

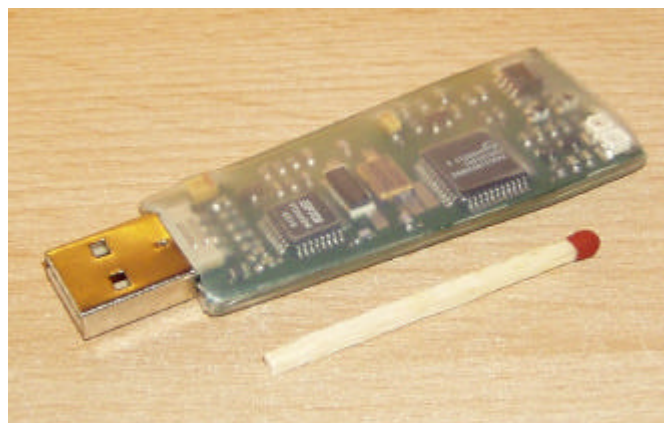
Physikalischer Zufallszahlen Generator

PRG310

USB1.1-Interface

Erzeugen echter Zufallszahlen

- Kontinuierliche Generierung echter Zufallszahlen mit 115.200 bps
- Konstante höchste statistische Qualität auch im erweiterten Temperaturbereich
- Kein Pseudozufall oder kryptografische Algorithmen verwendet
- Für den industriellen Einsatz geeignet
- Wählbare digitale Nachbearbeitung
- Garantierte 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 PRG310** eignet in hervorragender Art und Weise, einfache und stabile Generierung von echten Zufallszahlen in konstanter hoher statistischer Qualität zu ermöglichen und **erfüllt Anforderungen an einen idealen Zufallsgenerator**. Zur Erhöhung der Entropie der generierten Zufallselemente kann eine digitale Nachbearbeitung durch Verknüpfung aufeinanderfolgender Zufallsbits ausgewählt werden.

Zur Evaluierung der Ausgabedaten des PRG310 wurden umfangreiche statistische Tests durchgeführt. So wurden die Diehard-Test-Suite, die NIST-Test-Suite sowie der statistische Test nach R. Gretmann auf mehrere erzeugte Bitfolgen des PRG310 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 USB1.1-Interface. Eine mitgelieferte Software (Windows '98 und 2000) generiert beliebig lange Dateien (max. 2,5GB) mit folgenden wählbaren digitalen Nachbearbeitungen der digitalisierten Zufallsdaten durch den integrierten Mikrocontroller:

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

Der PRG310 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: 75x28x4 (mm)
Stromversorgung: ca. 40mA aus USB-Port
Temperaturbereich: -20°C..+85°C
Schnittstelle: USB1.1 als virtuelle COM-Schnittstelle, 115.200 bps, Protokoll 8,N,1
Qualitätssicherung: automatischer Selbstabgleich von Verstärkung und Digitalisierung
0/1-Verhältnis: ohne digitale Nachbearbeitung garantiert im Bereich 0,49..0,51
(> 8.000 Bit)

Der PRG310 beinhaltet ein Patent für den Teil des physikalischen Zufallsgenerators.