

Physikalischer Zufallszahlen Generator

PRG400

USB1.1-Interface

Erzeugen echter Zufallszahlen

- Kontinuierliche Generierung echter Zufallszahlen bis 800.000 bps
- Konstante höchste statistische Qualität
- Kein Pseudozufall oder kryptografische Algorithmen verwendet
- Permanente statistische Online-Kontrolle
- 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 PRG400** 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 PRG400 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 PRG400 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 nach geschalteter **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. 2,0GB) mit folgenden wählbaren digitalen Nachbearbeitungen der digitalisierten Zufallsdaten durch den integrierten Mikrocontroller:

- Keine digitale Nachbearbeitung (mit ca. 800.000 bps)
- XOR-Verknüpfung 2-fach, 3-fach oder 4-fach (mit ca. 600.00..700.00 bps)
- Von Neumann-Verknüpfung (mit ca. 150.00 bps)

Der PRG400 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: 115x80x35 (mm)
Stromversorgung: ca. 120mA aus USB-Port
Temperaturbereich: -20°C..+85°C
Schnittstelle: USB1.1 als virtuelle COM-Schnittstelle, 921.600 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 PRG400 beinhaltet ein Patent für den Teil des physikalischen Zufallsgenerators.