Physikalischer Zufallszahlen Generator

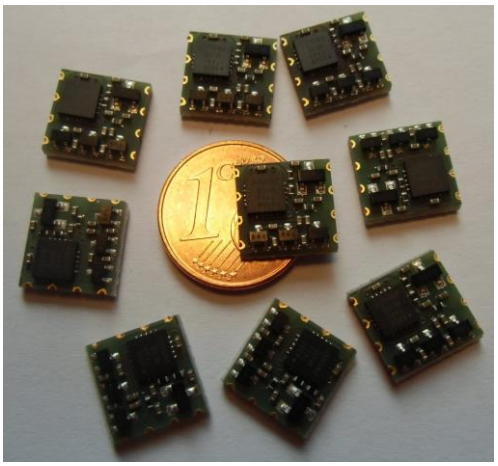
PRG600

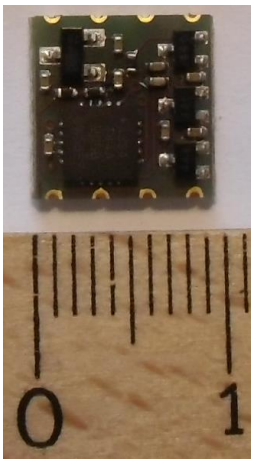
SPI-Interface

Erzeugen von Zufallszahlen der Klasse PTG.3

(Rauschquelle mit hoher Entropie und kryptografische Nachbearbeitung)

- Kontinuierliche Generierung kryptografisch sicherer Zufallszahlen
- Thermisches Rauschen als Entropiequelle (Entropie > 7,97 Bit/Byte)
- Ausgabegeschwindigkeit 4 Kbit/s oder 40 Kbit/s umschaltbar
- Überwachung des Rauschsignals durch Frequenzmessung
- Permanente statistische Online-Kontrolle (P2-Generator nach AIS31)
- Erfüllt alle Kriterien nach AIS31, NIST und Diehard
- Sleep-Modus für sehr geringe Stromaufnahme (< 15µA)
- Zur Implementierung in eigene Applikationen mit minimalen Abmessungen





Die Erzeugung von Zufallszahlen hat auf vielen Gebieten der Technik und Wissenschaft große Bedeutung. So basieren beispielsweise kryptografische Verfahren zumeist auf derartige Zufallszahlen, die mit geeigneten mathematischen Algorithmen Pseudozufallszahlen erzeugen. Streng genommen sind diese Pseudozufallszahlen nicht zufällig, denn mit Kenntnis des erzeugenden Algorithmus ist jede Person in der Lage immer genau die gleiche Folge von Zufallszahlen zu reproduzieren, bzw. die nachfolgenden Zufallszahlen vorauszusagen. Es ist daher von eminenter Bedeutung, eine manipulationssichere Quelle für Zufallssignale zu besitzen, deren erzeugte zufällige Bits sichere kryptografische Verfahren ermöglichen.
Der physikalischen Zufallszahlengenerator PRG600 eignet sich in hervorragender Art und Weise, eine einfache und stabile Generierung von kryptografisch sicheren Zufallszahlen in konstanter hoher statistischer Qualität zu ermöglichen.
Ein stochastisches Modell für den PRG600 erklärt die robuste und hohe Entropie, die Stabilität der Funktionalität im Kontext mit der Rauscherzeugung und Sicherungseigenschaften zur Überwachung des Rauschsignals.
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.“ Die Forderungen der Klasse PTG.3 erfüllt der PRG600:

- 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.

Die kryptografische Nachbearbeitung erfolgt mit Mayer-Einwegfunktionen und AES128-Algorithmus, wobei ein 16-Byte-Startwert aus Zufallsrohdaten 16-Byte-Ausgabedaten nach Schema generiert. Dadurch werden auch bei einem kurzzeitigen Ausfall oder Manipulation der Rauschquellen statistisch gleichverteilte und unabhängige Zufallsdaten ausgegeben.
Zur Evaluierung der Ausgabedaten des PRG600 wurden umfangreiche statistische Tests durchgeführt. Dabei wurden die Diehard-Test-Suite, die NIST-Test-Suite sowie ein eigener statistische Test auf mehrere erzeugte Bitfolgen des PRG600 angewendet. Keine dieser Testfolgen konnte Unterschiede zu einem idealen Zufallszahlen-Generator aufzeigen.
Thermische Rauschquelle für das Zufallssignal ist ein Transistor. Die Signalamplitude der Rauschquelle ist so hoch, dass keine Verstärkung erforderlich ist. Die Digitalisierung und Nachbearbeitung des Rauschsignals erfolgt in einem nachgeschalteten Mikrocontroller.
Der PRG600 kann für statistische Untersuchungen, zur Generierung für Schlüssel und Parameter für kryptografische Verfahren und zur Erzeugung von Zufallszahlen für ein One-Time-Pad-Verfahren eingesetzt werden.

Technische Eigenschaften:

Abmessungen:	10x10x2 (mm)
Stromversorgung:	< 4mA bei 3,3V, im Sleep-Modus < 15µA
Temperaturbereich:	0°C..+70°C
Schnittstelle:	synchrones Interface (SPI) als Master (Takt, Daten)
Qualitätssicherung:	permanenter Online-Test und Überwachung der Rauschquelle
0/1-Verhältnis:	garantiert im Bereich 0,499..0,501 (> 100 KByte)
Entropie:	>7,97 Bit/Byte, aus Zufallsrohdaten nach Shannon ermittelt
Logik-Signale:	Eingang: Sleep-Modus, Speed-Modus, Reset, Ausgang: Error