Physikalischer Zufallszahlen Generator

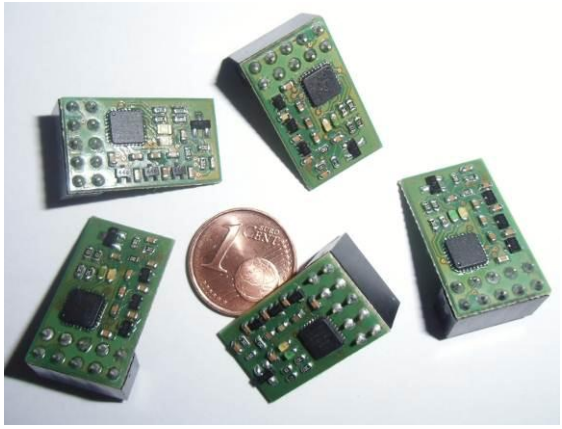
PRG620

UART-Interface

Kontinuierliche Generierung von Zufallszahlen der Klasse PTG.3

(Rauschquelle mit hoher Entropie und kryptografischer Nachbearbeitung)

- **Kein Kommando-Interface, permanente Ausgabe von Zufallszahlen**
- Füllung des Entropie-Pools unter Linux (4096 Bit) in 100ms
- Ausgabegeschwindigkeit > 40 Kbit/s bei 115.200 bps der UART
- Überwachung des Rauschsignals durch Frequenzmessung
- Permanente statistische Online-Kontrolle pro Sekunde
- Erfüllt alle Kriterien nach AIS31, NIST und Diehard
- Für den Einsatz auf dem Raspberry-Pi-Board und kompatiblen Systemen



Mit dem PRG620 steht ein professioneller Zufallsgenerator der Klasse PTG.3 (hybrider Zufallsgenerator) für die permanente Generierung von kryptografisch sicheren Zufallszahlen zur Verfügung. Dieser Zufallsgenerator hat ein UART-Interface und arbeitet ohne Kommando-Interface. Nach PON werden kontinuierlich Zufallszahlen mit hoher Geschwindigkeit ausgegeben. Ein permanent im Hintergrund laufendes Sicherheitssystem garantiert, dass bei Ausfall oder Manipulation der Rauschquellen die Zufallsausgabe sofort eingestellt und solange weiter getestet wird, bis alle Qualitätskriterien wieder eingehalten werden.
Die generierten Zufallszahlen sind garantiert kryptografisch sicher und werden vorzugsweise zur Entropieerhöhung und -bereitstellung in Sicherheitsapplikationen verwendet. Unter Linux gibt es bekanntlich immer wieder Probleme mit der Bereitstellung von Zufall im Entropie-Pool. Besonders kritisch wird die Situation, wenn keine Eingabegeräte an einem Server zur Verfügung stehen.
Ein stochastisches Modell für den PRG620 erklärt die robuste und hohe Entropie, die Stabilität der Funktionalität im Kontext mit der Rauscherzeugung und Sicherungseigenschaften zur Überwachung des Rauschsignals.
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 PRG620 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 PRG620 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 PRG620 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:	22*13*12,0 mm (mit Pfostensteckverbinder)
Stromversorgung:	< 7mA bei 3,3V
Temperaturbereich:	0..70°C
Schnittstelle:	UART-Interface, 115,2 Kbit/s, Protokoll 8,N,1
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
Ausgabegeschwindigkeit:	> 40 Kbit/s
Kontakt:	info@ibbergmann.org, www.ibbergmann.org