

Physikalischer Zufallszahlen Generator

WPRG320

Bluetooth-Interface

Erzeugen echter Zufallszahlen

- Kontinuierliche Generierung echter Zufallszahlen bis 230.000 Bit/s
- Thermisches Rauschen als Zufallsquelle
- Kein Pseudozufall oder kryptografische Algorithmen verwendet
- Konstante höchste statistische Qualität auch im erweiterten Temperaturbereich
- Permanente statistische Online-Kontrolle
- Erfüllt alle Kriterien nach AIS31, NIST und Diehard
- Garantierte konstante Qualität durch automatischen Selbstabgleich



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 WPRG320** 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 WPRG320 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 eigener statistische Test auf mehrere erzeugte Bitfolgen des WPRG320 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 Bluetooth-Interface. Eine mitgelieferte Windows-Software generiert beliebig lange Dateien (max. 2,0GB) mit folgenden wählbaren Nachbearbeitungen der digitalisierten Zufallsdaten durch den integrierten Mikrocontroller:

- Von Neumann-Verknüpfung
- XOR-Verknüpfung 2-fach, 3-fach oder 4-fach
- Keine digitale Nachbearbeitung

Weiterhin sind Funktionen implementiert, die eine alternative Generierung echter Zufallszahlen mit programmierbarer deterministischer digitaler oder analoger Abtastung ermöglichen. Sie dienen vor allem der Gewinnung neuer Erkenntnisse auf dem Gebiet der Erzeugung von Zufallsdaten.

Der WPRG320 kann für statistische Untersuchungen, zur Generierung für Schlüssel und Parameter für kryptografische Verfahren und zur schnellen Erzeugung von Zufallszahlen für ein One-Time-Pad-Verfahren eingesetzt werden.

Technische Eigenschaften:

Abmessungen:	95x60x29 (mm)
Stromversorgung:	2x Mignon-Batterien (ca. 30 h Laufzeit) oder Steckernetzteil (6V)
Temperaturbereich:	0°C..+60°C
Schnittstelle:	Bluetooth 2.0 als virtuelle COM-Schnittstelle, 230.400 Bit/s, 8,N,1
Qualitätssicherung:	automatischer Selbstgleich von Verstärkung und Digitalisierung
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 WPRG320 beinhaltet Schutzrechte für den Teil des physikalischen Zufallsgenerators.