But there are also events that seem to be completely withdrawn from human influence, because nobody can be recognized as the cause for such an event. Religious people will hold a divine or transcendent power responsible for these events. For them, this power is able to induce inexplicable occurrences. Coincidence as an existentially touching experience has the character of fate, which does not have a merely immanent cause. Nevertheless, this coincidence is attributed a particular intention. A divine power causes something to happen to someone because it is able to do so and additionally has a certain intention for its actions.

According to the classical theory of the four causes, which distinguishes between the efficient and the final cause, the divine or the transcendent according to the outlined thesis about coincidence is the trigger of an event, as well as the origin of a certain intention that the affected person has for its recipient. Coincidence in the form of good or bad luck, religiously seen, hints at a supernatural authority that intentionally causes an event that can neither be predicted nor anticipated to happen to someone.

In this sense, the transcendent has to be regarded as an authority that on the one hand has power over developments both in nature and in human history, and on the other hand has its own intentions and goals, as long as it is connected to the world or humans. If the mentioned occurrences, which are classified as coincidences, are denied their final aspect, meaning that the transcendent power is denied its ability of intention, then this authority is depersonalized. Behind a favorable or unfavorable coincidence, there is no intention anymore, but an event that has befallen one without any addressing. If coincidence is handled that way, one interprets it as fate or *kismet*, an event that has not been caused by a divine power, but that, even though it interrupted history, also the history of the individual, does not have a purpose. While one expects addressing of an event in the case of it being caused by the divine, a stroke of fate hits the individual unplanned and without the possibility of seeing a higher meaning in it. A person is affected without any possible explanation of why exactly this person is allowed to be fortunate or has to suffer from misfortune. Fate influences history, but does not have purpose, and is without teleology.

Modern natural sciences look for coincidence on the basis of understanding it as fate. Doing so, they follow methodical guidelines of their own disciplines, which hold causality as central category of scientific mode of explaining, but differentiate strictly between effective and final causality. Intentions, purposes, and aims have been almost completely eliminated as possibilities of explaining natural phenomena. Ignoring the anthropic principle, which, in its attenuated form, serves as a principle of explanation *ex post*, final causality does not apply anymore as a legitimate way of explanation. This is based on the dictum handed down by Pierre-Simon de Laplace, which he is said to have responded to Napoleon when he asked why Laplace consistently did not speak of God in his “*Mécanique Céleste*”. Laplace said: “*Je n’avais pas besoin de cette hypothèse-là*”. This denial of God as a method of explanation for scientifically explainable nature can be set equal to the elimination of the question of a goal or purpose of nature, which God had previously been regarded as final instance for. Charles Darwin follows this view in “*On the Origin of Species*” and in “*The Descent of Man*” also for animate nature and conceived evolutionary natural phenomena in this way as development without intention.

With methodical exclusion of final possibilities, it becomes necessary for the understanding of coincidence—even if its existential meaning for the human is kept in mind—not to consult final but, exclusively, effective causality. Coincidence is considered as a causal, but no longer as a final event. For a scientific theory, this requirement means that one is able to explain coincidence strictly by efficient

causality. For this it suggests itself to set an accidental event in a way that a causal nexus, which is supposed to help explain an event, meets another one in such a way that both cross at one point and, therefore, something coincidental happens. A crossing like this causes an element of surprise, since, partially, two causal conditions can be stated for the event, but it is impossible to find a causal nexus that is sufficient for the explanation and in which all causal chains are at least indirectly linked to one another. Two events, which can both be declared as causal for themselves (but the coincidence of the two cannot) meet.

This view of coincidence is characterized on the one hand by the lack of final causality and on the other hand by the attempt to discover the reason of the event via effective causality without naming a structure of causally linked conditions, much less a closed complex of causes. This perspective on coincidence stays unsatisfactory in the way that the question why the involved causal chains have overlapped exactly at this moment, will not cease to arise. Usually, one assumes that there has to be a reason for this, because we hold the proposition of the (sufficient) reason (*nihil est sine ratione sufficiente*) as true. This means that—ontologically spoken—nothing can happen without any sufficient reason that evokes the event. If one thinks this way, then the for coincidence assumed unfoundedness is attempted to be cast aside. So it is tried to not hold the coincidence of the event as true, but to defend the causal uniformity of all natural events.

There are two possible ways to escape this difficult situation. First, one can try to assess the causal connection as still needing to be found. The connection is assumed to, on principle, be able to be found, even though this approach—due to an unknown reason—is not seen as possible in the present.

Second, one can try to justify the unfoundedness of coincidence. In this case, reasons for the inability to find links between the causal chains are looked for. One asks for reasons why there are no causes that connect all the events together. On a meta level, reasons should be found that explain why there are no causes on the first level. With this, it is attempted to keep the causal unity, even if it is attenuated. The absence of the possibility to explain an event by means of causes on the first level is admitted, but on the second level, it is attempted to find reasons for the fact that causes cannot be found.

More radical than the mentioned attempts to rescue causal unity and to relativize coincidence along with this process is the assumption that for certain events, neither causal links nor algorithms can be found. Instead of finding reasons for the lack of causes, one admits that the fact has to be treated ontologically, that there are contradictions in natural events that make the principle of sufficient reason and a causally closed nature seem questionable.

This is not the assumption that one's inability to think or the temporary lack of scientific explanation forces one to speak of coincidence. Rather, this concept of coincidence assumes that reality is partially chaotic and, in this sense, not explainable. Unlike a chaos theory, which, despite the multiplying of small differences at the beginning to big differences in the result (after many iterations), assumes the fundamental causality of the event, coincidence, viewed like this, is

based on fundamental ontological chaos. This means that coincidence lacks both final and global efficient causality. Coincidence has become randomness.

For a scientific concept of coincidence, such a theory signifies getting to the limits of causal thought in general. Extending beyond the methodical guidelines of Laplace and Darwin to eliminate final causes as possibilities of explanation as a whole, one arrives at the limits of the explicable if randomness is focused on. Because apart from the only for a thing-ontology relevant types of causation (namely the material and the formal cause in the Aristotelian sense) with the cessation of teleology only efficient causation stays scientifically relevant. If this is questioned, too, then the venture of explaining nature or reality causally has come to its own limit. The methodic possibilities of causation seem to be exhausted by coincidence in the sense of randomness. Such coincidences are only discovered without having the possibility of being explained. Natural sciences, in consequence, are set back to reflect their own preconditions.

Maybe this is the reason why the question of coincidence and randomness is highly attractive even, or especially to, natural sciences.

Graz, Austria
November 2019

Reinhold Esterbauer

Preface

When speaking about randomness, people tend to think toward statistics, like distributions and likelihoods for certain outcomes, and—especially in cryptography—unpredictability. Somewhat ironically, statistics defines a random variable as a measurable mapping, which in no way alludes to matters of unpredictability (the term is not even used in any of the common definitions). So, randomness in statistics and randomness in cryptography are inherently different things, albeit the latter clearly relies on the former. In cryptography, we are primarily interested in independence, uniform distributions, and unpredictability. None of these is necessarily implied by good statistical properties if we think about distributions only: consider the infinite bit-sequence 01010101.... Obviously, the distribution of 0 and 1 within that string is perfectly uniform, but it is equally obvious to predict; even worse, it is clearly periodic. Sequences that are nonperiodic are easy to find (like the mantissa of any irrational number such as $e, \pi, \sqrt{2}$) but are usually not useful for cryptography. Spigot algorithms for many such numbers allow the computation of individual digits without having to compute the whole mantissa up to the sought digit, and we could use a secretly chosen irrational¹ to seed the pseudorandom generator that just computes digits in the mantissa. But such numbers may have bad statistical properties that make them easy to predict from a record of past values. Are there sequences that are easy to compute, have good statistical properties, and never become periodic? Yes, there are, such as the famous Champernowne constant, which is defined by concatenating all naturals into the mantissa in increasing order, i.e.,

$$C := 0.1234567891011121314151617\dots$$

This number is clearly irrational, since it will eventually contain sequences of zeroes (or other digits) of arbitrary length, so there cannot be a fixed period. Even better, it can be shown that it is a *normal number*, meaning the following: Let a

¹Picking such numbers from integer parameters is easy, since, for example, the polynomial $ax^2 + bx + c$ has all irrational roots whenever a, b, c are odd numbers; likewise, $\sqrt[n]{1 + (a/b)^n}$ is necessarily irrational by the Fermat–Wiles theorem for positive integers a, b .

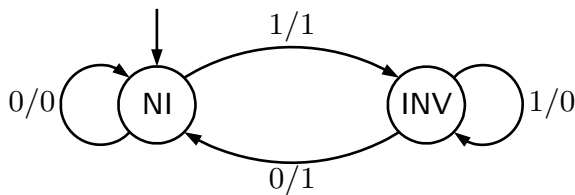
random string w over the alphabet Σ be given, say $\Sigma = \{0, 1, 2, \dots, 9\}$. Assume that the symbols (digits) in w occur independently and uniformly distributed over Σ , i.e., we create w by drawing its symbols with replacement from Σ . Then, w has a “natural” probability of $\Pr(w) = |\Sigma|^{-|w|}$, when $|w|$ denotes the length of w (in digits). A normal number, such as the Champernowne constant, is characterized by the fact that *every* random string w will occur throughout the mantissa with its natural probability (just as defined before). So, C , as well as any other normal number, would have the perfect statistical properties: In computing digits from it and concatenating them into strings toward our random output, we get an output with perfect statistical properties. A celebrated theorem of E. Borel even states that almost all numbers are normal in that sense. Though very many of them exist, however, only a few are explicitly known, and the Champernowne constant is one of them. Though it is very easy to compute and has the perfect properties regarding the distribution of substrings over the mantissa, its trivial predictability makes them useless for cryptographic purposes.

For these (among other) reasons, cryptographic random number generators typically use a transformation function f to compute fresh random values from past random values. Different constructions such as pseudorandom number generators (PRNGs) or pseudorandom functions (PRFs) exist [1], all of which have their predictability properties tightly tied to computational intractability hypotheses (see [3] for an overview). Let us look at a typical way of how a PRNG based on iterations can be constructed: we have a function f and pick a random value x_0 from which we iterate a sequence $x_{n+1} := f(x_n)$ for $n = 0, 1, \dots$. If f is a mapping between finite sets, any such sequence necessarily becomes periodic, and estimates about when this happens are known [2]. Can we escape the issue by letting f work on infinite domains? More explicitly, can we use a function f that evaluates deterministically but acts stochastically? Again, the answer is positive, since every chaotic function does so. Why not use one of the two most famous examples, which are the logistic map $f(x) = \lambda \cdot x(1 - x)$ or the tent map $f(x) := \mu \cdot \min\{x, 1 - x\}$, where the actual behavior is governed by the choice of $\lambda > 0$ or $\mu > 0$. The two are closely related (in fact, they are topological conjugates), but the tent map has some very appealing properties:

- If the iteration starts from an irrational value x_0 , the resulting sequence never becomes periodic.
- It has sensitive dependence on initial conditions, intuitively meaning that any arbitrarily close but incorrect guess of $x'_0 \neq x_0$ will make the resulting sequence diverge arbitrarily far from the true sequence originating from x_0 . This is sometimes understood as “loss of information” upon every step, since the tent map is non-injective, meaning that for every image, there are at least two pre-images possible. Effectively, this means that we could never infer the seed from just observing the sequence, which at first glance sounds like a perfect property to go for. Unfortunately, we will see that although this is true, the effect is nonetheless devastating.

- Given an irrational number x_0 to start from and using $\mu = 2$, the tent map’s action on an irrational number in binary with bits $b_1b_2b_3\dots$ is simply this:
 - shift the decimal point one place to the right.
 - If a 1 is left to the decimal point, invert all upcoming bits.

The tent map’s action can be described by a simple Mealy-automaton: let the state transition “a/b” mean that whenever the automaton reads a symbol “a” it outputs the symbol “b”. According to the above, we need an “inverting state” (INV) and a “non-inverting” state (NI) to compute the tent map from an irrational starting point x_0 by the automaton:



Let us analyze the intuition of combining a starting point like C with a chaotic map to unify the benefits of both: perfect statistical properties (from the normality of C) with unpredictability based on deterministic chaos (from the tent map). It is indeed a nice exercise to verify that the automaton will eventually “burn” all information contained in the seed (as we would expect from the sensitive dependence on initial conditions and the non-injectivity of the tent map), but two sequences may nonetheless converge into the *same* pseudorandom sequence sooner or later. More precisely, let $x_0 \neq x'_0$ be two starting values that differ from C only in a finite number of digits. Then, both starting points will eventually end up in the same output, meaning that whatever seed we use together with a fixed normal number (our choice of C was arbitrary here), the so-constructed pseudorandom generator is not even remotely useful for cryptographic purposes. Intuitively, this becomes evident when looking at the Mealy-automaton to evaluate the tent map: the machinery to compute the random outputs is finite, but for unpredictability, we need new information in each output that cannot be obtained from past observations. Since the irrational value C is part of the algorithm, with only the deviation from it being the secret, a deterministic (finite) machinery can obviously not be expected to “create” the necessary lot of information to ultimately gain unpredictability. This is what J. von Neumann expresses in his famous quote:

Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.

What is the lesson from all this? It tells us that we cannot naively assemble primitives with good statistical properties into a cryptographically useful random number generator (RNG); such intuitions can easily be misleading. The above ideas were chosen only for illustration but in general demonstrate that even perfect statistical properties, or seeming unconditional unpredictability (that we hoped to get from chaos theory, which is—unlike much of cryptography—not based on computational intractability) may together fail to deliver good results for cryptography. It ends up being that, at least for pseudorandom number sequences (whose reproducibility is often the only reason to prefer them over true randomness), seem to require more complex constructions and computational intractability remains an unavoidable fundament up to today. A working construction that is simple and has maximal periodicity is, for example, an AES-encryption of a secret counter, which could be implemented in one line of C++-like pseudocode: letting `i` be initialized to some secret value i_0 , we get the next random number as

```
AES(++i, k)
```

where k is another secret stored within the PRNG.

This is indeed a working construction, and the standard quality assessments for PRNG that we will later (in the book) see that the output meets the requirements of cryptographic applications.

The security of such a construction lies in the secrecy of the initial value i_0 and the secret k . Let us adopt a more general view, calling s the secret random seed, which is sampled from a random variable S . How would we quantify the “goodness” of the random seed? Shannon-entropy is commonly proposed as a measure, but this is only half-correct: “entropy” is the right direction, but *not* of Shannon’s type! Indeed, since we cannot prevent guessing a secret, how difficult would guessing s be?

Let the distribution of S be $\{(s_i, p_i = \Pr(S = s_i))\}_{i=1}^n$ with $s_i \in \{0, 1\}^\ell$ and $p_i \geq 0$ so that $p_1 + p_2 + \dots + p_n = 1$. The *min-entropy* of S is defined as

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

By this definition, we have for all s : $\Pr(S = s) \leq 2^{-H_\infty(S)}$. Now, let’s turn to the experiment of guessing the unknown seed s_0 , which occurs with probability p_0 : the average number N of trials until we succeed follows a geometric distribution with parameter p_0 , whose mean is

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

So, $H_\infty(S)$ obviously provides a lower bound for the average number of guesses until a success, so $H_\infty(S)$ can be taken as a measure of the difficulty! Can the Shannon-entropy be such a measure too? The answer is negative in general, due to the following example: