IBB Ingenieur-Büro Bergmann, Sonnenweg 3, 15537 Grünheide, info@ibbergmann.org

BENUTZERHANDBUCH

des Physikalischen Zufallsgenerators PRG600

Version 1.0

Autor: **Frank Bergmann**

Letzte Änderung: **11.11.2017 17:03**

1 Inhaltsverzeichnis

2 Copyright

IBB Ingenieurbüro Bergmann

Sonnenweg 3

D-15537 Grünheide

Ausgabe vom 05.12.2014

Haftung

Bei der Erarbeitung dieser Dokumentation wurde größter Wert auf die Vollständigkeit und Richtigkeit des Inhalts gelegt. Es kann dennoch keine Garantie für die Vollständigkeit und Richtigkeit übernommen werden.

Für Hinweise zu dieser Dokumentation sind wir dankbar.

Hotline

Die Hotline des Herstellers erreichen Sie unter +49(0)172 308 6554.

Warenzeichen

MS Windows ist eingetragenes Warenzeichen der Microsoft Corp.

3 Bedeutung von Zufallszahlen

Schon seit Jahrzehnten stellt die auf den ersten Blick trivial erscheinende Aufgabe mittels Computer Zufallszahlen zu erzeugen sowohl MathematikerInnen als auch InformatikerInnen vor große Probleme. Obwohl Taschenrechner, Betriebssysteme und Programmiersprachen über entsprechende Zufallsfunktionen verfügen, konnte diese komplexe Problemstellung noch nicht zufrieden stellend gelöst werden und stellt somit auch heute noch einen aktuellen Forschungsgegenstand dar. Ein Computer ist und bleibt eine deterministische Maschine, dazu geschaffen, auf eine konkrete Eingabe eine definierte Ausgabe zu liefern.

Viele Bereiche der Informatik sind in steigendem Ausmaß auf Zufallszahlen angewiesen. Durch die zunehmende weltweite Vernetzung von Rechnern haben Sicherheitsaspekte in den letzten Jahren an Bedeutung gewonnen. Schutzmechanismen gegen unbefugten Zugriff auf vertrauliche Daten sowie zur Authentifizierung und Identifikation von Kommunikationspartnern spielen eine immer größer werdende Rolle. Kryptographische Verfahren wie symmetrische Verschlüsselungs-, Public-Key- und Signaturverfahren bieten Möglichkeiten, diese Sicherheitsrisiken zu verringern. Gerade diese kryptographischen Basismechanismen kommen heutzutage kaum noch ohne Zufallszahlen aus. Beinahe jedes Kryptosystem benötigt irgendwann geheime, nicht vorhersagbare Zufallszahlen. Ohne Zufallsgeneratoren gäbe es keine Kryptographie! Man denke nur an folgende, exemplarische Einsatzgebiete: Schlüssel- und Parametererzeugung für symmetrische und asymmetrische Verschlüsselungsverfahren, Authentifikationsprotokolle wie das Challenge-Response-Verfahren, digitale Signatur-Verfahren (z. B. DSA, ElGamal), Diffie-Hellman-ähnliche Protokolle zur Schlüsselverteilung sowie Verschlüsselungsverfahren (One-Time-Pad, Stromchiffren).

Die Güte der in Kryptosystemen verwendeten Zufallszahlen wirkt sich unmittelbar auf deren Sicherheit aus. Die gesamte Sicherheit z.B. der per Pseudozufall erzeugten geheimen Schlüssel hängt ausschließlich von der Anfangsinitialisierung ab. Ein schwacher Seed (geringe Entropie der Zufallsquelle wie Passwort, Timer-Register, Tastaturanschläge, Mausbewegungen usw.) ist im statistischen Ergebnis nicht erkennbar, aber ein effizienter Angriffspunkt der Kryptoanalysis.

In zahlreichen Publikationen wurden Verfahren für die Erzeugung echter Zufallszahlen veröffentlicht. Die meist in Einzelfertigung angebotenen Geräte sind sperrig, kostenintensiv und setzen Spezialkenntnisse bei der Einstellung der Parameter voraus. Ungenügende statistische Qualität wird oftmals durch Verknüpfung mit Pseudozufallszahlen kaschiert, ohne auf die negativen Folgen für den Einsatz in kryptografischen Systemen zu verweisen.

Dem angebotenen physikalischen Zufallszahlengenerator PRG600 liegt daher die Aufgabe zugrunde, die Limitierung des Standes der Technik zu überwinden und in kostengünstiger Weise eine einfache und stabile Generierung von echten Zufallszahlen in konstanter hoher statistischer Qualität zu ermöglichen. Da sich die Parameter der elektronischen Schaltung automatisch optimieren, ist die statistische Qualität auch bei Spannungsschwankungen und Temperaturänderungen konstant und erfüllt Anforderungen an einen idealen Zufallsgenerator. Statistische Untersuchungen zeigten bereits bei den Rohdaten keine nachweisbaren Abhängigkeiten der Zufallsbits und eine sehr hohe Entropie.

Zur Evaluierung der Ausgabedaten des PRG600 wurden umfangreiche statistische Tests durchgeführt. So wurden die Diehard-Test-Suite, die NIST-Test-Suite sowie ein weiterer statistische Test auf mehrere erzeugte Bitfolgen angewendet. Keine dieser Testfolgen konnte Unterschiede zu einem idealen Zufallszahlen-Generator aufzeigen.

4 PRG600

Der PRG600 ist vorzugsweise für den Einsatz in mobilen Applikationen entwickelt worden und wird in Applikationen mit Lötkelchen eingelötet. Mit diesem physikalischen Zufallsgenerator können beliebig viele kryptografisch sichere Zufallszahlen generiert werden. Ein synchrones Zweidraht-Interface (SPI) ermöglicht die einfache Einbindung des kleinen Moduls in proprietäre Applikationen. Grundlagen der Entwicklung waren ein stochastisches Modell, sowie die Vorschriften und Empfehlungen der Bundesnetzagentur (BNetzA) im „Algorithmenkatalog 2014". Demnach wurde der PRG600 für die Klasse PTG.3 entwickelt und besteht aus einer physikalischen Rauschquelle mit hoher Entropie und einer digitalen Nachbearbeitung mit Mayer-Einwegfunktionen.

Mit logischen Signaleingängen können die Ausgabegeschwindigkeit und die Stromaufnahme variiert werden. Eine permanente Überwachung des Rauschsignals und der statistische Qualität des digitalisierten Rauschsignals garantieren kryptografische sichere Zufallszahlen.

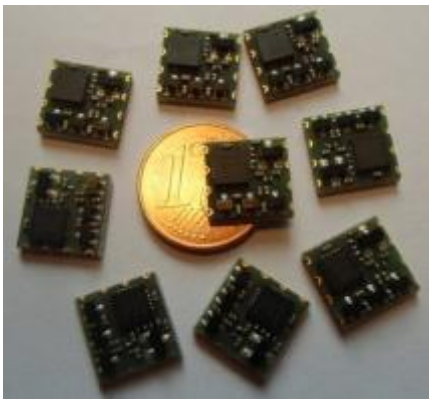


Abbildung: Exemplare des PRG600

In Deutschland hat die Regulierungsbehörde für IT-Sicherheit (Bundesnetzagentur BNetzA) folgende Verbindlichkeiten im „Algorithmenkatalog 2014" festgelegt:

„Für Zertifizierungsdienstanbieter wird die Verwendung von Zufallsgeneratoren der Funktionalitätsklassen *PTG.3* und DRG.4 im Grundsatz *ab 2015 verpflichtend* werden, sowohl allgemein bei der Erzeugung von Langzeitschlüsseln als auch bei der Erzeugung von Ephemeralschlüsseln."

Bemerkungen:

- Hybride Zufallszahlengeneratoren vereinen Sicherheitseigenschaften von deterministischen und physikalischen Zufallszahlengeneratoren.
- Hybride physikalische Zufallszahlengeneratoren der Klasse PTG.3 besitzen neben einer starken Rauschquelle eine starke kryptographische Nachbearbeitung mit Gedächtnis.
- PTG.3 stellt die stärkste Funktionalitätsklasse dar.

5 Technische Daten

Abmessungen:	10*10*2,0 mm
Versorgungsspannung:	3,3V (+/- 10%)
Stromaufnahme:	max. 3,5mA, im Sleep-Modus max. 15µA
Temperaturbereich:	funktionell und statistisch stabil von 0°C..+70°C
Schnittstellen:	Zweidraht-SPI-Interface als Master
Qualitätssicherung:	- Tot-Test zur Überwachung der Rauschquelle - Online-Test zur statistischen Überwachung des digitalisierten Rauschsignals - Abschaltung der Zufallsausgabe bei Ausfall der Rauschquelle oder unzureichender statistischer Qualität des digitalisierten Rauschsignals
Entropie:	>7,997 Bits/Byte (ermittelt aus dem digitalisierten Rauschsignal nach Shannon)
0/1-Verhältnis:	garantiert im Bereich 0,499..0,501 (> 100 KByte)
Lötanschlüsse:	Raster 2,54mm, vergoldet

6 Anschlussbelegung

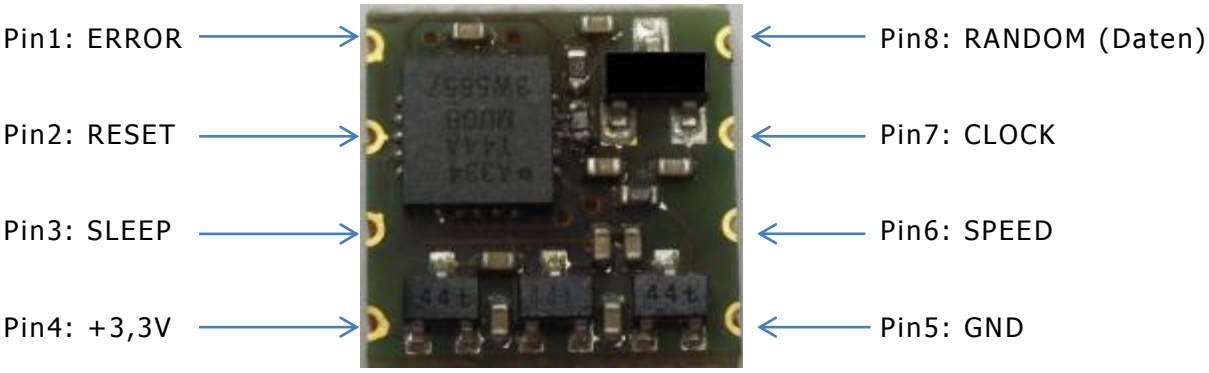


Abbildung: Anschlussbelegung des PRG600

7 Pin-Beschreibung

Pin	Signal	Richtung	Funktion
1	ERROR	Ausgang	Fehlermeldung, low-activ
2	RESET	Eingang	Modul rücksetzen, low-activ
3	SLEEP	Eingang	Reduzierte Stromaufnahme, low-activ
4	+3,3V	Stromversorgung	Normal: <3,5mA, Sleep-Modus: <15µA
5	GND	Bezugspotential	
6	SPEED	Eingang	Low: 4 Kbit/s, high: 40 Kbit/s
7	CLOCK	Ausgang	Daten gültig mit steigender Flanke
8	RANDOM	Ausgang	Zufallsdaten

8 Minimale Pin-Beschaltung

Minimalbeschaltung zur permanenten Ausgabe von Zufallsdaten mit 40 Kbit/s:

Pin4: +3,3V

Pin5: GND

Pin7: CLOCK

PIN8: RANDOM

Alle anderen Signale können unbeschaltet bleiben.

9 Abmessungen des PRG600

Die folgende Abbildung zeigt die Abmessungen des Moduls:

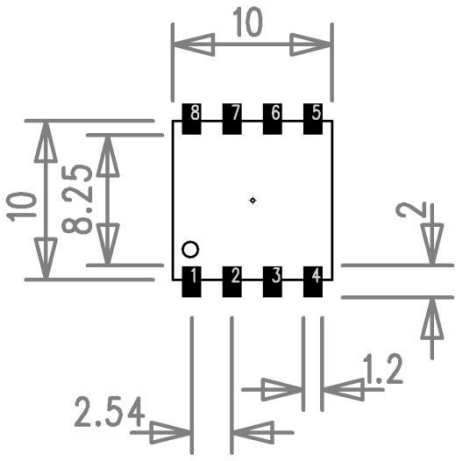


Abbildung: Abmessungen des PRG600

10 Stochastische Modell

Ein stochastisches Modell unterstützt Gutachten und Einschätzungen über die Qualität und Zuverlässigkeit eines Zufallsgenerators. Es beschreibt die Entropiequelle, die Verarbeitung des digitalisierten Rauschsignals, die kryptografische Nachbereitung und die Sicherheitsfunktionen zur Überwachung der Signalverarbeitung.

Das stochastische Modell des PRG600 wird in folgendem Schema verdeutlicht:

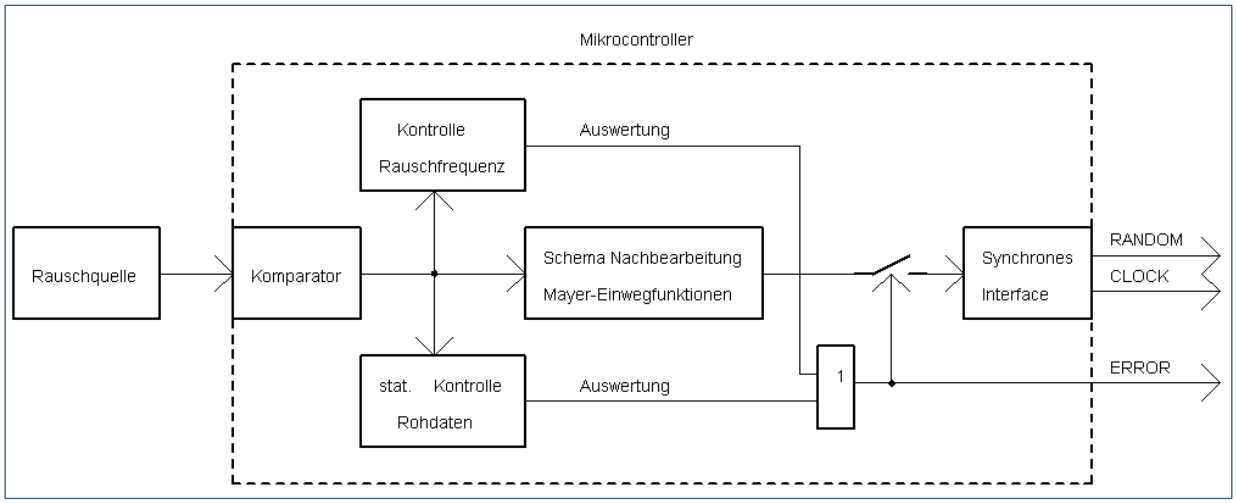


Abbildung: Stochastisches Modell als Schema

11 Prinzip der Rauscherzeugung des PRG600

Rauschen ist ein physikalisches Phänomen und stellt eine Störgröße mit breitem unspezifischem Frequenzspektrum dar. Dieses Frequenzspektrum besteht aus der Überlagerung mehrerer Schwingungen oder Wellen mit unterschiedlicher Amplitude und Frequenz beziehungsweise Wellenlänge. Diese Eigenschaften wurden erstmalig 1918 durch Walter Schottky beschrieben. Später wurde das thermische Rauschen experimentell durch John Bertrand Johnson verifiziert. Eine Modellvorstellung der spektralen Leistungsdichte des thermischen Rauschens erfolgte durch Harry Nyquist.

Das in diesem Zufallsgenerator verwendete 1/f-Rauschen bezeichnet ein Rauschen, dass mit steigender Frequenz in der Signalamplitude abnimmt, die Amplitudenverteilung ist umgekehrt proportional zur Frequenz (~ 1/f). Die verwendete Rauschquelle ist ein Transistor mit ausgeprägtem Avalanche-Effekt. Rauschen entsteht hier durch den Lawineneffekt (Avalancheeffekt) in der pn-Sperrschicht des Halbleiterbauelements.

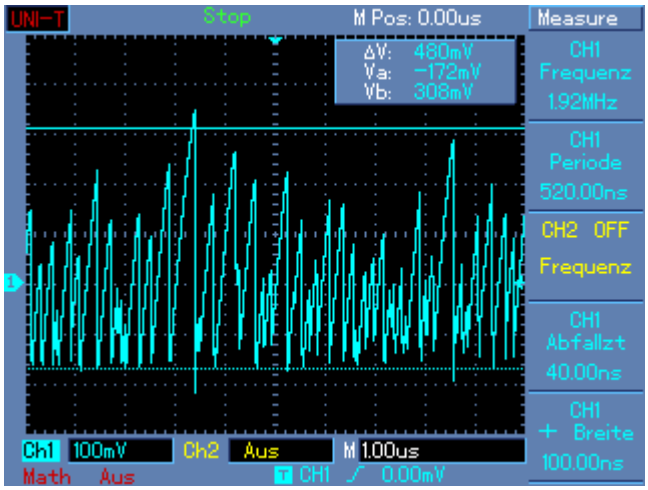


Abbildung: Rauschsignal des eingesetzten Transistors ohne Verstärkung

12 Generierung des Zufallssignals

Der als Rauschquelle eingesetzte Transistor kann reproduzierbar sehr hohe Rauschspannungen (>300mVss) bei einem breiten Rauschspektrum erzeugen, so dass keine Verstärkung erforderlich ist und der Signalpegel deutlich über dem Störpegel elektronischer Schaltungen liegt. Im Bild das Rauschsignal (blau) und das digitalisierte Zufallssignal (gelb). Diese Rauschquelle muss nicht ausgemessen werden, da sie, technologisch bedingt, immer gleiche Rauschamplituden und ein gleiches Frequenzspektrum erzeugt. Ursache des Rauschens ist ein ausgeprägter Avalanche-Effekt.

Zur Digitalisierung des generierten Rauschsignals wird ein integrierter Analog-Komparator des eingesetzten Mikrocontrollers verwendet. Die Referenzspannung wird aus dem Gleichspannungsanteil des Rauschsignals erzeugt.

Das Blockschaltbild zeigt wesentliche Komponente und Signale des PRG600:

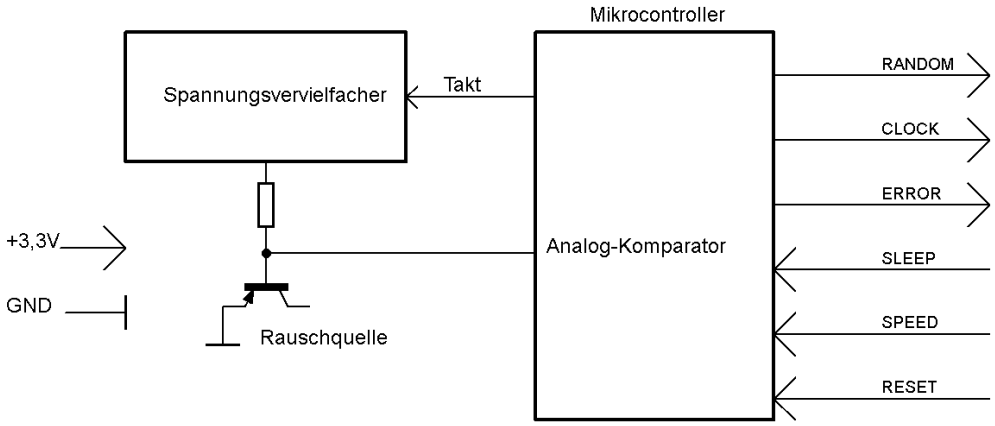


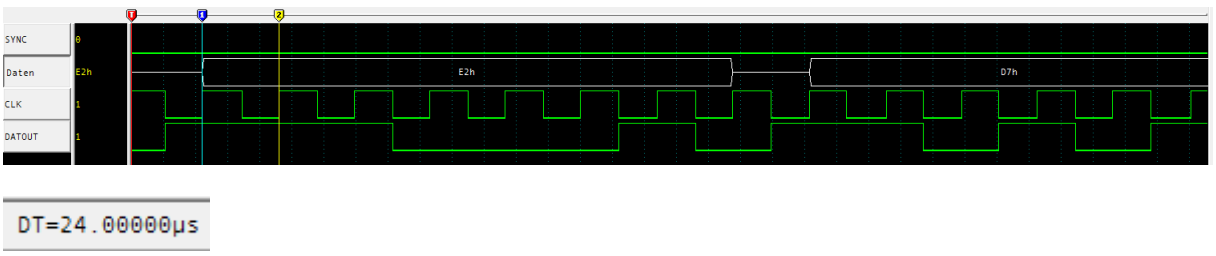
Abbildung: Blockschaltbild des PRG600

13 Signaturanalyse

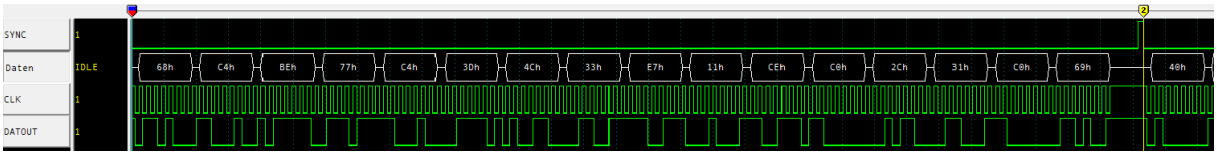
Im Folgenden werden Signaturanalysen der Datenausgabe und der Sicherheitsfunktionen erläutert. Dazu war es notwendig, in der Entwicklungs-Firmware Zusatzsignale zu generieren, um eindeutige Signalspiele zu demonstrieren.

13.1 Datenausgabe

Abgetastet werden die Zufallsdaten (*Datout*, bzw. in der Analyse als Byte-Werte mit *Daten*) immer mit der steigenden Flanke des Taktsignals (CLK). Das Intervall liegt bei einer Ausgabegeschwindigkeit von 40 Kbit/s bei 24µs. Da die Zufalls-Ausgabedaten statistisch gleichverteilt sind, ist vom Anwender keine Byte-Synchronisation erforderlich. Nur die Abtastung des Zufallssignals mit der steigenden Taktflanke bestimmt die Anzahl der benötigten Zufalls-Bits.



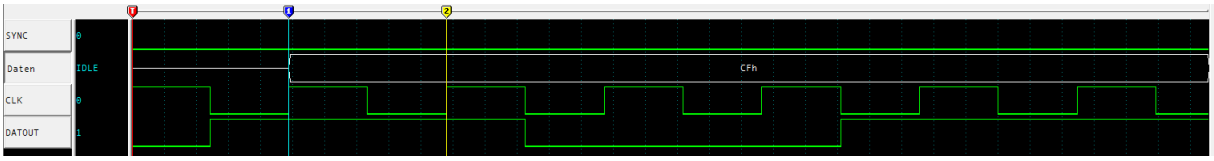
Das gleiche Signalspiel bei einer zeitlich erweiterten Darstellung:



DT=3.132500ms

Das Intervall eines Ausgabeblocks (16 Byte) nach Schema der kryptografischen Nachbearbeitung beträgt 3,1ms, ist aber nicht relevant im Kontext zur Erfassung der Ausgabedaten.

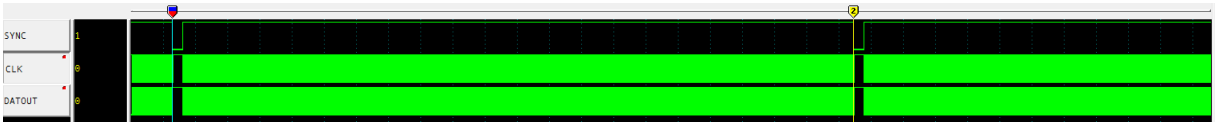
Die nächste Darstellung zeigt die Ausgabegeschwindigkeit mit 4,0 Kbit/s (Signal Speed low-activ).



DT=246.2500µs f=4.060914KHz

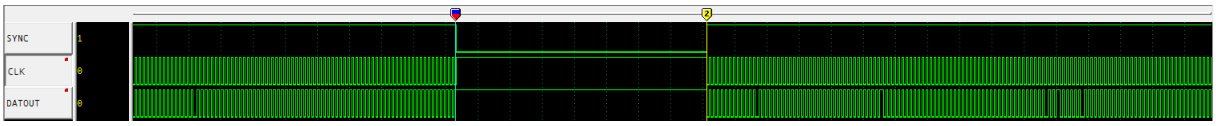
13.2 Online-Test

Signalanalyse des Online-Test pro Sekunde im Kontext zur Datenausgabe, diese ist während des Online-Test passiv. Das Signal SYNC reflektiert den Online-Test.



DT=1.057875s

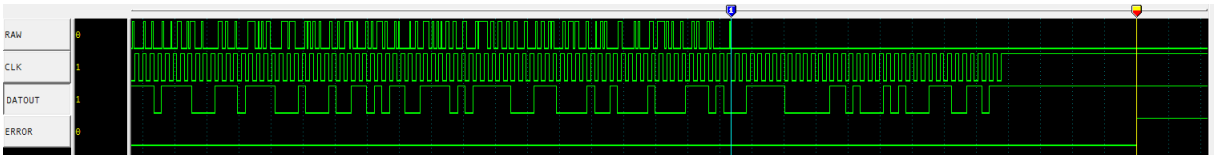
Der erfolgreiche Online-Test dauert 15,6 ms.



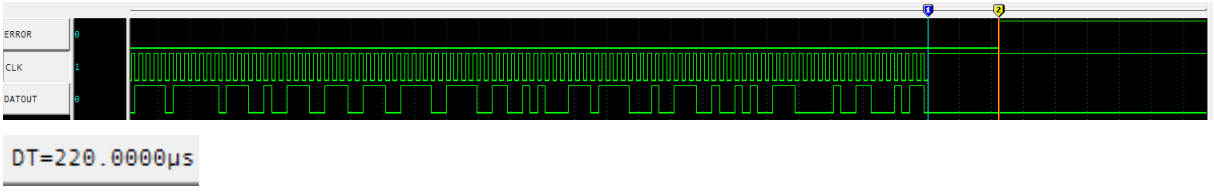
DT=15.62500ms

13.3 Fehlermeldung

Demonstriert wird der Ausfall des Rauschsignals: das ERROR-Signal ist invers (high-activ) dargestellt, in der Außenbeschaltung des Moduls ist es low-activ, das Signal „RAW" bildet das digitalisierte Rauschsignal ab. Durch Manipulation der Rauschquelle bricht das Rauschsignal zusammen und wird durch den Tot-Test oder Online-Test sicher detektiert:



Fehler im permanenten Online-Test: das ERROR-Signal ist am Ausgang des PRG600 low-activ



14 Entropie

Die Entropie der Zufallsrohdaten ist die entscheidende Eigenschaft eines Zufallsgenerators und sollte so hoch als möglich sein. Da der PRG600 keine Funktion zur Ausgabe von Zufalls-Rohdaten besitzt, wurde die Firmware des Mikrocontrollers in Laborversuchen modifiziert und mit verschiedenen Modulen die Entropie ausschließlich aus Rohdaten ermittelt. Dazu wurden jeweils 10Mbyte-Dateien generiert.

Folgende Entropiewerte (nach Shannon) der Rohdaten wurden für verschiedene Applikationen ermittelt:

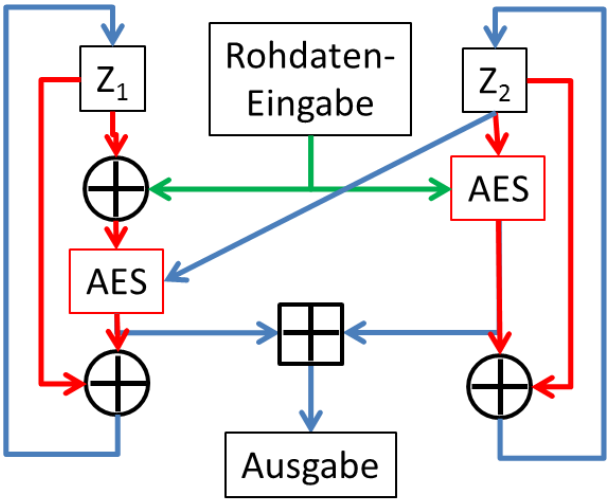
PRG600	Mittelwert 0/1	Entropie der Rohdaten
Modul 1	0.50399948	7.99963076
Modul 2	0.50329120	7.99974996
Modul 3	0.50348982	7.99971887
Modul 4	0.50285690	7.99981160
Modul 5	0.50412565	7.99960710

Die vollständigen Analysen der generierten Daten nach AIS31 sind auf der Internetseite des Autors verfügbar.

15 Schema der kryptografischen Nachbearbeitung

Auf Grund der sehr hohen Entropie des physikalischen Zufallsgenerators wurden die Funktionen für die Zufallsgenerierung für die Klasse PTG.3 (hybrider Zufallsgenerator) ausgelegt. Für diese Klasse können beliebig lange Zufallsfolgen generiert werden.

In der Klasse PTG.3 erfolgt die Nachbearbeitung der generierten Rohdaten mit Mayer-Einwegfunktionen mit folgendem Schema (rechtes Bild):



Diese Nachbereitung nutzt 2 Prinzipien des Entropiesammelns: das Aufxorieren der Rohdaten für z1 und die Glättung durch Aufxorieren des mit zufälligem Schlüssel verschlüsselten Zustands für z2. Beide Komponenten nutzen die Mayer-Einwegfunktion AES(k,s) xor k, um den vorangegangenen inneren Zustand zu schützen. Durch die XOR-Summe der Zwischenwerte kann nicht auf den inneren Zustand geschlossen werden.

Dadurch werden auch bei einem kurzzeitigen Ausfall oder Manipulation der Rauschquellen statistisch gleichverteilte Zufallsdaten ausgegeben.

16 Sicherheitsfunktionen

16.1 Tot-Test

Es ist ein Kontrollsystem installiert, welches das digitalisierte Rauschsignal am Anschluss des Mikrocontrollers überwacht. Unmittelbar vor *jeder* Block-Ausgabe (16 Byte) der nach Schema nachbearbeiteten Zufallsdaten wird eine Funktion aufgerufen, die folgende Aufgabe hat:

- Es wird die Zeit ermittelt die erforderlich ist, um vier wechselnde Flanken des digitalisierten Rauschsignals zu erfassen
- Wird nach 50µs (entspricht 40 KHz Rauschfrequenz) diese Bedingung nicht erfüllt, wird eine Fehlermeldung generiert, die zur sofortigen Einstellung aller Zufallsausgaben führt, das ERROR-Signal wird aktiviert
- Dieser Zustand ist nur ist nur durch einen sofort aktivierten erneuten Test oder PON aufzulösen
- Typische Zeiten, um die Bedingung zu erfüllen, sind 5..8µs

16.2 Permanenter Online-Test

Im permanenten Halbbytetest (zyklisch im Abstand von 1 Sekunde) zur Kontrolle der statistischen Qualität der Zufallsrohdaten werden zwei Kriterien überprüft:

- Sind die Werte innerhalb der statistischen Vorgaben, wird kein Fehler generiert
- Ist einer der 16 Werte im Halbbytetest gleich Null, wird von einem Totalausfall des digitalisierten Rauschsignals ausgegangen und jede Zufallsausgabe blockiert. Angezeigt wird dieser Zustand durch das ERROR-Signal (low-activ). Dieser Zustand kann nur durch PON oder den sofort wieder aktivierten Selbsttest mit positivem Ergebnis beendet werden.

Wird ein Fehler im Kontrollsystem festgestellt, wird der relevante Test solange wiederholt, bis ein positives Ergebnis ermittelt wird. Anschließend wird der alternative Test aktiviert. Sind beide Tests positiv, wird mit der Zufallsgenerierung fortgefahren.

17 Statistische Qualität

Dieser physikalische Zufallsgenerator generiert kontinuierlich Zufallsbits in herausragender statistischer Qualität. Eine Qualitätsaussage zu einem solchen Produkt ist aber nicht durch einen einzelnen statistischen Test möglich. In Zusammenarbeit mit Mathematikern und Kryptologen hat sich die Summe aus folgenden statistischen Tests für eine sichere Qualitätsaussage eines physikalischen Zufallsgenerators bewährt:

- Statistische Forderungen der AIS31-Dokumente für Rohdaten (keine digitale Nachbearbeitung, denn nichts beschreibt besser die Eigenschaften eines physikalischen Zufallsgenerators, als seine Rohdaten!)
- NIST-Test-Suite (Summe verschiedener Test der USA-Sicherheitsbehörde)
- Diehard-Test-Suite nach George Marsaglia
- Proprietärer statistischer Basistest

Zur Evaluierung wurden umfangreiche statistische Tests durchgeführt. So wurden die ausgewählten Tests auf mehrere erzeugte Bitfolgen angewendet. Keine dieser Testfolgen konnte Unterschiede zu einem idealen Zufallszahlengenerator aufzeigen. Darüber hinaus wurden Testergebnisse mit Untersuchungen von kryptographisch starken Pseudo-Zufallszahlengeneratoren, wie dem DES-, AES- und SH1-Generator verglichen. Die Vergleiche zeigten keine signifikanten Unterschiede zu den Testergebnissen dieser deterministischen Generatoren.

18 Anwendungen

Auf Grund der sehr hohen Entropie des physikalischen Zufallsgenerators wurden die Funktion für die Klasse PTG.3 (hybrider Zufallsgenerator) ausgelegt. Bezugnehmend auf die AIS31-Dokumente (Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren: www.bsi.bund.de/zertifiz/zert/interpr/ais31e.pdf).ist ein permanenter Online-Test und ein Tot-Test (Ausfall der Rauschquelle) der Zufallsrohdaten integriert. Fällt die Rauschquelle aus oder werden statistische Grenzen überschritten, wird die Ausgabe von Zufallsdaten blockiert.

Der stetig steigende Bedarf an Zufallszahlen in vielen Bereichen von Wissenschaft und Technik erfordert eine zuverlässige und stabile Generierung von Zufallszahlen mit physikalischem Zufall und sicherer Gewährleistung aller erforderlichen statistischen und funktionellen Normen. Damit sind vor allem Entwickler von Sicherheitsapplikationen in der Lage, Wirksamkeit und Widerstand gegen Angriffe besser zu kalkulieren. Besonders hohe Ansprüche an die Statistik von Zufallszahlen werden für kryptografisch sichere Zufallszahlen gestellt.

Exemplarische Beispiele für den Einsatz des PRG600:

- Implementierung in proprietäre Applikationen der IT-Sicherheit
- einfachere Administration und sichere Verschlüsselung bei drahtloser Datenübertragung: WLAN, Bluetooth, GSM, ZiggBee, Industriedatenfunk

- in mobilen Applikationen wie Smartphones, Tablets

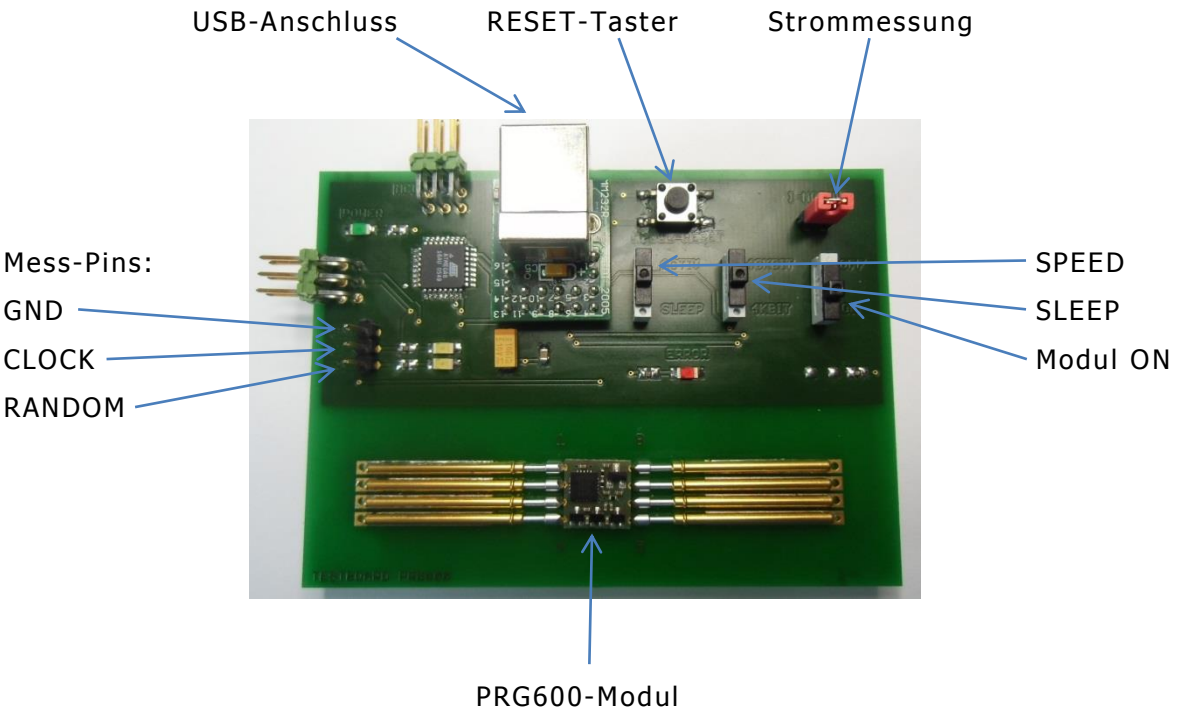
19 Einsatzumgebung

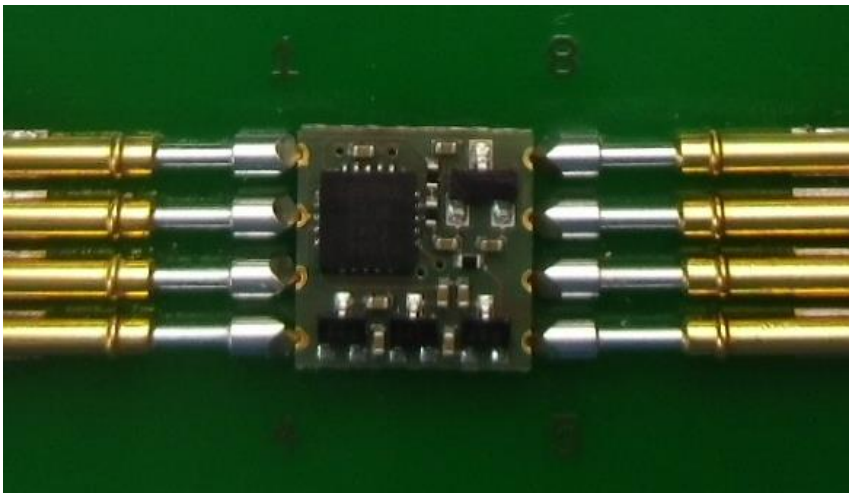
Der PRG600 ist für den permanenten Einsatz in beliebigen Applikationen entwickelt und getestet worden. Auch bei höheren Temperaturen (0°C bis +70°C) bleiben die Entropiewerte sehr hoch und unterschreiten die Vorgaben aus den AIS31-Dokumenten nicht. Alle Grenzwerte der Zufallsrohdaten (Entropie, Gleichverteilung) wurden nicht überschritten. Statistische Analysen, auch für erweiterte Temperaturbereiche, befinden sich auf der Internetseite des Autors.

20 Testsystem

Es wird ein Testsystem angeboten, mit dem die PRG600-Module funktionell und statistisch getestet werden können, ohne diese einlöten zu müssen. Mittels spezieller Nadeladapter werden die Module in die Kontaktvorrichtung geklemmt. Mit der kostenlos angebotenen Software PRG100 können beliebig lange Zufallsfolgen generiert und in einfacher Art und Weise ausgewertet werden.

20.1 Testadapter TA600





Abbildungen: Test-Adapter und Detailansicht

20.2 Software PRG100

Die Einstellung der PRG100-Software erfolgt kompatibel zu den PRG210-Modulen. Details sind in der Beschreibung zur Software PRG100 zu finden. Beispiele zu Konfiguration, Datengenerierung und Analysen sind in folgenden Abbildungen zu erkennen.

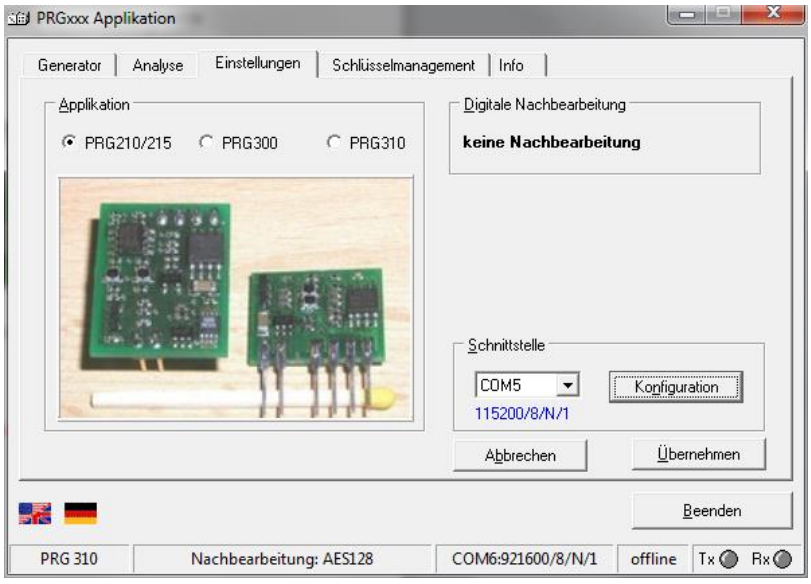


Abbildung: Einstellungen von Applikation und Schnittstelle

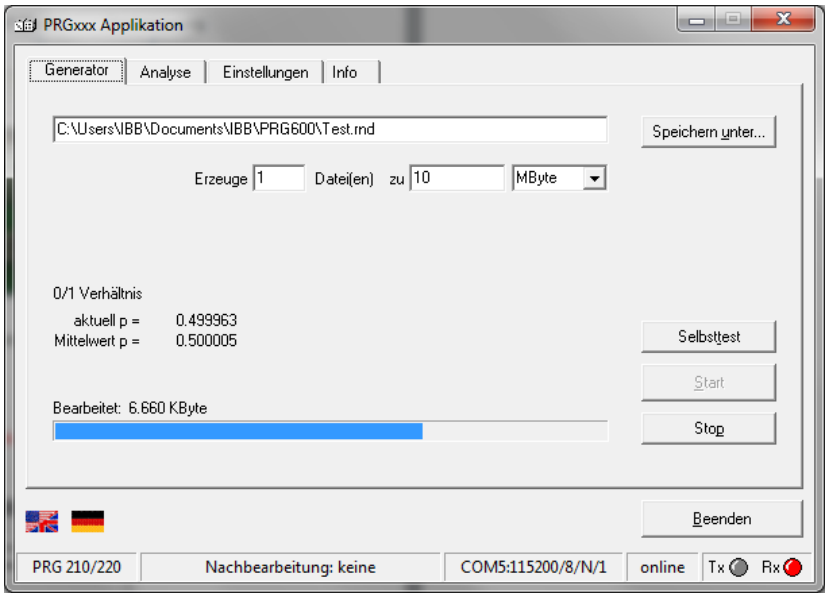


Abbildung: Generierung einer Datei von Zufallszahlen

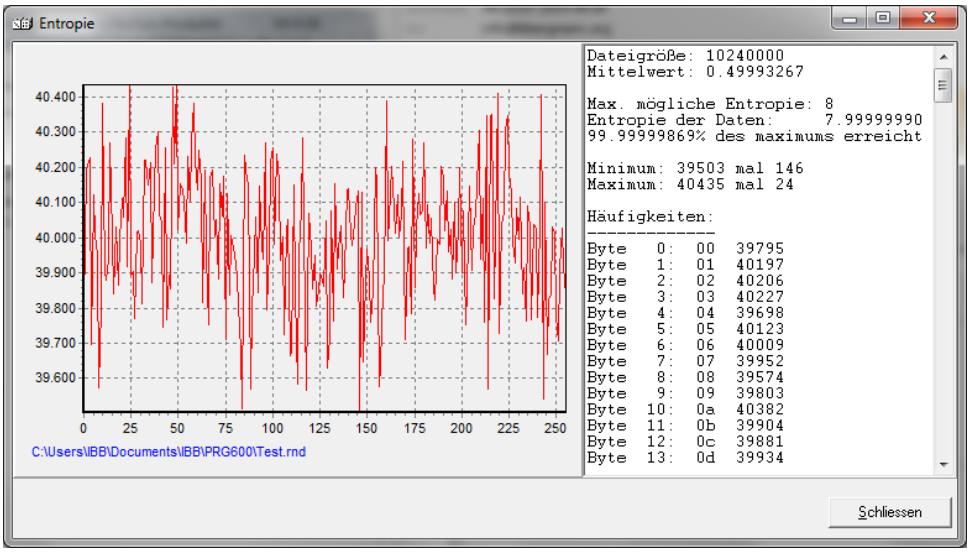


Abbildung: Auswertung der Häufigkeit der Zufallszahlen

21 Literatur

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012

[5] AIS20: Functionality classes and evaluation methodology for deterministic random number generators, Version 2.1, 02.12.2011, Bundesamt für Sicherheit in der Informationstechnik

[6] AIS31: Functionality classes and evaluation methodology for true (physical) random number generators, Version 2.1, 02.12.2011, Bundesamt für Sicherheit in der Informationstechnik

[7] Killmann, W. Schindler, „A proposal for: Functionality classes for random number generators“, Version 2.0, September 18, 2011

[8] Evaluation of random number generators, Version 0.8, Bundesamt für Sicherheit in der Informationstechnik