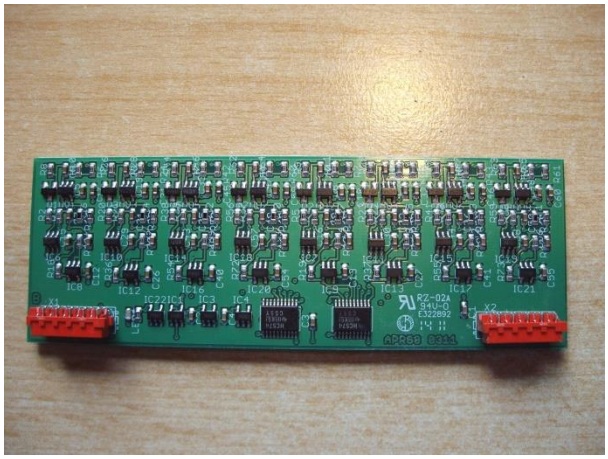
Spezialentwicklungen von Rausch- und Zufallsgeneratoren des IBB

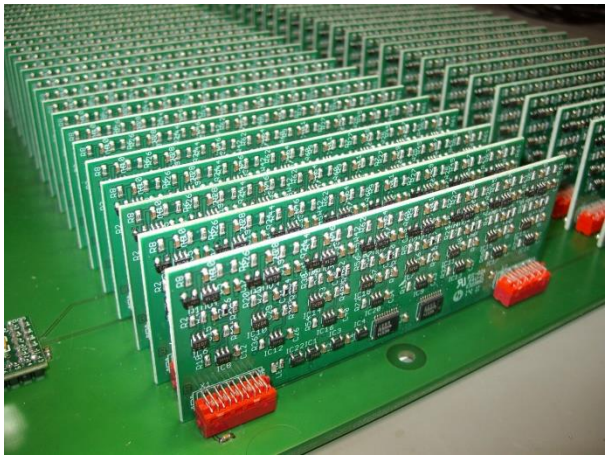
In Zusammenarbeit mit verschiedenen Unternehmen in Deutschland und der Schweiz sind interessante Applikationen entstanden. Diese wurden und werden erfolgreich in der Rauschforschung und zur Generierung kryptografisch sicherer Zufallszahlen unter Weltraumbedingungen eingesetzt.

Physikalischer Zufallsgenerator M512

Der physikalische Zufallsgenerator auf Basis von Rausch-Transistoren wurde entwickelt, um eine große Anzahl von Rauschgeneratoren auf kleinstem Raum zu konzentrieren. Dieses Gerät beinhaltet Superlative in der Entwicklung physikalischer Zufallsgeneratoren und ist, zumindest im kommerziellen Bereich, ohne Konkurrenz weltweit.



In einem 19-Zoll-Gehäuse mit einer Höheneinheit (5cm) sind **512 physikalische Zufallsgeneratoren** angeordnet, die sowohl analog (12Bit-Auflösung) als auch digital abgetastet werden können. Die hohe Abtastgeschwindigkeit von bis zu 1,34µs pro Generator lässt eine hohe Datenrate über einen USB-Port oder dem integrierten Ethernet-Interface zu.



Die Zufallsgeneratoren sind modular aufgebaut. Jeweils 8 komplette Zufallsgeneratoren bilden ein Modul. Die Zufallsgeneratoren sind abgleichfrei und besitzen einen stabilen Arbeitspunkt unter kommerziellen Bedingungen.

Der Leistungsverbrauch des M512 beträgt weniger als 4 Watt. Das Gerät wird aus einem externen Netzteil gespeist. Weiterhin können

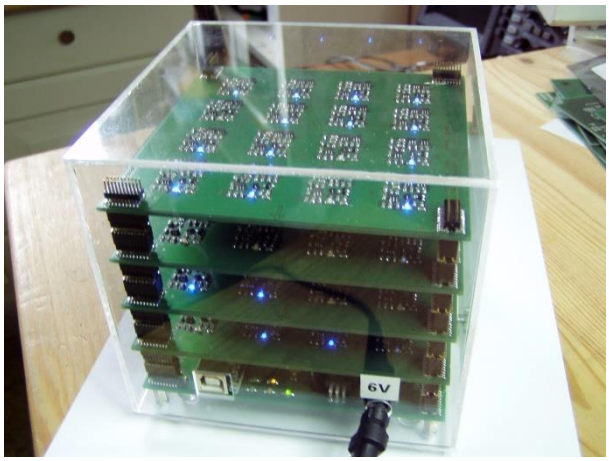
mehrere M512 zusammengeschaltet und absolut synchron abgefragt werden. Dabei fungiert ein M512 als Master und alle weiteren M512 als Slave. Die Synchron-Verbindung wird mit einem zweipoligen Kabel von Gerät zu Gerät hergestellt. Per Kommando über USB oder Ethernet wird der Modus eingestellt.
M512 erfüllt bei der Generierung digitaler Zufallsdaten alle Kriterien der AIS31-Forderungen und ist damit für die Herstellung kryptografisch sicherer Schlüssel und Parameter geeignet. Zwei synchron geschaltete M512 können pro Tag mehr als 15 GByte kryptografisch sicheren Zufall generieren.

Dreidimensionaler Rauschgenerator CUBUS

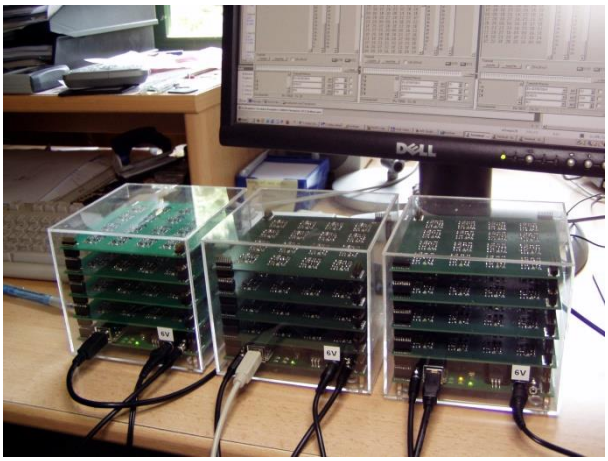
Die Applikation Cubus beinhaltet insgesamt 64 Rauschgeneratoren auf Basis von Rausch-Transistoren. Die Rausch-Transistoren sind in einer 4x4x4 Matrix im gleichen Abstand positioniert. Das netzgespeiste Gerät ist über ein USB-Interface mit einem PC verbunden. Hervorzuheben ist die absolut zeitgleiche Abtastung der analogen oder digitalen Rauschsignale. Weitere Eigenschaften:

- Manipulation durch Abschalten jedes Rausch-Transistors einzeln möglich
- Steuerung einer blauen Leuchtdiode für jeden Rausch-Transistoren
- Min. Abtastintervall
    - 16 Rausch-Transistoren analog: 1ms
    - 16 Rausch-Transistoren digital: 100µs
    - 64 Rausch-Transistoren analog: 5ms
    - 64 Rausch-Transistoren digital: 500µs
- Synchrone Abtastung mehrerer Cuben

Die absolut synchrone Abtastung der Rauschsignale durch drei Geräte wurde erprobt. Dabei arbeitet ein Cubus als Master zur Erzeugung des Synchronsignals. Damit konnten 192 Rauschgeneratoren (= 3 Cuben) analog und digital abgefragt werden. Das Prinzip kann beliebig erweitert werden und ist nur durch die zur Verfügung stehenden USB-Anschlüsse eines PC begrenzt.



Cubus mit blauen Leuchtdioden



Laboraufbau mit drei synchron abgetasteten Cuben

Universeller Zufallsgenerator UZG30

- 64 Module mit Rauschgeneratoren
- Jeder Rauschgenerator kann mit folgenden Verfahren Daten generieren
  - Analoge Abtastung
  - Digitale Abtastung
  - Spezielle Abtastung mit SRD-Technologie
- Interface über USB oder Netzwerk
- Kommandointerface kompatibel mit M512

Module des UZG30

Blick in das geöffnete Gerät

Raumfahrttauglicher TRNG auf Basis von Z-Dioden (RTRNG) als Physikalischer Zufallsgenerator für kryptografische Applikationen

- Grundlagen sind die Verbindlichkeiten der Bundesnetzagentur
- Entwicklung eines stochastischen Modells
- Entwicklung einer spezifischen Hardware auf Basis des PRG310 für extreme Umweltbedingungen

Das einsatztaugliche Security-Board mit dem Zufallsgenerator