Unechter und echter Zufall

- Zufall generell ist eine statistische Eigenschaft einer Folge von Elementen einer Menge von Werten.
- **Unechter Zufall** hat einen deterministischen Algorithmus als Grundlage, durch welchen eine periodische oder auch nichtperiodische Folge von Elementen einer Menge beschrieben wird. Freiheitsgrad ist der sogenannte Seed, welcher den Einstieg in die Folge beschreibt. Beispiele sind:
  - Nachkommastellen mathematischer Konstanten wie π oder e
  - rückgekoppelte Schieberegister
  - rekursiv berechnete Folgen von Zahlen nach Verfahren der linearen Kongruenz ($x_n = (a*x_{n-1} + b) \bmod k$)
- **Echter Zufall** hat einen physikalischen Effekt mit nicht deterministischem Verhalten als Grundlage, z.B.:
  - thermisches Rauschen in Bauelementen
  - Jitter von Oszillatoren
  - atomare Zerfallsprozesse
- Unechter ist von echtem Zufall anhand der Statistik nicht unterscheidbar!

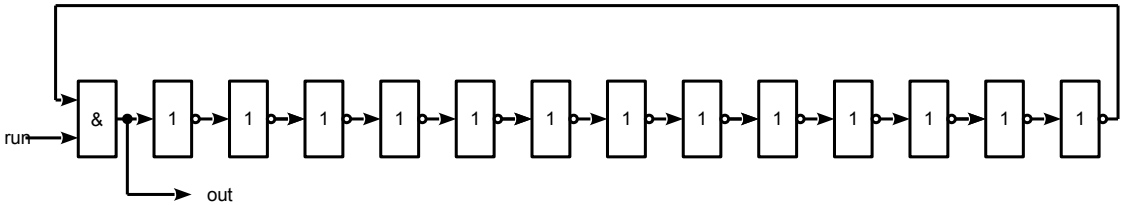
Wesen und Bedeutung echten Zufalls

- Ein echter Zufallszahlengenerator (**TRNG** - True Random Number Generator) erzeugt Zahlen mit höchst möglicher Unvorhersagbarkeit (Entropie).
- Bedeutung in der Kryptografie:
  - Generierung von Schlüsseln
  - Generierung von Nonces, IVs
- Echten Zufall möglichst dort erzeugen, wo er gebraucht wird -> auf dem Chip
- Klassisch wurde echter Zufall mit analogen Schaltungsstrukturen erzeugt. Aus Fertigungsgründen in der Halbleiterindustrie (Mixed Signal Prozesse, Shrinking) heute üblicherweise mit digitalen Schaltungsstrukturen. Beispiele:
  - Zufallsgenerator in Ivy Bridge Prozessoren von Intel
  - Zufallsgenerator in Smartcards

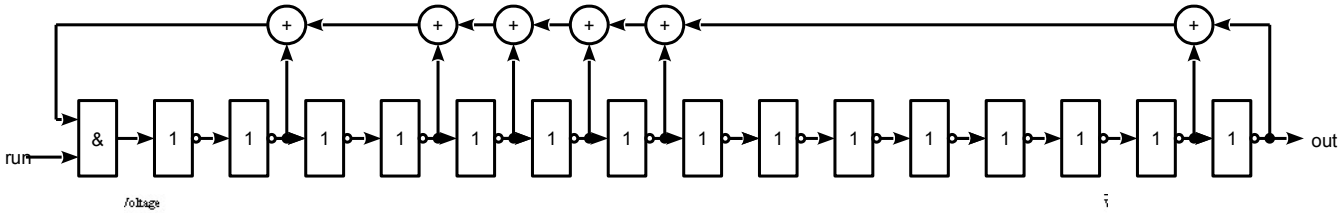
- Forschungsprojekt 2011-2013 vom BMBF gefördert:
  "Zuverlässige Erzeugung von echten Zufallszahlen in FPGAs“
  (TU-Dresden, Siemens, secunet)

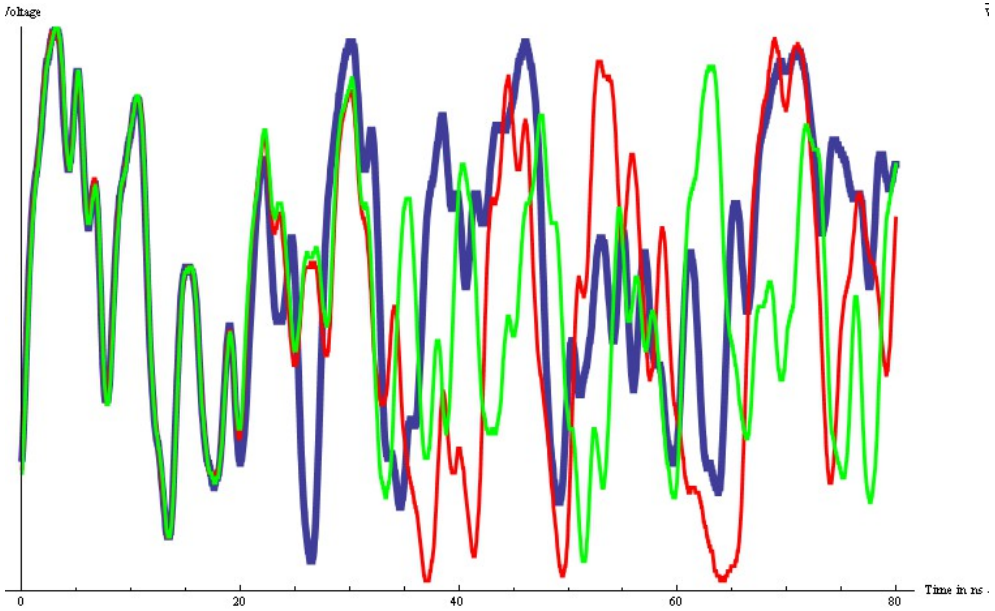
TRNGs: Ring Oszillator und Fibonacci Ring Oszillator (FIRO)

- Klassischer Ringoszillator (erzielbare Datenrate: mehrere kbps):



- Fibonacci Ring Oszillator (erzielbare Datenrate: mehrere Mbps):





secunet

Test und Zertifizierung echter Zufallsgeneratoren

- Minimalforderungen:
  - Gleichverteilung von 0 und 1
  - Unabhängigkeit aufeinanderfolgender Zahlen
- Standard-Offline Tests für Zufallszahlen (Bitströme)
  - NIST SP 800-22, Test-Suite zum Bewerten von Zufalls- und Pseudo-Zufallszahlen
  - BSI AIS31: "Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren"
- Aber: Kein Test kann nachweisen, dass es sich um echten Zufall handelt

- Zertifizierung in Deutschland durch BSI anhand von CC und AIS31:
  - Ergänzung des TRNG um Ausfall- und Online-Tests
  - Nachweis einer geforderten Statistik
  - Lieferung eines plausiblen Erklärungsmodells für den physikalischen Zufallseffekt