Didaktische Ansätze für Quantum Random Number Generators (QRNG)

Stefan Aehle*, Holger Cartarius*

*AG Fachdidaktik der Physik und Astronomie, Friedrich-Schiller-Universität Jena, 07743 Jena
stefan.aehle@uni-jena.de

Kurzfassung

Im Vormarsch der Quantentechnologien 2.0 sehen Enthusiasten und Medien den Quantencomputer an vorderster Front – auch, wenn dessen Entwicklung noch in den Kinderschuhen steckt. Viel greifbarer dagegen sind erste Errungenschaften der Quantensensorik und -kryptografie, wie die Erzeugung echter Zufallszahlen mittels quantenoptischer Zufallsgeneratoren (QRNGs). Diese schaffen es sich ganz bestimmte quantenmechanische Phänomene zu Nutze zu machen und sind inzwischen auch kommerziell verfügbar. Da sie auch relativ einfach zu erklären sind, können sie sich eignen, um Schülerinnen und Schülern Quantum Randomness näher zu bringen. Eine solche Betrachtung führen wir hier durch.

1. Einleitung

Trotz steigender Relevanz der Quantentechnologien 2.0 für Wirtschaft, Gesellschaft und Forschung, fällt es den Themen der modernen Physik häufig noch schwer, Einzug in den aktuellen Schulunterricht zu halten. Zweifellos ist es nicht zuletzt der fremdartigen Natur der Quantenphysik und der ihr fehlenden Alltagsnähe geschuldet, dass der Einstieg in Themen wie Quantencomputing, Quantensensorik und -kryptografie sich für viele Lernenden und Lehrenden schwierig gestaltet. Es ist das Akzeptieren der „Lücke“, die sich zwischen „beobachtbarer Realität und wohldefiniertem mathematischem Formalismus“ auftut und die Frage nach der Herkunft der Quantum Randomness [1], die schon den Gründervätern der Quantenphysik Kopfzerbrechen bereitete und auch heute noch viele Fragen aufwirft. Ein anschaulicher, jedoch selten didaktisch berücksichtigter Inbegriff jener Quantenzufälligkeit liegt im Kern einer der bereits heute weitverbreitetsten Quantentechnologien überhaupt: Quantum Random Number Generators (QRNGs) – Quantenzufallsgeneratoren. Dessen mögliche Eignung als didaktisches Beispiel wird im Folgenden vorgestellt. Genau in diesem Sinn eines Beispiels, das als Motivation für die Auseinandersetzung mit den Eigenheiten der Quantenphysik dienen kann, wollen wir das Thema verstehen. Didaktische Ansätze, die sich mit den weiterführenden Themen beschäftigen sind z.B. der milq-Ansatz aus Braunschweig [2], Seminare im Physiklehramtsstudium [3], Projekte mit digitalen Medien und Virtual-Reality-Unterstützung [4], neue Konzepte zur Quantendidaktik [5], der Didaktik von Quantencomputern [6], und fertige Experimentiersets [7].

2. Anschluss an den Lehrplan

Tatsächlich scheint der QRNG aufgrund seiner einfachen Bauweise und dem vergleichsweise geringen Umfang an nötigen Vorkenntnissen – auch themen- und fächerübergreifend – prädestiniert für Einsteigerformate: Neben der üblichen Positionierung am Rande eines traditionellen Oberstufen-Physikkurses, hat der QRNG möglicherweise das Potential, zum Beispiel im Mittelpunkt einer Projektarbeit zu Quantentechnologien 2.0 zu stehen und echten, greifbaren Alltagsbezug herzustellen. Mit der Veröffentlichung des ersten Smartphones mit eingebautem QRNG-Chip im Mai 2020 könnten Schülerinnen und Schüler die Technik schon bald in der Hosentasche mit sich tragen [8, 9]. Wie nachfolgend geklärt wird, braucht es fast nichts außer einen Ansatz zur Funktionsweise einer LED, der über die klassische Vorstellung hinaus geht, um das Prinzip QRNG nachzuvollziehen. Thematisch lässt sich dabei vor allem der quantenphysikalische Messprozess untersuchen, aber auch fächerübergreifend zur Statistik, Informatik und anderen mathematisch-technischen Bereichen arbeiten.

3. Was sind echte Zufallszahlen?

Zufallszahlen sind Zahlen, die in einem Prozess generiert werden, dessen Ergebnis zufällig und damit anschließend nicht zuverlässig reproduzierbar ist. Ob eine beliebige Zahl in einem solchen Prozess entstammt, ist unmöglich festzustellen, sodass es eine ganze Zahlenfolge braucht, um die Zufälligkeit zu untersuchen. Aber wie lässt sich Zufall messen? Aus Shannons Informationstheorie [10] ist bekannt, dass eine unendliche Zahlenfolge genau dann zufällig ist,

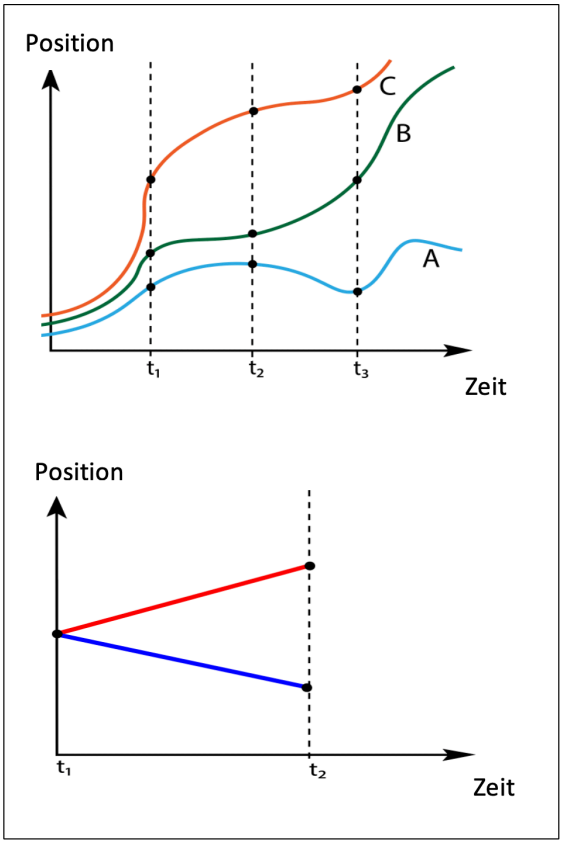

Abb.1: Vergleich eines klassischen (oben) und quantenphysikalischen (unten) Zufallsprozesses. In einem klassisch-chaotischen System laufen die Trajektorien bei minimalen Unterschieden in den Anfangsbedingungen exponentiell auseinander. Nimmt man nur zu bestimmten Zeiten *t* neue Werte auf, registriert man Zahlen, die in hoher Qualität Zufallszahlen repräsentieren können (Pseudo-Zufallszahlen). Im Gegensatz dazu entwickelt sich ein quantenphysikalischer Zustand zwar auch rein deterministisch in der Zeit, wenn man jedoch den Ort (oder eine andere Variable) feststellen will, führt man eine Messung durch und jeder Wert, der mit einer Wahrscheinlichkeit ungleich Null im Zustand vorkommt kann gemessen werden. Dies geschieht zufällig und unterliegt *keinem* deterministischen Prozess. Führt man Messungen in gewissen Zeitabständen aus, erhält man echte Zufallszahlen. Die Abbildung enthält nur zwei von prinzipiell unendlich vielen Möglichkeiten.

wenn auch deren Informationsgehalt unendlich ist, sie sich also nicht ohne Informationsverlust komprimieren lässt und sich Ziffern in immer neuen Kombinationen fortsetzen. In der Realität ist es aber unpraktisch, unendliche Zahlenfolgen zu prüfen, da die meisten Anwendungsbereiche nur endliche Zeit und Leistung aufbringen können, um Daten zu verarbeiten. Trotzdem haben sie den Anspruch *echte* Zufallszahlenfolgen zu verwenden. Es bleibt nur die Untersuchung endlicher Zahlenfolgen auf statistische Eigenschaften, die sie in der Theorie mit unendlichen Zufallszahlen gemein haben. Die eigentliche Messung des Zufalls gestaltet sich aber schwierig: Betrachtet man beispielsweise die Folge A = 1101011000 und die Folge B = 1111111111, so würde man wohl intuitiv Folge A als die „zufälligere“ von beiden erklären. Tatsächlich ergeben sich aber beide Zifferkombinationen als gleichwahrscheinlich. In der Praxis werden stattdessen möglichst große Datenmengen auf Korrelationen und Muster innerhalb der Folge überprüft. Eine ganze Batterie an stochastischen Testinstrumenten, wie die Statistical Test Suite des Nationalen Instituts für Standards und Technologie (NIST) [11] der Vereinigten Staaten, müssen zuverlässige Zufallszahlgeneratoren durchlaufen, um als sich solche einen Namen zu machen.

4. Zufallsgeneratoren

Random Number Generators (RNGs) lassen sich auf verschiedene Art und Weise nach ihrer Funktion oder Anwendung unterscheiden. Wesentliche Unterschiede ergeben sich für unsere Zwecke aber in den verschiedenen Methoden Zufälligkeit zu erzeugen, beziehungsweise sich natürliche Zufälligkeit zu Nutze zu machen. Zwei grundlegende Kategorien sind klassische RNGs, die auf chaotischer Entwicklung klassisch-physikalischer Systeme beruhen, und quantenphysikalische Zufallsgeneratoren, also QRNGs, die die fundamentalen Wesenszüge von Quantensystemen auskosten (vgl. Abb. 1). Dem hier vorgestellten QRNG gelingt dies auf so anschauliche Weise, dass es durchaus denkbar wäre, dessen Funktionalität im schulischen Physikunterricht zu untersuchen. Was alle RNGs miteinander verbindet, ist das Ziel, echte Zufallszahlen zu erzeugen, also keine Tendenzen oder Korrelationen zu erhalten, und möglichst schnell große Datenmengen auszugeben. Klassische RNGs schaffen das nach heutigem Stand sehr gut – sie erzeugen vieler Orts zuverlässig riesige Datenraten, sind flexibel einsetzbar und werden sogar standardmäßig zur Verschlüsselung von Kommunikation genutzt. Einerseits gibt es software-basierte Pseudo-RNGs, die aus einem sogenannten Seed value (Startwert) nach einem bestimmten Algorithmus eine Zufallszahl generieren – und das nach immer gleichem Muster: same input = same output. Die so generierten Werte sind natürlich alles andere als zufällig, sodass ein Dritter, der entweder Startwert oder Algorithmus kennt, das System problemlos manipulieren kann. Pseudo-RNGs eigenen sich also nur für Anwendungen, die auf echten Zufall verzichten können (z.B. Animationen, Spiele, etc.).

Andererseits gibt es klassisch-physikalische RNGs, welche komplexe makroskopische Prozesse nutzen, deren Dynamik aufgrund ihrer chaotischen der Natur kaum oder nur sehr schwer vorherzusagen sind – beispielsweise das Auslesen technischen Rauschens in Elektronikbauteilen oder das Ziehen von Zahlen aus einer Lotto-Trommel. Schon minimale Veränderungen in den Anfangsbedingen lenken das chaotische Verhalten des Systems zu unvorhersehbaren Ergebnissen, was es einem Dritten fast unmöglich macht,

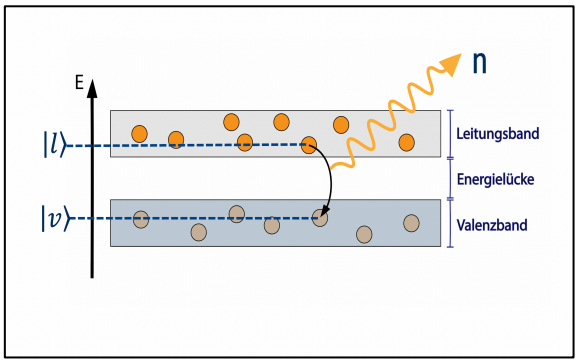

Abb.2: Übliche Darstellung des Elektronenübergangs von einem Zustand $|l\rangle$ im Leitungsband zu einem Zustand $|v\rangle$ im Valenzband unter Aussendung eines Photons. Tatsächlich findet eine Zeitentwicklung statt, bei der die Aufenthaltswahrscheinlichkeit des Elektrons im Valenzband „nur“ steigt. Wann es tatsächlich im Valenzband auftaucht, und ein Photon detektiert werden kann, unterliegt dem quantenphysikalischen Messprozess, der rein zufällig ist.

Sicherheitslücken zu erkennen. Nichtsdestotrotz taugen klassisch-physikalische RNGs nicht für alle Anwendungen: So chaotisch der Vorgang auch sein mag – makroskopisch bleibt es ein deterministischer Prozess, der mit genug Rechenleistung oder Zeit letztlich berechnet, zurückverfolgt und vorhergesagt werden kann. Außerdem gibt es oft Probleme in der Modellierung und Kontrolle solcher Prozesse, sodass selbst der Nutzer nicht nachvollziehen kann, ob sich schon systematisch bestimmte Verzerrungen der Werte ergeben. Trotz ihrer Nachteile finden klassische Zufallsgeneratoren Anwendung in vielen Bereichen, teils auch, weil es bisher an Alternativen mangelte: Glücksspiele in Lotterien, numerische Simulationen in der Naturwissenschaft (siehe Monte-Carlo-Methode [12]), und, wie bereits erwähnt, auch in der Kryptographie zur Verschlüsselung von Bankgeschäften und allen anderen Arten von digitaler Kommunikation.

Die einzige Alternative zu klassischen Zufallsprozessen und damit auch die einzige Möglichkeit, echte Zufälligkeit zu nutzen bieten QRNGs. Sie basieren auf der intrinsischen Zufälligkeit der Quantenphysik, die theoretisch und experimentell seit Anfang des 20. Jahrhunderts immer wieder bestätigt wurde. Die Zufallsnatur des Quantenobjekts erlaubt es, sich einfache Prozesse zu Nutze zu machen und deren Wahrscheinlichkeitsverteilung zu modellieren, um so auch auf Verzerrung zu überprüfen. Darüber hinaus zeigen die Bell-Ungleichungen, dass es keine „versteckten Parameter“ gibt, keine Unsicherheiten im Quantensystem, die ein Dritter unbemerkt erschließen kann. Wird der Prozess gestört, ändert sich das Ergebnis instantan. Auch die Praxistauglichkeit hat sich durch den technischen Fortschritt und Forschung im Bereich der Quantentechnologien der letzten Jahrzehnte immens verbessert. Der im folgenden Beispiel vorgestellte QRNG ist im Format nicht größer als ein Schuhkarton, verwendet Standard-Elektronikbauteile, und lässt sich per USB an jedes beliebige Computersystem anschließen. Andere Bauarten schaffen es inzwischen sogar, Smartphones mit QRNG-Chips auszustatten und echten Quantenzufall in Verbraucherhände zu bringen.

5. Beispiel eines QRNG

5.1. Bau und Funktion

Der 2010 an der Ludwig-Maximilians-Universität München entwickelte Quantenzufallsgenerator [13], der an dieser Stelle exemplarisch als didaktisch gut geeignete Umsetzung vorgestellt werden soll, basiert grundsätzlich auf der Zufälligkeit der Photonenemission einer LED-Lichtquelle. Das kompakte Gerät besteht nur aus einer LED, die im Einzel-Photonen-Bereich leuchtet, sowie einem einzelnen Photonendetektor. Nach den fundamentalen Gesetzmäßigkeiten der Quantenoptik folgt die Wahrscheinlichkeitsverteilung der Anzahl der emittierten Photonen bei konstanter Lichtintensität in einem bestimmten Messintervall – analog zum Kernzerfall – einer Poisson-Verteilung um einen Mittelwert. Einer geraden Anzahl an Photonen pro Zeitintervall ordnet man dabei eine „0“ zu, während eine ungerade Anzahl als „1“ interpretiert wird. Im Normalfall ist die Poisson-Verteilung aber insbesondere für kleine Zeitabstände unsymmetrisch, was letztlich dazu führen würde, dass „0“ und „1“ nicht gleichwahrscheinlich auftreten und so eine Tendenz der relativen Häufigkeiten in die ein oder andere Richtung (auch Bias genannt) aufträte. Durch Besonderheiten im Zusammenspiel von Quelle, Detektor und Ausleseelektronik ergeben sich speziell für dieses Modell bestimmte Totzeiteffekte, die diese Poisson-Verteilung aber so modifizieren, dass jeweils gerade und ungerade Anzahlen an Photonen gleichermaßen ohne signifikante Tendenz detektiert werden können [13]. So ergibt sich nach dem Auslesen tatsächlich eine zufällige Zahlenfolge aus Nullen und Einsen, die auf der Quantennatur von Elektronenübergängen in einer LED beruht.

5.2. Quantenphysik des Zufallsgenerators als greifbares didaktisches Element

Betrachtet man den Vorgang der Lichterzeugung einer LED im Detail, wird deutlich, warum im Münchner Aufbau von echter Quantum Randomness ausgegangen werden kann. Das klassische Bild der Funktionsweise einer LED erklärt das Verhalten des Elektrons als Teilchen, das vom Leitungsband in das energetisch tiefere Valenzband fällt und dabei Energie in Form eines Photons freisetzt. Die Rekombination von Elektronen und „Löchern“ zwischen den n- und p-dotierten Siliziumschichten wird auch im Physikunterricht modellhaft angeführt, um so den Elektronenübergang als zeitlich kontinuierlichen, klassischen Prozess zu veranschaulichen (s. Abb. 2). Jedoch lässt sich der Vorgang – mit entsprechender Vorbereitung

sogar in schulischen Kontexten – auch quantenmechanisch beschreiben: Das Elektron befindet sich nach Übergang in den p-dotierten Teil der Grenzschicht zu jedem belieben Zeitpunkt *t* entweder im Zustand des Leitungsbands $|\boldsymbol{l}\rangle$ oder schon im Zustand des Valenzbands $|\boldsymbol{v}\rangle$. Beide Zustände $|\boldsymbol{l}\rangle$ und $|\boldsymbol{v}\rangle$ befinden sich in Superposition und sind vor einer eindeutigen Messung gleichwahrscheinlich. Unter Berücksichtigung des emittierten Photons liefert die Zeitentwicklung der Schrödinger-Gleichung also:

$$|\boldsymbol{\Psi(t)}\rangle = \boldsymbol{a(t)}|\boldsymbol{l}\rangle|\boldsymbol{n=0}\rangle + \boldsymbol{b(t)}|\boldsymbol{v}\rangle|\boldsymbol{n=1}\rangle$$

Erst die Messung verrät, ob ein Photon zum Zeitpunkt *t* existiert ($|\boldsymbol{n=1}\rangle$) oder nicht ($|\boldsymbol{n=0}\rangle$). Dementsprechend bestimmt die Aufenthaltswahrscheinlichkeit des Elektrons den Ausgang der tatsächlichen Messung. Die Wahrscheinlichkeiten mit denen $|\boldsymbol{l}\rangle$ und $|\boldsymbol{v}\rangle$ gemessen werden ändern sich typischerweise mit der Zeit und ergeben sich aus:

$$|\langle \boldsymbol{n=1}|\boldsymbol{\Psi(t)}\rangle|^2 = |\boldsymbol{b(t)}|^2$$

$$|\langle \boldsymbol{n=0}|\boldsymbol{\Psi(t)}\rangle|^2 = |\boldsymbol{a(t)}|^2$$

Besonderes Augenmerk lenkt diese Herangehensweise auf den quantenmechanischen Messprozess und die eigentliche Zufallsnatur quantenphysikalischer Prozesse. Ohne unbedingt auf Begrifflichkeiten wie Verschränkung oder Unschärfe eingehen zu müssen, kann so auch im Schulunterricht Anreiz geschaffen werden, Quantenphysik anhand alltäglicher Objekte zu untersuchen. Das Entwicklerteam des im Beispiel vorgestellten QRNGs begründet mit ebenjener quantenmechanischen Perspektive die Echtheit und Zuverlässigkeit ihrer Zufallszahlen.

5.3. **Weiterführende Aspekte der technischen Umsetzung**

Nachdem ein Photon von der LED ausgesendet wurde, trifft es auf einen Photoelektronenvervielfacher (PTM), der die Messung in Form eines elektrischen Pulses in der Größenordnung weniger Nanosekunden weiterleitet. Das analoge Signal durchläuft einen Verstärker und wird in einer nachfolgenden Diskriminator-Schaltung in ein digitales umgewandelt**.** Die Diskriminator-Schaltung kann zwei Messereignisse nur dann auseinanderhalten, wenn diese mindestens die zeitliche Breite eines einzelnen Pulses getrennt voneinander eintreffen. Somit entstehen Totzeiten, die in anderen Versuchen eher unerwünscht sind, an dieser Stelle aber die Poisson-Verteilung statistisch optimieren und so auch hohe Zählraten mit vernachlässigbarerem Bias erlauben. Um systematisch die grobe Funktionalität des QRNGs zu überprüfen, führt im vorgestellten Modell ein FPGA-Logikchip bereits on-board erste statistische Tests an Zahlenfolgen von 1 Mbit pro Minute durch. So kann schon vorab Kontinuität des stochastischen Prozesses und Qualität der zufälligen Bits gewehrleistet werden, bevor das Ergebnis des Vorgangs über USB in einen Computer eingespeist wird. Ein solcher QRNG ist damit in der Lage, Zufallszahlen mit einer Rate von 50 Mbit pro Sekunde zu erzeugen, die auch alle gängigen statistischen Tests (STS des National Institute of Standards and Technology, DieHarder-Tests) eindeutig bestehen.

6. **Ausblick**

Wir haben hier eine Umsetzung eines QRNG vorgestellt, die aufgrund ihres einfachen Auftretens des quantenphysikalischen Zufallsprozesses besonders geeignet ist als alltagsrelevantes Beispiel im Unterricht eingeführt zu werden. Andere, ähnlich unkomplizierte QRNG-Bauweisen nutzen statt eines PMT beispielsweise den CMOS-Bildsensor eines Smartphones oder die CCD einer Digitalkamera [14]. So konnten sogar noch höhere Zufalls-Bitraten von 1.25 Gbits mit noch einfacheren Mitteln erreicht werden. Mit dem Umbau von Elementen weit verbreiteter Unterhaltungselektronik wie diesen, ist es prinzipiell jedermann mit dem nötigen Know-how möglich, diese Art von Quantentechnologie exemplarisch nutzbar zu machen. Es ist also möglich, auch ohne hochspezialisierte, quantenoptische Gerätschaften wie Einzelphotonenquellen, Strahlteiler und Detektoren quantenphysikalische Prozesse anzuwenden. Damit sei nicht gesagt, dass ein solches Projekt grundsätzlich im schulischen Rahmen umsetzbar ist, jedoch macht es dessen Konzeption und theoretische Hintergründe greifbarer und alltagsrelevanter als beispielsweise die des Quantencomputings.

Gleichzeitig bedeutet das auch, dass der kommerzielle Gebrauch von QRNG-Technologie technisch ausreift und auch in kleineren Maßstäben an gesellschaftlichem Interesse gewinnt. So werden jetzt neben dem ersten Smartphone mit QRNG-Chip auch zahlreiche Computerkomponenten vermarktet, die dem QRNG zum Hausgebrauch befähigen [15]. Dabei geht es meist nicht um Anwendungen für Forschungszwecke, sondern vor allem um Cyber-Security und Verschlüsselung von Daten. Um einschätzen zu können, ob das echte Vorteile gegenüber herkömmlichen, klassischen Verfahren mit sich bringt, ist grundlegendes Verständnis der quantenphysikalischen Hintergründe gefragt – ein weiterer Grund, QRNGs in den Physikunterricht von heute einzubauen.

7. **Literatur**

[1] Heusler S, Schlummer P, Ubben MS (2021): The Topological Origin of Quantum Randomness. Symmetry, 13(4):581.

[2] Müller R, Wiesner H (2002): Teaching Quantum Mechanics on an Introductory Level. American Journal of Physics 70, 200.

[3] Scheiger P, Nawrodt R, Cartarius H (2020): Interaktive und aktivierende Lehrkonzepte in der Theoretischen Physik. In: PhyDid B, Didaktik der Physik, Beiträge zur DPG-

Frühjahrstagung Bonn; Nordmeier V, Grötzebauch H (Eds.)
[4] Schlummer P, Laustroer J, Schulz-Schaeffer, Abazi A, Schuck C, Pernice W, Heusler S, Laumann D (2020). MiReQu: Mixed Reality Lernumgebungen zur Förderung fachlicher Kompetenzentwicklung in den Quantentechnologien. In: PhyDid B, Didaktik der Physik, Beiträge zur DPG-Frühjahrstagung; Nordmeier V, Grötzebauch H (Eds.)
[5] Bitzenbauer P, Meyn JP (2020): A new teaching concept on quantum physics in secondary schools. In: Physics Education 55(5) 055031
[6] Pospiech, G (2021): Quantencomputer & Co.: Grundideen und zentrale Begriffe der Quanteninformation verständlich erklärt, Springer Spektrum.
[7] quTools Homepage: https://qutools.com/quantenkoffer_science-kit/ (Stand 5/2021)
[8] Simons H (2020): Samsung Galaxy A Quantum is a phone with a quantum security chip. Android Authority, Url: https://www.androidauthority.com/samsung-galaxy-a-quantum-1118992/ (Stand 5/2021)
[9] Byford S (2021): Samsung's Galaxy Quantum 2 has quantum cryptography built in. The Verge, Url: https://www.theverge.com/2021/4/13/22381321/samsung-galaxy-quantum-2-announced-qrng-cryptography-chip (Stand 5/2021)
[10] Heise W, Quattrocchi P (1995): Informations- und Codierungstheorie: Mathematische Grundlagen der Daten-Kompression und -Sicherung in diskreten Kommunikationssystemen. Springer-Verlag Berlin Heidelberg.
[11] Heruley-Smith D, Hernandez-Castro J (2017): Quam Bene Non Quantum: Bias in a Family of Quantum Random Number Generators.
[12] Binder K, Heermann D (2010): Monte Carlo Simulation in Statistical Physics. Springer-Verlag Berlin Heidelberg.
[13] Fürst H, Weier H, Nauerth S, Marangon D, Kurtsiefer C, Weinfurter H (2010): High speed optical quantum random number generation. In: Optics Express, Vol. 18, Issue 12, S. 13029-13037.
[14] Sanguinetti B, Martin A, Zbinden H, Gisin N (2014): Quantum random number generation on a mobile phone. In Physical Review X 4.
[15] ID Quantique Whitepaper zum QRNG-Produkt: https://www.idquantique.com/random-number-generation/overview/ (Stand 5/2021)