Quantenoptisches Verfahren zur Erzeugung zufälliger Bitfolgen

Martin Ignaz Fürst

München 2011

Quantenoptisches Verfahren zur Erzeugung zufälliger Bitfolgen

Martin Ignaz Fürst

Dissertation
an der Fakultät für Physik
der Ludwig–Maximilians–Universität
München

vorgelegt von
Martin Ignaz Fürst
aus Neuburg a.d. Donau

München, den 24.06.2011

Erstgutachter: Prof. Dr. Harald Weinfurter
Zweitgutachter: Prof. Dr. Ulrich Gerland
Tag der mündlichen Prüfung: 04.08.2011

Zusammenfassung

Zufallszahlengeneratoren sind in der modernen Gesellschaft von großer Bedeutung und in vielen Bereichen verbreitet. In numerischen Simulationen, in der Glückspielindustrie, bei Authentifizierungsaufgaben wie zum Beispiel bei der Erzeugung von PIN/TAN Nummern als auch in kryptographischen Anwendungen finden sich Einsatzgebiete von Zufallszahlengeneratoren. Heutzutage werden dazu häufig algorithmische oder physikalische Ansätze verwendet, die aber auf Grund des Determinismus der klassischen Physik keine *echten*, sondern im Prinzip vorhersagbare Zufallszahlen erzeugen können. Die Unbestimmtheit und Unvorhersagbarkeit in der Quantenmechanik bietet jedoch die Möglichkeit *echte* Zufallszahlen erzeugen zu können.

In dieser Arbeit wird ein Zufallszahlengenerator auf Basis quantenmechanischer Effekte entwickelt. Dazu wird die Lichtemission einer Leuchtdiode (LED) als Zufallsquelle verwendet. Die Detektion einzelner Photonen erfolgt mithilfe eines Photomultipliers. Das Zufallsbit ergibt sich aus der Teilbarkeit durch zwei der in einem bestimmten Zeitintervall beobachteten Anzahl von Detektionsereignissen. Bei der Entwicklung des theoretischen Modells wird sowohl der Emissionsprozess der LED als auch der Detektions- und der elektronische Verarbeitungsprozess betrachtet. Dabei zeigt sich, dass sowohl der Abstoßungsprozess der Elektronen innerhalb des Halbleiterübergangs der LED als auch die hohe Abschwächung des Photonenstroms und die Totzeit, die bei der Detektion der Photonen auftritt, die detektierte Photonenstatistik und damit die Eigenschaften der Zufallszahlen bestimmen. Bemerkenswert ist, dass durch den Einfluss der Totzeit die Poissonstatistik der Photonen dahingehend verändert wird, dass gleichverteilte Bitfolgen selbst bei niedrigen Photonenzahlen erzeugt werden können. Im Fall einer Poissonstatistik tritt dies erst im Grenzfall unendlich hoher Photonenzahlen ein.

In einem kompakten experimentellen Aufbau kann dieses theoretische Modell bestätigt werden. Mit diesem Gerät können Zufallsbits mit einer Geschwindigkeit von bis zu $50\frac{\mathrm{MBit}}{\mathrm{s}}$ erzeugt werden. Eine abschließende Analyse der Zufallsbitfolgen mit statistischen Methoden zeigt außerdem kein Anzeichen von Regelmäßigkeiten in diesen Folgen.

Der in der vorliegenden Arbeit entwickelte Zufallszahlengenerator wird zukünftig in ein Quantenkryptographiesystem der LMU München integriert. Eine einfache Skalierbarkeit dieses Geräts und die damit verbundene Steigerung der Erzeugungsrate erlaubt den Einsatz in modernen Kryptographiesystemen mit Geschwindigkeiten im Bereich von $> 1\frac{\mathrm{GBit}}{\mathrm{s}}$.

Abstract

In our modern society random number generators are widely circulated. Numerical simulations, the gambling industry, authentication tasks like the generation of pin/tan numbers all the way to cryptographic environments are applications for random number generators. Today algorithmic or physical deterministic approaches are used, which cannot produce *true* random numbers. The indeterminacy and unpredictability in quantum mechanics however provide the possibility to generate *true* random numbers.

In this work a random number generator is developed using quantum mechanical effects. The random source is based on the light emission of a light emitting diode. The emitted photons are detected by a photomultiplier tube. The random bit values are extracted by counting the number of photons detected in a certain time interval. Both the photon emission process of the LED, the detection process and the electronical pulse recognition circuit are considered in developing the theoretical model. It turns out that the main contributions to the final detected photon number distribution come from a coulomb blockade effect of electrons inside the semiconductor junction of the LED, the optical attenuation of the photons and the dead time of the detection circuitry. Remarkably the effect of the dead time modifies the photon statistics in such a way that equally distributed random bit sequences can be generated even at low mean photon numbers. In case of a Poissonian statistics this would require an infinitely high photon number.

In a compact experimental setup this theoretical model can be verified. Random bit rates of up to 50 MBit/s can be generated. A final analysis of bit sequences with statistical methods do not reveal any regularities in these sequences.

In future this random number generator will be integrated into the quantum key distribution setup of the LMU Munich. An increase in the generation rate by scaling the setup would allow to adopt this system in modern cryptographic applications with rates of up to 1 GBit/s.

Inhaltsverzeichnis

Kapitel 1

Einleitung

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

Der Zufall übt auf Menschen eine besondere Faszination aus. Bereits in der Antike gab es Glücksspiele zur Unterhaltung und zum Zeitvertreib, bei denen der unvorhersagbare, zufällige Ausgang den besonderen Reiz dieser Spiele ausmachte. Als Zufallsgenerator wurde zum Beispiel ein Würfel mit unterschiedlich markierten Flächen verwendet. Glücksspiele sind auch heute noch sehr beliebt und aufgrund des vielfältigen Angebots ein großes Einsatzgebiet von Zufallsgeneratoren.

Durch die Entwicklungen im letzten Jahrhundert sind allerdings weitere Einsatzgebiete von Zufallsgeneratoren hinzugekommen. Notwendig sind Zufallszahlen beispielsweise in computergestützten numerischen Simulationen oder in probabilistischen Algorithmen, wie zum Beispiel der Primzahlsuche. Durch die weltweite Vernetzung sowohl privater als auch wirtschaftlicher Bereiche in den letzten Jahren, gewinnt sowohl die Kryptographie als auch die Authentifizierung als Anwendung von Zufallszahlengeneratoren immer mehr an Bedeutung.

Es werden heute zwei grundlegend verschiedene Ansätze zur Erzeugung von Zufallszahlen verwendet. Algorithmische Zufallszahlen beruhen auf einer Rechenvorschrift, bei der aus einer Anfangszahl (engl: „Seed“) eine Folge von Zahlen berechnet wird. Wie in dem oben angeführten Zitat von *von Neumann* drastisch ausgedrückt, können diese Folgen nicht als echte Zufallszahlen betrachtet werden. Häufig ist es jedoch ausreichend, wenn diese so erzeugten Zahlenfolgen nur einige Eigenschaften von Zufallszahlen erfüllen.

Im Anwendungsgebiet der Numerik genügt es meist, dass die Zahlenfolge gleichverteilt ist und keine ausgeprägte Struktur besitzt. Ausschlaggebend ist in diesen Anwendungsgebieten vielmehr die Geschwindigkeit und die Effizienz der Erzeugung. Ergebnisse aus der Vergangenheit zeigen jedoch, dass solche Systeme für kryptographische Anwendungen nicht geeignet sind [1, 2].

Auf der anderen Seite gibt es Zufallszahlengeneratoren (ZZG), bei denen ein physikalischer Prozess die Grundlage zur Erzeugung von Zahlenfolgen, im Allgemeinen Bitfolgen ist. Diese ZZG werden auf Basis der zugrundeliegenden Prozesse in zwei Bereiche unterteilt. Zum einen dienen chaotische physikalische Prozesse als Zufallsquelle wie zum Beispiel elektronisches Rauschen in Dioden oder zeitlicher Jitter in Oszillatoren. Diese mit klassischer Physik beschreibbaren Abläufe sind deterministisch und nur die Komplexität verhindert eine Berechnung dieser Prozesse. Andererseits existieren ZZG auf Basis der Quantenphysik, deren Zufälligkeit auf fundamentalen Gesetzen der Quantenmechanik beruhen.

Die Idee zur Entwicklung eines Zufallszahlengenerators entstand in Zusammenhang mit einem bestehenden Quantenschlüsselverteilungexperiment[1] [3–5]. Die Sicherheit diesem Verfahren hängt maßgeblich von der Zufälligkeit der gesendeten Qubits ab, die in diesem Experiment mit einer Wiederhohlrate von 10 MHz erzeugt werden müssen. Deshalb wird ein Zufallszahlengenerator benötigt, dessen Zufälligkeit ebenfalls durch eine quantenmechanische Theorie gestützt wird. Da für jedes Qubit mindestens zwei Zufallsbits benötigt werden, muss zusätzlich eine hohe Erzeugungsgeschwindigkeit erreicht werden.

Überblick über die Arbeit:

Im ersten Abschnitt dieser Arbeit wird ein Überblick über den Stand der Forschungsarbeit im Zusammenhang mit quantenmechanischen ZZG gegeben. Das Hauptaugenmerk liegt anschließend auf der Realisierung unseres ZZG, dessen Zufallsprozess durch die Quantenmechanik beschrieben werden kann. Eine theoretische Beschreibung aller Komponenten des optischen ZZG führt den Zufall auf die Statistik emittierter Photonen einer Leuchtdiode zusammen mit der probabilistischen Natur einer Abschwächung zurück. Am Schluss der theoretischen Beschreibung steht ein stochastisches Modell, das bei einer Zertifizierung [6, 7] durch das Bundesamt für Sicherheit in der In-

[1] Quantenschlüsselverteilung wird auch oft missverständlich mit Quantenkryptografie bezeichnet obwohl die Verschlüsselung klassisch mithilfe des one time pads durchgeführt wird.

formationstechnologie (BSI) gefordert wird[2]. Im darauf folgenden Abschnitt werden die einzelnen optischen und elektronischen Komponenten des ZZG bestimmt und deren Verhalten in Bezug auf die Generierung einer Zufallsbitfolge untersucht. Bei der Analyse der Zufallsbits werden zunächst die Vorhersagen des stochastischen Modells verifiziert. Anschließend werden die Bitfolgen mithilfe von statistischen Tests auf eventuelle Korrelationen untersucht. Es werden einzelne Tests ausgewählt, deren Sensitivität an das Modell des ZZG angepasst ist. Für die Analyse von Zufallsbitfolgen wurden in diesem Forschungsbereich verschiedene Testbibliotheken zusammengestellt, die abschließend auf große Zufallsbitfolgen angewendet werden. Das Bestehen der statistischen Tests ist aber nicht als Beweis zu sehen, dass der ZZG tatsächlich zufällige Bitfolgen erzeugt, sondern lediglich, dass diese endlichen Folgen sich in guter Näherung zufällig verhalten. Gute algorithmische Zufallszahlengeneratoren, die rein deterministisch arbeiten, bestehen nämlich ebenfalls diese statistischen Tests. Der Beweis für die Zufälligkeit liegt deshalb sowohl im theoretischen Modell als auch in dessen experimenteller Bestätigung.

[2]Eine Zertifizierung ist für Geräte notwendig, die als Teil eines Kryptographiesystems eingesetzt werden, um deren Sicherheit zu gewährleisten.

Kapitel 2

Eigenschaften von Zufallszahlengeneratoren

Zufallszahlengeneratoren erzeugen im Allgemeinen eine Folge von Bits, deren Eigenschaften zu Beginn dieses Abschnitts definiert werden. In einem Überblick über verschiedene Strategien zur Implementierung von ZZG wird anschließend zwischen algorithmischen und experimentellen Ansätzen unterschieden. Eine weitere Klassifizierung letzterer kann man durch den grundlegenden physikalischen Prozess des Generators vornehmen. Ein ZZG, der zur Erzeugung von Zufallszahlen einen Prozess verwendet, bei dem das Resultat durch dessen Komplexität zufällig erscheint, bezeichnet man als physikalischen Zufallszahlengenerator(PZZG). Quantenmechanische Zufallszahlengeneratoren(QZZG) verwenden einen Prozess, dessen Zufälligkeit aus der Unbestimmtheit der Messung eines quantenmechanischen Zustands resultiert. Im darauffolgenden Abschnitt werden Beispiele für verschiedenen Strategien zur Realisierung eines QZZG aufgezeigt. Im Besonderen wird auf die Beschreibung der jeweiligen Stärken und Schwächen dieser Prinzipien eingegangen.

2.1 Eigenschaften von Zufallszahlen

Die Ausgabe eines ZZG ist in der Regel eine Abfolge von Bits, die in einem mathematischen Formalismus als Realisierung eines Zufallsexperiments $X_i = x_i$ beschrieben werden kann. Dabei wird das Experiment mit X_i bezeichnet, das Ergebnis eines Experiments $X_i = x_i$ mit $i \in 1 \dots n$. Durch die Einschränkung auf Bitfolgen kann x_i nur die Werte $0, 1$ annehmen. Die Elemente einer zufälligen Bitfolge müssen sowohl gleichverteilt als auch unabhängig voneinander sein.

Gleichverteilung: Die Wahrscheinlichkeit, dass eine bestimmte Realisie-

rung bei einem Zufallsexperiment eintritt, ist für alle Realisierungen gleich. Für den betrachteten binären Fall gilt daher:

$$P(X_i = 1) = P(X_i = 0) = \tfrac{1}{2}$$

Unabhängigkeit: Die Wahrscheinlichkeit, dass eine Realisierung x_i eintritt, ist unabhängig von der Historie an Zufallsexperimenten, das heißt unverändert unter Kenntnis aller zuvor erzeugten Zufallszahlen.

$$P(X_i = x_i) = P(X_i = x_i | X_{i-1} = x_{i-1} \ldots X_0 = x_0)$$

In der folgenden Analyse bestehender ZZG werden nicht nur die Zahlen auf deren Zufallseigenschaften untersucht, sondern insbesondere der physikalische Prozess. Aus diesem Grund wird eine weitere Eigenschaft definiert.

Unbestimmtheit: Bei vollständiger Kenntnis des quantenmechanischen Zustands des ZZG vor einer Messung bleibt die Wahrscheinlichkeit für das Eintreten einer Realisierung unverändert.

$$P(X_i = x_i | \text{Kenntnis des Systems}) = P(X_i = x_i) = \tfrac{1}{2} \tag{2.1}$$

Diese letzte Eigenschaft wird bei der Unterscheidung von physikalischen und quantenmechanischen ZZG wichtig.

2.2 Klassifizierung der Zufallszahlengeneratoren

In diesem Abschnitt werden verschiedene Ansätze zur Erzeugung von Zufallszahlenfolgen aufgezeigt. Obwohl algorithmische Methoden keine wirklich zufälligen Zahlen erzeugen, werden sie aufgrund der Effizienz bei der Generierung von Bitfolgen häufig eingesetzt. Physikalische Zufallszahlengeneratoren nutzen oft elektronische Effekte, um Zufallsbits zu erzeugen. Sie können jedoch mit Hilfe der klassischen Physik beschrieben werden, wodurch das Resultat prinzipiell deterministisch ist. Nur die Komplexität der oft chaotischen Abläufe verhindert, dass diese Bitfolgen heutzutage berechnet werden können. Im Gegensatz dazu basiert der Zufall in quantenmechanischen ZZG auf der Unbestimmtheit und Unvorhersagbarkeit der Quantenmechanik.

2.2.1 Algorithmische Zufallszahlengeneratoren

Bei dieser Art von ZZG werden, wie die Bezeichnung bereits suggeriert, Zahlenfolgen mit Hilfe eines Algorithmus aus einem Startwert (engl. Seed) berechnet. Durch dieses deterministische Vorgehen wird bei identischem Seed immer dieselbe Bitfolge generiert. Man bezeichnet diese Programme trotzdem als Zufallszahlengeneratoren, da die damit erzeugten Bitfolgen zumindest die erste Eigenschaft von Zufallsbitfolgen in Abschnitt 2.1 erfüllen. Die Unabhängigkeit der Bits kann nicht erfüllt werden, obwohl bei der Untersuchung von kurzreichweitigen[1] Abhängigkeiten die Bitfolgen keine Anzeichen einer Struktur aufweisen. Ein Merkmal dieser Generatoren, welche oft auch als Pseudozufallszahlengeneratoren bezeichnet werden, ist, dass sich nach einer bestimmten Periode die Zufallszahlen wiederholen[2]. Da diese Generatoren jedoch sehr schnell arbeiten, werden sie häufig eingesetzt. In numerischen Simulationen [8] werden zum Beispiel große Mengen von Zufallszahlen benötigt, die gleichverteilt sein sollten und für kurze Bitfolgen keine statistischen Abweichungen von idealen Zufallszahlen aufweisen sollten. Ein weiterer Vorteil dieses ZZG ist die einfache Reproduzierbarkeit von Simulationen, da nur jeweils der gleiche Startwert verwendet werden muss.

Wenn diese Art der Zufallszahlerzeugung bei kryptographischen Anwendungen bzw. der Authentifizierung eingesetzt wird, kann die Sicherheit beeinträchtigt werden, da durch die (bekannte) Berechnung der Zahlenfolgen die Zufallszahlen deterministisch sind [1, 2]. Dennoch werden heutzutage sehr komplexe algorithmische Zufallszahlengeneratoren in den meisten kryptografischen Anwendungen eingesetzt. Um die Sicherheit zu erhöhen, wird der Seed deshalb oft aus unbestimmten Ereignissen wie zum Beispiel Systemzeiten bei Festplattenzugriffen, Bewegungen der Maus, Tastaturanschlägen oder Zeitpunkte für Interruptroutinen etc. erneuert.

Das bekannteste Beispiel eines algorithmischen ZZG ist das *Lineare Rückgekoppelte Schiebe-Register* (LFSR) [9]. Die Funktionsweise beruht auf einem Schieberegister, dessen Eingang bei jedem Zyklus durch eine Kombination der Einträge neu berechnet wird. Durch die einfache Implementierbarkeit in Mikroprozessoren und programmierbarer Logik wird diese Art von Pseudozufallszahlgenerierung verbreitet eingesetzt.

[1] Kurzreichweitig bezieht sich in diesem Zusammenhang auf den Abstand der Bits in der Zufallszahlenfolge.

[2] Diese Periode kann bei modernen Algorithmen sehr groß sein: MT19937 hat eine Periode von $2^{19937} - 1$.

2.2.2 Physikalische Zufallszahlengeneratoren

Zu dieser Kategorie zählen Generatoren, deren zugrundeliegende Prozesse klassisch beschreibbar aber meist sehr komplex sind. Hierzu gehören „einfache“ Systeme wie zum Beispiel der Münzwurf, der Würfel oder das Roulette. Bei identischen Startbedingungen werden in diesen Experimenten im Prinzip aber gleiche Resultate erzeugt [10]. Erst durch kleine Abweichungen in den Startbedingungen, die dem Anwender nicht bekannt sind, erscheint das Ergebnis zufällig.

Weitere Beispiele dieser Kategorie sind Generatoren, die auf Rauschen in Widerständen [11] oder Halbleiterbauelementen [6, 12] zurückgreifen, um Zufallsbits zu erzeugen. Diese Systeme basieren auf der Digitalisierung der Rauschspannung an einem Widerstand oder einer Diode durch einen Komparator, dessen Schwelle der mittleren Rauschspannung entspricht. Um die Zufälligkeit noch zu erhöhen, werden dabei zwei identische Rauschquellen logisch kombiniert. Ein alternativer Ansatz verwendet zwei gegeneinander fluktuierende Oszillatoren wobei ein Oszillator am Daten-Eingang und einer am Takt-Eingang eines FlipFlop sitzt [13].

Der Einsatz solcher Generatoren in kryptographischen Anwendungsgebieten erhöht aufgrund der Komplexität der Prozesse die Sicherheit gegenüber algorithmischen Verfahren, basieren aber auf Abläufe, die mit Hilfe klassischer Physik beschreibbar sind und deshalb im Prinzip berechnet werden können.

2.2.3 Quantenmechanische Zufallszahlengeneratoren

Die Grundlage von quantenmechanischen Zufallszahlengeneratoren ist die Messung eines Quantensystems. Als Ergebnis der Messung treten die Eigenzustände des Messoperators jeweils mit einer bestimmten Wahrscheinlichkeit auf. Diese Wahrscheinlichkeitsverteilung dient als Grundlage zur Erzeugung von Zufallszahlen.
Die nachfolgende Übersicht gibt einen Überblick über den aktuellen Stand der Forschung auf diesem Gebiet.

Photonen und Strahlteiler: Passiert ein einzelnes Photon einen Strahlteiler, so kann der quantenmechanische Zustand $|\Psi\rangle$ nach dem Strahlteiler als Superpositionszustand, bestehend aus „Photon im transmittierten“ $|n_T\rangle$ und „Photon im reflektierten“ $|n_R\rangle$ Ausgang, beschrieben werden.

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|1_T\rangle|0_R\rangle + |0_T\rangle|1_R\rangle) \tag{2.2}$$

Dabei ist $|n\rangle$ der Photonenzahlzustand im jeweiligen Ausgang des Strahlteilers. Bei einem idealen Strahlteiler mit Teilungsverhältnis 50/50 wird das Photon in jedem Ausgang mit einer Wahrscheinlichkeit von 0.5 gemessen. Den Detektionsereignissen an beiden Ausgängen werden jeweils die Bitwerte 0 und 1 zugeordnet [14, 15].

Bei den Implementierungen [16, 17] wird ein polarisierender Strahlteiler verwendet. Zusammen mit einer polarisierten Lichtquelle (LED + Polarisator) und einer Halbwellen-Verzögerungsplatte kann so die Detektionswahrscheinlichkeit der beiden Detektoren an den Ausgängen des Strahlteilers annähernd gleich eingestellt werden. Als tatsächliche Einzelphotonquelle wurde in [18, 19] eine SPCM-Quelle[3] benutzt und ein Photon als Trigger verwendet.

Dem Ereignis, dass in beiden Detektoren gleichzeitig ein Photon detektiert wird, kann kein Bitwert zugeordnet werden. Er muss deshalb ignoriert werden. Durch die Anpassung der Detektionseffizienzen mit Hilfe eines polarisierenden Strahlteilers kann eine Schiefe in den Zufallszahlen oft nicht ausreichend behoben werden [16], wodurch eine Regularisierung [20, 21] notwendig wird. Mithilfe dieses Vorgehens wurden Zufallszahlen mit einer maximalen Rate von 1 Mbit/s erzeugt.

Einschränkende Faktoren dieses Verfahrens sind die Totzeit der Detektoren, die die maximale Anzahl an Detektionsereignissen beschränkt. Da pro Photon je ein Zufallsbit erzeugt wird, ist die Biterzeugungsrate damit limitiert. Gleichzeitig führt eine Schiefe in den Zufallsbits zu einer weiteren Reduktion der Zufallsbits (siehe Abschnitt 3.6).

Unbestimmter Emissionszeitpunkt: Der Emissionszeitpunkt einer spontanen Zerfallsquelle dient als Quelle zur Zufallsbiterzeugung. Die zeitlichen Abstände aufeinanderfolgender Zerfälle sind für unabhängige Emissions- und Absorptionsprozesse aufgrund deren Zufälligkeit exponentiell verteilt. Für die Erzeugung der Zufallsbits können unterschiedliche Verfahren verwendet werden.
Einerseits ist es möglich zwei aufeinanderfolgende Zeitintervalle zu vergleichen [22–25]. Dem Zufallsbit wird der Wert 0 zugeordnet, wenn das erste der beiden Intervalle größer ist und 1 wenn das zweite Intervall größer ist. Durch die Unabhängigkeit der Intervalllängen ist bei dieser Methode der Bitextraktion keine Schiefe in den Zufallszahlen zu erwarten. Durch eine endliche Zeitauflösung können zwei Zeitintervalle auchgleich groß sein. Diese Ereignisse tragen nicht zur Zufallszahler-

[3] SPCM=„spontaneous parametric down conversion“ ist ein nichtlinearer Prozess, bei dem ein Photon in einem nichtlinearen Kristall zwei Photonen mit halber Frequenz erzeugt.

zeugung bei.
Eine andere Möglichkeit besteht darin die Zeitabstände im Rahmen der Messgenauigkeit zu bestimmen. Die exponentielle Verteilung dieser Werte wird in kleine Teilbereiche aufgeteilt. Werden diesen Teilbereichen abwechselnd die Bitwerte 0/1 zugeordnet, können daraus gleichverteilte Zufallsbits erzeugt werden, wenn die Zeitauflösung ausreichend groß gegenüber dem mittleren Abstand zweier Detektionsereignisse ist [26]. Alternativ können die einzelnen Teilbereiche von 0 aufsteigend nummeriert werden, sodass ein detektiertes Photon mehrere Roh-Zufallsbits erzeugt. Durch die unterschiedlichen Wahrscheinlichkeiten der Teilbereiche muss eine maximale Information berechnet werden, die daraus extrahiert werden kann [27, 28]. Die Roh-Zufallsbits müssen dann mit einem geeigneten Verfahren auf diese maximale Länge reduziert werden[4].
Eine weitere Methode verwendet eine gepulst betriebene Lichtquelle, deren mittlere Intensität ein Photon innerhalb von n Pulsen enthält [29, 30]. Der Zeitpunkt, an dem ein Photon innerhalb dieser Sequenz $0 \ldots n-1$ detektiert wird, ergibt die Zufallszahl. Nach einer Detektion und eventuell einer Wartezeit, um die Totzeit des Detektors zu berücksichtigen, wird eine neue Pulssequenz gestartet.

Neben der Photonemission kann auch der radioaktive Zerfallsprozess als Zufallsquelle verwendet werden. Hierzu existieren keine experimentellen Arbeiten.

Ein Vorteil dieses Verfahrens besteht in der Effizienz mit der Zufallszahlen erzeugt werden können. Pro detektiertem Photon können auch mehrere Zufallsbits erzeugt werden. Dadurch werden Bitraten von bis zu 40 Mbit/s experimentell erreicht.

Unbestimmte Emissionsrichtung: Als Zufallsquelle kann die Verteilung des Intensitätsprofils einer Strahlungsquelle verwendet werden. So ist zum Beispiel die Richtung, in die bei einem radioaktiven Zerfall die Zerfallsprodukte emittiert werden, a priori zufällig. Durch zwei oder mehrere um eine radioaktive Quelle angeordnete Detektoren, können aus der Information, in welchem Detektor ein Ereignis registriert wird, Zufallsbits erzeugt werden [31].

In einem optischen Aufbau kann zum Beispiel das Emissionsprofil aus einer Monomoden-Glasfaser benutzt werden. Im Experiment von Ste-

[4] In [27] wird der SHA-256 Algorithmus zur Regularisierung verwendet. Gefahren dieser Vorgehensweise werden am Ende dieses Abschnitts diskutiert.

vanov [32] wurde mithilfe zweier Multimoden-Glasfasern jeweils Photonen aus einem bestimmten Raumwinkel am Ausgang der Monomoden-Glasfaser aufgesammelt. Aus der Information, in welcher der beiden Multimoden-Glasfasern ein Photon detektiert wurde, konnte ein Zufallsbit generiert werden. In [33] wurde der Aufbau skaliert und ein Detektorfeld mit 400x400 Pixeln verwendet. In diesem Experiment wurde lediglich gezeigt, wie man mit Hilfe von optischen Abschwächern dieses Feld homogen ausleuchten kann. Zufallszahlen wurden in diesem Experiment jedoch nicht erzeugt.

Ein entscheidender Vorteil dieser Idee ist die einfache Skalierbarkeit dieses Verfahrens. Dennoch bestehen Schwierigkeiten darin, dass Mehrfachereignisse, das heißt in mehreren Detektoren werden Photonen detektiert, nicht zur Generierung von Zufallsbits beitragen können. Andererseits führt eine unterschiedliche Detektionseffizienz zu einer Schiefe in den Zufallsbits, welche durch geeignete Regularisierungsalgorithmen [20, 21] entfernt werden muss. Beide Prozesse führen zu einer Reduktion der Zufallsbitrate. Letztendlich wird in [32] eine Zufallsbitrate von 100 kbit/s berichtet.

Photonenstatistik in einem Laserpuls: Der Quantenzustand aus einem gepulsten Laser kann als Superposition von Photonenzahlzuständen $|n\rangle$ beschrieben werden.

$$|\Psi\rangle = \sum_{n=0}^{\infty} P(n,\mu) \cdot |n\rangle \tag{2.3}$$

$P(n,\mu)$ ist dabei die Poisson-Wahrscheinlichkeitsverteilung mit dem Mittelwert μ. Ein Zufallsbit 0 wird in diesem System erzeugt, wenn während eines Laserpulses kein Photon detektiert wird. Der Bitwert 1 gilt, wenn mindestens ein Photon detektiert wird. Um eine gleichverteilte Bitsequenz zu erhalten, muss dabei die Pulsintensität präzise auf $\mu = 0.693$ gesetzt werden [34, 35].
Mit diesem Verfahren können hohe Zufallsbitraten erreicht werden, aber durch eine ungenügende Stabilisierung der Pulsintensität und der damit verbundenen Schiefe in den Zufallsbits muss eine Regularisierung angewendet werden. Obwohl experimentell bisher nur eine Bitrate von 1 Mbit/s erreicht wurde, kann dieses System relativ einfach auf erheblich höhere Datenraten erweitert werden.

Photonenstatistik in einem Zeitintervall: Sowohl Licht aus einer kohärenten Strahlungsquelle als auch aus einer inkohärenten Quelle wer-

den unabhängig voneinander emittiert. Bei konstanter Lichtleistung ergibt sich als Wahrscheinlichkeit n Photonen in einem definierten Zeitintervall T zu finden, eine Poissonverteilung. Diese Verteilung lässt sich auf unterschiedliche Weise zur Erzeugung von Zufallsbits verwenden. Einerseits kann auch hier die Unterscheidung getroffen werden, ob mindestens ein Ereignis detektiert wird oder keines (entspricht Bitwert 1 bzw. 0). Andererseits kann man eine ungerade und eine gerade Photonenzahl in einem Intervall den Bitwerten 0 und 1 zuordnen [24, 36–39]. Für sehr große mittlere Photonenzahlen $\mu \to \infty$ pro Intervall entsteht eine gleichverteilte Bitfolge. Alle bisherigen Implementierungen dieser Art beziehen sich auf radioaktive Quellen.

Der in dieser Arbeit beschriebene Zufallszahlengenerator basiert auf dieser Idee und verwendet einen optischen Aufbau.

Phasenrauschen eines Lasers: Eine weitere Zufallsquelle bietet das Phasenrauschen eines Lasers. Der Ursprung dieses Rauschens findet sich in der spontanen Emission, durch die jedes Photon mit einer zufälligen Phase erzeugt wird. In einem Mach-Zehnder Interferometer kann die Phasendifferenz eines Lasers zwischen Zeitpunkt t und Zeitpunkt $t + \tau$ gemessen werden. Diese Differenz wird mit Hilfe einer Photodiode gemessen und als Basis für die Biterzeugung verwendet. Ein Komparator generiert ein Bit 0, wenn die Amplitude des Signals der Photodiode unterhalb des Mittelwerts ist und ein Bit 1 bei Überschreitung dieses Werts [40, 41].[5]
Mithilfe dieses Prinzips lassen sich Zufallszahlen mit einer sehr hohen Rate erzeugen. Experimentell wurden 500 Mbit/s erzeugt. Dennoch muss bei diesem Verfahren angemerkt werden, dass elektronisches Rauschen eine Quelle für zusätzliches Rauschen ist, die eher als herkömmlicher physikalischer ZZG angesehen werden kann. Zusätzlich beeinträchtigt die Wahl der Diskriminierungsschwelle die Schiefe in den Zufallszahlen derart, dass diese durch Regularisierungsverfahren [20, 21] entfernt werden muss.

Rauschen des atomaren Spins: Als Zufallsquelle wird der Spin in einem atomaren Ensemble verwendet [42]. Quantenfluktuationen dieses Spins lassen sich mit Hilfe eines Messlasers messen und erzeugen mit einem zusätzlichen Schwellen-Diskriminator Zufallsbits. Experimentell konnten bisher nur Zufallsbits in der Größenordnung von 1 kbit/s erreicht

[5] Die Biterzeugung mit Hilfe des letzten Bits eines Analog-Digital-Wandlers, wie in [40] durchgeführt, führt aufgrund des elektronischen Fehlers bei der Digitalisierung zu einer weiteren pseudozufälligen Zufallsquelle.

werden. Wenn Spinszustände innerhalb eines Festkörpers werwendet werden, könnte dieses System sowohl sehr kompakt werden als auch erheblich höhere Raten produzieren.

Verschränkte Photonenpaarquelle: Bei Realisierungen eines ZZG mit Hilfe eines Strahlteilers wurden bereits verschränkte Photonenpaare verwendet, um einzelne Photonen zu generieren. Der Verschränkungszustand bietet desweiteren die Möglichkeit, den Quantenzustand als solchen mithilfe einer Bellschen Ungleichung (zum Beispiel CHSH Ungleichung [43]) zu untersuchen. Durch dieses Verfahren wird der Zustand als quantenmechanischer Zustand verifiziert. In Abhängigkeit vom Grad der Verletzung dieser Ungleichung können Zufallsbits erzeugt werden, für deren Beschreibung keine klassische Statistik verwendet werden kann [44]. Anzumerken ist hier, dass für die Messung der Photonenpaare oder wie in [44] verwendete verschränkte Ionenzustände bereits Zufallszahlen zur Polarisationsanalyse benötigt werden. Es können aber mehr Zufallsbits extrahiert werden als zur Messung gebraucht werden. Experimentell wurden bisher Zufallsbitraten von 42 Bits innerhalb eines Monats(!) demonstriert.

Messung des Vakuumzustandes: Der Quanten-Vakuumzustand eines Lichtfeldes kann mit Hilfe eines Strahlteilers gemessen werden. Dazu wird ein Laser mit geringem Intensitätsrauschen an einem Eingang des Strahlteilers eingekoppelt. Der zweite Eingang wird blockiert und dient somit als Eingang für den Vakuumzustand. Am Ausgang des Strahlteilers wird das Signal mit zwei Photodioden detektiert. Die Summe und Differenz dieser Signale gibt Aufschluss über die Rauschamplitude des Vakuumzustands [45, 46]. Die gemessene Amplitude des Quantenrauschens wird anschließend digitalisiert und Bitwerten zugeordnet. Dadurch werden Erzeugungsraten von bis zu 25 Mbit/s regularisierter Zufallsbits erreicht, ausgehend von einer Rohbitrate von 2 Gbit/s.

Die in den einzelnen Experimenten verwendeten Regularisierungsalgorithmen dienen grundsätzlich dazu, eine Schiefe in den Zufallszahlen zu entfernen und damit die erste Bedingung für Zufallsbits zu erfüllen. Abhängig von diesem Algorithmus können jedoch möglicherweise auftretende Korrelationen in der erzeugten Bitfolge verschleiert werden, sodass diese nicht mehr offensichtlich zu erkennen sind. Deshalb ist es bei der Analyse von regularisierten Bitfolgen immer notwendig auch die Roh-Bitfolgen zu analysieren, um gegebenenfalls Korrelationen erkennen zu können.

Kapitel 3

Theoretische Beschreibung

Das Prinzip unseres quantenoptischen Zufallszahlengenerators wird in diesem Abschnitt zu Beginn skizziert. Die darauf folgende theoretische Behandlung der einzelnen dafür notwendigen Komponenten dient zur Erstellung eines stochastischen Modells, das den Entropiezuwachs pro neu generiertem Zufallsbit quantifiziert. Dazu werden Auswirkungen der einzelnen Komponenten auf die Qualität der Zufallsbits untersucht. Am Ende dieses Abschnitts werden Regularisierungsalgorithmen vorgestellt, die bei Bedarf eine Gleichverteilung in der Häufigkeit der beiden Bitwerte sicherstellen.

3.1 Funktionsweise des Zufallszahlengenerators

3.1.1 Anforderungen an den Zufallszahlengenerator

Vor Beginn der Beschreibung des Funktionsprinzips werden Anforderungen an den Aufbau des Generators definiert.

Quantenprozess: Der zugrundeliegende quantenmechanische Prozess muss theoretisch beschrieben werden können.

Gleichverteilung: Viele in Abschnitt 2.2.3 beschriebene Generatoren erzeugen nur mit Hilfe von Regularisierungsalgorithmen gleichverteilte Zufallszahlen. Der hier gezeigte Aufbau soll ohne dieses Hilfsmittel auskommen.

Robust: Das Modell der Zufallszahlerzeugung soll zudem robust gegen Störungen wie zum Beispiel Lichtintensitätsschwankungen oder Spannungsschwankungen sein.

Hohe Bitrate: Eine hohe Erzeugungsrate und eine leichte Skalierbarkeit sollten erreicht werden.

Kompakt: Der Zufallszahlengenerator soll unter anderem in ein vorhandenes Quantenkryptographieexperiment integriert werden. Deshalb sollte der experimentelle Aufbau kompakt sein.

3.1.2 Prinzip der Zufallszahlerzeugung

Für die technische Umsetzung der Quelle des Zufalls wurde eine optische Implementierung gewählt [47, 48][1]. Eine Leuchtdiode (LED) als Lichtquelle stellt aufgrund ihres breiten Spektrums eine in Bezug auf die verwendeten Zeitskalen inkohärente Photonenquelle dar[2]. Die ausgestrahlte Photonenstatistik lässt sich damit mithilfe der Poissonstatistik beschreiben. Die Anzahl der detektierten Photonen n in einem festen Zeitintervall T (für $T \gg \tau_C^{LED}$) ist somit unabhängig vom betrachteten Zeitintervall und wird als Zufallsvariable verwendet. Eine gerade beziehungsweise ungerade Anzahl n wird den Bitwerten '0' beziehungsweise '1' zugeordnet. Im Grenzfall sehr großer mittlerer Photonenzahlen μ in einem Zeitintervall T stellt sich in guter Näherung ein Gleichgewicht in der Häufigkeit der Bitwerte 0/1 ein.

In den folgenden Abschnitten wird die LED in Bezug auf die emittierte Photonenstatistik theoretisch untersucht. Aufgrund von Effekten in der Raumladungszone kann es unter bestimmten experimentellen Umständen zu einer Veränderung der Statistik hin zu einer Sub-Poisson[3]-Verteilung kommen. Andererseits wird durch eine ineffiziente optische Ankopplung der LED an einen Detektor dieser Effekt unterdrückt. Daher stellt der Nachweis dieses Effekts eine große Herausforderung in Bezug auf die optische Kopplung der LED an einen Photodetektor dar.

Die Detektion erfolgt mit einem Photomultiplier (PMT), der gegenüber einer Avalanche Photodiode (APD) unter anderem den Vorteil einer höheren maximalen Zählrate besitzt. Neben der Digitalisierungselektronik modifiziert die sogenannte Totzeit die aufgenommene Photonenstatistik. Als Totzeit wird die Zeitspanne nach einer Detektion bezeichnet, während der kein weiteres Photon registriert werden kann. Beide Effekte fließen in das stochastische Modell des Zufallszahlengenerators ein, das in Abschnitt 3.5 zusammengefasst wird.

[1] Die Entwicklung dieses ZZG erfolgte im Rahmen eines vom Bundesamt für Sicherheit in der Informationstechnik geförderten Projekts. Berichte im Zusammenhang mit diesem Projekt beinhalten beinhalten auch eine kompakte Beschreibung und Analyse dieses ZZG.

[2] Kohärenzzeiten von LEDs liegen im Bereich von $\tau_C^{LED} \approx 10^{-14} s$ [49]

[3] sub-Poisson bezeichnet eine Verteilung, deren Varianz kleiner ist als der Erwartungswert.

3.2 Lichtquelle

In diesem Abschnitt wird die LED im Bezug auf die Verwendung in unserem ZZG untersucht. Bedeutend dabei ist die emittierte Photonenstatistik. Photonen werden in einer LED durch einen spontanen Emissionsprozess bei der Rekombination eines Elektron-Loch Paares erzeugt (vergleiche Abbildung 3.1). Dieser an einem p-n Übergang stattfindende Prozess erzeugt Photonen mit einer spektralen Verteilung mit einer Breite von $\Delta\lambda > 10$ nm. Die zeitliche Kohärenz ist damit beschränkt auf $\tau_C^{LED} < 10^{-13}$ s. Auf einer Zeitskala von einigen Nanosekunden können emittierte Photonen als inkohärent angesehen werden.

Wenn zusätzlich die Elektronen-Loch-Paar-Dichte konstant ist, ist der Emissionszeitpunkt der Photonen unabhängig voneinander (ähnlich dem radioaktiven Zerfallsprozess). Die Wahrscheinlichkeit, dass ein Photon im Zeitintervall dt emittiert wird, ist außerdem proportional zur Länge des Intervalls dt mit dem Proportionalitätsfaktor λ. Die Zufallsvariable N, die die Anzahl n der emittierten Photonen in einem Zeitintervall T angibt, folgt damit einer Poissonverteilung

$$P_{LED}(\mu, N = n, T) = \frac{(\mu)^n}{n!} e^{-\mu} \tag{3.1}$$

Hier gibt $\mu := \lambda \cdot T$ die mittlere Photonenzahl pro Zeitintervall T an (=Erwartungswert $E(N)$ der Verteilung). Eine Eigenschaft der Poissonverteilung ist, dass das Quadrat der Standardabweichung $\sigma^2(N)$ dieser Verteilung gleich dem Erwartungswert der Verteilung ist.

$$E(N) = \mu \tag{3.2}$$
$$\sigma^2(N) = \mu \tag{3.3}$$

Für den zeitlichen Abstand zweier Photonen ergibt sich ein exponentieller Zusammenhang:

$$P(t|\text{Photon bei } t' = 0) = \lambda \cdot e^{-\lambda \cdot t} \tag{3.4}$$

Die bisherige Betrachtung geht von einer konstanten Elektronen-Loch-Paar-Dichte aus. Im Folgenden wird detailliert erläutert unter welchen Umständen diese Eigenschaft nicht mehr gewährleistet sein kann.

Dazu wird in der weiteren Beschreibung zunächst eine LED mit Wirkungsgrad $\eta_{LED} = 1$ betrachtet. Abschnitt 3.3 befasst sich anschließend mit der Frage, wie ein endlicher Wirkungsgrad zusammen mit einer weiteren Abschwächung bei der Kopplung der LED an den Detektor die Photonenstatistik beeinträchtigt.

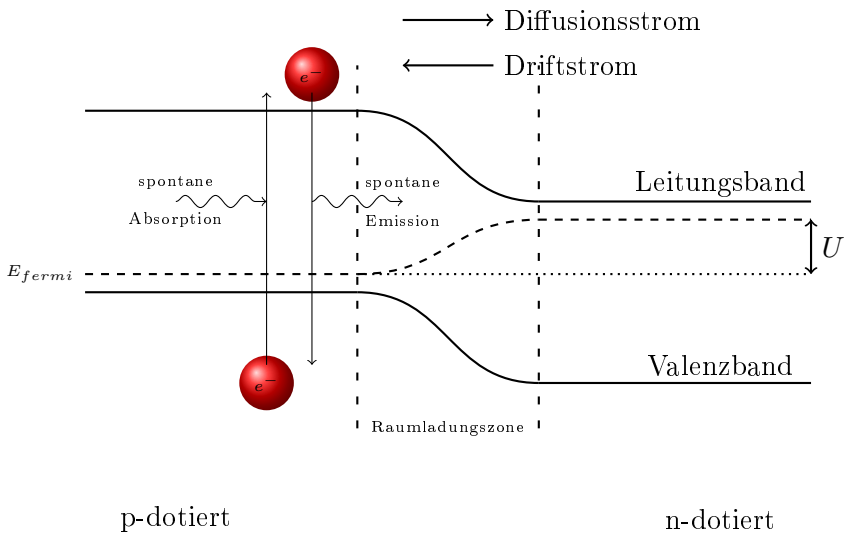


Abbildung 3.1: Schematische Darstellung eines p-n-Übergangs in einer LED. Nach rechts ist die Richtung orthogonal zur Grenzfläche aufgetragen; nach oben die Energie. E_{fermi} bezeichnet das Fermi-Niveau im Halbleiter.

Die Lichtemission der LED findet an einem p-n Übergang zweier Halbleiter statt (vergleiche Abbildung 3.1). Elektronen aus der n-dotierten Schicht driften bei angelegter externer Spannung U in die p-dotierte Schicht. Dort rekombinieren diese mit Löchern auf einer Zeitskala τ_{sp} und emittieren dabei je ein Photon. Der Strom an diesem Übergang setzt sich zusammen aus dem beschriebenen Driftstrom I_{fi} und einem Diffusionsstrom I_{bi} [50,51] in umgekehrter Richtung, der durch eine interne Konzentrationsdifferenz der Ladungsträger verursacht wird. Daraus ergibt sich die Strom-Spannungskennlinie in Durchlassrichtung für eine LED bei einer Temperatur $\mathcal{T}$:

$$I_{ges} = (I_{fi} - I_{bi}) = I_0(e^{\frac{eU}{k_B\mathcal{T}}} - 1) \tag{3.5}$$

I_0 ist die Summe aus den Generationsströmen (für eine detaillierte Beschreibung siehe zum Beispiel [52, 53]).

Vor der Betrachtung der Photonenstatistik wird zunächst die Elektronenstatistik berechnet, mit der die Elektronen den p-n Übergang passieren. Im Besonderen wird die Änderung dieser Statistik aufgezeigt, wenn bereits ein Elektron diesen Übergang überquert hat.

Da bei einem Elektronenübergang ein Spannungsabfall an diesem Über-

gang auftritt, wird die Wahrscheinlichkeit für den darauffolgenden Übergang beeinflusst. Zur Abschätzung betrachten wir die Änderung des Stroms I_{fi}, die bei einem Übergang eines Elektrons von der n-Schicht in die p-Schicht auftritt [51, 52].

$$\begin{aligned} \frac{I_{fi}(nach)}{I_{fi}(vor)} &= e^{-\frac{e\Delta U}{k_B \mathcal{T}}} \\ &= e^{-r} \end{aligned} \tag{3.6}$$

mit $r = \frac{e}{C_{dep}} / \frac{k_B \mathcal{T}}{e}$; $\Delta U = \frac{e}{C_{dep}}$ gibt die Spannungsänderung am Übergang bei diesem Prozess an. Jetzt kann man zwei Fälle unterscheiden:

Mesoskopischer Fall ($r \gg 1$)**:**
Im Fall extrem kleiner Temperaturen (T≈ 50 mK) und kleiner Kapazitäten ($C_{dep} \approx 1$ fF) verhindert der Übergang eines Elektrons den unmittelbaren Übergang eines folgenden Elektrons (*single electron coulomb blockade effect*). Die Änderung des Stroms I_{fi} in Gleichung (3.6) ist in diesem Fall sehr groß. Der abstoßende Effekt der Elektronen induziert damit eine Regularisierung des Elektronenstroms und damit eine Veränderung der Photonenstatistik hin zu einer Sub-Poisson-Verteilung. Dieser Fall wurde in zahlreichen Arbeiten sowohl theoretisch als auch experimentell untersucht [54, 55].

Makroskopischer Fall ($r \ll 1$)**:**
In diesem Fall kommt es durch den Übergang **eines** Elektrons zu einer vernachlässigbaren Änderung der Spannung am p-n Übergang und damit gilt $I_{fi}(nach) \approx I_{fi}(vor)$.

Da die LED unseres ZZGs bei Raumtemperatur betrieben werden soll, behandelt die nachfolgende Diskussion ausschließlich den makroskopischen Fall. Zu klären bleibt, unter welchen Bedingungen auch hier die Photonenstatistik von einer Poissonverteilung abweicht.

Ein abstoßender Effekt der Elektronen am p-n Übergang kann nur auftreten, wenn die Spannung am Übergang signifikant also um mindestens $\frac{e}{k_B \mathcal{T}}$ verändert wird [51]. Diese Änderung tritt im makroskopischen Fall nur auf, wenn sehr viele Elektronen den Übergang passieren. Dazu wird die Zeitskala τ_{te} („thermionic emission time“) eingeführt, bei der so viele Elektronen den Übergang passieren, dass die Spannung am Übergang um den zuvor genannten Wert abfällt.

$$\tau_{te} = \frac{\tau}{r} = \frac{k_B \mathcal{T}/e}{e/C_{dep}} \cdot \tau = \mathcal{N} \cdot \tau, \tag{3.7}$$

$\mathcal{N}$ gibt diese Anzahl der Elektronen an, die beim Passieren des Übergangs die Spannung um $\frac{e}{k_B T}$ verringert. τ gibt die Rate an, mit der Elektronen von der Stromquelle nachgeliefert werden $\tau = \frac{e}{I}$.
Zusammen mit dieser Zeitskala wird in der Arbeit von Imamoglu [56] die Wahrscheinlichkeit angegeben, dass z Elektronen die Barriere in der Zeit T passieren:

$$P(\mu, z, T) = \frac{1}{F(r,\mu)} \cdot \underbrace{\frac{\mu^z}{z!} \cdot e^{-\mu}}_{Poisson} \underbrace{\cdot e^{-\frac{r}{2}(z-\mu)^2}}_{Gauß} \tag{3.8}$$

mit $\mu := \frac{T}{\tau}$ und $F(r,\mu)$ als Normierungskonstanten.
Bei einer mittleren Zahl $\mu \ll \mathcal{N}$ (das heißt bei Zeiten $T \ll \tau_{te}$) reichen die Elektronen nicht aus, um die Spannung am p-n Übergang signifikant zu verändern. Der Effekt der Gaußverteilung in Gleichung (3.8) ist in diesem Bereich zu vernachlässigen. Die Rekombinationsereignisse sind als unabhängig voneinander anzusehen. Aus einer Poisson-Verteilung der Elektron-Loch-Rekombinationen folgt daher auch eine Poisson-Verteilung für die dadurch erzeugten Photonen.

Gilt aber $\mu \gg \mathcal{N}$, so kann während der Messzeit die Spannung am p-n Übergang um $k_B\mathcal{T}/e$ absinken. Dieser Effekt führt zu einer Blockade der folgenden Elektronen (*collective/macroscopic coulomb blockade effect*). Aus Gleichung (3.8) kann man für diesen Bereich entnehmen, dass hier $P(\mu, z, T)$ durch die Gaußverteilung bestimmt wird. Die Standardabweichung dieser Verteilung ist gegeben durch

$$\sigma = \frac{1}{\sqrt{r}} = \sqrt{\mathcal{N}} = \sqrt{\frac{k_B \mathcal{T} C_{dep}}{e^2}} \tag{3.9}$$

und damit unabhängig vom Erwartungswert $E(N) = \mu$. Die Standardabweichung ist somit kleiner ($\mu \gg \mathcal{N}$) als die Wurzel des Erwartungswerts und man erhält dadurch eine Sub-Poisson-Wahrscheinlichkeitsverteilung der Elektronen. Diese Sub-Poisson-Verteilung überträgt sich auf die Photonenstatistik nur eingeschränkt, da durch den zufälligen Prozess der spontanen Emission diese Verteilung modifiziert wird. Dennoch kann die Breite der Photonenzahlverteilung durch die der Elektronenverteilung abgeschätzt werden.

$$\sigma \in [\sqrt{\mathcal{N}}; \mu] \subset [0; \mu] \tag{3.10}$$

Unter großem experimentellen Aufwand und mit speziell dafür angefertigten Leuchtdioden ist es experimentell gelungen, diesen *makroskopischen Coulomb blockade effect* zu zeigen [50, 57, 58]. Um diesen Effekt zu detektieren, werden keine Einzelphotondetektoren verwendet, da diese über eine

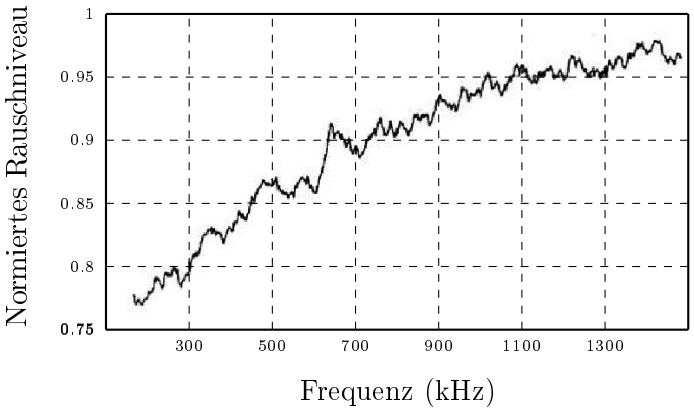


Abbildung 3.2: Experimentelle Resultate einer Messung des makroskopischen *coulomb blockade* Effekts aus [50]. Das Rauschniveau konvergiert bei hohen Frequenzen (kurzen Messzeiten) gegen das Poisson-Limit.

ungenügende Detektoreffizienz verfügen und damit die Regularisierung des Photonenstroms nicht auflösen könnten. Um eine sehr hohe Detektionseffizienz zu erreichen, werden in diesen Experimenten Halbleiterphotodioden bei der Herstellung der LED direkt auf diese aufgebracht. Dabei lassen sich Gesamtdetektionswahrscheinlichkeiten von ca. 40% erreichen. Die Messung des Rauschspektrums des Photostroms zeigt in einem gewissen Frequenzbereich eine verminderte Amplitude und ist somit der Beweis für die Sub-Poisson-Verteilung in der Photonenstatistik (siehe Abbildung 3.2).

Die Notwendigkeit einer sehr hohen Kopplungseffizienz der Lichtquelle an den Detektor, um Abweichungen der Photonenstatistik von der Poissonverteilung zu erkennen, ist im Aufbau des ZZGs von Vorteil, wie im anschließenden Kapitel gezeigt wird.

3.3 Abschwächung

In diesem Abschnitt wird gezeigt, wie sich die gemessene Photonenstatistik durch eine geringe Detektionseffizienz verändert. Im Folgenden wird die Effizienz der LED, die optische Ankopplung der LED an den Detektor und die Detektionseffizienz für die theoretische Betrachtung symbolisch durch einen Strahlteiler ersetzt [59–61] (vergleiche Abbildung 3.3). Dazu wird die Transmission der Photonen als unabhängig voneinander angenommen.

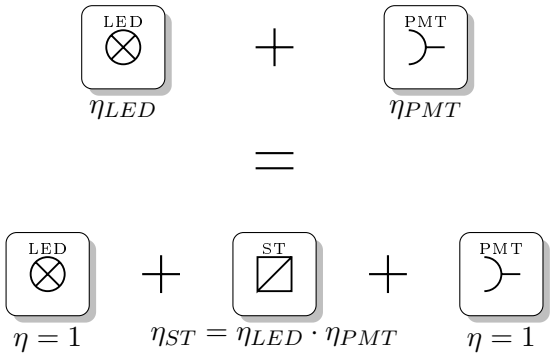


Abbildung 3.3: Die Abschwächung der Photonen von der Generierung in der LED bis zur Detektion im Photomultiplier kann theoretisch durch einen Strahlteiler modelliert werden. Die Transmission des Strahlteilers entspricht dabei dem Produkt der Effizienz der LED η_{LED}, der Abschwächung infolge der optischen Kopplung und der Detektionseffizienz η_{PMT}.

Für die Berechnung der resultierenden Statistik wird von einer Photonenstatistik mit einer mittleren Photonenzahl von μ_{LED} und einer Varianz von Δn_{LED} ausgegangen. Ein Photon am Strahlteiler wird mit einer Wahrscheinlichkeit von η_{ST} transmittiert und mit einer Wahrscheinlichkeit von $1 - \eta_{ST}$ reflektiert. Dadurch ist die erwartete mittlere Photonenzahl nach dem Strahlteiler

$$E(N) := \mu_{ST} = \eta_{ST} \cdot \mu_{LED} \tag{3.11}$$

Das Quadrat der Standardabweichung der Verteilung nach dem Strahlteiler wird beschrieben durch [59]

$$\begin{aligned}\sigma^2(N) &= \eta_{ST} \cdot \mu_{LED} - \eta_{ST}^2\Big(\mu_{LED} - (\Delta n_{LED})^2\Big) \\ &= \mu_{ST} - \eta_{ST}^2\Big(\mu_{LED} - (\Delta n_{LED})^2\Big) \\ &= \mu_{ST} - \mathcal{O}(\eta_{ST}^2)\end{aligned} \tag{3.12}$$

wobei $(\Delta n_{LED})^2$ die Varianz der Photonenzahlverteilung vor dem Strahlteiler angibt.

Aus Gleichung (3.12) kann man erkennen, dass sich die Varianz aus dem Erwartungswert der Verteilung und einem Term zweiter Ordnung in η_{ST} zusammensetzt, der die Abweichung zu einer Poissonverteilung angibt. Die Differenz $\mu_{LED} - (\Delta n_{LED})^2$ ist ein Maß für die Abweichung der Photonenstatistik der LED von einer Poissonstatistik und ist nach Gleichung (3.8) und (3.9) beschränkt auf das Intervall $[0, \mu_{LED}]$.

$$\mu_{ST} \geq \sigma^2(N) \geq \mu_{ST} \cdot (1 - \eta_{ST}) \tag{3.13}$$

Durch die niedrige Gesamteffizienz $\eta_{ST} = 10^{-8}$ in unserem experimentellen Aufbau können Abweichungen der Photonenstatistik von der Poissonstatistik selbst bei Auftreten des Blockade-Effekts nicht mehr beobachtet und somit vernachlässigt werden.

Als Fazit dieses Abschnitts kann man festhalten, dass durch den Einfluss der verschiedenen Beiträge zum Gesamtwirkungsgrad η_{ST} die Varianz der Photonenverteilung pro Zeitintervall durch

$$\mu_{ST} \geq \sigma^2(N) \geq \mu_{ST} \cdot (1 - 10^{-8}) \tag{3.14}$$

$$\Longrightarrow \sigma^2(N) \cong E(N) \tag{3.15}$$

eingeschränkt ist. Aus diesem Grund wird im weiteren Verlauf dieser Arbeit von einer Poisson-Photonenstatistik ausgegangen.

3.4 Detektion durch einen Photomultiplier

Aufgrund der hohen zu erreichenden Zufallsbitrate und somit auch einer hohen Photonendetektionsrate wird in diesem Aufbau ein Photomultiplier (PMT) verwendet. Dieser weist aufgrund seiner Funktionsweise gegenüber InGaAs-/ Silizium-Avalanche Photodioden (APD) eine wesentlich kleinere Totzeit auf[4]. (Mit Hilfe einer periodisch betriebenen InGaAs APD und einer selbst differenzierenden Elektronik wurde vor Kurzem eine Totzeit von < 10 ns erreicht [62]). Die absolute Detektionseffizienz spielt im ZZG eine untergeordnete Rolle, da die Zufallszahlen, wie bereits in Abschnitt 3.3 beschrieben, durch die ohnehin niedrige optische Kopplungseffizienz nicht weiter beeinflusst werden. Lediglich die Intensität der LED muss erhöht werden, um eine ausreichend hohe mittlere Detektionsrate zu erreichen.

3.4.1 Funktionsprinzip eines Photomultipliers

Um Auswirkungen des Detektionsprozesses auf die Statistik detektierter Photonen zu untersuchen, wird die Funktionsweise eines Photomultipliers erklärt.

Eintreffende Photonen lösen an einer Photokathode Elektronen aus, die mit Hilfe einer Kaskade von Dynoden, aus denen weitere Elektronen ausgeschlagen werden, verstärkt werden. Am Ende dieser Kaskade ist ein elektrischer Puls messbar [63]. Aufgrund unterschiedlicher Flugzeiten der Elektronen und einer begrenzten elektronischen Bandbreite hat dieser Puls eine endliche Länge (vergleiche Abbildung 3.4). Ein zur Digitalisierung dieser Signale verwendeter Schwellendiskriminator ignoriert Pulse, falls der zeitliche Abstand zum vorherigen Puls kleiner als die Pulsbreite ist. Aus diesem Grund wird die Pulsbreite im Folgenden auch als Totzeit τ_d betrachtet. Zudem verlängert dieser ignorierte Puls die Pulsbreite des digitalisierten Signals. Exemplarisch ist dieser Sachverhalt in Abbildung 3.4 dargestellt.

3.4.2 Einfluss der Totzeit auf die Photonenstatistik

In diesem Abschnitt wird der Einfluss untersucht, den die Totzeit des Photomultipliers auf die registrierte Photonenstatistik ausübt. Die einfallende Photonenstatistik wird auf Basis der Diskussion in Abschnitt 3.3 als Poisson-Photonenstatistik angenommen.

Mit einer festen Totzeit, das heißt mit keiner Verlängerung durch dicht aufeinanderfolgende Pulse, wurde in den Arbeiten von Müller [64–66] und Srinivas [67, 68] die Veränderung der Photonenstatistik ausgehend von einer Poissonstatistik berechnet. In [67, 68] wurde der Effekt vernachlässigt

[4] Si-APD: ~ 50 ns, InGAs-APD: ~ 1 μs bzw. PMT: ~ 2 ns

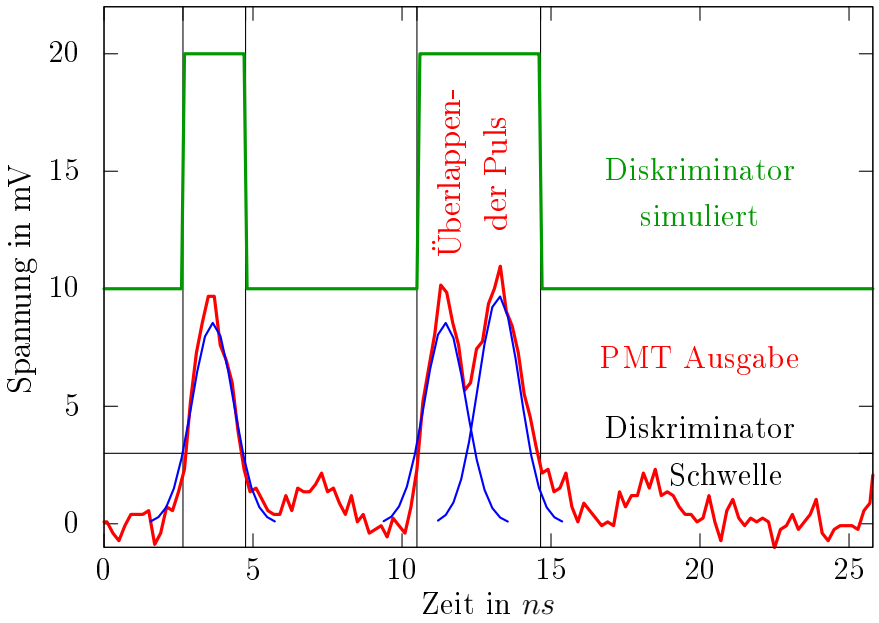


Abbildung 3.4: Gemessene elektrische Pulse aus einem Photomultiplier und die simulierte Ausgabe nach einem Schwellendiskriminator.

den ein Puls am Ende eines Zeitintervalls auf das nächste Intervall ausüben kann. Die Ergebnisse dieser Arbeiten werden in Abbildung 3.5 in Form der Photonenzahlverteilungen dargestellt.

Der Einfluss einer erweiterbaren Totzeit auf diese Verteilung, wie sie bei einem Photomultiplier zu erwarten ist (siehe Abschnitt 3.4.1), wurde in den Arbeiten von Omote und Libert [69, 70] berechnet.

Dazu wurde die Art der Auswirkung der Totzeit in zwei Bereiche unterteilt.

1. Innerhalb eines Intervalls T werden Pulse nicht registriert, wenn deren zeitlicher Abstand kleiner als τ_d ist.

2. Ein Photon zum Zeitpunkt t am Ende eines Intervalls ($t \in [T - \tau_d, T]$) verhindert eine mögliche Detektion eines Photons zu Beginn des nächsten Intervalls.

Die Photonenstatistik des einfallenden Lichts wird gemäß der Diskussion in Abschnitt 3.2 und 3.3 als Poissonstatistik angenommen (vergleiche Gleichung 3.1). Aus dieser Verteilung werden während der weiteren Berechnung [69] die Photonenereignisse herausgefiltert, deren Abstand zum vorhergehenden Ereignis kleiner als die Totzeit τ_d ist. Dies wirkt sich auf die

detektierte Photonenstatistik $P(\mu, n, T, \tau_d)$ aus:

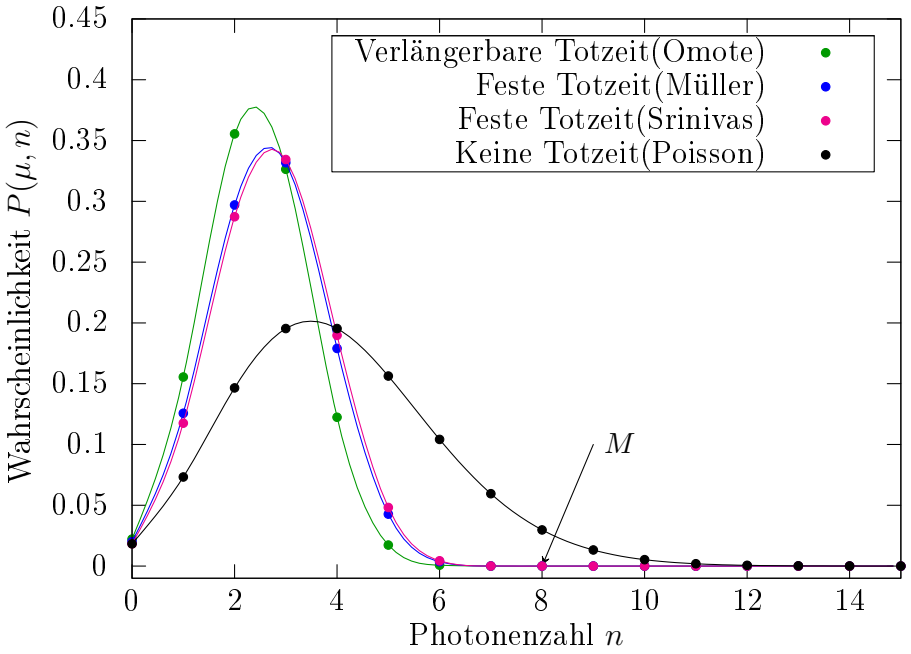


Abbildung 3.5: Die theoretische Photonenzahlverteilung für unterschiedliches Verhalten der Totzeit verwendet eine mittlere Photonenzahl von $\mu = 4$ (auftreffende Photonenzahl). Eine Totzeit von $\tau_d = 2.5$ ns sowie eine Intervalllänge von $T = 20$ ns werden eingesetzt. Die maximale Anzahl detektierbarer Photonen $M = 8$, verursacht durch die Totzeit, ist ebenfalls gekennzeichnet. Da die Wahrscheinlichkeitsverteilungen lediglich diskrete Funktionen für ganzzahlige Photonenzahlen sind, dienen die Kurven nur zur Visualisierung.

$$P(\mu, n, T, \tau_d) = \sum_{m=0}^{M-n} \frac{(-1)^m}{n!m!} \left(\left(1 - (n + m - 1) \frac{\tau_d}{T} \right) \mu_r \right)^{n+m} . \tag{3.16}$$

Durch die minimale Pulslänge τ_d eines Photonereignisses kann nur eine maximale Anzahl Photonen innerhalb eines Zeitintervalls T registriert werden.

$$M = \left\lceil \frac{T}{\tau_d} \right\rceil \quad . \tag{3.17}$$

Die Wahrscheinlichkeit mehr als M Photonen zu detektieren ist $P(\mu, n > M, T, \tau_d)0$. Darüber hinaus wird auch der Erwartungswert dieser Verteilung, die mittlere detektierte Zählrate μ_r, reduziert (vergleiche Abbildung 3.5).

$$\mu_r = \mu \cdot e^{-\mu \frac{\tau_d}{T}} . \tag{3.18}$$

Im Gegensatz zur Berechnung mit einer festen Totzeit, bei der sich diese mittlere Photonenzahl asymptotisch $\mu_r \xrightarrow{\mu\to\infty} M$ verhält, weist die mittlere Photonenzahl hier ein Maximum bei $\mu = \frac{T}{\tau_d}$ auf und tendiert anschließend zu 0 (vergleiche Abbildung 3.6).

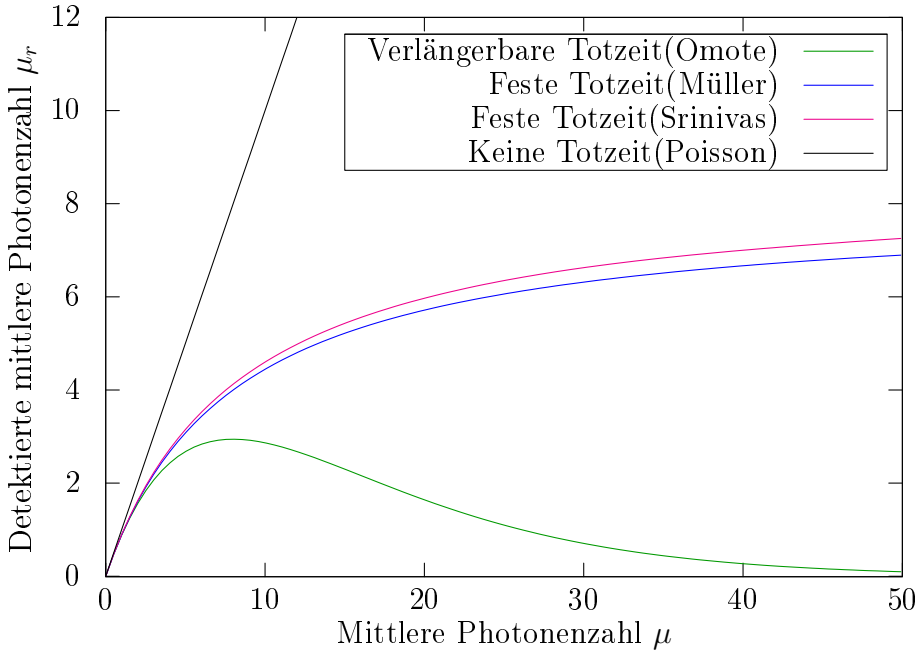


Abbildung 3.6: Mittlere detektierte Zählrate in Abhängigkeit der auftreffenden Intensität. Es wurde eine Totzeit von $\tau_d = 2.5$ ns sowie eine Intervalllänge von $T = 20$ ns eingesetzt.

Zusammenfassend wurde für die Beschreibung des ZZG bisher die detektierte Photonenstatistik einer LED betrachtet. Außerdem wurde berücksichtigt, dass bei der Detektion mit einem Photomultiplier eine verlängerbare Totzeit auftritt. Im Folgenden werden die Auswirkungen dieser Statistik auf die Zufallszahlen analysiert.

3.5 Stochastisches Modell

In den vorangegangenen Abschnitten wurde die Photonenstatistik des von einer LED emittierten Lichts und deren Modifikation auf Grund von Abschwächung und zusätzlichen Effekten bei der Detektion mit einem Photomultiplier untersucht. In diesem Kapitel wird nun die Qualität der Zufallszahlen untersucht. Zu diesem Zweck wird die Entropie berechnet, die ein neu generiertes

Bit besitzt, wenn alle zuvor generierten Bits bekannt sind.

$$H(X_i = x_i | X_{i-1} = x_{i-1} \dots X_0 = x_0) \tag{3.19}$$

Da diese Größe den Informationsgehalt eines Zufallsbits angibt und eine direkte Berechnung nicht möglich ist, wird eine untere Grenze dafür ermittelt. Aus diesem Grund werden im Folgenden verschiedene Faktoren untersucht, die diese untere Schranke beeinflussen: Gleichverteilung der Zufallsbits, Nächste-Nachbar-Korrelationen und längerreichweitige Korrelationen. Die Berechnungen werden in der weiteren Analyse für ein Zeitinterall $T = 20$ ns und eine Totzeit von $\tau_d = 2.5$ ns durchgeführt.

Zu Beginn werden die Wahrscheinlichkeiten für die Bitwerte 0 bzw. 1 und deren Abhängigkeit von der detektierten mittleren Photonenzahl μ_r untersucht.

Eine gerade bzw. ungerade Photonenzahl in einem Zeitintervall T wird den Bitwerten 0 bzw. 1 zugeordnet. Aufgrund dieser Zuordnung können die Wahrscheinlichkeiten für beide Bitwerte aus Gleichung (3.16) berechnet werden.

$$\begin{aligned} p_1 &= \sum_{n=0}^{\infty} P(\mu, 2 \cdot n + 1, T, \tau_d) \\ p_0 &= \sum_{n=0}^{\infty} P(\mu, 2 \cdot n, T, \tau_d) \end{aligned} \tag{3.20}$$

Dabei ist anzumerken, dass $P(\mu, n > M, T, \tau_d) = 0$ gilt (vergleiche Gleichung (3.16).

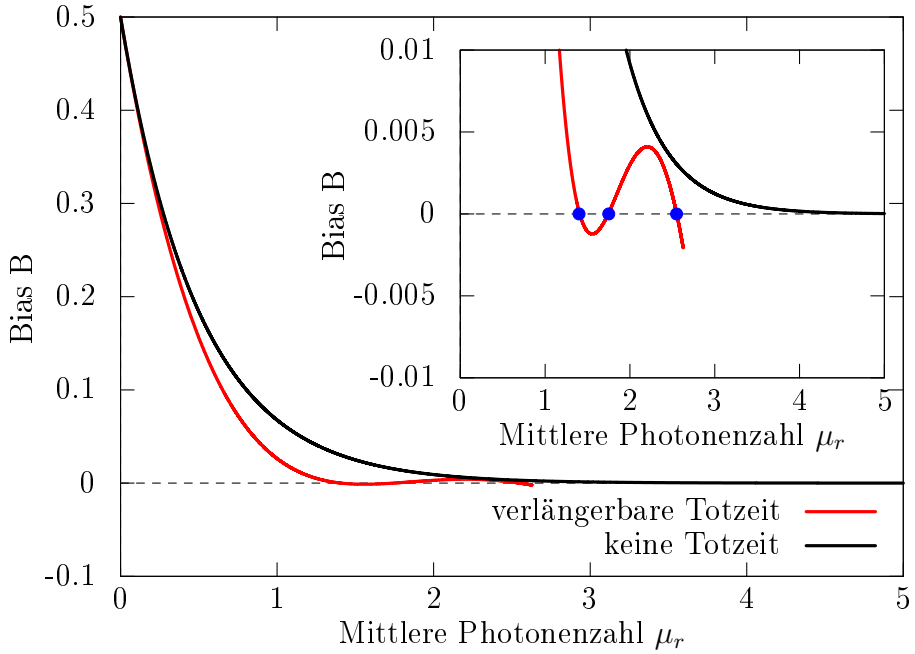


Abbildung 3.7: Die Schiefe B der Zufallsbits in Abhängigkeit von der mittleren Detektionsrate μ_r. Eine Totzeit von $\tau_d = 2.5$ ns sowie eine Intervalllänge von $T = 20$ ns werden eingesetzt. Das Inset ist eine Vergrößerung des Anzeigebereichs. Durch die maximal erreichbare Zählrate (vergleiche Abbildung 3.6) ist die rote Kurve beschränkt auf Werte $\mu_r < 2.95$. Die markierten Punkte im Inset zeigen Werte für μ_r, bei denen der Bias verschwindet.

Bei einem idealen Zufallszahlengenerator sind diese Wahrscheinlichkeiten gleich $p_0 = p_1 = \frac{1}{2}$. Die Abweichung dieser Wahrscheinlichkeiten vom Idealwert, im Folgenden als Bias oder Schiefe B (vergleiche Gleichung (3.21)) bezeichnet, wird in Abhängigkeit der mittleren detektierten Photonenzahl in Abbildung 3.7 dargestellt.

$$B = p_0 - 0.5 \tag{3.21}$$

Der Bias zeigt für Detektionen ohne Totzeit ein exponentielles Verhalten und $B \xrightarrow{\mu_r \to \infty} 0$ für sehr große Photonenzahlen. Im Fall einer verlängerbaren Totzeit existieren mittlere Photonenzahlen, bei denen der Bias verschwindet (in Abbildung 3.7 markiert). Bei diesen mittleren Photonenzahlen erhält man also eine gleichverteilte Zufallszahlenfolge. Die Zufallsbiterzeugung ist bei anderen mittleren Photonenzahlen ebenfalls möglich, der Bias in den Zufallsbits müsste aber noch durch Regularisierungsalgorithmen (siehe Abschnitt 3.6) eliminiert werden. Dieser Prozess reduziert die Erzeugungsrate in Abhängigkeit des Bias jedoch signifikant, weshalb für die Biterzeugung die mittleren

Zählraten mit verschwindendem Bias gewählt werden. Dadurch ergibt sich keine Reduktion der Entropie aus Gleichung (3.19) aufgrund der Schiefe in den Zufallszahlen.

Ein weiterer Parameter, der den Entropiegewinn des Zufallszahlengenerators einschränken kann, sind Korrelationen der Bits untereinander. Die Korrelation zweier Bits mit Bitabstand l lässt sich nach [71] folgendermaßen beschreiben

$$SCC_l = \frac{\sum_{k=1}^{N-l}(x_k - (B+0.5))(x_{k+l} - (B+0.5))}{\sum_{k=1}^{N}(x_k - (B+0.5))^2} \tag{3.22}$$

wobei N die Anzahl der Zufallsbits angibt. Für den Fall, dass die Zufallsbits gleichverteilt ($B = 0$) sind, kann man diesen Zusammenhang vereinfachen zu [22]

$$SCC_l = p_{00}^l + p_{11}^l - p_{01}^l - p_{10}^l \tag{3.23}$$

mit den Paarwahrscheinlichkeiten p_{xx}^l mit Abstand l.

Aufgrund der hohen Abschwächung der Photonen der LED bis zur Detektion werden keine Abhängigkeiten der Bits untereinander beobachtet. Der Überlapp eines Totzeitintervalls von einem Zeitintervall in das darauffolgende generiert jedoch Korrelationen benachbarter Bits. Zur Abschätzung dieser Nächste-Nachbar-Korrelationen wird die Tatsache verwendet, dass aus Zufallsbits, die mit einem Zeitintervall von $T = \tau$ aufgenommen werden, Zufallsbits berechnet werden können, die mit einem Zeitintervall $T = 2\tau$ aufgenommen worden wären, indem man zwei benachbarte Bits zusammenfasst (siehe Tabelle 3.1).

$T = \tau$	$T = 2 \cdot \tau$
00	0
01	1
10	1
11	0

Tabelle 3.1: Umrechnung von Zufallsbits aufgenommen mit einem Ausleseintervall $T = \tau$ in Zufallsbits aufgenommen mit einem Intervall $T = 2\tau$.

Unter der Bedingung, dass die Zufallsbits gleichverteilt sind, kann man aus Gleichung (3.23) und Tabelle 3.1 folgenden Zusammenhang zwischen den Nächste-Nachbar-Korrelationen ($l = 1$) bei einem Zeitintervall $T = \tau$ und dem Bias bei einem Zeitintervall $T = 2\tau$ ableiten:

$$\begin{aligned} SCC_1(\mu, T = \tau, \tau_d) &= p_{00+11}(\mu, T = \tau, \tau_d) - p_{01+10}(\mu, T = \tau, \tau_d) \\ &= p_0(2 \cdot \mu, T = 2 \cdot \tau, \tau_d) - p_1(2 \cdot \mu, T = 2 \cdot \tau, \tau_d) \\ &= 2 \cdot B(2 \cdot \mu, T = 2 \cdot \tau, \tau_d). \end{aligned} \tag{3.24}$$

Für die Parameter, die in Abbildung 3.7 gewählt wurden, ergibt sich für den Korrelationskoeffizienten $SCC_1 = 2.0 \cdot 10^{-7}$.

Innerhalb dieser theoretischen Beschreibung können keine langreichweitigen oder komplexeren Korrelationen gefunden werden. Ursachen für derartige Korrelationen könnten im experimentellen Aufbau in langfristigen Spannungs- beziehungsweise Temperaturschwankungen an verwendeten optischen und elektronischen Komponenten gefunden werden. Diese Auswirkungen werden aber in der vorliegenden theoretischen Beschreibung nicht berücksichtigt.

Aus der Photonenemission der LED und der nachfolgenden Detektion können keine weiteren Korrelationen abgeleitet werden, als die, die durch die Totzeit der Detektion in Form Nächster-Nachbar-Korrelationen auftreten. Zur Berechnung einer Grenze für die bedingte Entropie in Gleichung (3.19) werden der Bias und diese Korrelationen verwendet.

$$H(X_i = x_i | X_{i-1} = x_{i-1}) \geq 1 - 1.4 \cdot 10^{-14} \tag{3.25}$$

Diese Abschätzung der Entropie, das Photonenzahlhistogramm (vergleiche Abbildung 3.5) und die Abhängigkeit des Bias von der mittleren Photonenzahl (vergleiche Abbildung 3.7) ergeben das stochastische Modell des ZZG. In Abschnitt 5.1 wird dieses Modell experimentell verifiziert.

3.6 Regularisierungsalgorithmen

Das Problem vieler physikalischer Zufallszahlengeneratoren ist ein Ungleichgewicht in der Erzeugung der Bitwerte 0/1. Da in den meisten Einsatzgebieten dieser Generatoren eine Gleichverteilung vorausgesetzt wird, gibt es eine Reihe von Regularisierungsalgorithmen, um dieses Ungleichgewicht zu entfernen, ohne jedoch die Zufälligkeit zu beeinträchtigen. Alle diese Operationen haben eine Reduktion der Zufallsfolge in Abhängigkeit zur ursprünglichen Schiefe der Zufallszahlen zur Folge. Die Regularisierungseffizienz η_r der unterschiedlichen Ansätze wird am Ende dieses Abschnitts in Abbildung 3.8 verglichen.

3.6.1 von-Neumann Algorithmus

Bei der von-Neumann Regularisierung [21] werden Bits aus der Zufallszahlenfolge paarweise nicht überlappend mit folgender Zuordnung verarbeitet. Die Bitpaare 00 und 11 werden gestrichen und den Bitpaaren $01, 10$ werden die Bits $0, 1$ zugeordnet (vergleiche Tabelle 3.2). Unter der Bedingung, dass die ursprüngliche Bitfolge keine Korrelationen enthält, ist das Resultat

Eingangsbits		Ausgangsbit
00	→	verworfen
01	→	0
10	→	1
11	→	verworfen

Tabelle 3.2: Zuordnung der Bits beim Regularisierungsalgorithmus nach von-Neumann.

dieser Regularisierung eine gleichverteilte Bitfolge. Dieses sehr einfache Verfahren hat den Nachteil, dass selbst bei einer annähernden Gleichverteilung der Zufallsbits $1 - \eta_r = 75\%$ der Bits verworfen werden.

3.6.2 Iterierter von-Neumann Algorithmus

Um die niedrige Effizienz des von-Neumann Verfahrens zu erhöhen, existiert ein iterativer von-Neumann Algorithmus von Peres [20]. Der erste Iterationsschritt ist die gewöhnliche von-Neumann Regularisierung. In den weiteren Iterationsschritten werden jeweils die Bitpaare, die dort verworfen werden, in einem Bitstrom weiterverarbeitet. Zusammen mit einem zweiten Bitstrom aus den XOR verknüpften Eingangsbits wird darauf erneut der gewöhnliche von-Neumann Algorithmus angewendet. Die Regularisierungseffizienz in Abhängigkeit der Anzahl der Iterationen k und dem in der Eingangsbitfolge enthaltenem Bias wird zudem in der Arbeit von Peres angegeben.

$$\eta_k(p_0) = p_0 p_1 + \frac{1}{2}\eta_{k-1}\left(p_0^2 + p_1^2\right) + \frac{1}{2}(p_0^2 + p_1^2) \cdot \eta_{k-1}\left(\frac{p_0^2}{p_0^2 + p_1^2}\right) \tag{3.26}$$

Aus Abbildung 3.8 lässt sich die Effizienzsteigerung gegenüber dem von-Neumann Algorithmus selbst nach zwei Iterationsschritten deutlich erkennen. Dieser Gewinn ist natürlich durch einen erhöhten Rechenaufwand erkauft.

3.6.3 Elias Algorithmus

Ein alternativer Ansatz um die Effizienz der von-Neumann Regularisierungsmethode zu erhöhen, wurde durch Elias [72] entwickelt. Dabei wird die Bitfolge ebenfalls in Blöcke aufgeteilt, deren Länge N im Gegensatz zum von-Neumann Schema variabel gestaltet werden kann ($N \geq 2$). Die Zuordnung der Ausgabebits analog zu Tabelle 3.2 ist dabei komplizierter. Dazu werden die Blöcke der Länge N in Klassen nach der Anzahl k der Bitwerte 1 geordnet. In jeder dieser Klassen befinden sich $\binom{N}{k}$ Elemente. Die Binärdarstellung von

k(Anzahl der 1)	$\binom{N}{k}$ (binär)	Zuordnung
0	1(1)	verworfen
1	4(100)	{[0001],[0010], [0100],[1000]} →{[00],[01],[10],[11]}
2	6(110)	{[0011],[0101], [0110],[1001], [1010],[1100]} →{[00],[01],[10], [11],[0],[1]}
3	4(100)	{[1110],[1101], [1011],[0111]} →{[00],[01],[10],[11]}
4	1(1)	verworfen

Tabelle 3.3: Bitzuordnung beim Regularisierungsalgorithmus nach Elias.

$\binom{N}{k}$ wird anschließend dazu benutzt, um die Zuordnung der Eingangsblöcke zu den Ausgangsbits herzustellen. In Tabelle 3.3 ist ein Beispiel dieser Zuordnung für eine Blocklänge von $N = 4$ dargestellt. Eine untere Grenze für die Effizienz dieses Verfahrens ist ebenfalls in der Arbeit von Elias angegeben:

$$\eta_N(p_0) \geq \sum_{k=0}^{N} \binom{N}{k} p_0^k (1-p_0)^{N-k} \frac{log_2\binom{N}{k}}{N} - \frac{3}{N} \tag{3.27}$$

In Abbildung 3.8 ist der Effizienzgewinn bei einer Blocklänge von $N = 8$ deutlich zu erkennen. Ein Vorteil dieser Methode ist eine verhältnismäßig einfache Möglichkeit der hardwarenahen Implementierung.

Eine Übersicht der Effizienz der einzelnen Regularisierungsschemata ist in Abbildung 3.8 gegeben. In dieser Graphik sind die Effizienz der von-Neumann Regularisierung, dem iterativen Algorithmus mit 2 und 8 Schritten, die Methode nach Elias mit Blocklängen $N = 8$ und $N = 32$ und die Bitentropie dargestellt. Letztere stellt die maximal erreichbare Effizienz von Regularisierungsmethoden dar und wird von den Verfahren nach Peres und Elias im Grenzfall einer hohen Anzahl von Iterationen bzw. einer großen Blocklänge erreicht.

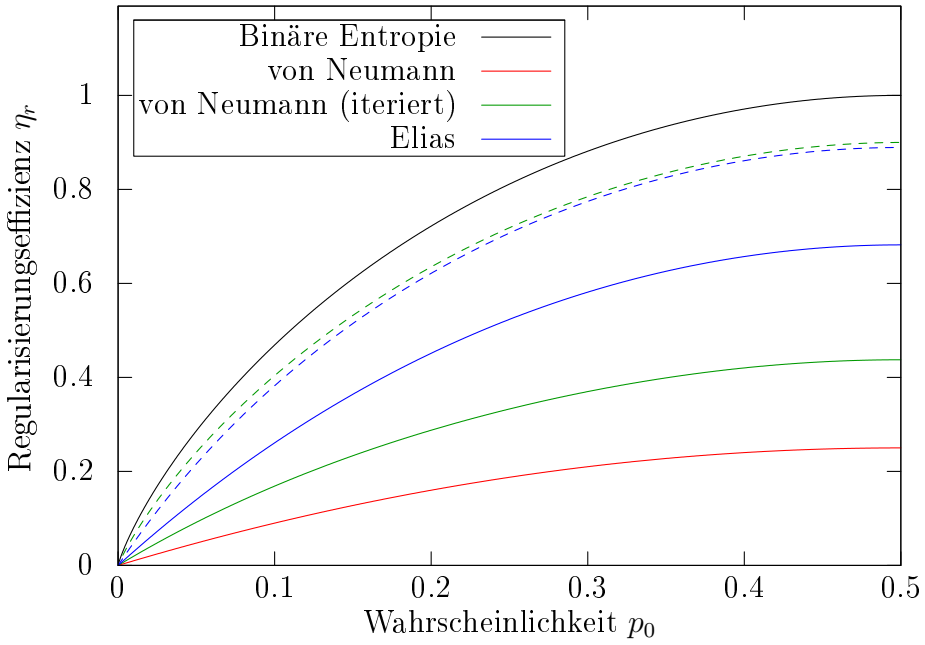


Abbildung 3.8: Effizienz verschiedener Regularisierungsmethoden. Die Regularisierung nach Peres wurde mit 2 (———) und 8 (– – – –) Iterationen durchgeführt. Die Methode nach Elias wird mit einer Blocklänge von 8 (———) und 32 (– – – –) Bit berechnet.

Allen Regularisierungsverfahren gemeinsam ist die Voraussetzung, dass die Eingangsbitfolge keine Korrelationen aufweisen darf. Um Korrelationen aus einer Bitfolge zu eliminieren, existieren weitere Verfahren. Um Korrelationen erster Ordnung (vergleiche Gleichung (3.23)) zu entfernen, kann eine Methode von Samuelson und Pratt angewendet werden, die wiederum die Bitfolge verkürzt. Für die Details dieser Methode sei hier auf die Arbeit von Samuelson [73] verwiesen.

Die vorgestellten Verfahren zeichnen sich dadurch aus, dass diese garantieren, aus einer unausgeglichenen Bitfolge bezüglich der Bitwerte eine gleichverteilte, im Allgemeinen kürzere Bitfolge zu erzeugen. Zusätzlich werden in vielen experimentellen ZZG auch Hash-Algorithmen verwendet, die ebenfalls gewährleisten sollen, dass der Informationsgehalt eines Bits maximal ist. Diese Funktionen (wie zum Beispiel SHA-1, SHA-2, „2-universal hash functions“) reduzieren den Eingangsbitstrom, wobei der Reduktionsfaktor a priori bekannt sein muss. Nichtsdestoweniger können diese Funktionen nicht garantieren, aus einer nicht gleichverteilten Bitfolge eine gleichverteilte Bitfolge zu erzeugen.

Kapitel 4

Experimenteller Aufbau

Nachdem im letzten Abschnitt bereits die wichtigsten Komponenten des ZZG benannt wurden, folgt in diesem Kapitel die Beschreibung des kompletten Aufbaus des ZZG. Dabei liegt der Schwerpunkt auf dem Zufallssignal von der Entstehung in der LED bis zur Extraktion der Zufallsbits in einem FPGA[1]. Abbildung 4.1 zeigt eine Übersicht über den experimentellen Aufbau des ZZG, der im Folgenden näher beschrieben wird.

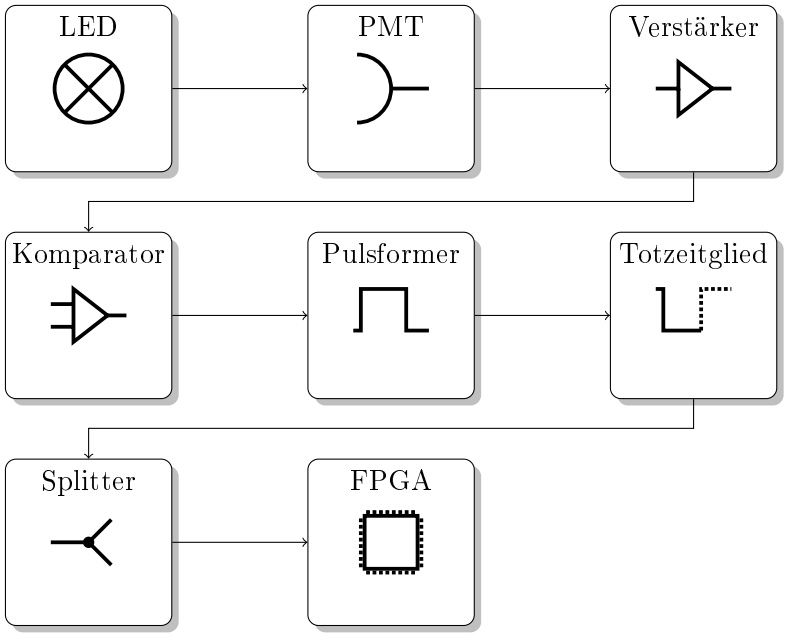


Abbildung 4.1: Der schematische Aufbau des Zufallszahlengenerators zeigt die einzelnen Komponenten und zusätzlich den Signalverlauf.

[1]FPGA=field programmable gate array

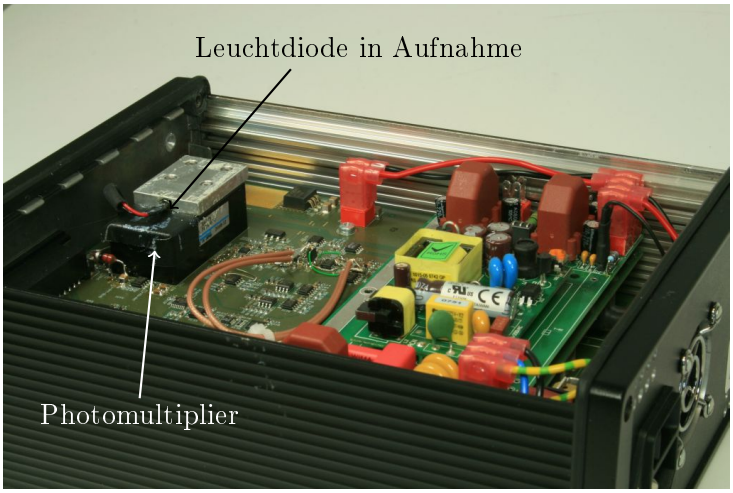


Abbildung 4.2: Systemaufbau des Zufallszahlengenerators.

Als Lichtquelle dient eine breitbandige rote LED ($\lambda \sim 628$ nm, $\Delta\lambda \sim 35.6$ nm, vergleiche Abbildung 4.3). Die Regelung der Intensität dieser LED wird über die gemessene Zählrate am Photomultiplier realisiert, welche eine zwischen 0 und 4 mA einstellbare Konstantstromquelle verwendet. Bei der Charakterisierung der Photonenstatistik der LED konnte der Einfluss des Coulomb-Blockade-Effekts vor allem wegen der starken Abschwächung nicht beobachtet werden (vergleiche Ende Abschnitt 3.2). Die Kohärenzzeit τ_C der LED kann man mithilfe des Spektrums (vergleiche Abbildung 4.3) bestimmen.

$$\tau_C = \frac{\lambda^2}{c\,\Delta\lambda} = 3.7 \cdot 10^{-14}\ \mathrm{s} \tag{4.1}$$

Hier zeigt sich zusätzlich, dass Interferenzeffekte (ähnlich Specklemustern in der Zeit) erst bei sehr viel kleineren Zeitskalen als der verwendeten Auslesерate $T \gg \tau_C$ auftreten und somit die Detektionsstatistik nicht beeinflussen.

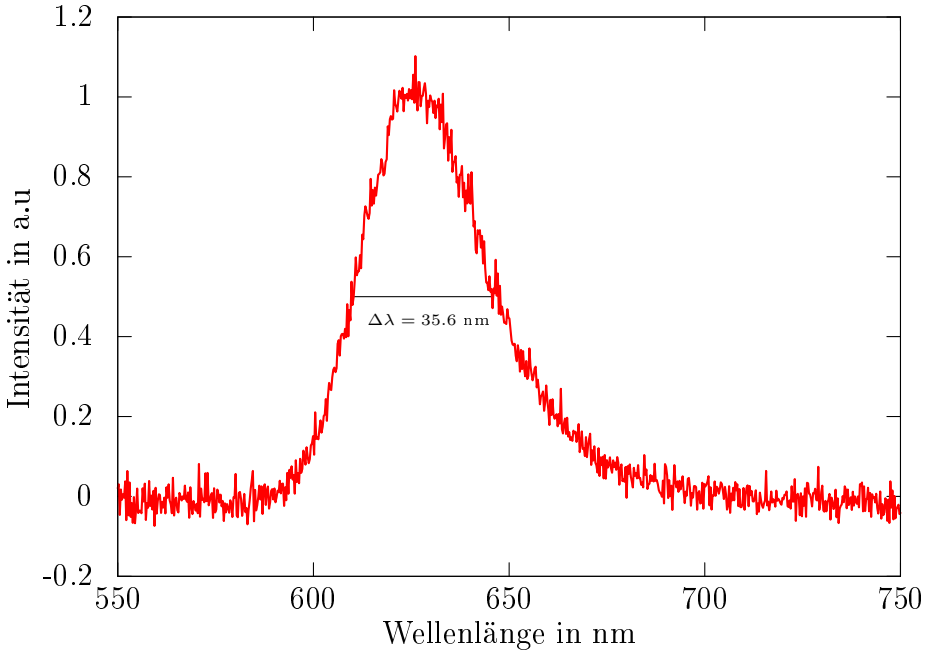
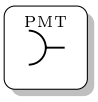


Abbildung 4.3: Spektrum der LED.

Eine mechanische Halterung, die an das Eintrittsfenster des Photomultipliers montiert wird, sorgt für die optische Kopplung der LED an den Detektor (vergleiche Abbildung 4.2).



Zur Detektion einzelner Photonen stehen mehrere Möglichkeiten zur Verfügung, zum Beispiel Avalanche Photodioden (APD), Photomultiplier, supraleitende Einzelphotondetektoren und Quantenpunkt-Einzelphotondetektoren, wobei die letzten beiden aufgrund des hohen experimentellen Aufwands von vornherein ausgeschlossen werden. Der Vorteil einer Halbleiter Avalanche Photodiode ist der kompakte Aufbau und eine damit verbundene einfache Skalierbarkeit des Zufallszahlengenerators. Ein wesentlicher Nachteil liegt aber in der großen Totzeit dieser Detektoren von $25 - 1000$ ns [74], die die Rate, mit der Zufallsbits erzeugt werden können, stark limitiert. Zudem ist der elektronische Schaltungsaufwand, mit der kleine Totzeiten erreicht werden können, extrem groß und erhöht die Anfälligkeit des ZZG für Störungen innerhalb der Elektronik.

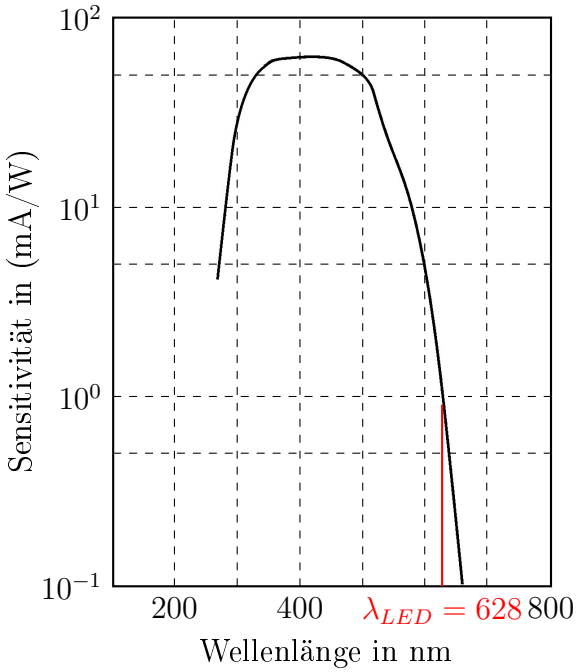


Abbildung 4.4: Sensitivität des Photomultipliers in Abhängigkeit der Wellenlänge (entnommen aus dem Datenblatt [75]).

Eine Alternative bietet ein Photomultiplier (PMT), dessen Totzeit lediglich auf die Dauer eines elektronischen Pulses beschränkt ist. In diesem Experiment kommt ein kompaktes Photomultiplier Modul[2] mit einer Pulsdauer von ca. 2 ns zur Anwendung. Diese kurze Pulsdauer erreicht der Hersteller durch optimierte räumliche Anordnung der Dynoden innerhalb des Photomultipliers (vergleiche Tabelle 4.2 in [63]). Das Eintrittsfenster aus Borosilicate misst ca. 1x1 cm^2 und transmittiert Licht der Wellenlänge $\lambda > 300$ nm. Die Sb-Rb-Cs Photokathode ist sensitiv im Wellenlängenbereich von $320-650$ nm (vergleiche Abbildung 4.4). Da die Detektionseffizienz für den Zufallszahlengenerator nicht entscheidend ist, kann diese Konfiguration in Kombination mit der roten LED $\lambda = 628$ nm verwendet werden.

Die integrierte Hochspannungsversorgung sowie die einzelnen Dynoden und ein Stromverstärker für das Ausgangssignal sind in dem 6x2x2 cm^3 großen Modul integriert. Die Hochspannung kann über einen analogen Anschluss ($U_s = 0..1$ V) eingestellt werden. Nach Herstellerempfehlung wurde diese analoge Spannung auf 800 mV eingestellt.

[2] Hamamatsu H6779-None

Vor der Digitalisierung wird das Signal des PMT mithilfe von zwei, in Reihe geschalteten Operationsverstärkern verstärkt. Dadurch erreicht man eine mittlere Signalamplitude von ca. 250 mV am Eingang des Komparators. Die Amplitudenverteilung des verstärkten Signals ist in Abbildung 4.5 dargestellt. Deutlich erkennbar ist dabei sowohl die mittlere Signalamplitude registrierter Photonen als auch die Amplitude, die durch elektronisches Rauschen erzeugt wird.

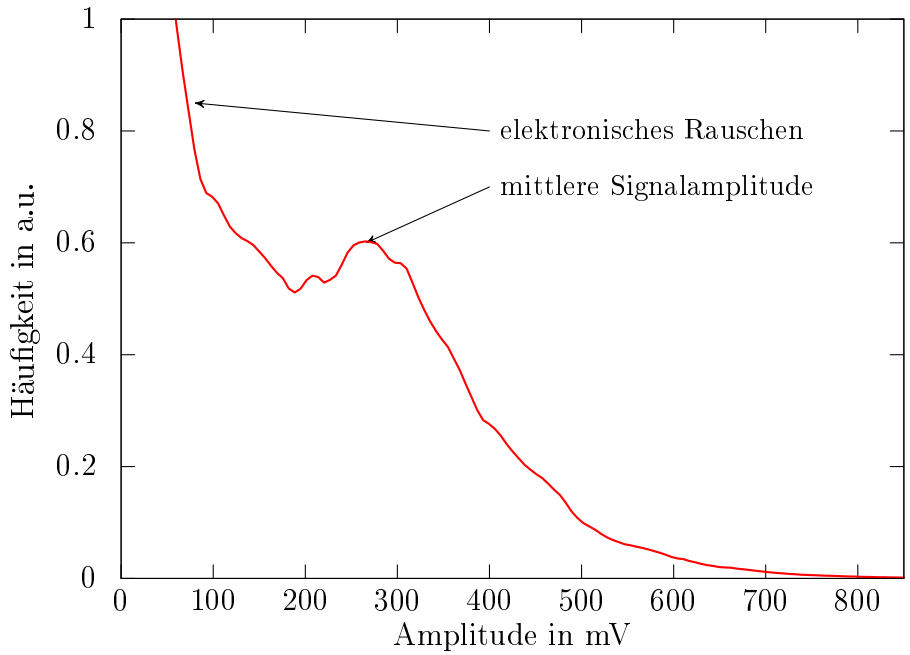
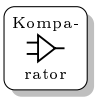


Abbildung 4.5: Amplitudenverteilung des Photomultipliersignals am Ausgang der Verstärkerstrecke. Dieses Histogramm wurde mithilfe eines Oszilloskops (Lecroy WaveRunner 204XI-A) mit einer Bandbreite von 2 GHz erstellt.



Die Digitalisierung des verstärkten analogen PMT Signals erfolgt zur Unterdrückung des elektronischen Rauschens mit einem Schwellen-Komparator. Zur Festlegung der Diskriminatorschwelle wird die Zählrate in Abhängigkeit dieser Schwellenspannung gemessen. Am Eingang des Komparators liegt der invertierte Ausgang des Verstärkers, das heißt das invertierte Signal des ursprünglichen Pulses. In Abbildung 4.6 ist diese Messung bei einem Strom der LED von $I_{LED} = 1.57$ mA dargestellt (entspricht dem Arbeitspunkt des ZZG). Zusätzlich wurde dieselbe Messung ohne eine LED wiederholt, um den Beitrag der Dunkeldetektionsrate zu bestimmen. Es wird deutlich, dass diese

Rate drastisch zunimmt, wenn die Diskriminatorschwelle unterhalb des elektronischen Rauschens des Signals liegt. Die Wahl der Schwelle bei 550 mV gewährleistet ein niedriges Verhältnis der Dunkelzählrate zur Signalzählrate von $SNR = \frac{1}{7 \cdot 10^7} = 1.42 \cdot 10^{-8}$.

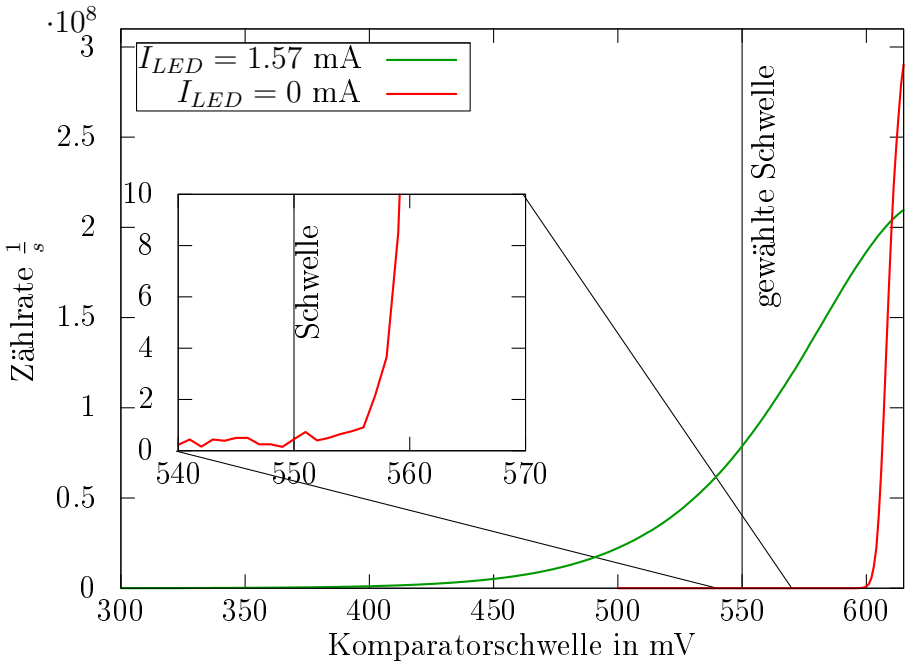
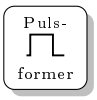


Abbildung 4.6: Zählrate der digitalisierten Pulse in Abhängigkeit der Komparatorschwelle. Es wurde eine Schwellenspannung von 550 mV gewählt.



Der Pulsformer stellt sicher, dass ein registrierter elektrischer Puls immer mindestens eine Länge von ca. 1.5 ns aufweist. Diese Eigenschaft gewährleistet, dass minimale Verarbeitungszeiten, sogenannten „Setup- und Hold-“ Zeiten, innerhalb des FPGA nicht verletzt werden. Somit werden metastabile Zustände [76] bei Flip-Flops, verursacht durch diese Zeitverletzungen, innerhalb des FPGA vermieden (Derartige Zustände führen zu einem nicht deterministischen Verhalten des FPGA).

Zusätzlich wird noch ein Totzeitglied eingesetzt, um die Zeit zwischen zwei aufeinanderfolgenden Pulsen auf einen minimalen zeitlichen Abstand von ca. 1.5 ns zu begrenzen. Dies dient ebenfalls zur Vermeidung metastabiler Zustände innerhalb des FPGA. Zusammen mit der Pulsformer-Logik haben zwei stei-

gende Flanken aufeinanderfolgender elektrischer Pulse einen minimalen zeitlichen Abstand von ca. 3 ns. Diese Zeit kann somit als Totzeit der gesamten elektronischen Schaltung angesehen werden. Dabei bleibt anzumerken, dass diese Zeit durch theoretische Signallaufzeiten in den verwendeten elektronischen Komponenten und Laufzeiten in den Zuleitungen zusammengesetzt ist. Die exakte Bestimmung dieser Totzeit erfolgt in Kapitel 5.1 und führt zu einer Totzeit von 2.75 ns.

Um die Verarbeitungsgeschwindigkeit innerhalb des FPGA zu verringern, werden außerdem die Photonenpulse jeweils abwechselnd in einem von zwei separaten Eingängen des FPGA angelegt. Dies erfolgt mit Hilfe von zwei diskreten Flipflops, deren Ausgänge jeweils abwechselnd mit jedem Detektionsereignis ihren Zustand ändern.

Am Eingang des FPGA[3] wird die Anzahl der elektronischen Pulse der beiden Eingänge in zwei logischen Zählern (4-Bit tief) aufgenommen. Das periodische Auslesen dieser Zähler am Ende eines Zeitintervalls T stellt eine Herausforderung dar, da das Eintreffen der elektronischen Pulse asynchron zum Auslesetakt geschieht. Aufgrund dieser Asynchronität besteht die Gefahr von metastabilen Zuständen innerhalb des FPGA [76]. Deshalb werden die beiden Zähler jeweils um weitere drei Zähler auf insgesamt zwei mal vier Zähler erweitert. Abwechselnd wird einer der vier Zähler jedes Eingangs mit dem nächsten Photonereignis dieses Eingangs inkrementiert. Dadurch haben die einzelnen Zähler jeweils den gleichen oder einen um eins unterschiedlichen Wert. Beispielsweise können folgende Zählerstände registriert werden: 0-0-0-0; 0-0-0-1; 0-0-1-1; 0-1-1-1; 1-1-1-1; 1-1-1-2. Das stellt sicher, dass nur jeweils maximal ein Zähler zu einem Zeitpunkt eine Zustandsänderung erfährt. Das Auslesen der vier Zähler pro Eingang am Ende eines Messintervalls hat zur Folge, dass nur in einem Zähler ein metastabiler Zustand auftreten kann. Das Resultat eines solchen fehlerhaften Zählers ist nicht deterministisch, das heißt der Zähler kann alle Zustände (0 bis 15) annehmen. Dieser metastabile Zustand tritt in unserem Aufbau mit einer Häufigkeit in der Größenordnung von $5 \cdot 10^{-3} \frac{1}{s}$ auf.

[3]Verwendet wird ein Spartan3 400 der Firma Xilinx

Durch den Vergleich der Zustände der vier Zähler können fehlerhafte Ereignisse, wie zum Beispiel der Zählerstand 1-1-1-3, detektiert und anschließend korrigiert werden. Hier bleibt anzumerken, dass metastabile Zustände unerkannt bleiben, wenn der Zählerstand einen scheinbar korrekten Wert annimmt. Eine Eigenschaft von metastabilen Zuständen ist, dass diese länger als einen Auslesezyklus dauern können [76]. Ein derartiger Fehler wird ebenfalls detektiert und anschließend verworfen, da er nicht korrigiert werden kann, da in diesem Fall zwei Zähler betroffen sind, so zum Beispiel 1-1-2-3. Die Wahrscheinlichkeit solcher Ereignisse in unserem Aufbau ist in der Größenordnung von $10^{-10}\frac{1}{s}$. Als Ergebnis liefert dieser Algorithmus die Anzahl von Photonen für jeden Eingang separat. Auf Grundlage der Summe dieser beiden Zählerstände am Intervallende T wird ein Zufallsbit erzeugt. Eine ungerade Anzahl entspricht dem Bitwert '1', und eine gerade Anzahl dem Bitwert '0'. Die weitere Datenverarbeitung besteht im Wesentlichen aus bereits implementierten Online-Tests (siehe Abschnitt 5.2) und der Übersendung der Zufallsbits an einen PC über eine USB2.0 Verbindung. Diese Prozesse erfolgen in einem weiteren FPGA sowie einem DSP (*digital signal processor*).

Kapitel 5

Analyse der Zufallszahlen

Eine Schwierigkeit bei der Analyse von Zufallszahlen besteht darin, dass die Zufälligkeit bei endlich großen Datenmengen nicht bewiesen werden kann. Deshalb ist es essentiell, zu Beginn der Untersuchung das theoretische Modell durch Messungen an den verschiedenen Komponenten zu untermauern. Außerdem werden in diesem Kapitel unterschiedliche Tests diskutiert, die während des Betriebs innerhalb des ZZG ablaufen und einen korrekten Betrieb sicherstellen sollen. Diese Tests wurden entwickelt, um den Anforderungen an ZZG in kryptographischen Einsatzgebieten [7] gerecht zu werden. Abschließend dient die Analyse generierter Zufallsbits dazu, mögliche Schwächen der Implementierung zu erkennen. Aus einer Vielzahl an möglichen Testroutinen werden spezielle Tests ausgewählt, um gezielt mögliche Schwächen unseres ZZG zu untersuchen. Dazu zählen vor allem Tests, die kurzreichweitige Korrelationen aufdecken. Verfügbare Sammlungen von statistischen Tests, die vor allem zur Analyse von algorithmischen Zufallszahlengeneratoren entwickelt worden sind, untersuchen zusätzlich auch längerreichweitige Korrelationen innerhalb der Bitfolgen.

5.1 Test des stochastischen Modells

Die ersten durchzuführenden Tests beziehen sich auf die Vorhersagen des stochastischen Modells in Abschnitt 3.5. Aufgrund der Tatsache, dass man die Zufälligkeit der Biterzeugung allein durch die Analyse endlicher Bitfolgen nicht nachweisen kann, ist dieser Abschnitt der Bedeutendste in der Untersuchung des ZZG.

Die in Abbildung 3.5 gezeigte Wahrscheinlichkeitsverteilung der Photonenzahl wird mit Hilfe eines 4-Bit-Zählers innerhalb des FPGA gemessen. Die Größe des Zählers ist ausreichend, da die Photonenzahl innerhalb eines

Intervalls von $T = 20$ ns aufgrund der Totzeit von $\tau_d = 2.75$ ns auf maximal 8 beschränkt ist (vergleiche Abbildung 3.5). Dieses Histogramm wurde über 10^4 s aufgenommen und ist in Abbildung 5.1 dargestellt. Dafür wurde die Helligkeit der LED so eingestellt, dass sich eine mittlere, detektierte Zählrate von $\mu_r = 1.43$ ergab. Diese Zählrate entspricht dem ersten Nulldurchgang des Bias in Abbildung 3.7 und somit dem Arbeitspunkt des ZZG. Die theoretische Verteilung wurde mit der Totzeit τ_d aus den in Abbildung 5.2 gezeigten Daten berechnet..

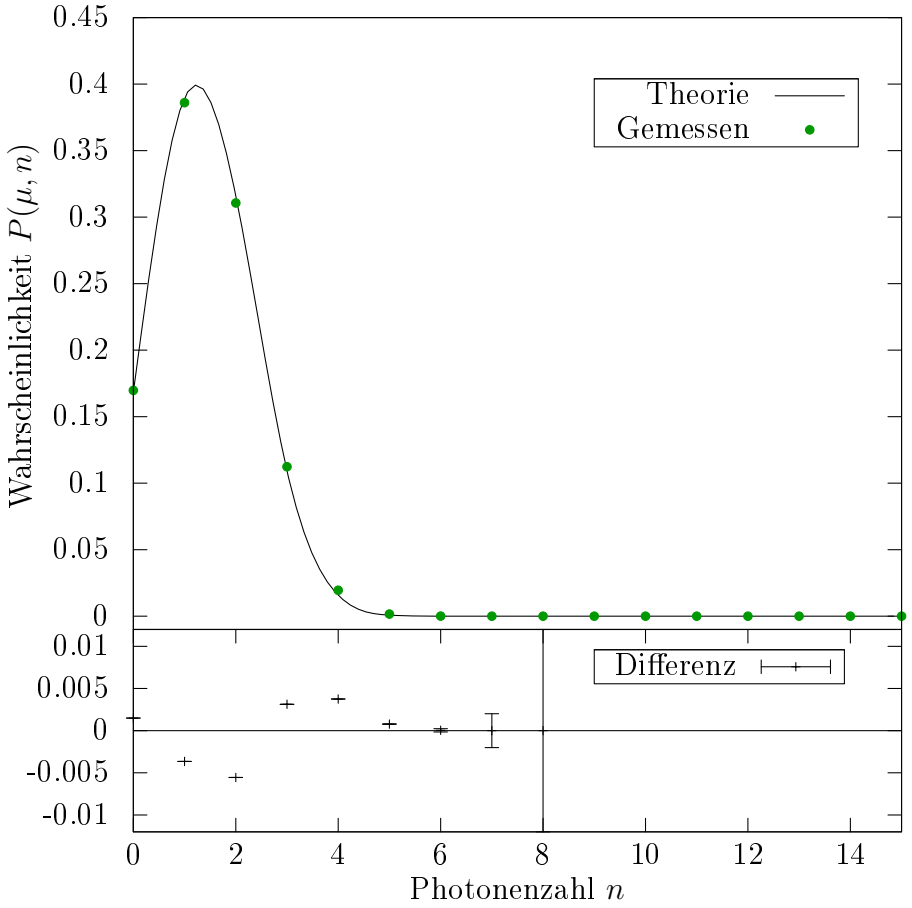


Abbildung 5.1: Gemessene Photonenstatistik mit einer Zählrate von $\mu_r = 1.43$ bei einer Intervalllänge von $T = 20$ ns. Eine Visualisierung der diskreten theoretischen Photonenstatistik in Form der durchgezogenen Kurve vereinfacht den Vergleich mit den experimentellen Werten, die über 10^4 s aufgenommen worden sind. Zusätzlich ist die Differenz der Theorie zu den experimentell ermittelten Werten in der unteren Kurve dargestellt.

Die Abweichung der experimentellen Werte von dieser theoretischen Kurve sind ebenfalls in Abbildung 5.1 abgebildet. Dabei ergeben sich statistisch signifikante Abweichungen von der theoretischen Vorhersage in der Größenordnung von $\pm 5 \cdot 10^{-3}$. Deren Ursache konnte in der vorliegenden Arbeit aufgrund der geringen Auswirkungen nicht bestimmt werden.

Als weiterer Test des stochastischen Modells wird der Bias in Abhängigkeit von der mittleren Photonenzahl durch Variation der Helligkeit der LED gemessen (Abbildung 5.2). Dazu werden zuerst für jeden Messpunkt 10 MByte lange Zufallsfolgen analysiert, wodurch eine statistische Signifikanz von $\sigma = 5.46 \cdot 10^{-5}$ erreicht wird. Um den statistischen Fehler bei sehr kleinen Werten des Bias zu verringern, wurden zusätzlich in diesem Wertebereich der mittleren Detektionshäufigkeit jeweils 1000 MByte große Zufallsfolgen ausgewertet.

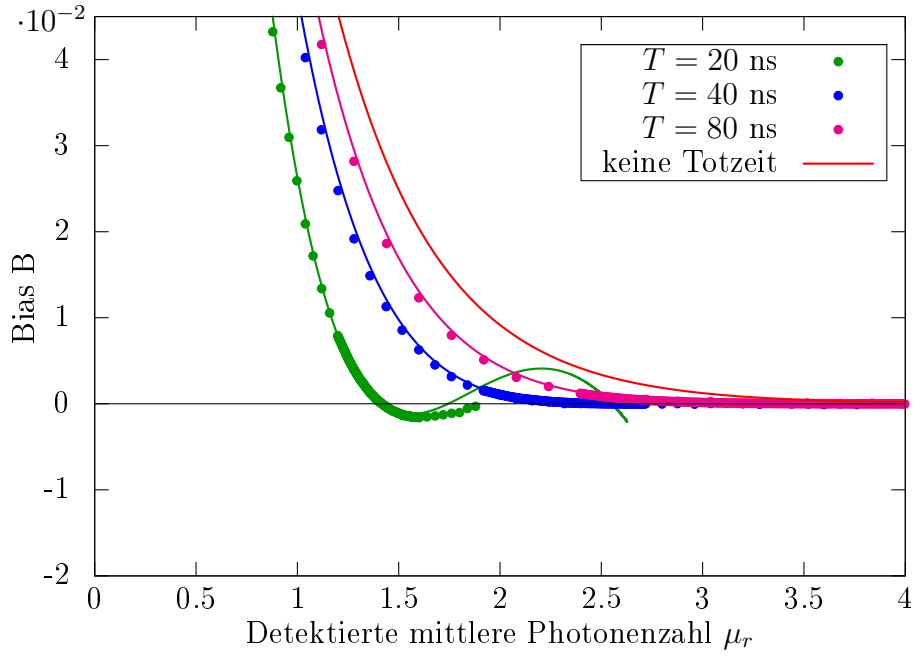


Abbildung 5.2: Gemessene Schiefe der Zufallszahlen. Für die Analyse wurde eine Messzeit von $T = 20$ ns, $T = 40$ ns und $T = 80$ ns eingestellt. Für jeden Messpunkt wurden 10 im Bereich kleiner Biaswerte 1000 MByte große Bitfolgen aufgenommen und daraus der Bias bestimmt.

Aus der Anpassung der theoretischen Vorhersage an die experimentellen Resultate konnte die Totzeit $\tau_d = 2.75$ ns als freier Parameter bestimmt werden. Die theoretischen Vorhersagen werden durch die Analyse in weiten Teilen bestätigt (vergleiche Abbildung 5.2 und 5.3). Für sehr hohe mittlere

Photonenzahlen und damit Zählraten über $8 \cdot 10^7 \frac{Photonen}{s}$ entstehen Abweichungen vom Modell. Ein wesentlicher Grund dafür ist vermutlich der verwendete Photomultiplier, dessen Spezifikationen maximale Detektionsraten von $5 \cdot 10^7 \frac{Photonen}{s}$ zulassen.

Bei einer nur moderaten Überschreitung dieser Spezifikation lassen sich keine signifikanten Unterschiede zwischen der theoretischen Vorhersage und der Schiefe der Zufallszahlen feststellen. Bei einer weiteren Überschreitung dieser Spezifikationen wäre eine Änderung der Amplitudenverteilung des Photomultipliersignals denkbar, die wiederum durch die Verwendung des Schwellendiskriminators einen direkten Einfluss auf die Länge der Totzeit haben könnte.

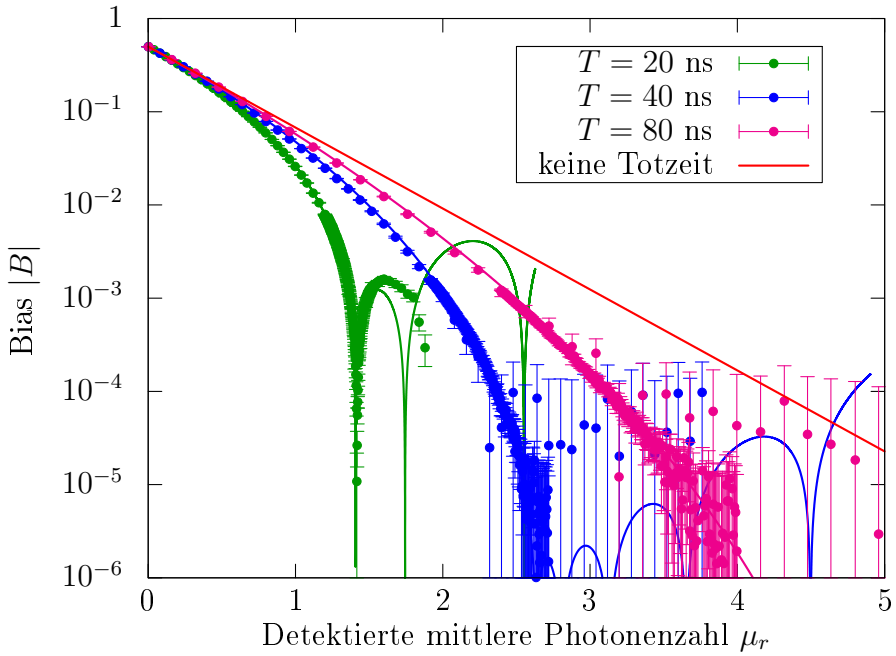


Abbildung 5.3: Gemessene Schiefe der Zufallszahlen. Für die Analyse wurde eine Messzeit von $T = 20$ ns, $T = 40$ ns und $T = 80$ ns eingestellt. Für jeden Messpunkt wurden 10 bzw. im Bereich kleiner Biaswerte 1000 MByte Daten aufgenommen und daraus der Bias bestimmt. Diese Abbildung ist eine logarithmische Darstellung von Abbildung 5.2.

Die Auswirkungen der verlängerbaren Totzeit im Vergleich zu einer totzeitfreien Detektion ist in Abbildung 5.3 deutlich zu erkennen. Die mittlere Zählrate, bei der eine gleichverteilte Zufallsfolge generiert wird, konnte experimentell bestätigt werden. Es bleibt aber dennoch anzumerken, dass durch Temperaturänderungen des gesamten experimentellen Aufbaus und insbeson-

dere des Photomultipliers vermutlich die Totzeit (< 100 ps) beeinflusst wird. Eine messbare Auswirkung äußert sich in einer Modifikation dieser mittleren Zählrate.

Alle weiteren Tests werden mit Zufallsbits durchgeführt, die am ersten Nulldurchgang des Bias bei einer mittleren Photonenzahl von $\mu_r = 1.43$ und einer Intervalllänge $T = 20$ ns aufgenommen werden. Dadurch wird garantiert, dass die Zufallsfolgen gleichverteilt sind.

5.2 Anlauf- und Onlinetests

Der Zufallszahlengenerator muss aufgrund des Einsatzes in einem kryptographischen Gesamtsystem kontinuierlich auf Funktionsfähigkeit überprüft werden. Zusätzlich dürfen keine Zufallsbits ausgegeben werden, wenn deren Qualität unterhalb eines bestimmten Niveaus abfällt. Aus diesem Grund werden verschiedene Tests ausgewählt, die innerhalb des Geräts sowohl beim Start als auch im laufenden Betrieb durchgeführt werden. Grundlage für die Auswahl der Testroutinen ist die Empfehlung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) [7].

Test auf Totalausfall

Zunächst muss sichergestellt werden, dass die Rauschquelle[1] nicht komplett ausgefallen ist. Aus diesem Grund wird in aufeinanderfolgenden Intervallen überprüft, ob mindestens ein Photon detektiert wurde. Wenn kein Photon in N Intervallen detektiert wurde, wird angenommen, dass die Rauschquelle ausgefallen ist und der Zufallszahlengenerator wird stillgelegt. Bei der Wahl der Anzahl N muss zwischen einer niedrigen Ausfallrate bei ordnungsgemäßem Betrieb und einem schnellen Ansprechen bei tatsächlichem Ausfall der Rauschquelle abgewogen werden. Bei $N = 23$ beträgt die Ausfallwahrscheinlichkeit des Zufallszahlengenerators 10^{-6} pro Jahr bei kontinuierlichem Betrieb innerhalb der Spezifikationen. Im Gegensatz dazu wird ein Ausfall der Rauschquelle nach 23 Intervallen also nach 460 ns erkannt. Dadurch kann mit einem 23 Bit langen Zwischenspeicher verhindert werden, dass Bits den ZZG nach Ausfall der Rauschquelle verlassen.

[1] Rauschquelle: In diesem Zufallszahlengenerator wird die LED zusammen mit der Detektionselektronik als Rauschquelle bezeichnet.

Monobit Test

Der in Abschnitt 5.3.1 gezeigte Test wird aufgrund der theoretischen Abhängigkeit des Bias von der Photonen-Zählrate als Online-Test ausgewählt. Außerdem wurde in diesem Test ein mehrstufiges Vorgehen gewählt. Der Onlinetest wird bestanden, wenn die statistische Größe S aus Gleichung (5.1) innerhalb der Grenzen $|S| < 16.5$ liegt. Der ZZG wird stillgelegt, wenn dieser Test 4 Mal in Folge fehlgeschlagen ist.

χ^2- Test auf 4-Bit Worte

Dieser komplexe Test wurde aus [7] übernommen. Dabei wird jeweils die Häufigkeit von 128 4-Bit Worten einem χ^2 Anpassungstest unterzogen. Mehrere Abbruchbedingungen werden auf Basis dieses Wertes definiert. Eine aus wiederholten Messungen berechnete Historienvariable wird kontinuierlich überprüft, um langfristige, kleine Änderungen der Qualität der Zufallsbits aufzudecken. Ebenso führen sehr extreme Resultate des χ^2-Anpassungstest zum Scheitern. Nach 3 aufeinanderfolgenden misslungenen Tests wird der ZZG stillgelegt.

Dieser Test dient dazu sowohl offensichtliche Schwächen des ZZG zu erkennen als auch langfristige Änderungen in der Qualität der Zufallszahlen auszuschließen.

Konstante Zählrate

Dieser Test misst innerhalb von 50 ms Intervallen die detektierte Photonenzählrate N, um sicherzustellen, dass die Qualität der Zufallszahlen des ZZG nicht durch zu große Intensitätsfluktuationen gemindert wird. Ein Akzeptanzintervall von $\Delta N = 4.5 \cdot 10^5$ um den erwarteten Wert von $N = 3.58 \cdot 10^6$ wird dabei angewendet, um die Fluktuationen in der Schiefe der Zufallszahlen auf $\Delta B = 10^{-4}$ zu begrenzen. Die Stilllegung des ZZG wird erst bei vier aufeinanderfolgenden Verletzungen dieses Intervalls veranlasst, um die Ausfallhäufigkeit des ZZG im korrekten Betrieb zu begrenzen.

Temperatur und Versorgungsspannung

Zusätzlich zu den bisherigen Online-Tests wird während des Betriebs die Temperatur und sämtliche Versorgungsspannungen insbesondere der des Photomultipliers überwacht. Als Kriterien für eine Stilllegung des ZZG für diese Überwachung dienen bisher die in den Datenblättern der verwendeten elektronischen Bauteile angegebenen Grenzwerte. Da Temperaturschwankun-

gen des Photomultipliers den Arbeitspunkt des ZZG beeinflussen, müssen Grenzwerte für diesen Parameter jedoch noch angepasst werden.

5.3 Stochastische Tests

In diesem Abschnitt werden Bitfolgen untersucht, die bei einer mittleren Zählrate von $\mu_r = 1.43$ und einem Messintervall von $T = 20$ ns aufgenommen wurden. Da der Prozess der Zufallsgenerierung keine langreichweitigen Korrelationen vermuten lässt, wurden zuerst statistische Tests ausgewählt, die speziell kurzreichweitige Korrelationen sowie die Schiefe der Bitfolge testen. Zur statistischen Analyse wird das Verfahren des Hypothesen-Tests [77] angewendet. Dabei wird als Nullhypothese H_0 die Aussage verwendet, dass ein idealer ZZG vorliegt. Die alternative Hypothese H_1 besagt, dass kein idealer ZZG vorliegt. Im Anschluss wird ein Test gewählt und die zugehörige Testgröße auf einer Bitfolge berechnet. Daraufhin wird die Wahrscheinlichkeit berechnet, dass unter Annahme der Nullhypothese diese oder eine extremere Testgröße eintritt. Diese im Folgenden als p-Wert bezeichnete Wahrscheinlichkeit wird mit einem gewählten Signifikanzniveau α verglichen. Die Nullhypothese wird verworfen, wenn der p-Wert unterhalb des Signifikanzniveaus liegt. Eine detaillierte Beschreibung ist im Anhang A.1 gegeben.

5.3.1 Monobit-Test

Der Monobit-Test [78] untersucht die Gleichverteilung der Bitwerte 0 und 1 in einer Bitfolge und dient somit zur Untersuchung der Schiefe am Arbeitspunkt des Zufallszahlengenerators. Zusätzlich ist dies einer der Tests, der als Anlauf- und Onlinetest (siehe Abschnitt 5.2) innerhalb des Zufallszahlengenerators für dessen Funktionsprüfung eingesetzt wird [7].

Teststatistik

Bei diesem Test wird die Anzahl N_1 der Bitwerte 1 aus einer Bitfolge der Länge N bestimmt. Daraus wird die Testgröße

$$S = \frac{N_1 - (N - N_1)}{\sqrt{N}} \tag{5.1}$$

berechnet, die für $N \gg 1$ normalverteilt ist. Der p-Wert (siehe Anhang A.1.1), der die Wahrscheinlichkeit angibt, dass ein idealer Zufallszahlengenerator den beobachteten oder einen extremeren Wert annimmt, wird durch

$$p = \operatorname{erfc}(|S|/\sqrt{2}) \tag{5.2}$$

bestimmt. Als Signifikanzniveau wird $\alpha = 0.01$ gewählt, das heißt die Nullhypothese wird angenommen, sofern $p > \alpha$ ist.

Ergebnis

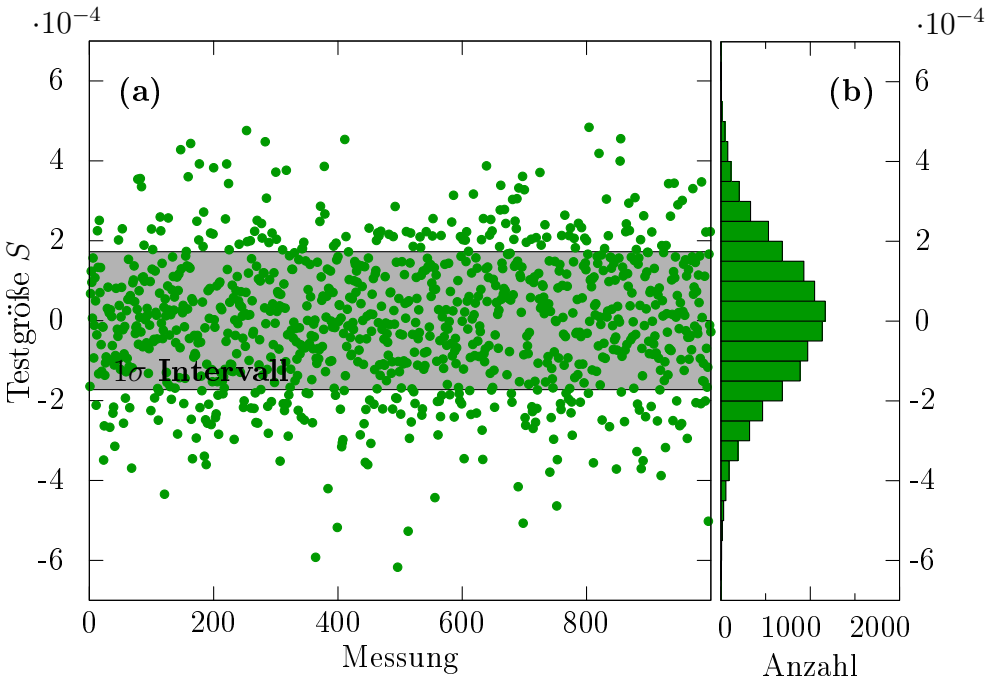


Abbildung 5.4: Messwerte des Monobit-Testparameters S: Statistik über 10^4 8 Mbit lange Zufallszahlfolgen **(a)**. Die statistische Streuung dieses Parameters ist in Form des $1\,\sigma$-Intervalls gekennzeichnet. Aufgrund der großen Anzahl der Messwerte ist in dieser Abbildung nur jeder zehnte Punkt dargestellt. Ein Histogramm dieser Messwerte verdeutlicht die statistische Streuung **(b)**.

Beschreibung mittlere Zählrate	Bias B (Dateigröße 1000 MByte)	Kuiper-Test p-Wert
$\mu_r = 1.43$	$5.2 \cdot 10^{-6}$	0.388083
$\mu_r = 1.40$	$1.1 \cdot 10^{-3}$	0.000000

Tabelle 5.1: Das Resultat des Kuiper Tests angewendet auf die Ergebnisse des Monobittests in Abbildung 5.4.

Zur Veranschaulichung dieses Tests werden nicht nur Zufallsbits untersucht, die bei einer mittleren Photonenzahl von $\mu_r = 1.43$ aufgenommen wurden,

sondern es wird eine zweite Zufallsdatei mit einer mittleren Photonenzahl von $\mu_r = 1.40$ aufgenommen, bei der eine Schiefe in den Zufallsbits vorliegt. Um die Aussagekraft dieses Tests zu erhöhen, werden 10^4 unabhängige Monobit-Tests jeweils auf einer Bitlänge $N = 8$ Mbit[2] durchgeführt und anschließend die Verteilung der daraus gewonnenen p-Werte mithilfe eines Kuiper Tests [79] untersucht (siehe Anhang A.3). Die Testgröße S ist in Abbildung 5.4 dargestellt. Zudem ist die Verteilung der p-Werte in Abbildung 5.5 gezeigt.

Die resultierenden p-Werte des Kuiper-Tests für die beiden Zufallsdateien sind in Tabelle 5.1 gegenübergestellt.

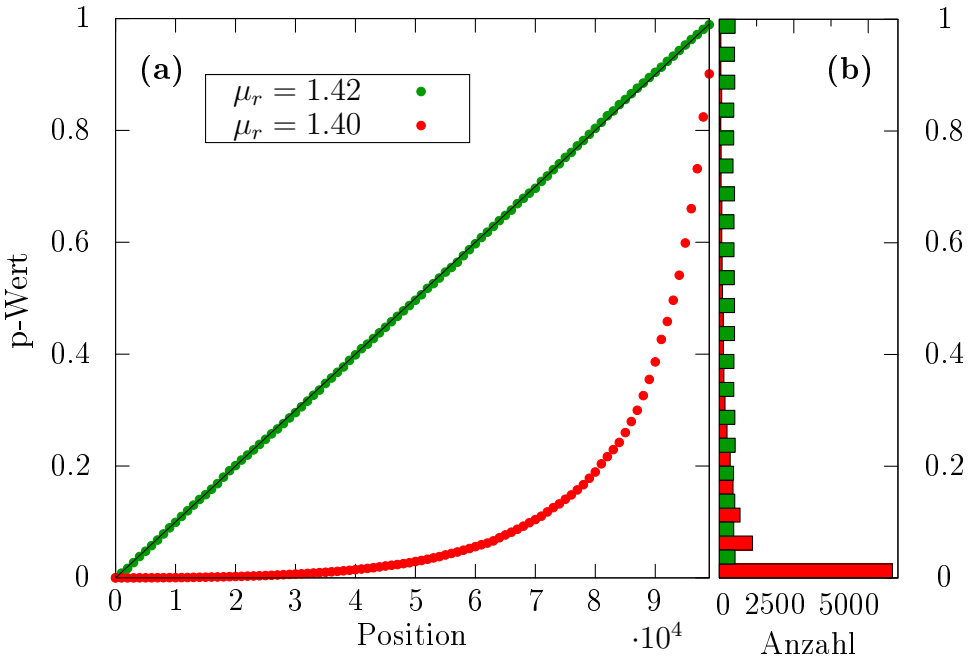


Abbildung 5.5: Resultate des Monobit-Tests angewendet auf 10^4 einzelne Zufallsfolgen der Länge 8 Mbit. Aufgetragen sind in Abbildung **(a)** die p-Werte der einzelnen Tests nach aufsteigender Sortierung des Datensatzes. Rot gekennzeichnet sind die p-Werte für die Zufallszahlen aufgenommen bei $\mu_r = 1.40$, die einen Bias von $1.1 \cdot 10^{-3}$ aufweisen. Die grünen Punkte sind die Werte für die gleichverteilte Zufallsfolge, die bei $\mu_r = 1.43$ aufgenommen wurde. Aufgrund der großen Anzahl der Messwerte ist nur jeder zehnte Punkt dargestellt. In der rechten Abbildung **(b)** ist ein Histogramm dieser beiden Kurven über alle Datenpunkte zu sehen.

[2]Mbit $= 1024 \cdot 1024$ Bit

Weisen die Zufallszahlen eine kleine Schiefe auf, erkennt man bei der Auswertung der p-Werte des Monobit-Tests in Abbildung 5.5 einen deutlichen Unterschied in der Verteilung der p-Werte. Zu beachten bleibt, dass die Durchführung eines einzelnen Monobit-Tests auch bei beiden Messungen zu p-Werten oberhalb des Signifikanzniveaus führen konnte und somit ein einzelner Test im Rahmen der gemessenen Daten als bestanden gelten würde. Die Durchführung dieses zweistufigen Tests ergab jedoch ein eindeutiges Ergebnis. Im Rahmen der gemessenen Daten wies der ZZG im Bezug auf den Monobit-Test am Arbeitspunkt von $\mu_r = 1.43$ keine Auffälligkeiten auf.

5.3.2 Autokorrelation

Nach der Analyse der Daten bezüglich der Gleichverteilung der Bits, werden in diesem zweiten Test Korrelationen zwischen Bitwerten untersucht.

Teststatistik

Der Test besteht in der Messung und Berechnung des Autokorrelationskoeffizienten [71] für verschiedene Bitabstände (siehe Gleichung (3.22)).

$$SCC_l = \frac{\sum_{k=1}^{N-l}(x_k - (B+0.5))(x_{k+l} - (B+0.5))}{\sum_{k=1}^{N}(x_k - (B+0.5))^2} \tag{5.3}$$

Die statistische Standardabweichung ist gegeben durch

$$\sigma_{SCC} = \frac{1}{\sqrt{N}} \tag{5.4}$$

woraus der p-Wert dieses Tests hergeleitet werden kann

$$p = \mathrm{erfc}(|SCC_l|/\sqrt{8}) \tag{5.5}$$

Ergebnis

Zuerst werden die Autokorrelationskoeffizienten mit dem Abstand $l = 1$ wieder aus 10^4 einzelnen Zufallsfolgen mit einer Länge von jeweils 8 Mbit berechnet. Diese Werte sind in Abbildung 5.6 dargestellt. Die statistische Standardabweichung ist ebenfalls gekennzeichnet. Zur weiteren Analyse wird die Verteilung der p-Werte der Autokorrelationskoeffizienten einem Kuiper-Test unterzogen.

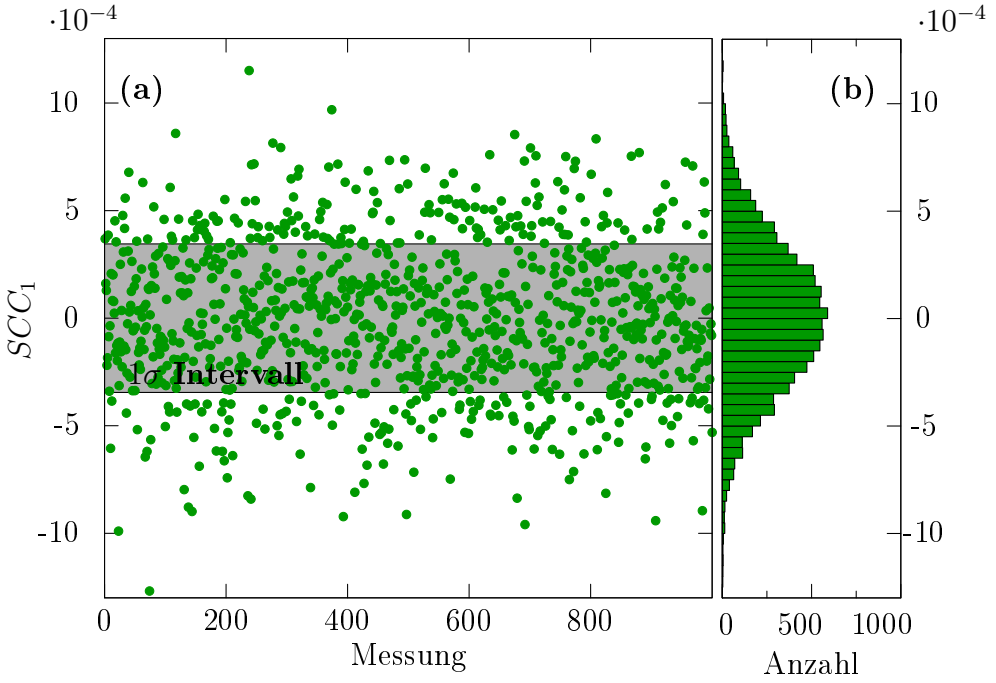


Abbildung 5.6: Autokorrelationskoeffizient mit einem Bitabstand $l = 1$. Die Berechnung erfolgte an aufeinanderfolgenden 8 Mbit langen Zufallsfolgen **(a)**. Aufgrund der großen Anzahl der Messwerte ist nur jeder zehnte Punkt dargestellt. Zur Veranschaulichung ist zusätzlich ein Histogramm dieser Autokorrelationswerte in Abbildung **(b)** aufgetragen.

Eine Anwendung des Kuiper Tests auf die Verteilung der Werte für den Autokorrelationskoeffizienten ergibt einen p-Wert von $p_{Kuiper} = 0.66$. Daher kann davon ausgegangen werden, dass die generierten Zufallszahlen keine Nächste-Nachbar-Korrelationen aufweisen.

Zusätzlich wurde der Autokorrelationskoeffizient mit Bitabständen von $l = 1 \ldots 100$ innerhalb einer 10^4 MByte Zufallsdatei berechnet. In Abbildung 5.7 ist das Ergebnis dargestellt. Die statistische Abweichung dieser Verteilung $\sigma = 3.45 \cdot 10^{-6}$, resultierend allein aus der endlichen Länge der Zufallsdatei, ist ebenfalls gekennzeichnet.

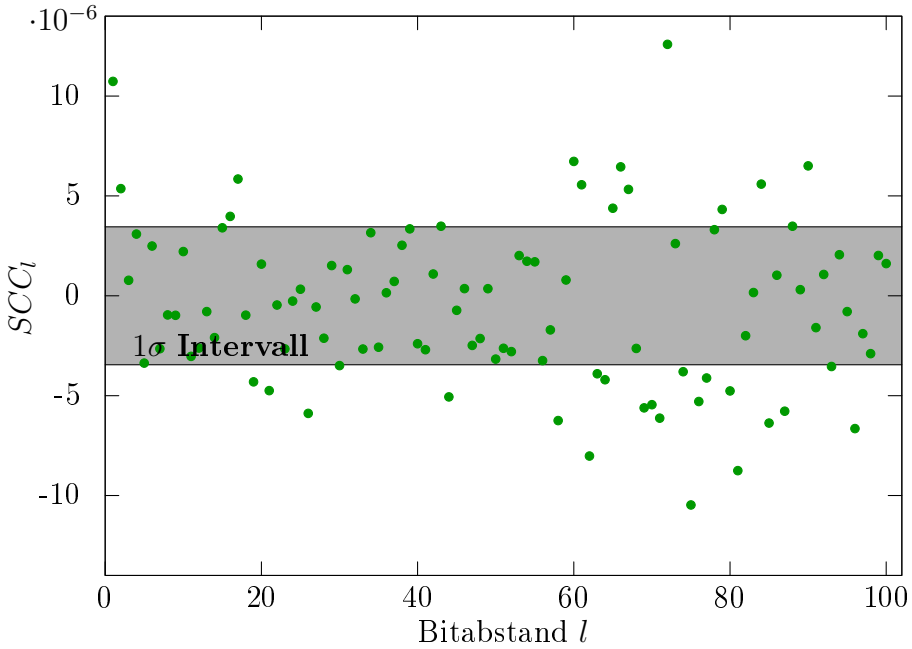


Abbildung 5.7: Der Autokorrelationskoeffizient in Abhängigkeit des Abstands l zwischen den Bits. In diesem Experiment wurden 10^4 MByte Zufallszahlen untersucht. Die statistische Abweichung ist mit $\sigma = 3.45 \cdot 10^{-6}$ gekennzeichnet.

In Abbildung 5.7 können keine signifikanten Bitkorrelationen erster Ordnung in der untersuchten Zufallsfolge identifiziert werden. Aus der theoretischen Beschreibung 3.5 abgeleitete Nächste-Nachbar-Korrelationen können mit den untersuchten Zufallsdateien nicht gefunden werden. Für eine statistische Signifikanz derartiger Korrelationen müßten Zufallsfolgen > 3 TByte analysiert werden.

5.3.3 Test auf gleichbleibende Bitfolgen (Runs)

Dieser Test untersucht die Zufallszahlen nach der Häufigkeit von gleichbleibenden Bitsequenzen [78]. Dazu wird die Anzahl der Vorkommnisse von Zahlenkolonnen $X^k_{0/1}$ der Länge k ausschließlich bestehend aus den Bitwerten 0/1 bestimmt. Die Länge k wird beschränkt auf $k < 64$. Der Erwartungswert der Verteilung $X^k_{0/1}$ ist unter der Annahme gleichverteilter Zufallszahlen gegeben durch

$$E(X^k_{0/1}) = \left(\frac{1}{2}\right)^{k+2} \tag{5.6}$$

Auf diesen Daten wird ein χ^2-Test durchgeführt.

$$\chi^2_{0/1} = \frac{1}{N-1}\sum_{k=1}^{64}(X^k_{0/1} - E(X^k_{0/1}))^2 \tag{5.7}$$

Der p-Wert der χ^2-Verteilung ist gegeben durch

$$p_{0/1} = Q(64/2, \chi^2_{0/1}/2) \tag{5.8}$$

mit der regularisierten Gamma Funktion der unteren Grenze

$$Q(a,x) = \frac{1}{\Gamma(a)}\int_x^\infty t^{a-1}e^{-t}dt \tag{5.9}$$

Ergebnis

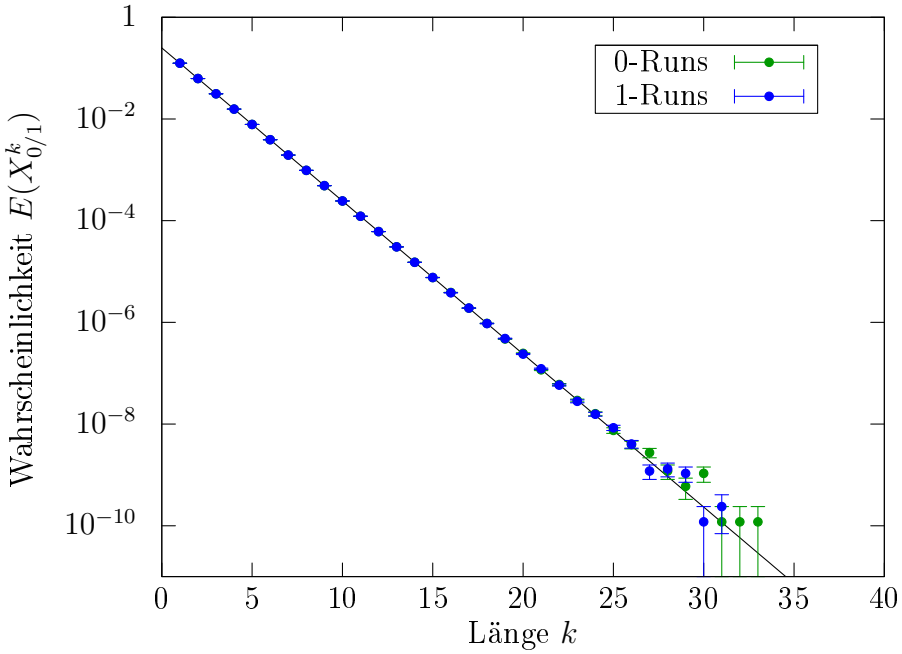


Abbildung 5.8: Die Wahrscheinlichkeit einer konstanten Bitfolge (mit den Werten 0 (grün) und 1 (blau) in Abhängigkeit von der Länge k. Diese Häufigkeiten wurden aus einer 1000-MByte-Zufallszahlenfolge berechnet. Werte der 0-Folgen sind auf Grund der Symbolgröße erst bei kleinen Wahrscheinlichkeiten $E(X^k_{0/1})$ sichtbar.

Zur Analyse wird eine 1000-MByte-Zufallsfolge verwendet, die am Arbeitspunkt des ZZG aufgenommen wurde. Die Wahrscheinlichkeit für das Auffinden einer gleichbleibenden Bitfolge ist in Abbildung 5.8 in Abhängigkeit der Länge dieser Folge dargestellt. Die theoretische Verteilung ist ebenfalls gekennzeichnet.

In Tabelle 5.2 sind die χ^2-Werte und die dazugehörigen p-Werte für die konstanten Bitfolgen 0 und 1 dargestellt.

Bitwert	χ^2-Wert	p-Wert
0	64.06	0.4745
1	47.64	0.9372

Tabelle 5.2: Test der gleichbleibenden Bitfolgen mithilfe des χ^2- Tests. Untersucht wurde eine 1000 MByte lange Zufallszahlenfolge.

Aus den gemessenen p-Werten kann man keinen signifikanten Unterschied zu einem idealen Zufallszahlengenerator feststellen. Der zweite Wert in Tabelle 5.2 mit 93% ist zwar in diesem Datensatz relativ hoch, zeigte jedoch bei wiederholten Messungen keine statistische Abweichung vom Erwartungswert.

5.3.4 Standardisierte Test-Bibliotheken

Die Wahl geeigneter Tests zur Analyse von Zufallszahlenfolgen ist im Allgemeinen sehr schwierig. Im vorherigen Kapitel wurden einzelne statistische Tests ausgewählt, die speziell für den untersuchten ZZG dessen zu erwartenden Schwachpunkte analysieren. Ganze Bibliotheken von statistischen Tests zur Analyse von Zufallsbitfolgen stehen zur Verfügung, die ursprünglich zum Test algorithmischer Zufallszahlengeneratoren entwickelt wurden. Dazu zählen die NIST Bibliothek [80], die Dieharder Bibliothek [81], die TestU01 Bibliothek [82] und ältere, wie zum Beispiel Diehard [83] und ENT [84]. In dieser Arbeit werden die in diesem Gebiet am häufigsten verwendeten Testbibliotheken NIST und Dieharder vorgestellt und auf Zufallszahlenfolgen des ZZG angewendet.

NIST

Ein vom „National Institute of Standards and Technology“ (NIST) entwickeltes Programm [80] untersucht Zufallsfolgen mit 16 unterschiedlichen Tests. Jeder einzelne dieser Tests wird 1000 Mal auf jeweils 1 MByte langen Abschnitten der Zufallszahlenfolge angewendet.

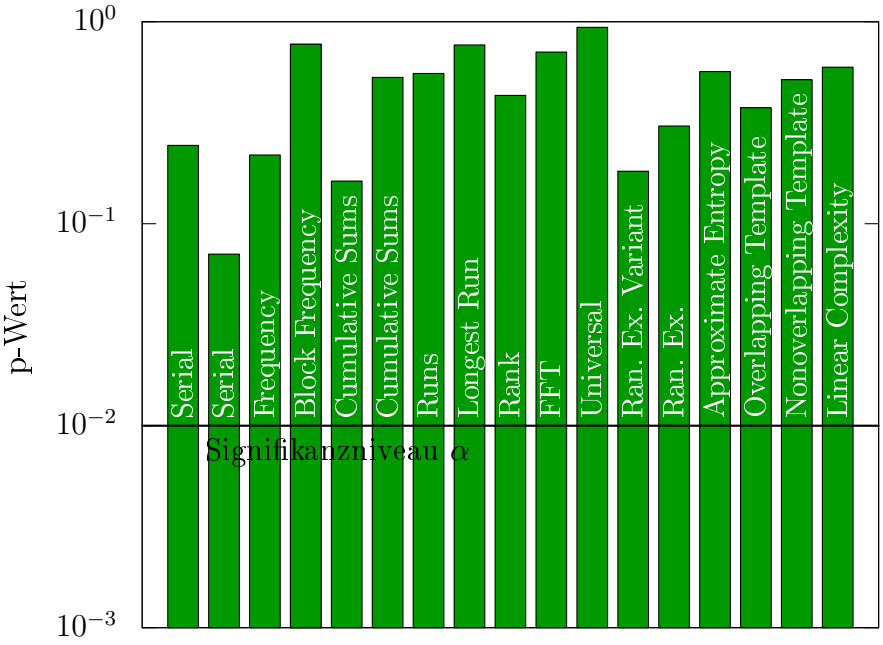


Abbildung 5.9: Abschließende p-Werte als Ergebnis eines χ^2-Tests auf die Verteilung der p-Werte der unterschiedlichen statistischen Test innerhalb der NIST Bibliothek angewendet auf 1000 MByte Zufallszahlen. In den Tests „Serial “und „Cumulative Sums “werden zwei unterschiedliche p-Werte berechnet.

Die so erhaltenen 1000 p-Werte sind für einen idealen ZZG gleichverteilt. Dies wird durch die Anwendung eines χ^2-Tests und die Berechnung eines abschließenden p-Werts getestet. Zur Berechnung und Bedeutung der p-Werte wird auf den Anhang A.1.1 verwiesen. Für die Berechnung und Bewertung dieser Resultate wird ein Signifikanzniveau von $\alpha = 0.01$ festgelegt.

In Abbildung 5.9 sind die abschließenden p-Werte für die 15 verschiedenen Tests graphisch aufgetragen. Der Bitabstand für den der „Serial“-Test ausgeführt wird, wird auf 2 gesetzt, da in diesem ZZG keine langreichweitigen Korrelationen zu erwarten sind. Nächste-Nachbar-Korrelationen können dagegen auftreten (siehe Abschnitt 3.5). Diese könnten mithilfe des Tests aufgedeckt werden. Die weiteren Einstellungen dieser Test-Bibliothek wurden auf die Standardwerte gesetzt [78]. Bei Tests mit mehr als zwei p-Werten als Resultat wurde nur der erste p-Wert aufgetragen. Die weiteren p-Werte dieser Tests befinden sich in Anhang B.1.

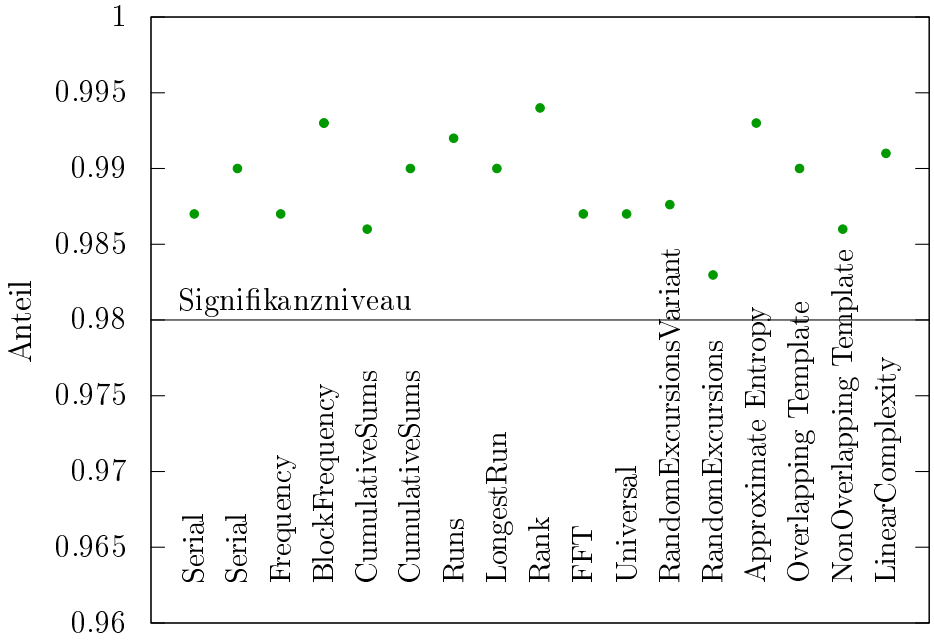


Abbildung 5.10: Der Anteil bestandener Tests innerhalb der NIST Bibliothek angewendet auf 1000 MByte Zufallszahlen.

Abbildung 5.9 zeigt, dass dieses Testprogramm die untersuchten Zahlenfolgen als zufällig erkennt, da alle p-Werte oberhalb des Signifikanzniveaus von $\alpha = 0.01$ liegen. Da die p-Werte gleichverteilt sind, dürfen einzelne Werte, wie zum Beispiel in Abbildung B.2, auch unterhalb des Signifikanzniveaus liegen. Wiederholte Messung zeigen jedoch keine Häufung nicht bestandener Tests.

Neben dem χ^2-Test, angewendet auf die p-Wert-Histogramme der einzelnen Tests, wird zusätzlich noch der Anteil der p-Werte angegeben, die oberhalb des Signifikanzniveaus liegen. Die statistische Grenze, innerhalb der dieser Anteil für Blöcke der Länge 1 MByte mit einer Wahrscheinlichkeit von $1 - \alpha = 99\%$ liegt, ist bei 0.98 (vergleiche [78]). Das Ergebnis dieses Tests ist in Abbildung 5.10 zusammengestellt. Auch hier liegen alle Werte innerhalb der Signifikanzgrenze.

Abschließend kann festgehalten werden, dass mithilfe der NIST Bibliothek keine Unterschiede der Zufallszahlen aus dem ZZG gegenüber denjenigen aus einem idealen Zufallszahlengenerator festgestellt werden konnten.

Dieharder

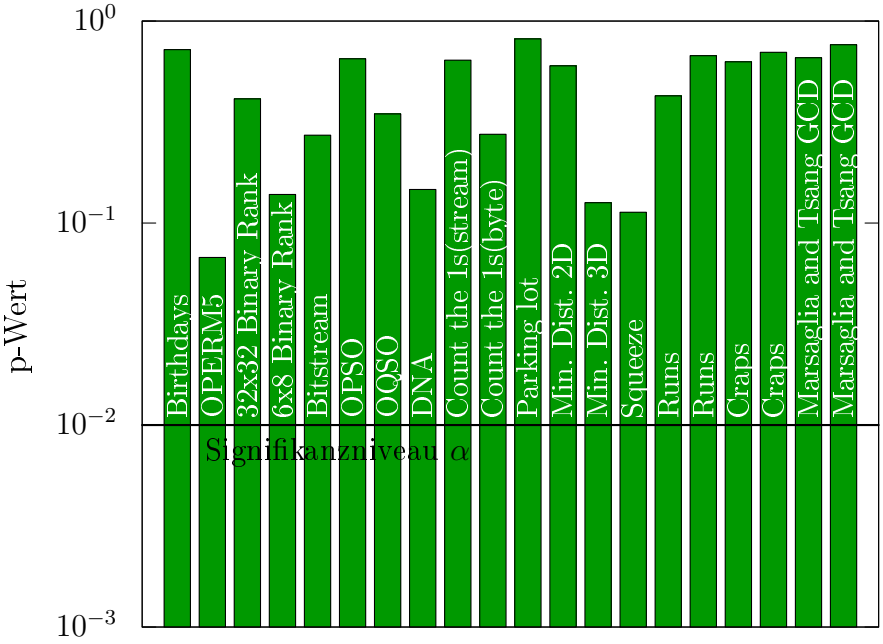


Abbildung 5.11: Resultate des Dieharder Programms angewendet auf eine 1000 MByte lange Zufallsbitfolge. Aus den Tests „Runs“, „Craps“ und „Marsaglia and Tsang GCD“ erhält man jeweils 2 einzelne p-Werte.

Eine weitere Bibliothek für einen Test von Zufallszahlen wird als „Dieharder“ [81] bezeichnet. Die Weiterentwicklung des ursprünglichen Diehard-Programms [83] beinhaltet 17 unterschiedliche Zufallstests. Die analysierte Datenmenge unterscheidet sich individuell bei den verschiedenen Tests, die jeweils 1000 mal durchgeführt werden (für Details wird auf die Anleitung von [81] verwiesen). Die resultierende Verteilung an p-Werten wird schließlich einem Kuiper-Test (siehe Anhang A.3) unterzogen.

Die resultierenden p-Werte sind in Abbildung 5.11 zusammengefasst. Außerdem sind innerhalb dieser Testbibliothek weitere Tests aus der NIST Bibliothek und weitere Tests, die mit „RGB “ bezeichnet werden, implementiert. Darin enthalten ist zum Beispiel der serielle Test der NIST Bibliothek, der mit Bitabständen von $2 \ldots 16$ durchgeführt wird. Die Ergebnisse dieser Tests sind in Anhang B.2 zusammengefasst.

Name	p-Wert	Bestanden
Birthday	0.7220	ja
Rank 32x32	0.0675	ja
Rank 6x8	0.4120	ja
Bitstream	0.2724	ja
OPSO	0.6504	ja
OQSO	0.3471	ja
DNA	0.1466	ja
Count 1s S	0.6406	ja
Count 1s B	0.2750	ja
Parking lot	0.8158	ja
2D-Sphere	0.6001	ja
3D-Sphere	0.1261	ja
Squeeze	0.1131	ja
Runs 1	0.4262	ja
Runs 2	0.6740	ja
Craps 1	0.6283	ja
Craps 2	0.7004	ja
Marsaglia 1	0.6581	ja
Marsaglia 2	0.7637	ja

Tabelle 5.3: p-Werte der einzelnen statistischen Tests innerhalb der Dieharder Bibliothek.

Auch in dieser Testbibliothek konnten keine Abweichungen relativ zu einem idealen ZZG beobachtet werden.

Zusammenfassend zeigen diese stochastischen Analysen, dass die Hypothese eines idealen ZZG angenommen werden muss. Auch ohne die Anwendung von Regularisierungsalgorithmen weisen die Zufallszahlen keine statistischen Auffälligkeiten auf. Dennoch muss abschließend festgestellt werden, dass das stochastische Modell und die experimentellen Messungen in Abschnitt 5.1 die entscheidendsten Abschnitte in der Beschreibung des ZZG sind.

Kapitel 6

Zusammenfassung und Ausblick

In der vorliegenden Arbeit wird ein Zufallszahlengenerator auf Basis eines quantenmechanischen Zufallsprozesses vorgestellt. Der Schwerpunkt liegt dabei auf einer detaillierten Beschreibung des Prozesses unter Berücksichtigung aller Einflüsse.

Grundlage des Zufallszahlengenerators [85] ist die Statistik, mit der Photonen von einer Leuchtdiode emittiert werden beziehungsweise mit der sie schließlich in einer Einzelphotondetektion registriert werden. In erster Linie kann diese Statistik aufgrund des inkohärenten Emissionsprozesses innerhalb des p-n Übergangs der Leuchtdiode mit Hilfe der Poissonverteilung beschrieben werden. Eine grundlegende, theoretische Analyse dieses Prozesses führt auf den „coulomb blockade effect“, infolge dessen die Elektronen beim Übergang in der Raumladungszone der LED einem regularisierenden Prozess unterworfen werden. Diese Regularisierung äußert sich im Prinzip in der Photonenstatistik als „antibunching“, das heißt einer verminderten Streuung der registrierten Photonenzahlen. Durch die enorme Abschwächung des Photonenstroms von ca. 80 dB bis zur Detektion mittels eines Photomultipliers kann dieser regularisierende Effekt jedoch vernachlässigt werden. Auch konnte in zahlreichen Tests kein Indiz dafür erkannt werden. Obwohl ein Photomultiplier keine intrinsische Totzeit nach der Detektion eines Photons aufweist, tritt durch die elektronische Nachverarbeitung des Detektionspulses aufgrund der endlichen Bandbreite elektronischer Komponenten eine Totzeit τ_d auf. Zusammen mit der Beschreibung der Leuchtdiode als Quelle sind die Auswirkungen dieser Totzeit auf die detektierte Photonenstatistik Grundlage eines stochastischen Modells des Zufallszahlengenerators.

Die Zufallszahlen werden aus der Anzahl detektierter Photonen innerhalb eines Zeitintervalls $T = 20$ ns ermittelt. Die Zuordnung der Bits 0/1 zu einer geraden/ungeraden Photonenzahl ermöglicht die Entstehung einer gleichverteilten Bitfolge. Dank der Totzeit bei der Detektion kann eine gleichverteil-

te Bitfolge schon bei einer Photonenzählrate von ca. 70 MHz erreicht werden. Dadurch konnte erstmals auf jedwede Nachbearbeitung der Zufallszahlen verzichtet werden. Die so erzeugten Bitfolgen wurden in statistischen Tests untersucht. Dabei wurden verschiedene Methoden angewendet und mit den theoretischen Werten einer idealen Zufallsfolge verglichen. Bei diesen Analysen mit Hilfe von Hypothesentests wurden neben den etablierten Testbibliotheken Dieharder und NIST auch eigene Tests entwickelt und angewendet. Die verwendeten stochastischen Tests zeigten im Rahmen der statistischen Varianz aufgrund der endlichen Länge keine signifikanten Unterschiede zu einer idealen Zufallsfolge.

Wie bereits einleitend erwähnt, ist die Sicherheit in Quantenkryptographiesystemen von der Zufälligkeit der verwendeten Quantenzustände abhängig. Der in dieser Arbeit entwickelte Zufallszahlengenerator soll zukünftig in das bestehende Kryptographiesystem der LMU München integriert werden. Die wachsende Geschwindigkeit, mit der solche Systeme aktuell arbeiten könnten, erfordert außerdem eine weitere Steigerung der Erzeugungsrate von Zufallszahlen basierend auf quantenmechanischen Prinzipien. Bei diesen Kryptographieexperimenten werden derzeit Raten > 1 Gbit/s [86] erreicht (durch eine begrenzte Rechenkapazität wird diese Rate nur kurzfristig erreicht). Aufgrund der leichten Skalierbarkeit des vorgestellten Zufallszahlengenerators mithilfe von Photomultiplier- Arrays[1] zusammen mit der Erzeugungsrate von 50 Mbit/s pro Bildpunkt sollten Geschwindigkeiten von > 1 Gbit/s mit den hier entwickelten Methoden realisierbar sein.

Nicht nur die Quantenkryptographie sondern auch moderne Verschlüsselungstechniken benötigen große Mengen an Zufallszahlen, die bisher mithilfe von algorithmischen Zufallszahlengeneratoren, manchmal in Kombination mit physikalischen Zufallszahlengeneratoren, erzeugt werden. Zukünftig werden weitere Entwicklungsschritte, wie zum Beispiel die Erhöhung der Geschwindigkeit oder eine behördliche Zertifizierung, wie sie bei kryptographischen Geräten üblicherweise vorgenommen wird, beim Bau quantenmechanischer Zufallszahlengeneratoren notwendig werden, um diese neuen Methoden in allen Zweigen der Kryptographie einsetzen zu können.

[1] derzeit sind einfache Arrays mit 8x8 Bildpunkten erhältlich

Anhang A

Mathematische Grundlagen

In diesem Abschnitt werden Methoden vorgestellt, die im Laufe der Analyse der Zufallszahlen in Abschnitt 5.3 benötigt werden. Zuerst wird dabei der Hypothesentest als Methode zur statistischen Auswertung eingeführt [77]. Abschließend werden die statistischen Tests χ^2- Anpassungstest und Kuiper-Kolmogorov-Smirnov Test vorgestellt.

A.1 Hypothesen Test

Statistische Tests überprüfen, ob eine Stichprobe, das heißt in diesem Fall eine Folge von Zufallszahlen, mit einer Hypothese in Einklang ist. Die sogenannte Nullhypothese H_0 besagt in dieser Analyse, dass ein idealer Zufallszahlengenerator vorliegt. Die alternative Hypothese H_1 schließt diese Nullhypothese aus [77].

H_0**: Nullhypothese:** idealer Zufallszahlengenerator

H_1**: alternative Hypothese:** kein idealer Zufallszahlengenerator

Zusätzlich wird eine Teststatistik S gewählt, die auf der Stichprobe berechnet wird $S = s_g$. Anschließend muss entschieden werden, ob aufgrund des Testresultats die Nullhypothese angenommen oder verworfen wird. Bei diesem Vorgehen können zwei unterschiedliche Fehlentscheidungen auftreten, die im Allgemeinen als Fehler erster und zweiter Art bezeichnet werden.

Fehler erster Art: Die Nullhypothese wird trotz Richtigkeit nur aufgrund eines statistisch möglichen Ausreißers verworfen. Zur Beurteilung der Hypothese wird ein Signifikanzniveau α für die Wahrscheinlichkeit eines Fehlers 1.Art eingeführt.

Fehler zweiter Art: Die Nullhypothese wird beibehalten, obwohl sie falsch ist.

Bei der Wahl des Signifikanzniveaus muss darauf geachtet werden, dass die Fehler erster und zweiter Art selten eintreten. Analog zu dem in den Testbibliotheken festgelegten Signifikanzniveau wird in dieser Arbeit $\alpha = 0.01$ gewählt.

A.1.1 p-Wert

Der p-Wert dient zur Bewertung eines statistischen Tests. Er gibt an mit welcher Wahrscheinlichkeit ein Ergebnis s_g oder ein noch extremeres Ergebnis eintritt unter Gültigkeit der Nullhypothese H_0. Man unterscheidet einseitige und beidseitige Tests.

$$p_{einsetig} = P(s \gtreqless s_g | H_0) \tag{A.1}$$

$$p_{beidseitig} = 2 \cdot min(P(s \geq s_g | H_0), P(s \leq -s_g | H_0)) \tag{A.2}$$

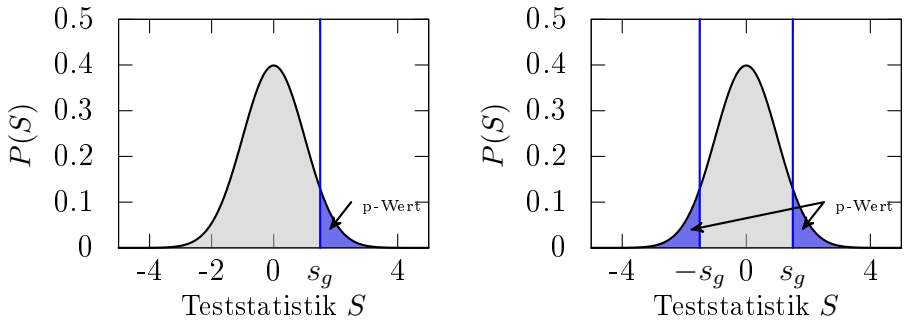


Abbildung A.1: Beispiel zur Berechnung des p-Wertes. Die Teststatistik S ist normalverteilt. Das Resultat der Stichprobe ist s_g. Bei einem einseitigen Test(links) und zweiseitigen Test(rechts) ist der p-Wert gegeben aus den blau gekennzeichneten Flächen.

In Abbildung A.1 ist gezeigt, wie sich der p-Wert für eine normalverteilte Teststatistik S für einen ein- und zweiseitigen Test ergibt. Ein Vergleich des p-Werts mit dem Signifikanzniveau α entscheidet über die Annahme oder Ablehnung der Nullhypothese.

$$p \geq \alpha \rightarrow \text{ Annahmebereich für } H_0$$
$$p < \alpha \rightarrow \text{ Ablehnungsbereich für } H_0$$

A.2 χ^2 Anpassungstest

Mit Hilfe des χ^2 Tests werden die Abweichungen einer gemessenen Verteilung S_g^i von einer theoretischen Verteilung S^i bewertet. Dazu werden diese Abweichungen zu einer Testvariable χ^2 folgendermaßen zusammengefasst.

$$\chi^2 = \sum_i^K \frac{(S_g^i - S^i)^2}{S^i} \tag{A.3}$$

Die Verteilung dieser Werte folgt einer χ^2-Verteilung [87] mit $K-1$ Freiheitsgraden (vergleiche Abbildung A.2).

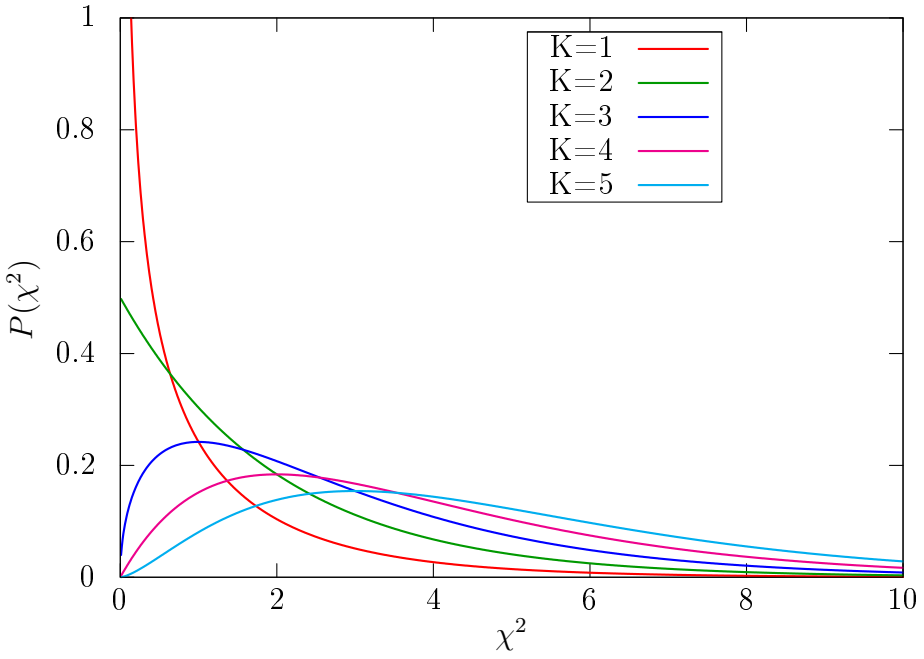


Abbildung A.2: χ^2-Verteilung mit K Freiheitsgraden.

Der p-Wert kann mithilfe der regularisierten Gamma Funktion der unteren Grenze

$$Q(a,x) = \frac{1}{\Gamma(a)} \int_x^\infty t^{a-1} e^{-t} dt \tag{A.4}$$

berechnet werden:

$$p = Q(K/2, \chi^2/2). \tag{A.5}$$

In der vorliegenden Arbeit wird dieser Test in Abschnitt 5.3.3 verwendet, um die diskrete Verteilung der Anzahl gleichbleibender Bitfolgen mit der

theoretischen Verteilung zu vergleichen. Außerdem findet dieser Test Anwendung in der NIST-Bibliothek zur Überprüfung der Histogramme der p-Werte auf deren Gleichverteilung.

A.3 Kuiper-Kolmogorov-Smirnov-Test

Der Kuiper-Kolmogorov-Smirnov Test [79] bewertet die maximale Abweichung einer gemessenen Verteilung $S_g(x)$ von einer theoretischen Verteilung $S(x)$.

$$D_+ = max_{-\infty<x<\infty}(S_g(x) - S(x)) \tag{A.6}$$
$$D_- = max_{-\infty<x<\infty}(S(x) - S_g(x)) \tag{A.7}$$

Die Kuiper Teststatistik V ist definiert als:

$$V = D_+ + D_- \tag{A.8}$$

Der p-Wert für einen gemessenen Wert V_g ist gegeben [88] durch

$$p(V > V_g) \approx Q_{KP}([\sqrt{N} + 0.155 + \frac{0.24}{\sqrt{N}}] \cdot V] \tag{A.9}$$

mit

$$Q_{KP}(\lambda) = 2\sum_{i=1}^{\infty}(4i^2\lambda^2 - 1)e^{-2i^2\lambda^2} \tag{A.10}$$

Ein Vorteil dieses Tests ist dessen Unabhängigkeit von der zugrundeliegenden theoretischen Verteilung. Die meisten statistischen Tests benötigen als theoretische Verteilung eine Normalverteilung. Andererseits muss eine kontinuierliche Wahrscheinlichkeitsverteilung $S_g(x)$ existieren.

Dieser Test findet Anwendung in dieser Arbeit, für die Untersuchung auf Gleichverteilung von p-Werten. Auch in der Dieharder-Bibliothek wird diese Methode angewendet, um diese Gleichverteilung zu analysieren.

Anhang B

Test Bibliotheken

Aufgrund der Vielzahl an Ergebnissen innerhalb der Testbibliotheken werden an dieser Stelle die in der Beschreibung der Testbibliothek fehlenden Resultate der Untersuchung der Zufallszahlen zusammengefasst. Die Details der Analyse finden sich in den jeweiligen Kapiteln in Abschnitt 5.3.

P-Werte, die unterhalb des Signifikanzniveaus liegen werden rot gekennzeichnet. Da die p-Werte gleichverteilt sind, ist das Auftreten von Werten unterhalb des Signifikanzniveaus kein Zeichen einer nicht zufälligen Zufallszahlverteilung sondern bestätigt diese zusätzlich.

B.1 NIST

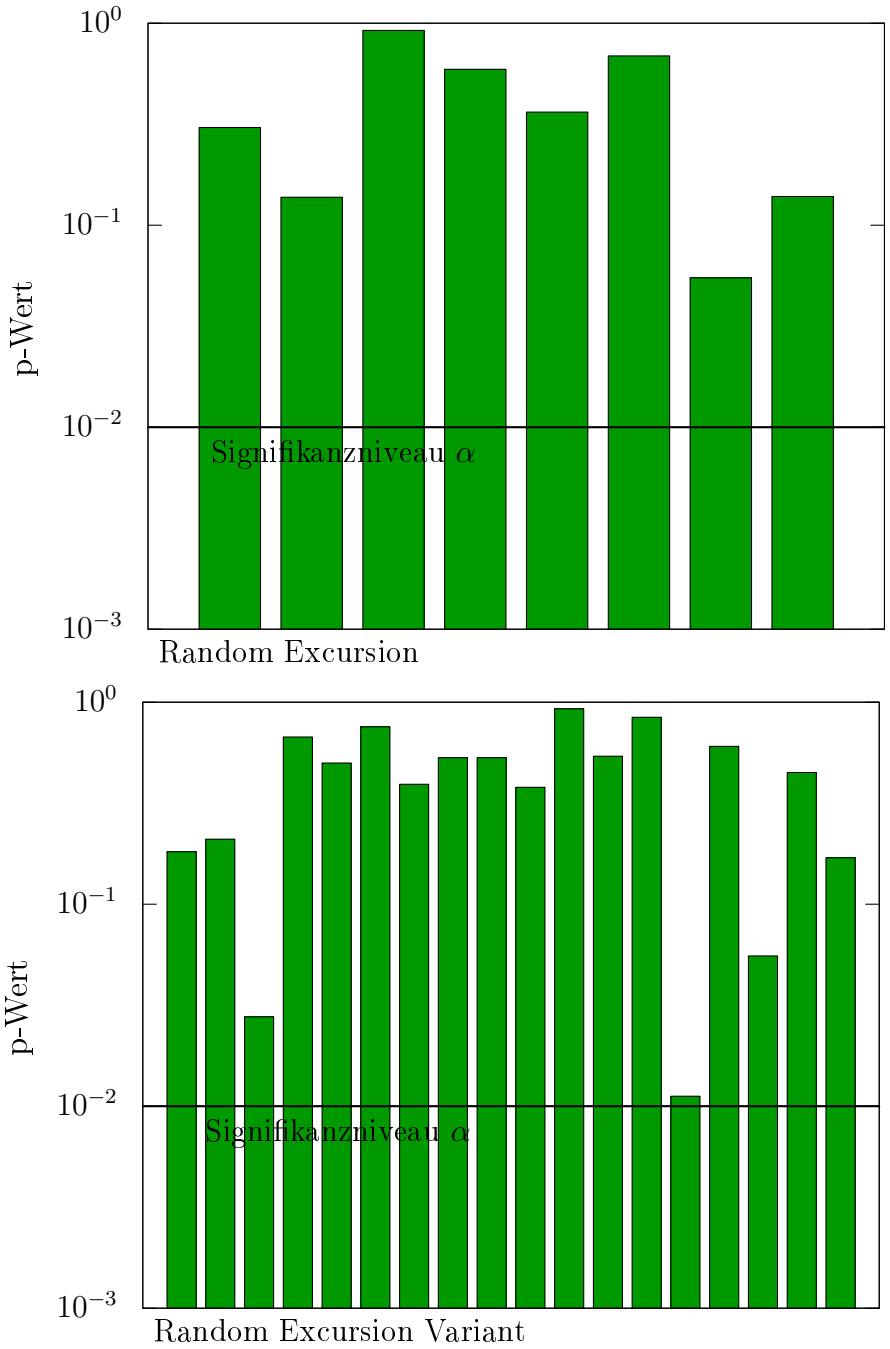


Abbildung B.1: Alle p-Werte des Random Excursion Tests (oben) und des Random Excursion Variant Tests (unten) der Nist Testbibliothek.

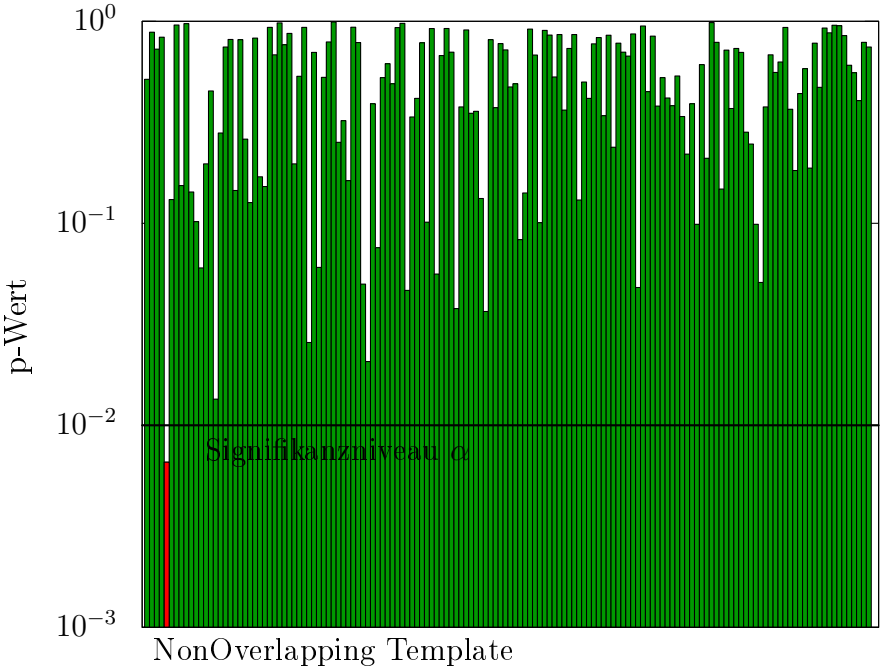


Abbildung B.2: Alle p-Werte des NonOverlapping Template Tests der Nist Testbibliothek.

B.2 Dieharder

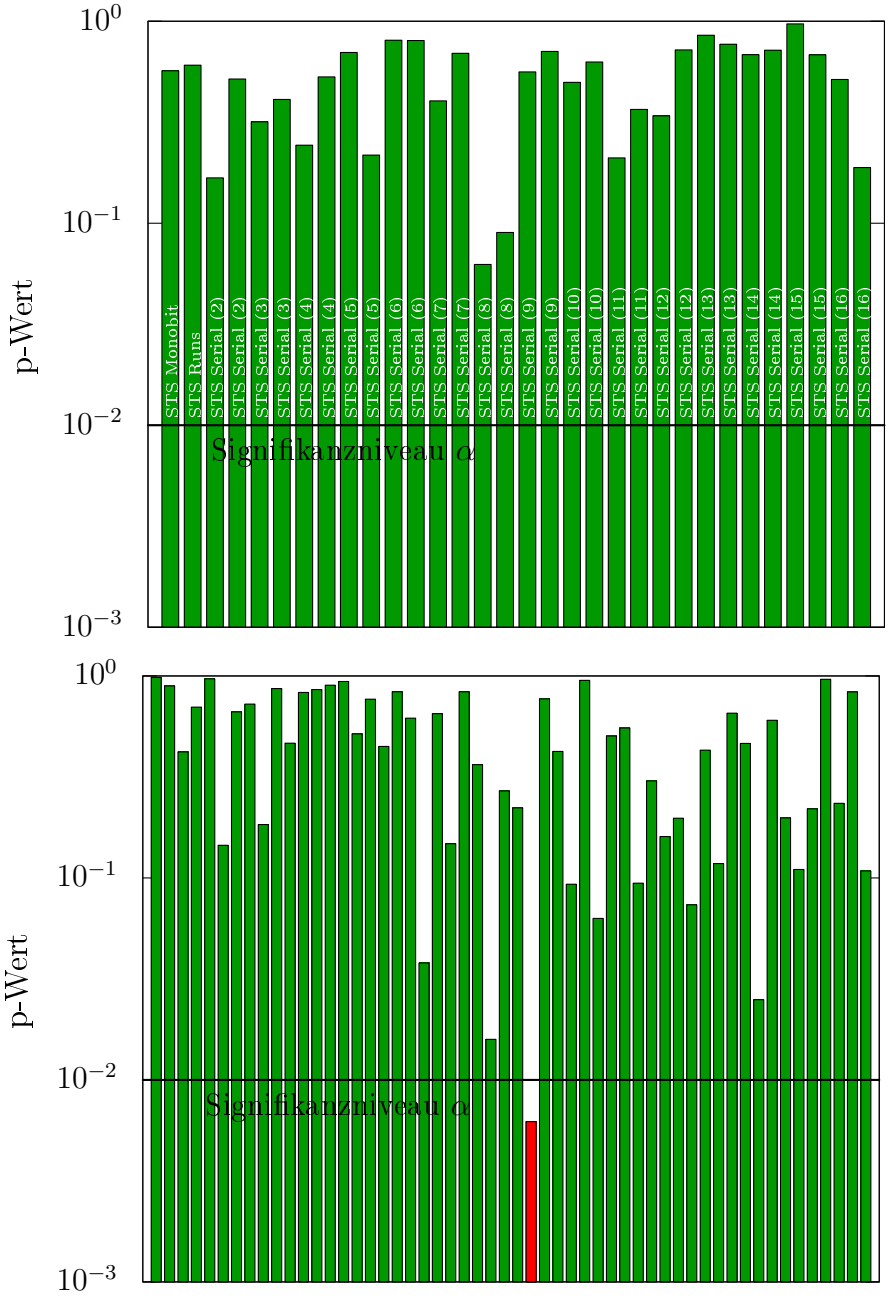


Abbildung B.3: Alle p-Werte der statistischen Tests, die aus der NIST Bibliothek in die Dieharder Bibliothek portiert worden sind (oben) und die Resultate der RGB“- Tests (unten).

Abbildungsverzeichnis

Tabellenverzeichnis

Publikationen

Publikationen im Zusammenhang mit dieser Arbeit:

- Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km
  T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, Ch. Kurtsiefer, J.G. Rarity, A. Zeilinger and H. Weinfurter,
  Physical Review Letters 98, 010504 (2007).

- Entanglement-based Quantum Communication over 144 km
  R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fürst, M. Meyerburg, J.G. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger,
  Nature Physics 3, 481-486 (2007).

- The SECOQC quantum key distribution network in Vienna
  M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden and A. Zeilinger,
  New Journal of Physics 11, 075001 (2009)

- Information leakage via side channels in freespace BB84 quantum cryptography
  S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier and H. Weinfurter,
  New Journal of Physics 11, 065001 (2009)

- High Speed Optical Quantum Random Number Generation.
  M. Fürst, H. Weier, S. Nauerth, D.G. Marangon, and H. Weinfurter,
  Optics Express 18:13029, 13037 (2010).

Literaturverzeichnis

[1] L. Dorrendorf, Z. Guttermann, and B. Pinkas. Cryptanalysis of the random number generator of the windows operating system. Cryptology ePrint Archive, Report 419, 2007.

[2] Z. Gutterman, B. Pinkas, and T.h Reinman. Analysis of the linux random number generator. Cryptology ePrint Archive, Report 86, 2006. http://eprint.iacr.org/.

[3] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007.

[4] H. Weier, T. Schmitt-Manderbach, N. Regner, Ch. Kurtsiefer, and H. Weinfurter. Free space quantum key distribution: Towards a real life application. *Fortschritte der Physik*, 54:840–845, 2006.

[5] Ch. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity. Quantum cryptography: A step towards global key distribution. *Nature*, 419:450, 2002.

[6] W. Killmann and W. Schindler. A design for a physical rng with robust entropy estimators. *Lecture Notes in Computer Science*, 5154:146–163, 2008.

[7] W. Killmann and W. Schindler. A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators (v3.1)., 2001.

[8] P. L' Ecuyer. Random numbers for simulation. *Communications of the ACM*, 33(10):85–97, 1990.

[9] http://de.wikipedia.org/wiki/Linear_r%C3%BCckgekoppeltes_Schieberegister.

[10] P. Diaconis, S. Holmes, and R. Montgomery. Dynamical bias in the coin toss. *SIAM Review*, 49(2):211–235, 2007.

[11] C. S. Petrie and J. A. Connelly. A noise-based ic random number. *Circuits and Systems I: IEEE Transactions on Fundamental Theory and Applications*, 47:615–621, 2000.

[12] http://www.fdk.co.jp/cyber-e/pi_ic_rpg100.htm.

[13] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo. A high-speed oscillator-based truly random number source for cryptographic applications on a smart card ic. *Transactions on Computers, IEEE*, 52:403–409, 2003.

[14] J. G. Rarity, P. C. M. Owens, and P. R. Tapster. Quantum random-number generation and key sharing. *Journal of Modern Optics*, 41(12):2435–2444, 1994.

[15] W. Dultz, G. Dultz, E. Hildebrandt, and H. Schmitzer. Method for generating a random number on a quantum mechanics basis and random generator, 1999.

[16] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71(4):1675–1680, 2000.

[17] P. X. Wang, G. L. Long, and Y. S. Li. Scheme for a quantum random number generator. *Journal of Applied Physics*, 100:056107, 2006.

[18] O. Kwon, Y.-W. Cho, and Y.-H. Kim. Quantum random number generator using photon-number path entanglement. *Applied Optics*, 48(9):1774–1778, 2009.

[19] E. Hildebandt. *Quantenoptische Zufallsgeneratoren Methoden und Analysen*. PhD thesis, Johann Wolfang Goethe Universität Frankfurt am Main, 2002.

[20] Y. Peres. Iterating von neumann's procedure for extracting random bits. *Annals of Statistics*, 20(1):590–597, 1992.

[21] J. von Neumann. Various techniques used in connection with random digits. *National Bureau of Standards AMS*, 12:36–38, 1951.

[22] M. Stipcevic and B. M. Rogina. Quantum random number generator based on photonic emission in semiconductors. *Review of Scientific Instruments*, 78(4):045104, 2007.

[23] J. Walker. Hotbits: Genuine random numbers, generated by radioactive decay. http://www.fourmilab.ch/hotbits/.

[24] A. Alkassar, T. Nicolay, and M. Rohe. Obtaining true random binary numbers from a weak radioactive source. *Lecture Notes in Computer Science*, 3481:634–646, 2005.

[25] A. Figotin, I. Vitebskiy, V. Popovich, G. Stetsenko, S. Molchanov, A. Gordon, C. Quinn, and N. Stavrakas. Random number generator based on the spontaneous alpha-decay, 2004.

[26] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields. A high speed, postprocessing free, quantum random number generator. *Applied Physics Letters*, 93(3):031109, 2008.

[27] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat. Photon arrival time quantum random number generation. *Journal of Modern Optics*, 56(4):516–522, 2009.

[28] J. B. Alpeter, E. Jeffrey, and P. G. Kwiat. Quantum random number generator, 2006.

[29] N. Luetkenhaus, J. L. Cohen, and H.-K. Lo. Efficient use of detectors for random number generation, 2007.

[30] H.-Q. Ma, Y. Xie, and L.-A. Wu. Random number generation based on the time of arrival of single photons. *Applied Optics*, 44(36):7760–7763, 2005.

[31] J. Edelkind, I. M. Vitebskiy, A. Figotin, and V. Popovich. Random number generator based on directional randomness associated with naturally occurring random events, and method therefor, November 1999.

[32] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden. Optical quantum random number generator. *Journal of Modern Optics*, 47:595–598, April 2000.

[33] A. J. Martino and G. M. Morris. Optical random number generator based on photoevent locations. *Applied Optics*, 39(8):981–989, 1991.

[34] W. Wei and H. Guo. Bias-free true random-number generator. *Optics Letters*, 34(12):1876–1878, 2009.

[35] W. Wei, J. W. Zhang, T. Liu, and H. Guo. Quantum random number generator based on the photon number decision of weak laser pulses. http://arxiv.org/abs/0811.0082, 2008.

[36] C. H. Vincent. The generation of truly random binary numbers. *Journal of Physics E: Scientific Instruments*, 3(8):594–598, 1970.

[37] M. Gude. *Ein quasi-idealer Gleichverteilungsgenerator basierend auf physikalischen Zufallsphänomenen*. PhD thesis, RWTH Aachen, 1987.

[38] M. Gude. Concept for a high performance random number generator based on physical random phenomena. *Frequenz*, 39:187–190, 1985.

[39] S. Takeuchi and T. Nagai. Hich performance random pulser based on photon counting. *IEEE Transactions on Nuclear Science*, 33:946–949, 1986.

[40] H. Guo, W. Tang, Y. Liu, and W. Wei. Truly random number generation based on measurement of phase noise of laser. http://arxiv.org/abs/0908.2893, 2009.

[41] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Optics Letters*, 35(3):312–314, 2010.

[42] G. E. Katsoprinakis, M. Polis, A. Tavernarakis, A. T. Dellis, and I. K. Kominis. Quantum random number generator based on spin noise. *Physical Review A*, 77(5):054101, 2008.

[43] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[44] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by bells theorem. *Nature*, 464(7291):1021–1024, 2010.

[45] Ch. Gabriel, Ch. Wittman, D. Sych, R. Dong, W. Mauerer, U. Andersen, Ch. Marquardt, and G. Leuchs. A generator for unique quantum random numbers based on vacuum states. *to be published*, 2010.

[46] T. Symul, S. Assad, and P. K. Lam. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *to be published*, 2010.

[47] Martin Fürst. Bsi projekt qpn (quantenbasiertes private network) projekt nr. 664b. not published, 2008.

[48] Martin Fürst. Bsi projekt qrng (quantum random number generator); nachfolgeprojekt von qpn. not published, 2009.

[49] G. Vannucci and M. C. Teich. Computer simulation of superposed coherent and chaotic radiation. *Applied Optics*, 19(4):548–553, 1980.

[50] J. Kim, H. Kan, and Y. Yamamoto. Macroscopic coulomb-blockade effect in a constant-current-driven light-emitting-diode. *Physical Review B*, 52:2008, 1995.

[51] J. Kim and Y. Yamamoto. Theory of noise in p-n junction light emitters. *Physical Review B*, 55:9949, 1997.

[52] J. Kim, Y. Yamamoto, and S. Somani. *Nonclassical Light from Semiconductor Lasers and LEDs*. Springer Verlag, 2001.

[53] Ch. Kittel. *Einführung in die Festkörperphysik*, volume 7. Auflage. R. Oldenburg Verlag, 1988.

[54] A. Imamoglu and Y. Yamamoto. Nonclassical light generation by coulomb blockade of resonant tunneling. *Physical Review B*, 46:15982–15991, 1992.

[55] A. Imamoglu, Y. Yamamoto, and P. Solomon. Single-electron thermionic emission oscillations in p-n microjunctions. *Physical Review B*, 46:9555–9563, 1992.

[56] A. Imamoglu and Y. Yamamoto. Noise suppression in semiconductor p-i-n junctions: Transition from macroscopic squeezing to mesoscopic coulomb blockade of electron emission processes. *Physical Review Letters*, 70:3327, 1993.

[57] K. Tanaka, A. Higashi, H. Yuji, R. Masuyama, Y. Kadoya, and M. Yamanishi. Wideband sub-poissonian light generation in light-emitting diodes incorporating a heavily-doped active region. *Applied Physics Letters*, 81:3317, 2002.

[58] J. Abe, G. Shinozaki, T. Hirano, T. Kuga, and M. Yamanishi. Observation of the collective coulomb blockade effect in a constant-current-driven high-speed light-emitting-diode. *Journal of the Optical Society of America B*, 14:1295, 1997.

[59] R. Loudon. *The quantum theory of light.* Oxford University Press, third edition edition, 2000.

[60] H. A. Bachor and T. C. Ralph. *A guide to experiments in quantum optics.* Whiley-VCH Berlin, second edition, 2004.

[61] M. Fox. *Quantum Optics: An Introduction.* Oxford University Press, 2006.

[62] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields. High speed single photon detection in the near-infrared. *Applied Physics Letters*, 91:041114, 2007.

[63] Hamamatsu Photonics. *Photomultiplier Tubes: Basics and Application.* Hamamatsu Photonics K.K., third edition (3a) edition, 2007.

[64] J. W. Müller. Dead-time problems. *Nuclear Instruments and Methods in Physics Research*, 112:47–57, 1973.

[65] J. W. Müller. Some formulae for a dead-tim-distorted poisson process. *Nuclear Instruments and Methods in Physics Research*, 117:401–404, 1974.

[66] J. W. Müller. Generalized dead times. *Nuclear Instruments and Methods in Physics Research A*, 301:543–551, 1991.

[67] M. D. Srinivas. Dead time corrections to photon counting statistics i: Classical theory. *Pramana*, 17(3):203–216, 1981.

[68] M. D. Srinivas. Dead time corrections to photon counting statistics ii: Quantum theory. *Pramana*, 17(3):217–227, 1981.

[69] K. Omote. Dead time effects in photon-counting distributions. *Nuclear Instruments and Methods in Physics Research*, 293(3):582–588, 1990.

[70] J. Libert. Statistique de comptage: á propos d´une expérience récente. *Nuclear Intruments and Methods*, 126:589–590, 1975.

[71] D. E. Knuth. *The Art of Computer Programming (Seminumerical Algorithms)*, volume II. Addison Wesley, third edition, 2008.

[72] P. Elias. The efficient construction of an unbiased random sequence. *The Annals of Mathematical Statistics*, 43(3):865–870, 1972.

[73] P. A. Samuelson. Constructing an unbiased random sequence. *Journal of the American Statistical Association*, 63:1526–1527, 1968.

[74] M. Stipcevic, H. Skenderovic, and D. Gracin. Characterization of a novel avalanche photodiode for single photon detection in vis-nir range. *arXive.org*, page 1004.0441, 2010.

[75] Hamamatsu Photonics. Datenblatt photomultiplier h6779.

[76] P. Horowitz and W. Hill. *The Art of Electronics*. Camebridge University Press, second edition, 1989.

[77] Gopal K. Kanji. *100 Statistical Tests*. Sage Publications Ltd., third edition edition, 2006.

[78] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo. A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2008.

[79] N. H. Kuiper. Tests concerning random points on a circle. *Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen*, 63:38–47, 1962.

[80] J. Soto. Statistical testing of random number generators. http://csrc.nist.gov/rng/rng5.html, 1999.

[81] R. G. Brown. Dieharder test suite v3.29.4beta. http://www.phy.duke.edu/~rgb/General/dieharder.php, 2009.

[82] P. L'Ecuyer and R Simard. Testu01: A c library for empirical testing of random number generators. *ACM Transactions on Mathematical Software*, 33(4):22, 2007.

[83] G. Marsaglia. Diehard test suite. http://www.stat.fsu.edu/pub/diehard/, 1995.

[84] J. Walker. Ent pseudorandom sequence tester. http://www.fourmilab.ch/random/, 1985.

[85] M. Fürst, H. Weier, S. Nauerth, D.G. Marangon, and Weinfurter H. High speed optical quantum random number generation. *Optics Express*, 18:13029–13037, 2010.

[86] R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, H. Zbinden, and N. Gisin. Ghz qkd at telecom wavelengths using up-conversion detectors. *New Journal of Physics*, 8:32, 2006.

[87] I. N. Bronstein, K. A. Semendjajew, G. Musiol, and H. Mühlig. *Taschenbuch der Mathematik*. Harri Deutsch Verlag, 4. auflage edition, 1999.

[88] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery. *Numerical Recipies in Fortran 77: The Art of Scientific Computing*. Camebridge University Press, edition 2 edition, 1992.

Curriculum Vitae

Persönliche Daten:

Nachname:	Fürst
Vorname:	Martin Ignaz
Geburtsdatum:	19.02.1978
Geburtsort:	Neuburg a.d. Donau
Familienstand:	verheiratet, 1 Kind
Staatsangehörigkeit:	deutsch

Schulische Ausbildung:

1984-1988:	Grundschule Nassenfels
1988-1994:	Knabenrealschule Rebdorf mit Abschluss mittlere Reife
1994-1998:	Apian Gymnasium Ingolstadt mit Abschluss Abitur
1999-2005:	Studium Allgemeine Physik an der Technischen Universität München mit Abschluss Diplom
seit 2005:	Promotion an der Ludwig Maximilian Universität München

Berufliche Praxis:

1998-1999:	Zivildienst im Rettungsdienst des Bayerischen Roten Kreuzes in Ingolstadt
2005-2007:	Promotionsstelle an der Ludwig Maximilian Universität München
seit 2007:	Promotionsstelle bei der Firma qutools GmbH in München
seit 2009:	Promotionsstelle an der Ludwig Maximilian Universität München