

Bau eines Zufallsgenerators auf Basis nichtdeterministischer Entropiequellen

Robert J. Pietsch

Facharbeit im Fach Physik (MSS12 - SJ 2018/19)

Abstract

In der heutigen Gesellschaft spielt die digitale Datenübertragung eine große Rolle. Egal, ob wir beim Online-Banking Geld überweisen oder im Chat mit anderen Personen private Nachrichten austauschen, ist eine sichere Datenübertragung wünschenswert. Um diese zu gewährleisten, werden die Daten verschlüsselt übertragen. Für die Verschlüsselungen werden Zufallszahlen benötigt, die ein Angreifer nicht erraten darf, da die Daten sonst entschlüsselt werden könnten. Die Zufallszahlen wurden in der Vergangenheit mit komplexen Algorithmen erzeugt, die aber nicht echt zufällig sind. Kennt man alle Parameter, so kann man die Zufallszahlen erraten und mit diesen die Verschlüsselung brechen.

In meinem Projekt habe ich einen nichtdeterministischen, also physikalisch echten Zufallsgenerator gebaut, der dieses Problem mit echt zufälligen Zufallszahlen lösen soll. Hierfür messe ich verschiedene physikalisch zufällige Phänomene wie radioaktive Zerfälle und akustisches Umgebungsrauschen und berechne daraus Zufallswerte. Der Zufallsgenerator ist als Peripheriegerät für Endanwender umgesetzt und kann per USB ausgelesen werden.

Dokumentenversion: Fassung vom 01.04.2019

Inhaltsverzeichnis

1 Einführung	1
1.1 Zielsetzung	1
1.2 Anwendungsfälle	1
2 Physikalischer Hintergrund	2
2.1 Determinismus und Zufall	2
2.2 Radioaktivität & Der Glühstrumpf	3
2.3 Funktionsweise eines Geigerzählers	3
2.4 Elektrisches Rauschen	4
3 Praktische Umsetzung	5
3.1 Ideen und Ansätze	5
3.2 Messweise & Testaufbau	5
3.3 Zufällige Zeitabstände (digitale Messung)	6
3.3.1 Chaos-/Doppelpendel	6
3.3.2 Radioaktive Zerfälle	6
3.4 Zufällige Messwerte (analoge Messung)	7
3.4.1 Akustisches und elektrisches Rauschen	7
3.4.2 Transmission am Halbspiegel	7
3.5 Umsetzung als Peripheriegerät	8
4 Einschätzung der Umsetzung	9
4.1 Aufstellung eines Bewertungsmodells	9
4.1.1 Die „Zufälligkeit“ der Messmethoden	9
4.1.2 Die Geschwindigkeit der Zufallszahlengenerierung	9
4.1.3 Die Sicherheit der Zufallsgeneratoren	9
4.2 Anwendung des Bewertungsmodells auf die verschiedenen Ansätze	10
5 Zusammenfassung & Fazit	12
6 Anhang	13
6.1 Grafiken, Tabellen und Diagramme	13
6.2 Quellenverweise	19

1 Einführung

1.1 Zielsetzung

Es gibt viele Prozesse im Alltag, die von den meisten Menschen als zufällig angesehen werden. So wirken das Ergebnis eines Münzwurf oder die Lottozahlen als unvorhersehbar und zufällig. In der Realität sind solche Prozesse aber nur so lange zufällig, wie man nicht genügend Informationen über diese kennt. So kann man den Ausgang eines Münzwurfs mit Informationen über die Gravitation, die mechanische Wurfbewegung und die Masse und Form der Münze vorhersehen. Die Quelle der verschiedenen zufällig wirkenden Ergebnisse sind das verschiedene Verhalten der Person, die die Münze wirft, und Veränderungen der Umgebung.

Dieses Konzept der Vorherbestimmung der Ergebnisse nennt sich Determinismus. Auch die von Computern verwendeten Zufallsgeneratoren sind nicht echt zufällig, sondern sind mathematische Funktionen, die auf Basis eines sich verändernden Startwerts (*Seed*) zufällig scheinbar zufällige Zahlen generieren. Diese Art von Zufallsfunktionen wird als *pseudo-random number generator* bezeichnet^[1] und ist meistens mithilfe einer mathematischen Einwegfunktion implementiert, damit aus der resultierenden Zufallszahl nicht auf den Seed geschlossen werden kann.^[2] Ein Beispiel hierfür ist die Modulofunktion: $x \bmod 4 = 3$. x kann den Wert 7 beinhalten, aber auch den Wert 11 oder 15. Eine andere Eigenschaft solcher Generatoren ist die Tatsache, dass sich die Reihenfolge der Werte ab einem bestimmten Punkt wiederholt und die Werte somit erratbar sind. Eine niedrigere Wiederholungsfrequenz steigert hierbei die Qualität des Generators, macht aber dessen Implementierung komplexer.

In meiner Facharbeit möchte ich einen physikalisch echten, also nichtdeterministischen Zufallsgenerator bauen. Dieser soll verschiedene physikalische Zufallsprozesse nutzen und in Zufallszahlen umrechnen. Nach der Konstruktion des Generators möchte ich die Menge der Zufallszahlen außerdem statistisch auswerten und damit die Qualität der Zufallszahlen bewerten.

1.2 Anwendungsfälle

Verschlüsselung In der Kryptographie spielen Zufallszahlen eine zentrale Rolle, da diese für die Schlüsselgenerierung genutzt werden. Die kryptographischen Schlüssel sind vergleichbar mit Passwörtern, mit denen eine Nachricht kodiert ist. Kennt man die Zufallszahl und den Algorithmus, mit dem die Schlüssel erzeugt werden, so ist man in der Lage, die Verschlüsselung auszuhebeln.^[3] Ein einfacher pseudo-zufälliger Generator ist somit ungeeignet, um sensible Daten zu verschlüsseln. Trotzdem sind noch immer pseudo-zufällige Generatoren auch in der Kryptographie der Standard, und es wird an immer komplexeren Zufallsalgorithmen geforscht. Ein nichtdeterministischer Zufallsgenerator hat das Potential, dieses Problem elegant zu lösen.

Glücksspiel Die Nutzung von echtem Zufall birgt auch Vorteile beim Glücksspiel, da hierbei die Manipulationsmöglichkeiten eingeschränkt werden können. So können Spieler z.B. nicht die Lottozahlen vorhersagen und Manipulationen der Veranstalter sind leichter nachzuweisen.

2 Physikalischer Hintergrund

2.1 Determinismus und Zufall

Determinismus definiert die Grundprinzipien der klassischen Physik. Unter diese fallen die Newton'sche Mechanik, die Wärmelehre, die Elektrizitätslehre und die Optik. Die Idee des Determinismus' ist eine universelle Vorbestimmtheit aller Aktionen, die auf den Pfeilern der Kausalität und Objektivierbarkeit ruhen.^[4]

Kausalität Bei der Kausalität geht man davon aus, dass eine Reaktion immer von einer anderen Aktion verursacht worden sein muss. So kann die Zuführung von Energie eine Wirkung verursachen, die Zuführung muss aber in der Zeit vor dem Ergebnis liegen. Außerdem kann durch Kenntnis der Ursache die Folge vorhergesagt werden, wodurch man mit einer ausreichenden Menge an Wissen über den aktuellen Zustand des Universums die Zukunft vorhersagen könnte. Ein Beispiel für diese Sichtweise ist das Herabfallen eines Apfels auf den Kopf einer Person, bei der sich in Folge des Aufpralls eine Beule bildet. Die Beule ist beim Herabfallen des Apfels vorhersehbar, kann sich der klassischen Mechanik nach nicht bilden, solange sie nicht durch den Apfel verursacht wurde (Man sehe von anderen Kausalitäten, die Beulen erzeugen, ab). Die moderne Quantenphysik widerspricht dieser These der Kausalität, indem sie davon ausgeht, dass manche Ursachen keine fest vorhersehbare Folge haben und somit zufällig sind.^[4] Diese Idee mache ich mir im Projekt zur Nutze, indem ich versuche, vorab unbestimmte Folgen zu messen und diese in Zahlenwerte umzurechnen.

Objektivierbarkeit Das Konzept der Objektivierbarkeit sieht vor, dass ein Prozess objektiv beschreibbar ist, ohne dass dieser davon beeinflusst wird. Das bedeutet, dass die Beobachtung eines Experiments oder die Messung verschiedener Rahmendaten eines Prozesses diesen nicht verändert.^[4] Bezogen auf das Beispiel mit dem herabfallenden Apfel kann man sagen, dass ein Zuschauer den Apfel fallen sehen kann, ohne dass die später getroffene Person verschont bleibt. Greift der Zuschauer aber in den Prozess ein, indem er z.B. den Betroffenen warnt, so verändert sich die Rolle vom Beobachter zur Ursache, und die Person unter dem Baum kann die Beule vermeiden. Auch hier interveniert die moderne Quantenphysik, indem nachgewiesen wurde, dass sich manche physikalischen Objekte je nach Beobachtung verändern. Ein Beispiel hierfür ist der Welle-Teilchen-Dualismus, welcher vorsieht, dass sich z.B. Licht je nach Messweise wie Wellen oder wie Teilchen verhält.^[5] Für mein Projekt sind Objektivierbarkeit und Welle-Teilchen-Dualismus größtenteils irrelevant, da ich die Folgen der Prozesse nach der Messung nicht weiter verwende.

Philosophische Sichtweisen Determinismus spielt abseits der Physik auch eine Rolle in der Ethik und Philosophie, da man sich die Frage stellt, ob der Mensch in seinem Handel frei ist. So vertreten einige Philosophen wie Immanuel Kant die Ansicht, der Mensch könne aus der Kausalität durch Willensstärke ausbrechen, andere sehen den Mensch gefangen im Determinismus und als „Marionette des Universums“.^[6] Die Quantenphysik widerspricht beiden Thesen mit der Idee, dass es unendlich viele Paralleluniversen mit allen möglichen Ausgängen verschiedener Ursachen gibt und somit alles möglich ist.^[7]

2.2 Radioaktivität & Der Glühstrumpf

Radioaktivität Radioaktivität beschreibt die Veränderung eines instabilen Atomkerns unter Aussendung ionisierender Strahlung. Ein Kern ist instabil, wenn er sehr groß ist und ein starkes Ungleichgewicht zwischen Protonen- und Neutronenzahl herrscht. Es gibt drei im Rahmen dieser Arbeit relevanter Arten dieser Veränderungen¹, nämlich die α - und β^- -Zerfälle, sowie die γ -Emission. Bei der ersten Art, den α -Zerfällen, gibt ein Atomkern zwei Protonen und zwei Neutronen (einen Heliumkern) ab, wodurch sich dessen Kernladungszahl um zwei und die Massenzahl um vier Einheiten senkt. Der Kern wird somit leichter, wodurch die Stabilität steigt. α -Strahlung ist stark ionisierend, was bedeutet, dass diese Strahlung andere Atomkerne beim Auftreffen verändert und Elektronen aus den zugehörigen Atomhüllen des getroffenen Teilchens gestoßen werden. Diese Veränderung der Teilchen kann auch in den Zellen von Lebewesen stattfinden und dort z.B. das Erbgut verändern und beschädigen. Aus diesem Grund ist ein ausreichender Schutz vor ionisierender Strahlung notwendig. Für α -Strahlung genügt ein Blatt Papier, um diese vollständig abzuschirmen. Die zweite Zerfallsart ist der β^- -Zerfall, bei dem ein Neutron im Kern in ein Proton, ein Elektron und ein Neutrino geteilt wird. Hierdurch steigt die Kernladungszahl um eine Einheit, die Massenzahl bleibt unverändert. Nach der Teilung werden das Elektron (gen. β^- -Teilchen) und das Neutrino abgestrahlt. β^- -Strahlung ist deutlich weniger ionisierend als α -Strahlung, benötigt jedoch zur Abschirmung eine mehrere Millimeter dicke Metallplatte. Die dritte Sorte, die γ -Strahlung, tritt sowohl als Nebenprodukt von α - und β^- -Zerfällen, als auch eigenständig auf. Hierbei verändert sich weder die Kernladung noch die Massenzahl. γ -Strahlung ist eine hochfrequente elektromagnetische Welle mit niedrigem Ionisierungsvermögen, die nur schwer abschirmbar ist. Den wirksamsten Schutz vor γ -Strahlen bieten dicke Bleiwände, die meisten anderen Materialien halten diese Strahlung kaum oder nicht auf. Neben der Zerfallsart ist die Halbwertszeit eine wichtige Größe. Sie beschreibt die Zeit, in der aus einer bestimmten Menge eines Nuklids die Hälfte zerfallen ist. Der Zerfallszeitpunkt eines Kerns ist zufällig, daher ist die Halbwertszeit ein statistischer Wert und muss nicht exakt zutreffen. [8] [9] [10]

Der Glühstrumpf Bei Glühstrümpfen handelt es sich um Campingartikel, die normalerweise zur Verstärkung von Gaslampen genutzt werden. Es handelt sich hierbei um ein feinmaschiges Netz aus Baumwolle oder Seide, welches mit einer Salzlösung mit Thoriumnitrat versetzt wurde. Thoriumnitrat ist ein leicht radioaktiv, da es aus radioaktiven Thorium-229-Nukliden, Sauerstoff und Stickstoff besteht. $^{229}\text{Thorium}$ ^[11] zerfällt unter Abgabe von α -Strahlung bei einer Halbwertszeit von ca. 8000 Jahren zu $^{225}\text{Radium}$ ^[12]. Diese Radioaktivität mache ich mir zunutze, um die zufälligen Zeitabstände zwischen den Zerfällen zu messen.

2.3 Funktionsweise eines Geigerzählers

Ein Geigerzähler besteht normalerweise aus zwei Komponenten: Ein Geiger-Müller-Zählrohr erkennt die radioaktiven Zerfälle und die Zählelektronik gibt das Signal dann entweder akustisch oder visuell an den Benutzer aus. Die Zählelektronik enthält bei manchen Modellen nur die Stromversorgung und einen Summer für die einzelnen Signale. Komplexere

¹In dieser Erklärung werden der K-Einfang und der β^+ -Zerfall ausgelassen, da diese über den Rahmen dieser Facharbeit stark überschreiten.

Modelle enthalten zudem einen kleinen Speicher und ein elektronisches Zählwerk, mit dem die Zahl der Zerfälle auf einer Anzeige ausgegeben wird.

Das Zählrohr ist ein zylinderförmiger Gegenstand mit einer Öffnung an der Front und zwei elektrischen Kontakten an der Rückseite. Innen befindet sich ein Metallzylinder, welcher mit einem Füllgas gefüllt ist. Zentral läuft ein dünner Zähldraht entlang der Mittelachse des Zählrohrs. Damit das Füllgas nicht entweicht, ist die Öffnung mit einem sog. Glimmfenster abgeschlossen, welches aber trotzdem α - und β -Teilchen, und γ -Strahlung durchlässt. Der Zähldraht ist positiv geladen und fungiert als Anode, der Metallzylinder wirkt als negativ geladene Kathode. Durch diesen Aufbau entsteht ein radialsymmetrisches elektrisches Feld um den Zähldraht.

Trifft nun ionisierende Strahlung auf ein Zählgasatom (meist eine Mischung aus einem Edelgas und einer organischen Substanz wie Ethanoldämpfen), so wird dieses in ein Paar aus Elektron und Ion geteilt. Die beiden geladenen Teilchen bewegen sich aufgrund des elektrischen Feldes voneinander weg, das positiv geladene Ion hin zum Metallzylinder und das negativ geladene Elektron hin zum als Anode wirkenden Zähldraht. Bei seinem Weg zum Zähldraht trifft das Elektron auf weitere Atome, wodurch Photonen abgegeben werden. Diese Photonen ionisieren wiederum weiter Zählgasatome, wodurch eine Elektronenlawine entsteht, die sich in Richtung des Zähldrahts bewegt. Sobald die Elektronen auf den Zähldraht treffen, entsteht ein Spannungsimpuls. Damit dieser messbar ist, müssen die Elektronen in möglichst kurzer Zeit am Zähldraht ankommen. Die Geschwindigkeit der Elektronen wird vom elektrischen Feld beeinflusst, weswegen ein möglichst starkes Feld wünschenswert ist. Die Feldstärke ist wiederum von der angelegten Spannung abhängig, aus diesem Grund werden liegt standardmäßig eine Spannung von 100V am Zählrohr an, die durch die Spannungsspitzen bei gemessener Strahlung variiert. Nach dem Auftreffen eines ionisierenden Teilchens muss die Gasentladung im Zählrohr umgekehrt werden, damit der Prozess wiederholt werden kann. Damit dies geschehen kann, muss die Kettenreaktion der Entladung gestoppt werden. Hierfür tritt das sog. Löschgas (z.B. Ethanoldämpfe) in Aktion, welches die Photonen absorbiert und die Kettenreaktion somit bremst.^[13]^[14]

2.4 Elektrisches Rauschen

Unter Rauschen versteht man in der Physik sich verändernde Abweichungen von zu erwartenden Messwerten, weswegen man Rauschen auch als Störgröße bezeichnet. Elektrisches Rauschen beschreibt die Fluktuation der Spannung und Stromstärke in einem Stromkreis, die auch bei gleichbleibenden Rahmenbedingungen auftreten. Die wichtigsten Ursachen für elektrisches Rauschen sind Schrotrauschen, thermisches Rauschen und die ungleichmäßige Transmission innerhalb von Halbleitern. Schrotrauschen basiert auf der Idee, dass Elektronen ihre Ladung unabhängig voneinander bewegen und die resultierende Stromstärke nur ein statistischer Wert aus diesen einzelnen sich bewegenden Ladungen ist. Thermisches Rauschen basiert auf der Tatsache, dass sich ohmsche Widerstände je nach Temperatur in ihrem Bremsverhalten verändern. Treffen viele Elektronen auf die Teilchen im Widerstand, so werden diese in Schwingung versetzt und der Widerstand wird warm. Ähnliche Effekte lassen sich auch in Halbleitern finden, die ihre Eigenschaften aufgrund der durchfließenden Ströme leicht verändern.

Eine wichtige Eigenschaft des Rauschens ist die Zufälligkeit. Die einzelnen Effekte lassen sich nicht vorhersagen, da die Bewegung der Elektronen zufällig ist.^[15]^[16]^[17]

3 Praktische Umsetzung

3.1 Ideen und Ansätze

Ich habe mich zu Beginn der Arbeit über verschiedene physikalische Zufallsquellen informiert. Zu den bekanntesten zählen die folgenden Konstruktionen:

- Einzelne Photonen, die beim Auftreffen auf einen Strahlteiler (Halbspiegel) mit 50%iger Wahrscheinlichkeit reflektiert und mit gleicher Wahrscheinlichkeit durchgelassen werden,
- Radioaktive Zerfälle, und deren zeitliche Abstände,
- Das mechanische Chaospendel, welches unvorhersagbare Bewegungen vollzieht, und
- Elektrisches Rauschen innerhalb von Elektronik-Komponenten

Außerdem habe ich mir die Frage nach der Umsetzung als Peripheriegerät gestellt. Hierzu habe ich mich für den Arduino als Mikrocontroller entschieden. In der Bau- und Testungsphase habe ich das „Arduino Uno“-Modell verwendet. Für das fertige Modell nutze ich das „Arduino Nano“-Modell, welches kompakter als das Testboard, aber leider in Puncto Umbauen beim Testen nicht so flexibel ist. Die Arduino-Platinen eignen sich gut zum Sammeln der physikalischen Messwerte und zur sicheren Übertragung an PCs bzw. Server. Zudem sind die Arduino-Chips leicht in einem Dialekt der Programmiersprache C zu programmieren, wodurch der Fokus beim Konstruieren bleibt und effizientes Testen möglich ist. Zusätzlich gestaltet sich die Implementierung der Datenübertragung zwischen den Arduinos und den Computersystemen als einfach, da der Arduino sich als serieller Anschluss in den Betriebssystemen registriert, welcher allgemein kompatibel ist.

3.2 Messweise & Testaufbau

Bei der Auswertung der in Sektion 3.1 genannten Entropiequellen lassen sich die Messwerte entweder in analog und digital einordnen. Unter die Kategorie „digital“ bzw. „binär“ fallen die zeitlichen Messungen, da diese nur prüfen, ob ein bestimmter Schwellwert der Stromstärke erreicht ist und dies als Signal für den Beginn oder das Ende eines Zeitintervalls nutzen. Mit „analogen“ oder „absoluten“ Messwerten ist die Messung der Stromstärke gemeint. Radioaktive Zerfälle lassen sich digital messen, da bei jedem Zerfall ein Stromkreis kurzzeitig geschlossen wird. Gleiches gilt auch für Lichtschranken, die vom Chaospendel unterbrochen werden, und dabei einen Stromkreis zum Arduino öffnen. Elektrisches Rauschen wird sinnvollerweise analog gemessen. Die vollständigen Erklärungen der verschiedenen Messweisen folgen in den Sektionen 3.3 und 3.4.

Testaufbau Zur Auswertung dieser Signale habe ich den in Abb. 1 und Abb. 2 (s. Anhang) gezeigten Versuchsaufbau entwickelt. In diesem stellt der Druckknopf (**SW1**) den Eingang für zeitliche Signale und der Photowiderstand (**D1 BP104**) den Eingang für die Strommesswerte dar. Die Arduino-Anschlüsse mit der Kennzeichnung **A*** sind analoge Ein- und Ausgänge und können absolute Stromspannungen/-stärken in 1024 Stufen von 0V bis 5V messen oder abgeben. Dagegen sind die Anschlüsse mit der Bezeichnung **D*** digital und können nur prüfen, ob ein Schwellwert überschritten wurde. Die LEDs (**LED1 - LED3**) sind als Statusindikatoren verbaut. Beim Testen wurden der Schalter und die Photodiode durch die richtigen Messvorrichtungen ersetzt.

Zufallszahlen Die resultierenden Zufallszahlen sollen in einem Bereich von 0 bis 255 liegen. Dies hat den Grund, dass $256 = 2^8$ Möglichkeiten allen möglichen Zuständen eines 8-Bit-basierten Byte in der elektronischen Datenverarbeitung entspricht.

3.3 Zufällige Zeitabstände (digitale Messung)

Zeitabstände lassen sich leicht in die gewünschten Zufallszahlen umrechnen, indem man den Zeitabstand mit dem Modulo-Operator durch 256 teilt.

3.3.1 Chaos-/Doppelpendel

Die Bewegung eines Doppelpendels wird in der Physik als chaotisch bezeichnet, was bedeutet, dass diese bei einer kleinen Änderung der Anfangsparameter (z.B. der Stoß, mit dem das Pendel angeregt wird) komplett anders stattfindet. Die Auslenkung des Doppelpendels ist zwar deterministisch, wird aber trotzdem als schwer berechenbar angesehen. Aus diesem Grund habe ich auch diese Idee als Vorstufe eines idealen nichtdeterministischen Zufallsgenerators in Betracht gezogen und eine mögliche Konstruktion geplant, diese jedoch nicht umgesetzt.

Der Konstruktionsplan kann als Schaubild im Anhang als Abb. 3 gefunden werden. Der gelbe Pfeil stellt die Aktivierungskraft dar, die in regelmäßigen Abständen auf das Pendel wirken soll, um dieses zu bewegen und zu bremsen. Der äußere Pendelarm soll dann in seiner chaotischen Bewegung die Lichtschranke(n) in zufälligen Zeitabständen unterbrechen, wodurch Signale an den Arduino gesendet werden. Vorteil dieser Konstruktion ist der Preis, da ein solches Pendel mit in Baumärkten erhältlichen Teilen gebaut werden kann und Lichtschranken einfach mit Photodioden und LEDs zu konstruieren sind. Nachteil der Konstruktion sind die Größe des Aufbaus, der Verschleiß mechanischer Teile und der oben genannte Determinismus.

3.3.2 Radioaktive Zerfälle

Die zeitlichen Abstände zwischen radioaktiven Zerfällen sind zufällig, sodass ich nur ein elektrisches Signal im Moment eines Zerfalls benötige, um diese auszuwerten. Meine ursprüngliche Idee war die Verwendung eines Geigerzähler-Moduls für den Arduino (s. Abb. 4 im Anhang), welches ein Signal bei jedem Zerfall ausgibt. Da ein solches Modul in der Anschaffung aber relativ teuer ist, habe ich einen fertigen Geigerzähler geöffnet (s. Abb. 7 im Anhang) und diesen modifiziert. Normalerweise enthält der Geigerzähler einen Summer als akustische Ausgabe für Zerfälle, diesen habe ich aber aus der Platine des Zählers entfernt und an den beiden Lötpunkten des Summers zwei aus dem Gehäuse führende Kabel verlötet. Der Geigerzähler gibt beim Piepsen etwa 4V Spannung an den Summer, diese reicht aus, um mit einem Relais einen Stromkreis zum Arduino zu schalten. Der fertige Aufbau kann in Abb. 6, der zugehörige Schaltkreis in Abb. 5 im Anhang gefunden werden. Vorteil dieser Methode ist, dass diese relativ zuverlässig und kompakt ist und der hierfür genutzte Glühstrumpf eine ungefährliche radioaktive Intensität über eine Halbwertszeit von mehr als 7000 Jahren besitzt^[12]. Außerdem kann die natürliche Strahlenbelastung in der Umgebung genutzt werden. Nachteil dieser Methode sind der Anschaffungspreis von ca. 250 USD (\approx 220 Euro) und die Gefahren, die die Verwendung eines radioaktiven Isotops mit sich bringen.

3.4 Zufällige Messwerte (analoge Messung)

Die Bestimmung von Zufallszahlen aus zufälligen Messwerten ist komplexer, zwei Ideen für diese sind die Verwendung einer sog. Hashing-Funktion (mathematische Einwegfunktion zur Prüfsummenberechnung) wie MD5, bei der aus der resultierenden Hexadezimalzahl zwei Stellen entnommen werden ($2^8 = 16^2$), oder die Messung von acht verschiedenen Werten mit kurzen Zeitabständen, bei denen das resultierende Byte aus den acht Messwertbits (0 für einen geraden und 1 für einen ungeraden Messwert) zusammengesetzt wird.

3.4.1 Akustisches und elektrisches Rauschen

Misst man akustische Lautstärken oder elektrische Ströme, so erhält man einen zufälligen Störwert, das sog. Rauschen. Kombiniert man beides, so erhält man einen hohen Rauschfaktor. Diese Idee mache ich mir zunutze, indem ich mit einem Mikrofon den Ton eines Summers messe und diesen als elektrisches Signal verstärke. Das resultierende Signal enthält ein starkes Rauschen und deswegen fluktuiert relativ stark, wie auch im Diagramm 8 im Anhang gesehen werden kann. Die Messwerte des Aufbaus habe ich mit beiden oben genannten Methode ausgewertet und zu Zufallswerten umgerechnet, die genauen Ergebnisse folgen in Sektion 4.2. Dabei wird der Summer für den Zeitraum der Messung immer eingeschaltet, sobald die fertige Zufallszahl existiert, wird der Summer wieder abgestellt.

Vorteil dieser Messweise ist der Kompaktheitsgrad und der Preis, Nachteil ist das störende Piepsen des Summers bei der Generierung von Zufallszahlen.

3.4.2 Transmission am Halbspiegel

Ein Strahlteiler bzw. Halbspiegel halbiert einen eintreffenden Lichtstrahl, indem dieser zur Hälfte reflektiert und zur Hälfte durchgelassen wird. Treffen einzelne Photonen auf den Strahlteiler, so werden diese auf Zufallsbasis mit einer jeweils 50%igen Wahrscheinlichkeit durchgelassen oder reflektiert. Meine Idee für einen Aufbau, der diesen Effekt nutzt, ist die folgende: Ein schwacher Laser emittiert Photonen, die sich allesamt linear auf einen optischen Filter zubewegen und dort größtenteils absorbiert werden. Die übriggebliebenen einzelnen Photonen werden dann zufällig an einem Halbspiegel reflektiert oder zu einem Detektor durchgelassen. Ein Plan dieses Aufbaus kann im Anhang als Abb. 10 gefunden werden. Diese Art der Zufallsgenerierung ist zwar sehr schnell und kompakt, scheitert jedoch einer Vorrichtung zur Erkennung einzelner Photonen. Um einzelne Photonen zu erkennen, lässt man normalerweise die Photonen eine photochemische Reaktion auslösen, die wiederum zu einer chemischen Kettenreaktion führt, die über einen Farbindikator erkennbar ist. Dieser Prozess ist aber nur schwer reversibel, weswegen man spezielle, auch für die Reversion geeignete Substanzen benötigt, die für Einzelanwender schwer erhältlich sind. Fertige Einzelphotonendetektoren sprengen den finanziellen Rahmen für Heimanwender und somit auch die Zielsetzung des Projekts.

3.5 Umsetzung als Peripheriegerät

Hardwareseitig nutze ich den nativen USB-Anschluss des Arduinos übertragen, welcher sich als serieller Anschluss ausgibt und so einfache Datenübertragung ermöglicht. Seriell bedeutet in diesem Falle, dass eine Folge von Bytes, also Datenpakete in beiden Richtungen (Arduino→PC und umgekehrt) gesendet und empfangen werden kann. Die gesendeten daten verbleiben in einem Puffer, bis dieses gelesen und ausgewertet wurde. Für die Kommunikation der Zufallszahlen mache ich mir diese Eigenschaft zunutze, indem ich ein Request-Reply-Schema nutze. Das heißt, dass der Computer einen Befehl als Zeichenfolge gefolgt von einem Zeilenumbruch-Byte („\n“ oder auch *Newline-Byte*) überträgt und danach auf eine Antwort vom Arduino wartet. Diese Antwort wird ebenfalls mit einem Zeilenumbruch-Byte abgeschlossen, woraufhin die protokollgetreue Kommunikation beendet ist. Eine Liste mit allen Befehlen und erwarteten Antworten findet sich im Anhang als Abb. 11.

Programmierung des Arduinos Der Arduino ist in einem C++-Dialekt für Mikrocontroller programmiert worden. Er misst die Stromstärken an seinen Anschlüssen und rechnet die Werte je nach Programmierung mit verschiedenen Algorithmen in Zufallszahlen von 0 bis 255 um. Außerdem übernimmt er die oben spezifizierte Kommunikation mit dem PC. Der Quellcode der Arduino-Programme befindet sich in meinem GitHub-Repository unter <https://github.com/pietrobe03/randuino/tree/master/arduino-scripts>.

Programmierung des Computers In den gängigen Betriebssystemen spricht man bei offenen Programmen von Prozessen. Diese werden in Vorder- und Hintergrundprozesse eingeteilt, wobei erstere die sichtbaren Fenster (z.B. der Webbrowser) und letztere die versteckt laufenden Dienste (z.B. zur Aufrechterhaltung der Wlanverbindung) sind. Es kann immer nur ein Prozess auf eine serielle Verbindung zugreifen, weswegen ich das Auslesen der Zufallszahlen mit zwei Prozessen gelöst habe. Der erste Prozess läuft dauerhaft im Hintergrund und prüft, ob ein Arduino mit Randuino-Software angeschlossen ist. Ist dies der Fall, so baut der Hintergrundprozess eine Verbindung auf und blockiert diese für alle anderen Prozesse. Somit ist eine grundlegende Abhörsicherheit geschaffen. Der zweite Prozess kann beim ersten Prozess anfragen, ob eine Zufallszahl verfügbar ist, woraufhin die Anfrage weitergeleitet wird und die Antwort validiert, zurückgeleitet und ausgegeben wird. Zur Programmierung beider Programme verwende ich die Programmiersprache C++, jedoch unter Zuhilfenahme der Qt5-Bibliothek^[18], da diese Kompatibilitätsprobleme unter verschiedenen Betriebssystemen löst. Der Quellcode der Kommunikationsbibliothek für C++ und Qt5 befindet sich in meinem GitHub-Repository unter <https://github.com/pietrobe03/randuino/tree/master/randuino-lib>.

Fertiger Aufbau Der Zufallsgenerator wurde im Rahmen des Projekts vollständig konstruiert. Ich habe hierfür auch eine Hülle mit Platz für den verwendeten Geigerzähler und die vollständige Verschaltung gestaltet und mit einem 3D-Drucker gedruckt. Die Simulation des Gehäuses kann im Anhang als Abb. 12 gefunden werden. Sie wurde mit der Software „Autodesk Inventor“ erzeugt.

4 Einschätzung der Umsetzung

4.1 Aufstellung eines Bewertungsmodells

Ziel meines Projekts ist nicht nur die Konstruktion eines Zufallsgenerators, sondern auch die Validierung und Optimierung dessen. Dabei achte ich auf die folgenden Parameter:

4.1.1 Die „Zufälligkeit“ der Messmethoden

Pseudo-Zufallszahlen haben die Eigenschaft, dass sie nach einer bestimmten Menge periodisch werden und immer die gleichen Ergebnisse produzieren. Außerdem verhalten sich diese oft gleich, wenn sie mit dem gleichen Startwert gestartet werden. Diese Probleme sollten bei meinen Konstruktionen nicht vorkommen, da diese auf nichtdeterministischen Zufallsquellen basieren. Ein weiterer Punkt sind die Wahrscheinlichkeiten der einzelnen Zufallszahlen. Der Arduino ist so programmiert, dass er die Messwerte der Entropiequellen in Werte von 0 bis 255 umwandelt. Dabei sollten alle Werte eine ungefähr gleiche Wahrscheinlichkeit haben. Um diese Thesen zu prüfen, werde ich mit jeder Entropiequelle 20'000 Werte (20'000 Werte werden nach dem FIPS 140-Standard für Zufallszahlen als repräsentativ angesehen.^[19]) generieren und diese auf Wahrscheinlichkeiten und sich wiederholende Patterns (Muster) testen. Beim ersten Test sollte jede Zahl ungefähr 78 Male vorkommen, beim zweiten Test sollten keine Patterns gefunden werden können. Sollten bestimmte Werte auch nach mehreren Test besonders häufig erscheinen, so werde ich versuchen, die Wahrscheinlichkeiten durch neue Rechenalgorithmen anzugeleichen. Falls sich Patterns bilden, so werde ich die Messung umkonstruieren müssen, da diese, wie bereits beschrieben, bei nichtdeterministischen Entropiequellen nicht vorkommen sollten. Um die Zufallsdatensätze auf Patterns zu testen, prüfe ich mit einem dafür geschriebenen Programm, ob sich innerhalb der Zufallswertemenge Ketten mit mehr als vier aufeinanderfolgenden Werten wiederholen, und ob diese Wiederholungen Mustern folgen.

4.1.2 Die Geschwindigkeit der Zufallszahlengenerierung

Bei der Zeitpunktmessung ist die Geschwindigkeit der Zufallszahlengenerierung von der Rate der eintreffenden Signale abhängig. So kann ein radioaktiv schwächeres Isotop die Geschwindigkeit massiv senken, da der Geigerzähler seltener ausschlägt. Eine Lösung dafür ist ein Puffer, welches Zufallszahlen zwischenspeichern und den Prozess beschleunigen kann.

Die Methode, bei der Messwerte direkt von einem Sensor gelesen werden, hat eine solche Limitation nicht, kann aber trotzdem nicht unlimitiert große Mengen an Zufallszahlen erzeugen, da sich sonst z.B. das An- und Abklingen des Rauschens (vgl. Abbildung 6) bestimmen ließen. Damit solche Werte nicht erratbar sind, darf der Messwert nicht direkt übermittelt werden, sondern muss vorher mit einer Einwegfunktion verschleiert werden.

4.1.3 Die Sicherheit der Zufallsgeneratoren

Eine weitere Zielsetzung meines Projektes ist die Sicherheit des Zufallsgenerators. So sollte es einem Angreifer z.B. nicht möglich sein, die Zufallswerte aus einem vom Geigerzähler verursachten Geräusch zu erraten. Außerdem überlege ich, eine Verschlüsselung für die Zufallszahlenübertragung implementieren.

4.2 Anwendung des Bewertungsmodells auf die verschiedenen Ansätze

Radioaktive Zerfälle Die Zufallszahlen werden bei dieser Methode generiert, indem der Arduino bei hoher Zählfrequenz von null bis 255 zählt und wieder zurückspringt. In dem Moment, indem ein neues Signal eintrifft, wird der aktuelle Wert des Zählers als neue Zufallszahl ins Puffer geschrieben. Meine Hypothese ist, dass die nicht periodischen, zufälligen Zeitabstände der radioaktiven Zerfälle für eine annähernd gleichmäßige Werteverteilung sorgen und keine periodischen Effekte zu erkennen sind.

Betrachtet man nun das Diagramm mit der Werteverteilung von 20'000 generierten Zufallswerten (Abb. 13) so erkennt man eine ungefähr gleichmäßige Verteilung mit leichten Ausreißern. Zu erwarten wäre ein Durchschnitt von ca. 78,13 Vorkommnissen pro Zufallswert, die durchschnittliche Abweichung hiervon beträgt 6,82 (entspricht 9%). Die größte Abweichung beträgt 26,13 Vorkommisse bei dem Zufallswert 66, was 33% Abweichung entspricht. Bei der Auswertung eines anderen Zufallszahlensatzes, der mit der gleichen Methodik erzeugt wurde, hatte die Zahl 66 74 Vorkommnisse. Als Durchschnitt aller Zufallswerte wird 127,5 erwartet, der tatsächliche Durchschnitt beträgt 125,46, was einer Abweichung von 1,60% entspricht. Außerdem wird erwartet, dass 10'000 der Zufallszahlen ganzzahlig durch zwei teilbar sind, der tatsächliche Wert weicht mit 10170 nur um 1,60% ab. Alle diese Werte bestätigen die Hypothese eines Zufallsgenerators mit etwa gleich verteilten Wahrscheinlichkeiten. Der Fakt, dass beim Suchen nach Mustern keine Ketten mit übermäßiger Häufigkeit gefunden wurden, lässt darauf schließen, dass der Generator nichtdeterministisch ist.

In puncto Geschwindigkeit ist diese Art der Generierung bei ungefähr einer Zehntelsekunde pro Zufallszahl einzurordnen, sofern man mit einem radioaktiven Gegenstand wie einem Glühstrumpf die Generierung beschleunigt. Ruft man nur die im Puffer gesicherten Werte ab, so ist dieser Generator noch schneller.

Akustisches und elektrisches Rauschen (Berechnung durch Hashing) Bei dieser Methode wird bei jeder Anfrage nach einer Zufallszahl ein verstärktes Rauschsignal gemessen und mit der Hashing-Funktion MD5 in eine Zufallszahl umgerechnet. Laut Spezifikation erzeugt MD5 eine sog. Prüfsumme, eine 32-stellige Hexadezimalzahl, bei der jede Ziffer (0 bis F) an jeder Stelle mit gleicher Wahrscheinlichkeit auftreten kann.

Betrachtet man nun das Diagramm mit der Werteverteilung von 20'000 generierten Zufallswerten (Abb. 14) so erkennt man eine sehr ungleichmäßige Verteilung mit starken Ausreißern. Die durchschnittliche Abweichung von den erwarteten 78,13 Vorkommnissen beträgt 42,32 (entspricht 54,17%). Die größte Abweichung beträgt 211,87 Vorkommisse bei dem Zufallswert 77, was einer Abweichung von 271,18% entspricht. Bei der Auswertung eines anderen Zufallszahlensatzes, der mit der gleichen Methodik erzeugt wurde, hatte die Zahl 66 74 Vorkommnisse. Als Durchschnitt aller Zufallswerte wird 127,5 erwartet, der tatsächliche Durchschnitt beträgt 129,52, was einer Abweichung von 1,58% entspricht. Außerdem wird erwartet, dass 10'000 der Zufallszahlen ganzzahlig durch zwei teilbar sind, der tatsächliche Wert weicht mit 9955 nur um 0,40% ab. Die großen Ausreißer und ungleiche Verteilung widersprechen der Hypothese eines Zufallsgenerators mit etwa gleich verteilten Wahrscheinlichkeiten. Von einer weiteren Betrachtung dieser Mess- und Rechenweise wurde abgesehen, stattdessen wird die Berechnung durch Bitfolgen genutzt. Die ungleiche Verteilung trotz der MD5-Spezifikation lassen sich darauf zurückführen, dass die gleichmäßige Verteilung nur gilt, wenn man alle möglichen Werte und nicht nur die vergleichsweise kleine Menge der Messwerte als Parameter für die MD5-Funktion einsetzt.

Akustisches und elektrisches Rauschen (Berechnung durch Bitfolgen) Bei dieser Methode werden bei jeder Anfrage nach einer Zufallszahl acht verstärkte Rauschsignale kurz nacheinander gemessen und je nach dem, ob der gemessene Wert gerade oder ungerade ist, eine 0 oder eine 1 als Bit in einem Byte. Das finale Byte lässt sich dann wiederum in eine Zahl von 0 bis 255 umrechnen. Da bereits sehr schwache Rauschsignale die gemessene Stromstärke um zufällig einige Messeinheiten variieren lassen, stelle ich wieder die Hypothese auf, dass es eine ungefähr gleichmäßige Werteverteilung geben wird und dass die Zufallswerte keinem Muster folgen.

Betrachtet man nun das Diagramm mit der Werteverteilung von 20'000 generierten Zufallswerten (Abb. 15) so erkennt man eine ungefähr gleichmäßige Verteilung mit leichten Ausreißern. Genau wie bei den beiden vorherigen Messungen wäre ein Durchschnitt von ca. 78,13 Vorkommnissen pro Zufallswert zu erwarten, die durchschnittliche Abweichung hiervon beträgt 7,66 (entspricht 9,8%). Die größte Abweichung beträgt 30,87 Vorkommnisse bei dem Zufallswert 144, was 39,51% Abweichung entspricht. Bei der Auswertung eines anderen Zufallszahlensatzes, der mit der gleichen Methodik erzeugt wurde, hatte die Zahl 144 nur 69 Vorkommnisse. Als Durchschnitt aller Zufallswerte wird 127,5 erwartet, der tatsächliche Durchschnitt beträgt 126,74, was einer Abweichung von 0,60% entspricht. Außerdem wird erwartet, dass 10'000 der Zufallszahlen ganzähnlich durch zwei teilbar sind, der tatsächliche Wert weicht mit 9997 nur um 0,03% ab. Alle diese Werte bestätigen die Hypothese eines Zufallsgenerators mit etwa gleich verteilten Wahrscheinlichkeiten. Auch hier wurden beim Suchen nach Mustern keine Ketten mit übermäßiger Häufigkeit gefunden, legt auch hier die Annahme, dass der Generator nichtdeterministisch ist, nahe.

Diese Generator erzeugt die Zufallswerte mit einer Geschwindigkeit von etwa 200ms pro Zufallszahl, da die zeitlichen Abstände zwischen den acht Messungen den Generator bremsen. Verwendet man keine zeitlichen Abstände, so misst der Arduino nicht schnell genug die Stromstärken neu und nutzt mehrfach den selben Messwert für die weitere Berechnung.

5 Zusammenfassung & Fazit

Insgesamt habe ich es geschafft, bis zum jetzigen Zeitpunkt zwei der vier geplanten Konstruktionen in funktionsfähige Aufbauten umzusetzen und habe beide Zufallsgeneratoren nach verschiedenen Kriterien geprüft und bewertet. Insgesamt habe ich hierbei erkannt, dass der auf radioaktiven Zerfällen basierende Zufallsgenerator bereits Zufallszahlen einer höheren Güte produziert, während mein erster auf elektrischem Rauschen basierte Ansatz (Generierung durch eine Hashingfunktion) bisweilen sehr ungleich verteilte Zufallswerte von somit eher niedrigerer Güte produziert. Der zweite Ansatz für die Zufallszahlengenerierung aus elektrischem Rauschen (Berechnung der Zufallszahl aus einer Bitfolge) eignet sich hingegen sehr gut.

Im Laufe der Ausarbeitung hat sich mein Blickwinkel auf das Projekt von der alleinigen Konstruktion eines nichtdeterministischen Zufallsgenerators zur Optimierung und Findung der besten Methode verschoben.

Diese Arbeit wurde außerdem in einer abgewandelten Form für die Teilnahme bei Jugend forscht genutzt und erreichte bis zum Zeitpunkt der Abgabe einen Regional- und einen Landessieg und damit die Teilnahme am Bundeswettbewerb, welcher erst nach Abgabe dieser Arbeit stattfinden wird.

Erklärung der eigenständigen Anfertigung der Facharbeit

Ich, Robert J. Pietsch, versichere, dass ich die vorliegende Facharbeit selbstständig verfasst und keine außer den angegebenen Hilfsmitteln verwendet habe. Alle Textstellen, die dem Wortlaut nach anderen Texten entsprechen, wurden entsprechend gekennzeichnet. Dies gilt ebenso für Bilder und Zeichnungen. Mir ist bewusst, dass wahrheitswidrige Angaben als Täuschungsversuch behandelt werden.^[20]

Ort, Datum und Unterschrift

Danksagung

Zum Schluss möchte ich mich noch recht herzlich bei allen denen bedanken, die mich bei der Ausarbeitung und bei Versuchen mit guten Tipps und Materialien unterstützt haben.

6 Anhang

6.1 Grafiken, Tabellen und Diagramme

Testaufbau (zu 3.2)

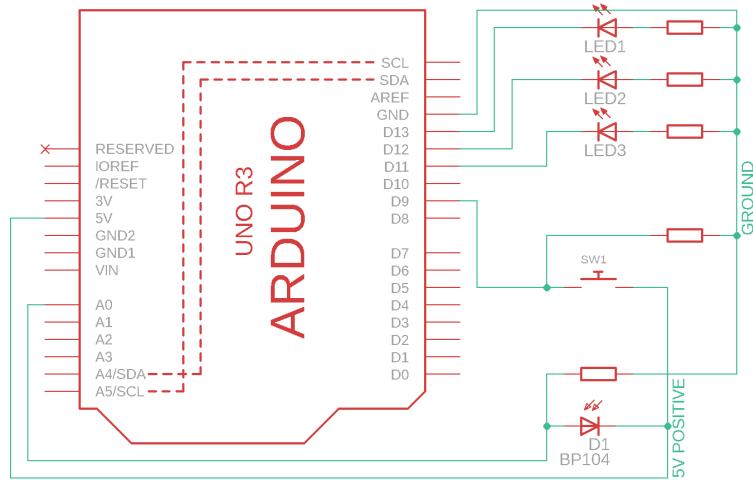


Abbildung 1: Verschaltung (Testaufbau)

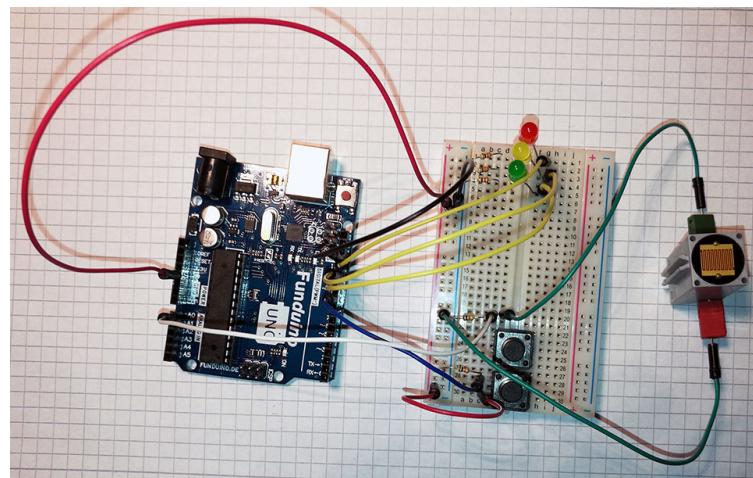


Abbildung 2: Testaufbau

Praktische Umsetzung (zu 3.3 und 3.4)

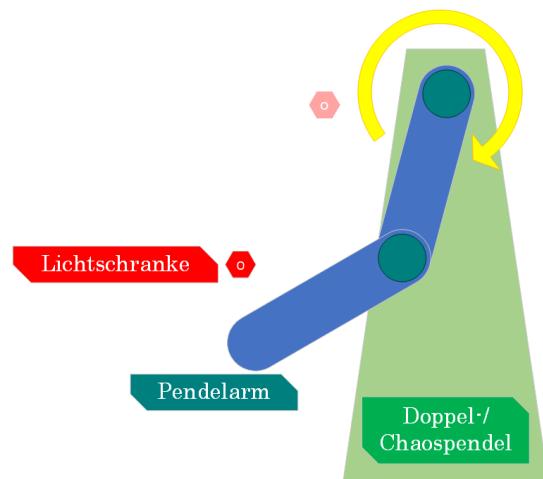


Abbildung 3: Konstruktionsidee Chaospendel (mit Lichtschranken)

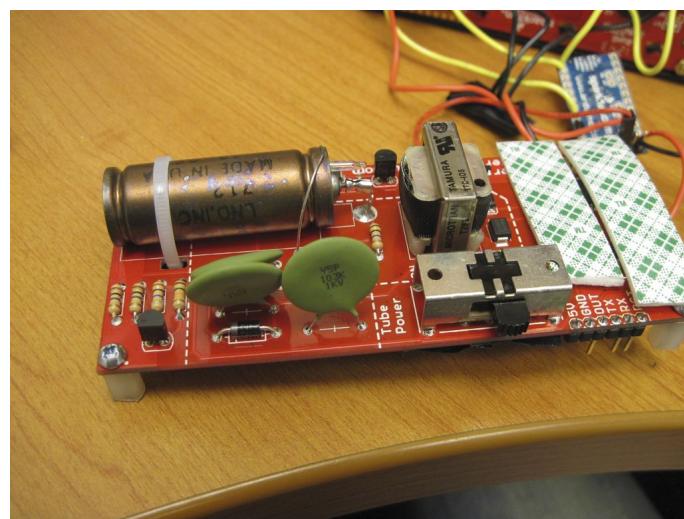


Abbildung 4: Arduinomodul mit Geigerzähler^[21]

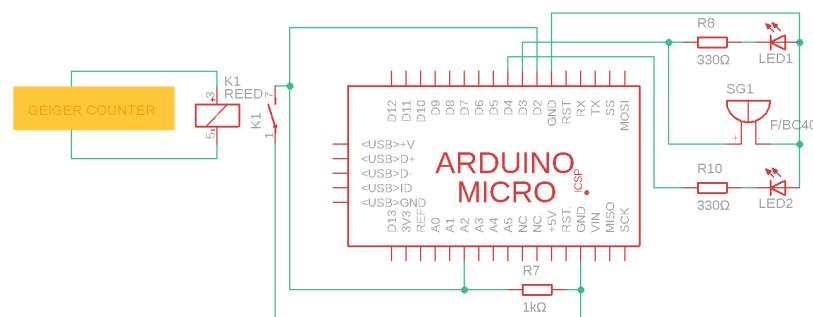


Abbildung 5: Finaler Schaltkreis mit Geigerzähler

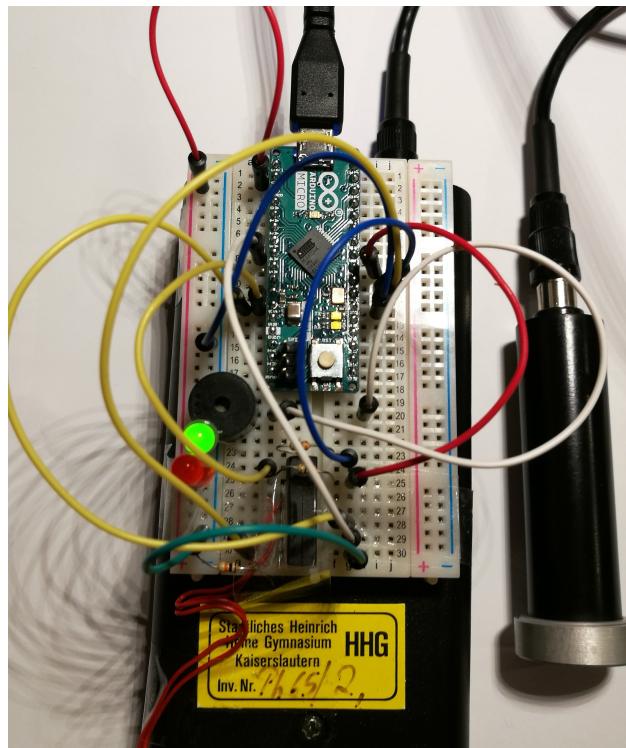


Abbildung 6: Finaler Aufbau mit Geigerzähler

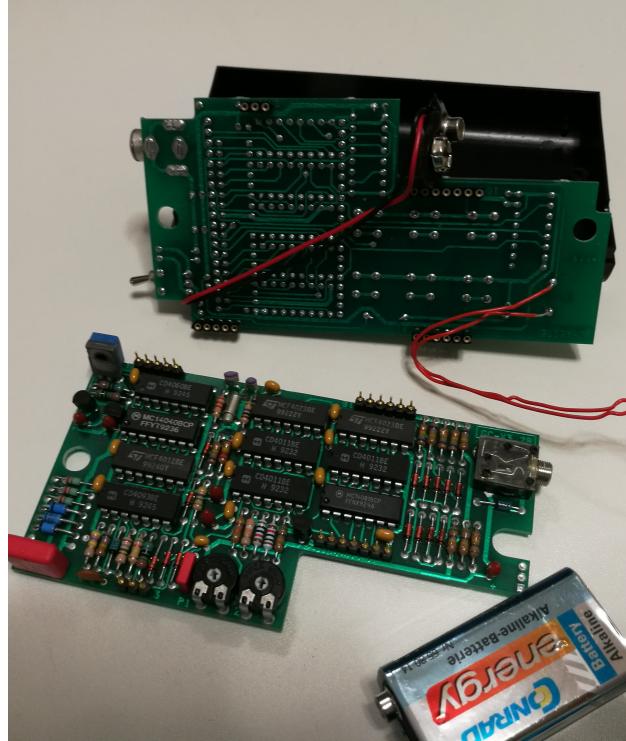


Abbildung 7: Geöffneter Geigerzähler mit Signalabgreifung

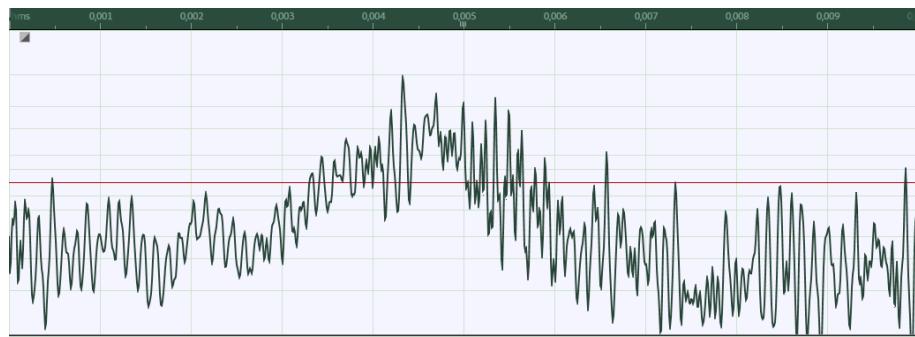


Abbildung 8: Elektrisches Rauschen (Messintervall: $\Delta t = 0.01s$)

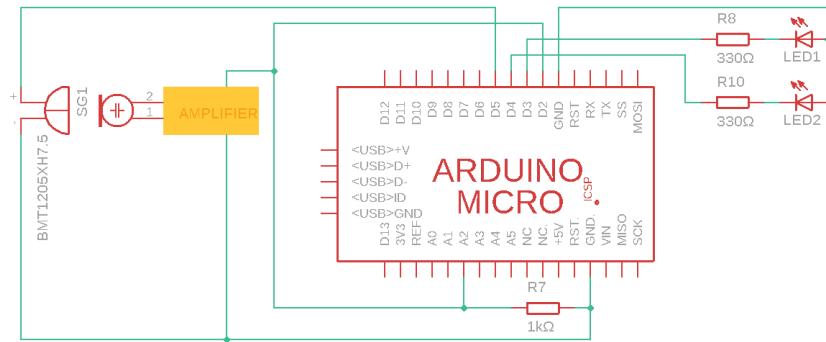


Abbildung 9: Finaler Schaltkreis mit akustischem Rauschen

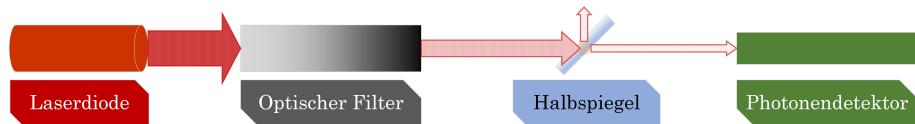


Abbildung 10: Konstruktionsidee: Photonenablebung am Halbspiegel

Umsetzung als Peripheriegerät (zu 3.5)

Befehl	Antwort	Beschreibung
connect	randuino	Sendet den Gerätetyp zurück. Wird zur Identifikation beim Verbindungsauftbau benötigt.
single	Zufallszahl oder buffer_empty	Sendet eine Zufallszahl oder eine Meldung bei der Zeitpunktmeßung, dass keine Zufallswerte verfügbar sind.
buffer	B: Puffergröße	Sendet die Zahl der verfügbaren Zufallszahlen. Dieser Befehl ist nur bei der Zeitpunktmeßung verfügbar.
heartbeat	still_alive	Bestätigt eine aktive Verbindung.

Abbildung 11: Befehle und Antworten (jeweils ohne Zeilenumbruch)

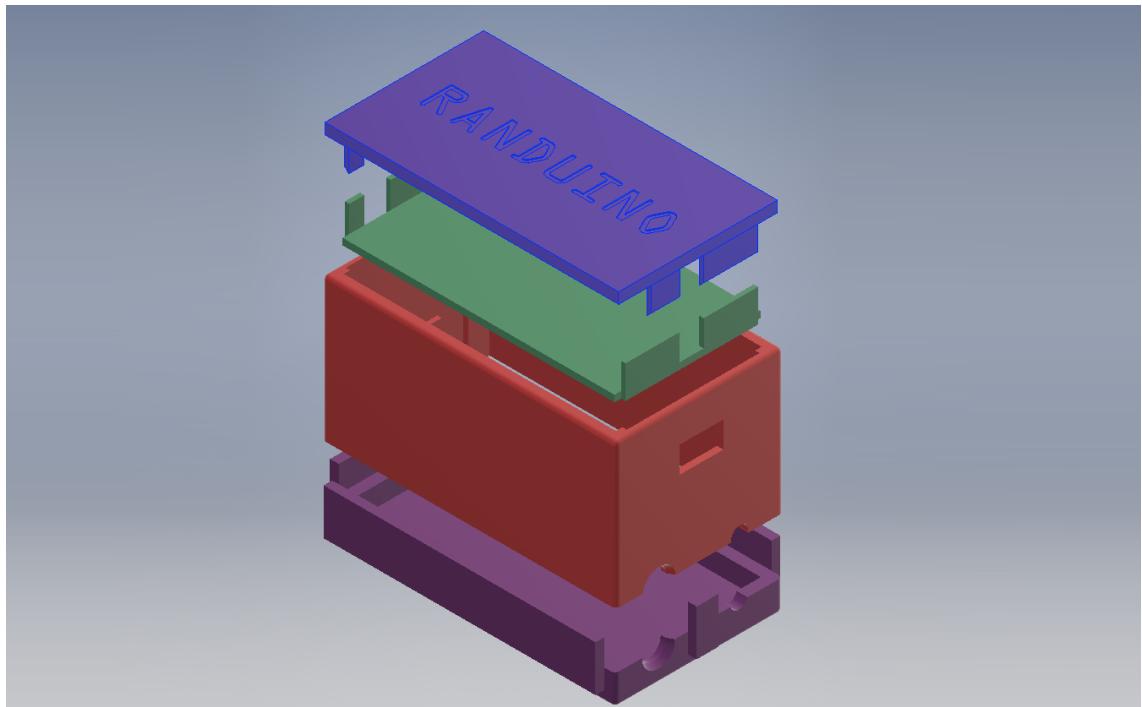


Abbildung 12: Computersimulation der Hülle des Peripheriegeräts

Anwendung des Bewertungsmodells (zu 4.2)

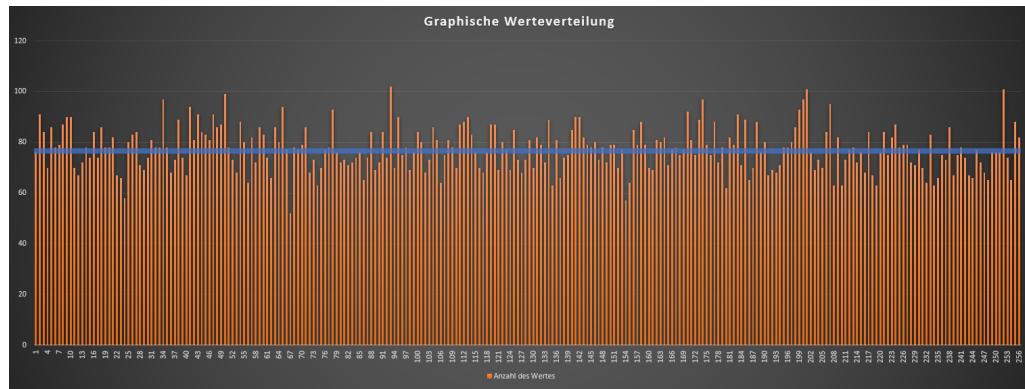


Abbildung 13: Werteverteilung „Radioaktive Zerfälle“

(In blau die erwartete Zahl der Vorkommnisse bei gleicher Verteilung)

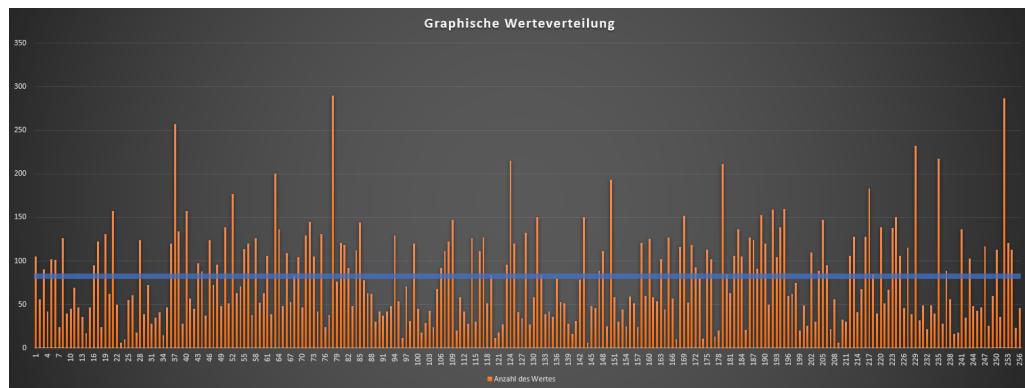


Abbildung 14: Werteverteilung „Rauschen (Hashing)“

(In blau die erwartete Zahl der Vorkommnisse bei gleicher Verteilung)

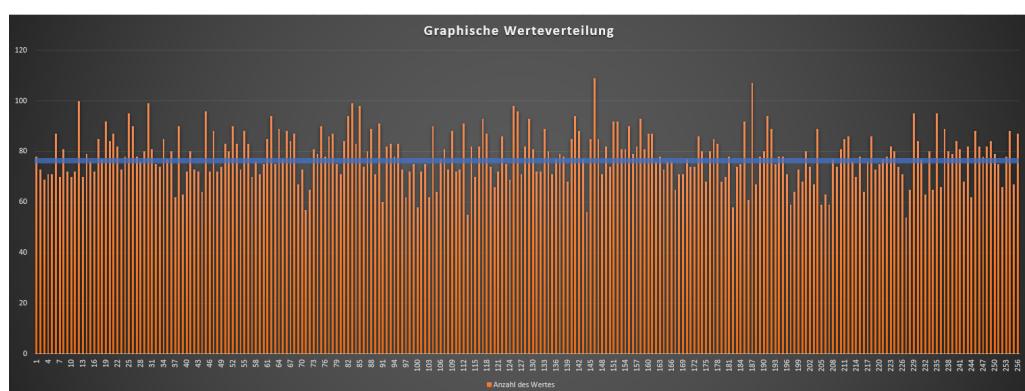


Abbildung 15: Werteverteilung „Rauschen (Bitfolge)“

(In blau die erwartete Zahl der Vorkommnisse bei gleicher Verteilung)

6.2 Quellenverweise

In Klammern hinter den Quellenverweisen befinden sich die Daten der jeweiligen letzten Zugriffe.

- [1] <https://www.random.org/randomness>
Absatz "Pseudo-Random Number Generators (PRNGs)" (18.03.2019)
- [2] <https://www.elektronik-kompendium.de/sites/net/1910301.htm>
Absatz "Pseudozufallsgenerator" (19.03.2019)
- [3] <https://ee.stanford.edu/~hellman/publications/24.pdf>
Abschnitt "Introduction" (18.03.2019)
- [4] Grehn J. & Krause J. (2007) Metzler Physik (4. Auflage). Braunschweig, Deutschland: Schrödel. Seite 106f.
- [5] <https://www.spektrum.de/lexikon/physik/welle-teilchen-dualismus/15525>
Gesamter Artikel (21.03.2019)
- [6] <http://www.philosophieverstaendlich.de/stichworte/determinismus>
Absatz „Kausaler Determinismus“ (21.03.2019)
- [7] <https://www.welt.de/kultur/article152337968/Sind-wir-von-unsichtbaren-Parallelwelten-umgeben.html>
Gesamter Artikel (21.03.2019)
- [8] <https://leifiphysik.de/kern-teilchenphysik/radioaktivitat-einfuhrung>
Gesamte Seite (23.03.2019)
- [9] <https://www.leifiphysik.de/kern-teilchenphysik/radioaktivitaet-einfuehrung/ionisierung-durch-strahlung>
Gesamte Seite (23.03.2019)
- [10] Grehn J. & Krause J. (2007) Metzler Physik (4. Auflage). Braunschweig, Deutschland: Schrödel. Seiten 482f und 486ff.
- [11] <https://de.wikipedia.org/wiki/Glühstrumpf> - Gesamte Seite (22.03.2019)
- [12] Hollemann A.-F. & Wiberg N. (1985) Lehrbuch der Anorganischen Chemie (33. Edition). Berlin, Deutschland & New York, USA: de Gruyter & Co. S. 1281 u. 1288f
- [13] <https://www.leifiphysik.de/kern-teilchenphysik/radioaktivitaet-einfuehrung/geiger-mueller-zahlrohr>
Gesamte Seite (23.03.2019)
- [14] <http://www.rapp-instruments.de/Radioaktivitaet/Detektoren/Geigercounter/Geigercounter.htm>
Gesamte Seite (23.03.2019)
- [15] https://www.uni-frankfurt.de/68943623/Elektronisches_Rauschen-231020171.pdf - Kapitel I - III (24.03.2019)
- [16] https://www.antennen-emv.tu-berlin.de/fileadmin/fg13/Lernmaterialien/analog_10_Elektronisches_Rauschen.pdf - Kapitel 10.1 „Rauschursachen“ (24.03.2019)
- [17] [https://de.wikipedia.org/wiki/Rauschen_\(Physik\)](https://de.wikipedia.org/wiki/Rauschen_(Physik)) - Einleitung (24.03.2019)

[18] <https://qt.io/download> - Spalte „Open Source“ (22.03.2019)

[19] <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>
Kapitel 4.7.1 und 4.9 (22.03.2019)

[20] Es handelt sich bei dieser Erklärung um einen Vorgabetext der MSS-Leitung am
staatl. Heinrich-Heine-Gymnasium Kaiserslautern.

[21] <https://www.instructables.com/id/Arduino-Geiger-Counter/>
Abbildung „Sparkfun Geiger Counter“ (23.03.2019)

Graphiken ohne weitere Quellenangaben wurden von mir angefertigt, gleiches gilt auch für
Messreihen und Visualisierungen.