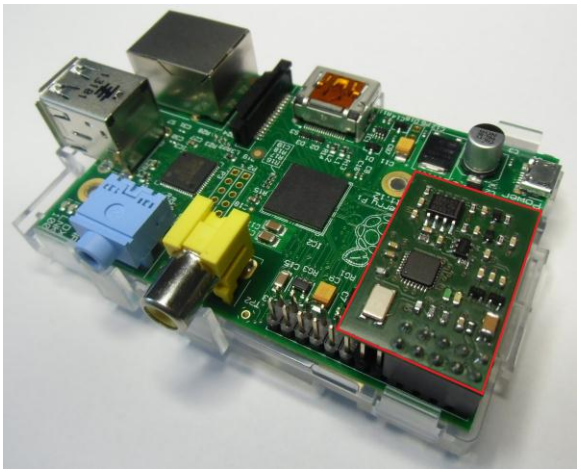
Physikalischer Zufallszahlen Generator

PRG260

UART-Interface für Raspberry-Modul

Erzeugen von Zufallszahlen der Klassen PTG.2 und PTG.3



- Kontinuierliche Generierung echter Zufallszahlen bis 300.000 Bit/s
- Thermisches Rauschen als Zufallsquelle
- Generierung von Rohdaten oder Zufallszahlen der Klassen PTG.2 und PTG.3
- Konstante höchste statistische Qualität auch im erweiterten Temperaturbereich
- Permanente statistische Online-Kontrolle (P2-Generator nach AIS31)
- Erfüllt alle Kriterien nach AIS31, NIST und Diehard
- Garantierte konstante Qualität durch automatischen Selbstabgleich
- UART-Interface mit 921 Kbit/s

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 PRG260** eignet sich in hervorragender Art und Weise, eine einfache und stabile Generierung von echten Zufallszahlen in konstanter hoher statistischer Qualität zu ermöglichen und **erfüllt Anforderungen an einen idealen Zufallsgenerator**. Zur Erhöhung der Gleichverteilung der generierten Zufallselemente kann eine digitale Nachbearbeitung durch Verknüpfung aufeinanderfolgender Zufallsbits ausgewählt werden.
Zur Evaluierung der Ausgabedaten des PRG260 wurden umfangreiche statistische Tests durchgeführt. Bereits bei der Untersuchung der Zufallsdaten ohne digitale Nachbearbeitung konnten keine Bit-Abhängigkeiten nachgewiesen werden. Weiterhin wurden die Diehard-Test-Suite, die NIST-Test-Suite sowie ein eigner statistische Test auf mehrere erzeugte Bitfolgen des PRG260 angewendet. Keine dieser Testfolgen konnte Unterschiede zu einem idealen Zufallszahlen-Generator aufzeigen.

Thermische Rauschquellen für das Zufallssignal sind Z-Dioden. Mittels **Differenzverstärker und Schmitt-Trigger**-Schaltkreis wird das Rauschsignal verstärkt und digitalisiert. Ein nachgeschalteter **Mikrocontroller** tastet das Zufallssignal ab und konvertiert es zu einem UART-Interface. Die mitgelieferte Software PRG100 (Windows) generiert und analysiert beliebig lange Dateien mit folgenden wählbaren digitalen Nachbearbeitungen der digitalisierten Zufallsdaten durch den integrierten Mikrocontroller:

- Keine digitale Nachbearbeitung
- Von Neumann-Verknüpfung (PTG.2)
- XOR-Verknüpfung 2-fach, 3-fach (PTG.2)
- Kryptografische Nachbearbeitung mit AES128 (PTG.3)

Der PRG260 kann für statistische Untersuchungen, zur Generierung von Schlüssel und Parameter für kryptografische Verfahren und zur schnellen Erzeugung von Zufallszahlen für ein One-Time-Pad-Verfahren eingesetzt werden.

Technische Eigenschaften:

Abmessungen:	30x20x12 (mm, mit Steckverbinder)
Stromversorgung:	ca. 40mA aus Port-Erweiterung
Temperaturbereich:	-20°C..+85°C
Schnittstelle:	UART-Schnittstelle, 921.600 Bit/s, Protokoll 8,N,1
Qualitätssicherung:	automatischer Selbstabgleich von Verstärkung und Digitalisierung, permanenter Online-Test und Überwachung der Rauschquelle
0/1-Verhältnis:	ohne digitale Nachbearbeitung garantiert im Bereich 0,49..0,51 (> 8.000 Bit)
Entropie:	>7,997 Bit/Byte, aus Zufallsrohdaten nach Shannon ermittelt

Der PRG260 beinhaltet Schutzrechte für den Teil des physikalischen Zufallsgenerators.