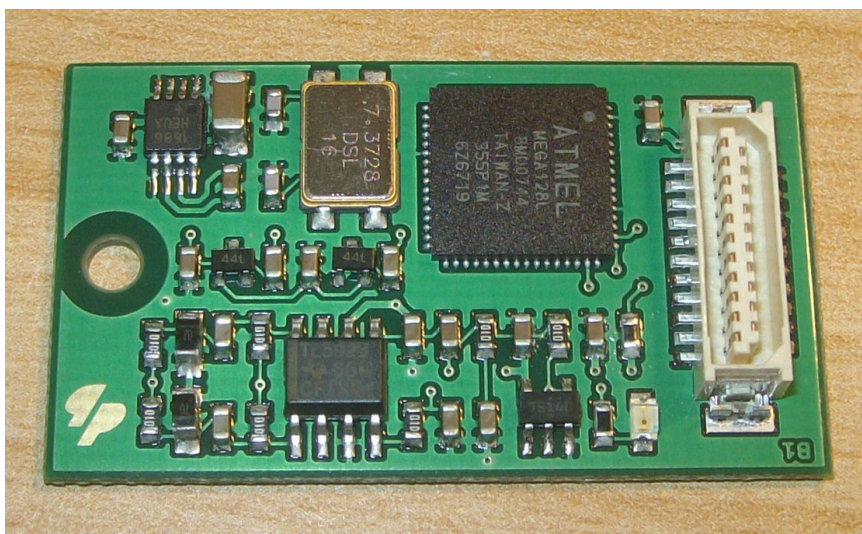


Frei programmierbares Modul CM220 mit physikalischem Zufallsgenerator

Universelles Modul für kundenspezifische Sicherheits-Applikationen

- Integrierter physikalischer Zufallsgenerator höchster statistischer Qualität
- Mikrocontroller Atmega128L
- Zwei serielle asynchrone Schnittstellen bis 921.600 Bit/s
- Diverse Logiksignale
- Entwicklungsumgebung verfügbar



Dieses universelle, kostengünstige und frei programmierbare Modul verfügt über leistungsstarke Komponente für die Entwicklung eigener Sicherheits-Applikationen. Kern dieses Moduls ist ein patentierter physikalischer Zufallsgenerator (TRNG) für kryptografische Anforderungen. Dieser TRNG erfüllt alle bekannten statistischen Tests für Rohdaten (AIS31-Normen) und einfach nachbearbeitete Zufallsdaten (z.B. dreifache XOR-Verknüpfung aufeinanderfolgender Zufallsbits), wie NIST-Test-Suite und Diehard-Test. Mit den integrierten Hardware-Komponenten sind beispielsweise folgende Sicherheits-Applikationen möglich:

- Zufallserzeugung für kryptografische Schlüssel und Parameter
- Schlüsselerzeugung und Schlüsselverwaltung im geschützten Bereich des Mikrocontrollers
- Ausgabe von schwarzen (verschlüsselten) Schlüssel
- Verschlüsselung von Daten bei der Übertragung über asynchrone Interface

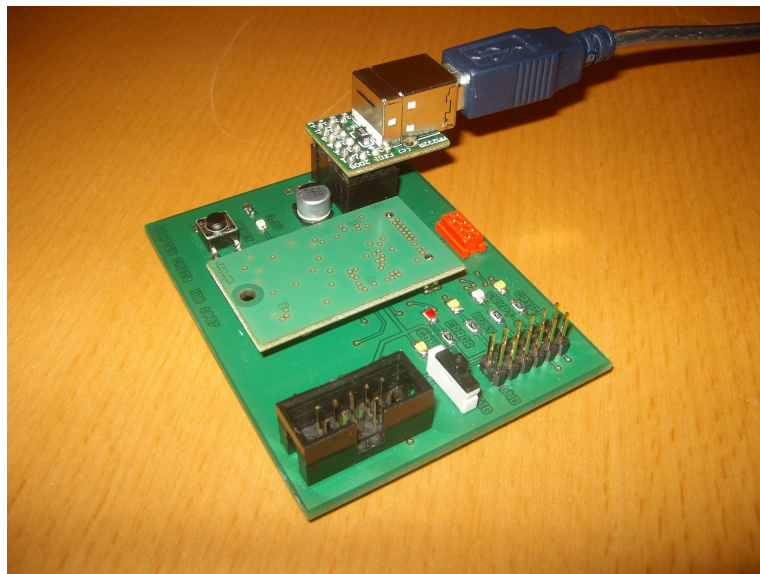
Folgende technische Eigenschaften verdeutlichen die Leistungsfähigkeit:

- Patentierter physikalischer Zufallsgenerator (EP 150 98 38)
- Serielle digitale Zufallsdaten mit ca. 7 MHz
- Mikrocontroller Atmega128L, 128 KByte Programmspeicher, 4 KByte SRAM, 4 KByte EEPROM
- Taktfrequenz 7,3728 MHz
- Zwei asynchrone serielle Interface bis 921.600 Bit/s (TTL-Pegel)
- vier Logiksignale am Steckverbinder frei Verfügbar
- Grüne Leuchtdiode
- Versorgungsspannung 3,3V
- Stromaufnahme ca. 20 mA
- Powerdown-Modus (ca. 200µA, TRNG abgeschaltet, Mikrocontroller im sleep-Modus)
- Arbeitstemperaturbereich -10°C bis +85°C
- Abmessungen 38x22x5 (mm)
- 21-poliger SMD-Stecker

Ausgeliefert wird jedes CM220 mit einer Testapplikation und einer Software (WINDOWS) für die Generierung von hochwertigen Zufallsdaten und deren Analyse.

Als Entwicklungsunterstützung ist ein Testadapter (TA220) mit folgenden Eigenschaften verfügbar:

- JTAG-Anschluß für einen HW-Emulator (Mikrocontroller -Entwicklung)
- USB-Interface für Kommunikationsaufgaben (FTDI-Chip)
- Leuchtdioden und Schalter zur freien Verwendung
- Pfostenstecker mit allen Schnittstellen-Signalen
- Wannenstecker für Daten- und Signalanschluss
- Reset-Taster für CM220-Modul



Bestellbezeichnung: CM220-1, TA220-1