

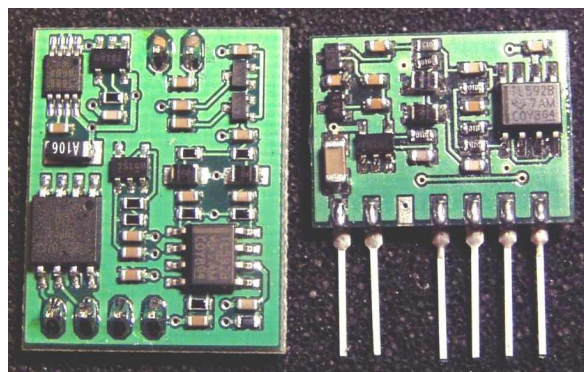
Physikalischer Zufallszahlen Generator

PRG210/220

OEM-Modul

Erzeugen echter Zufallszahlen

- Kontinuierliche Generierung echter Zufallszahlen mit ca. 50 Kbit/s
- Konstante höchste statistische Qualität mit interner Selbstkontrolle
- Kein Pseudozufall oder kryptografische Algorithmen verwendet
- Für den industriellen Einsatz geeignet
- Synchrone Datenausgabe
- Garantierte Qualität durch automatischen Selbstabgleich
- Permanente statistische Online-Kontrolle



PRG210

PRG220

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 manipulations sichere Quelle für Zufallssignale zu besitzen, deren erzeugte zufällige Bits sichere kryptografische Verfahren ermöglichen.

In zahlreichen Publikationen wurden Verfahren für die **Erzeugung echter Zufallszahlen** veröffentlicht. Die meist in Einzelfertigung angebotenen Geräte sind sperrig, kostenintensiv und setzen Spezialkenntnisse bei der Einstellung der Parameter voraus. Ungenügende statistische Qualität wird oftmals durch Verknüpfung mit Pseudozufallszahlen kaschiert, ohne auf die negativen Folgen für den Einsatz in kryptografischen Systemen zu verweisen.

Dem angebotenen physikalischen **Zufallszahlengenerator PRG210/220** liegt daher die Aufgabe zugrunde, die Limitierung des Standes der Technik zu überwinden und in kostengünstiger Weise eine **einfache und stabile Generierung von echten Zufallszahlen in konstanter hoher statistischer Qualität** zu ermöglichen. Da sich die Parameter der elektronischen Schaltung automatisch optimieren, ist die statistische Qualität auch bei Spannungsschwankungen und Temperaturänderungen konstant und **erfüllt Anforderungen an einen idealen Zufallsgenerator**. Für die abgetasteten Rohdaten sind keine Bit-Abhängigkeiten nachweisbar. Zur Erhöhung der Gleichverteilung der 0/1-Bits wird ausschließlich eine digitale Nachbearbeitung durch XOR-Verknüpfung aufeinanderfolgender Zufallsbits verwendet. Für eine Implementierung in Applikationen sind keine speziellen Maßnahmen, wie Schirmung oder gefilterte Stromversorgung, erforderlich. Störspannungen von Mikrocontrollern und anderen digitalen Schaltungen werden durch interne Schaltungsmaßnahmen unterdrückt.

Thermische Rauschquellen des Moduls sind Z-Dioden. Mittels **Differenzverstärker und Schmitt-Trigger**-Schaltkreis wird das Rauschsignal verstärkt und digitalisiert. Ein nach geschalteter **Mikrocontroller** verknüpft aufeinanderfolgende Zufallsbits XOR und erhöht somit die Gleichverteilung der Bits. Der Mikrocontroller generiert das synchrone Interface und überwacht das 0/1-Verhältnis in einem vorgegebenen Bereich. Bei Über- oder Unterschreitung des Bereiches wird ein Fehlersignal aktiviert.

Technische Eigenschaften:

Abmessungen:	PRG210: 25x20x3,5 (mm); PRG220: 15x20x5,0 (mm)
Stromversorgung:	5V/10mA (4,5..5,5V) oder 3,3V/14mA (3,0..3,6V)
Temperaturbereich:	-20°C..+85°C
Schnittstelle:	synchrones Interface, ca. 50 Kbit/s Fehlermeldung
Qualitätssicherung:	automatischer Selbstabgleich von Verstärkung und Digitalisierung Mikrocontroller zur Überwachung des 0/1-Verhältnis
0/1-Verhältnis:	garantiert im Bereich 0,49..0,51 (> 8.000 Bit)
Entropie:	>7,997 (ermittelt aus Rohdaten nach Shannon)

Der PRG210/220 beinhaltet ein Patent für den Teil des physikalischen Zufallsgenerators