On the fly evaluation of FPGA-based True Random Number Generator

VLSI-EDA-Lehrstuhl
Seminarvortrag von Kai Ludwig
am 04.07.2012

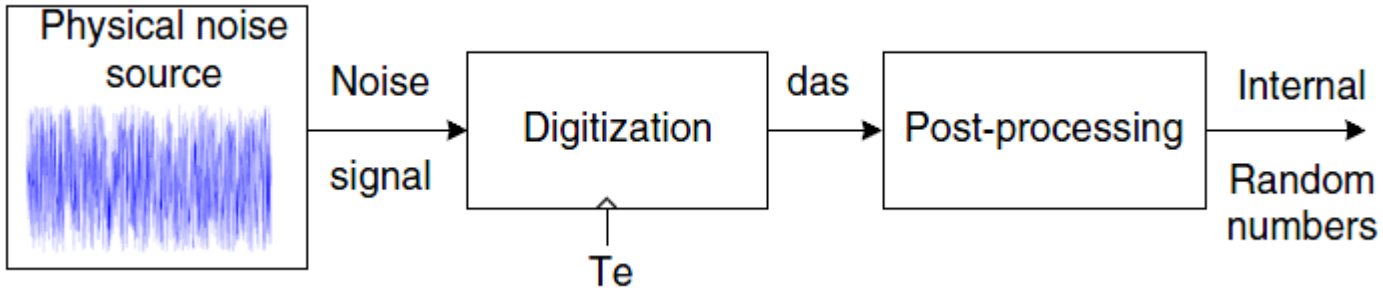
Gliederung

1. Random Number Generator
2. True Random Number Generator
3. Test und Vergleich von TRNG
4. Zusammenfassung
5. Quellen

- Verwendung:
  - Kryptographie
  - Test und Simulation
  - Kommunikation

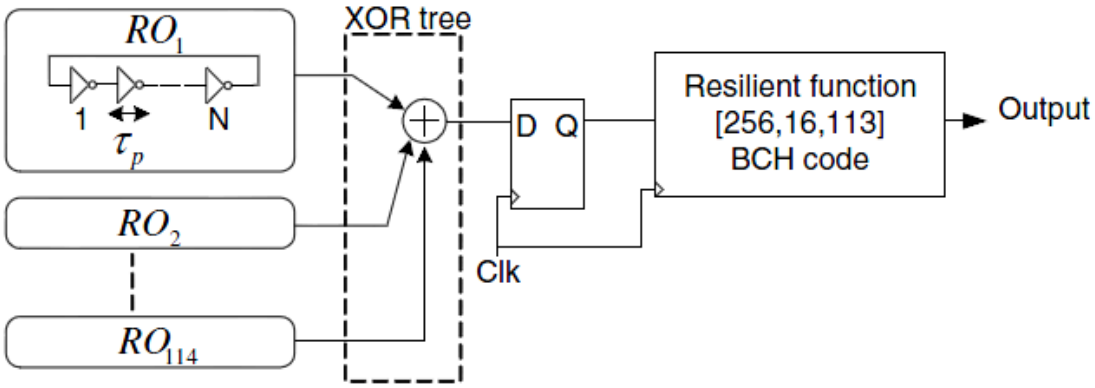
- Anforderung:
  - Statistisch unabhängig
  - Gleichverteilt
  - Unvorhersehbar

- Pseudo Random Number Generator
  - Deterministischer Algorithmus
  - Beliebige Verteilung
  - Hohe Datenrate
  - Benötigt Initalzustand (Seed)

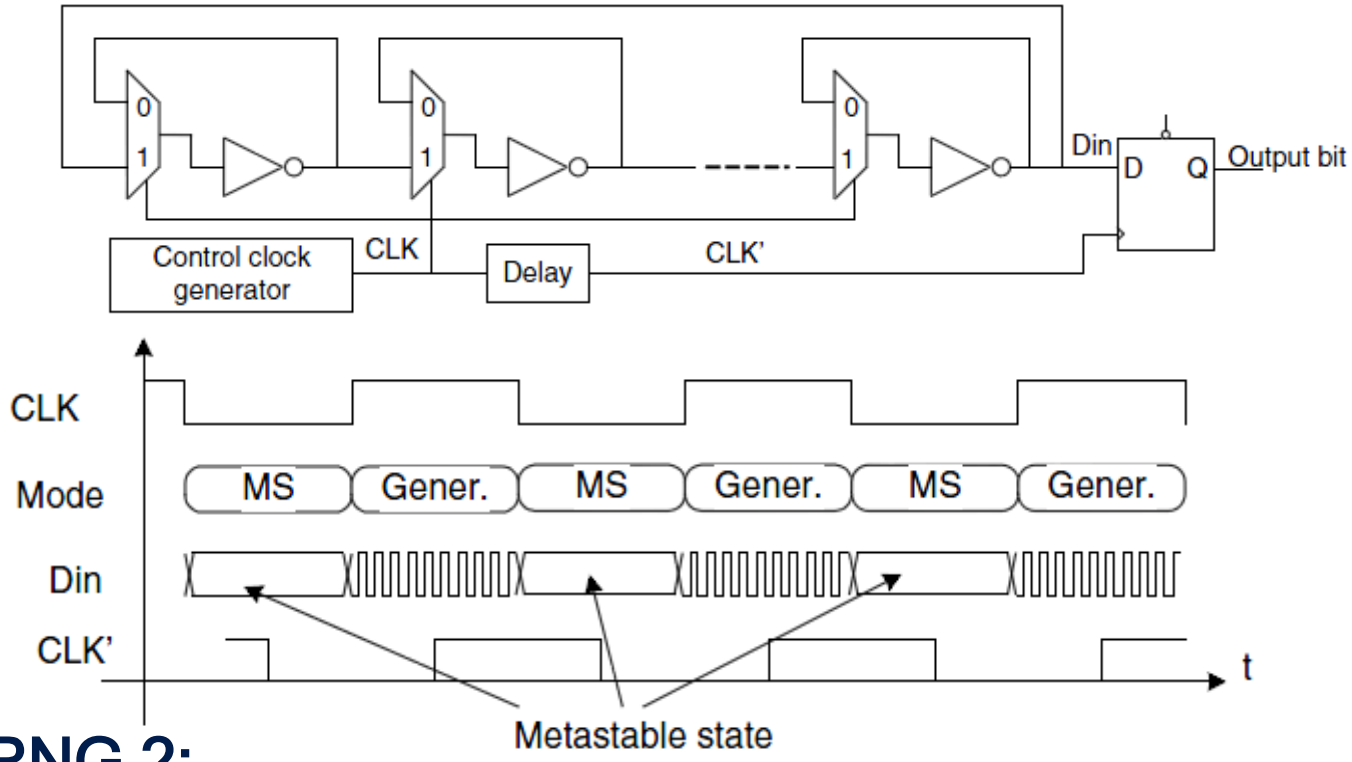


- Nicht-deterministische Erzeugung
- Abtastung von Phasenrauschen

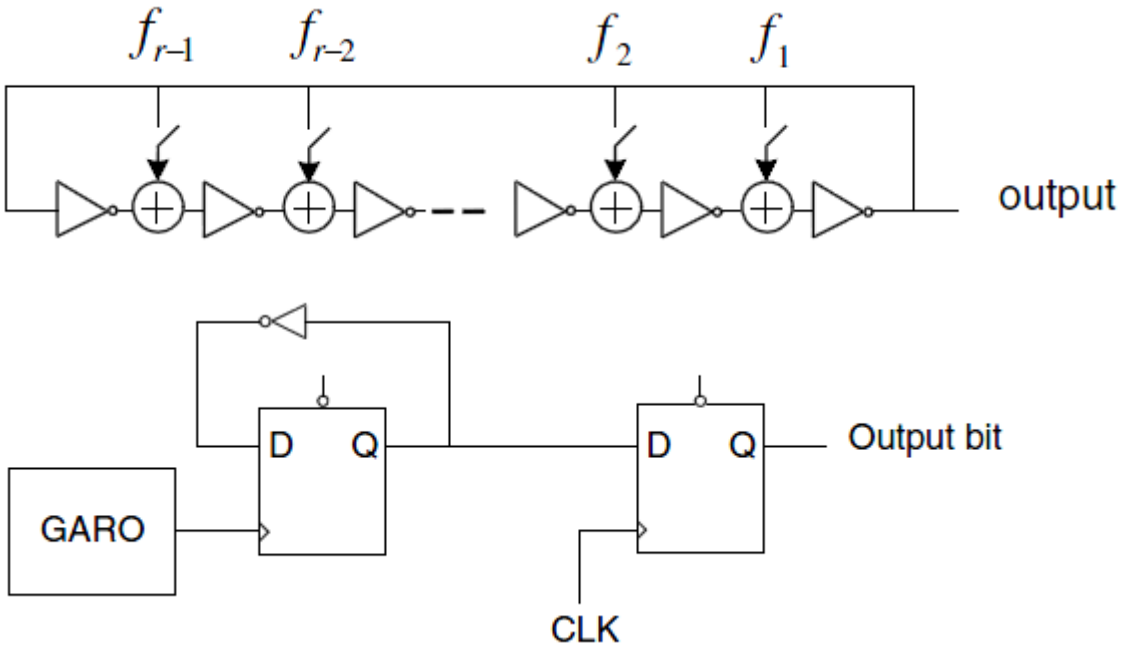
  (Ring-Oscillatoren, Phasenreglerschleifen)
- Geringe Datenrate



- TRNG 1:
  - f_{CLK} = 40 MHz
  - 114 RO mit 13 Invertern
  - Bose-Chaudhuri-Hocquenghem-Code



- TRNG 2:
  - Meta-stabiler RO
  - Inverter als unabhängige Noise-Quellen



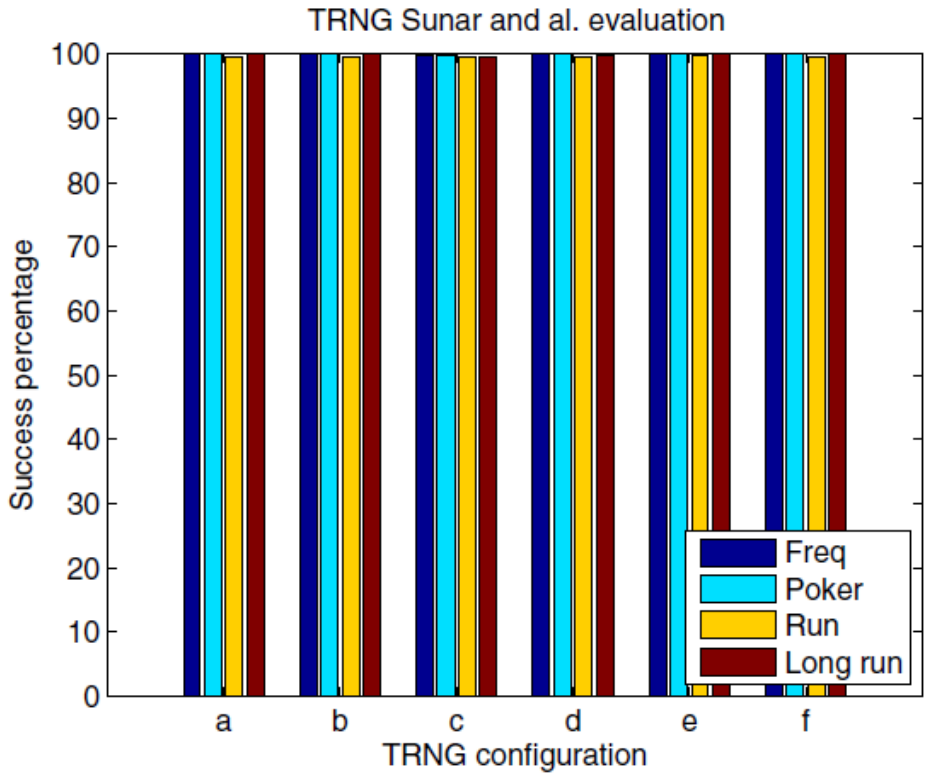
- TRNG 3:
  - GARO Generator
  - 6 CLK Run RO – 4 CLK Hold - 6 CLK Wait RO

- 2,5 Mbits/s
- Altera Stratix II EP2S60 (FPGA)
  - Möglicher Bereich: -40° C – 100° C
  - Empfohlener Bereich: 0° C – 55° C
  - Verwendete Temperaturen: 25° C, 55° C, 75° C
  - Ohne andere Aktivität, unter Volllast

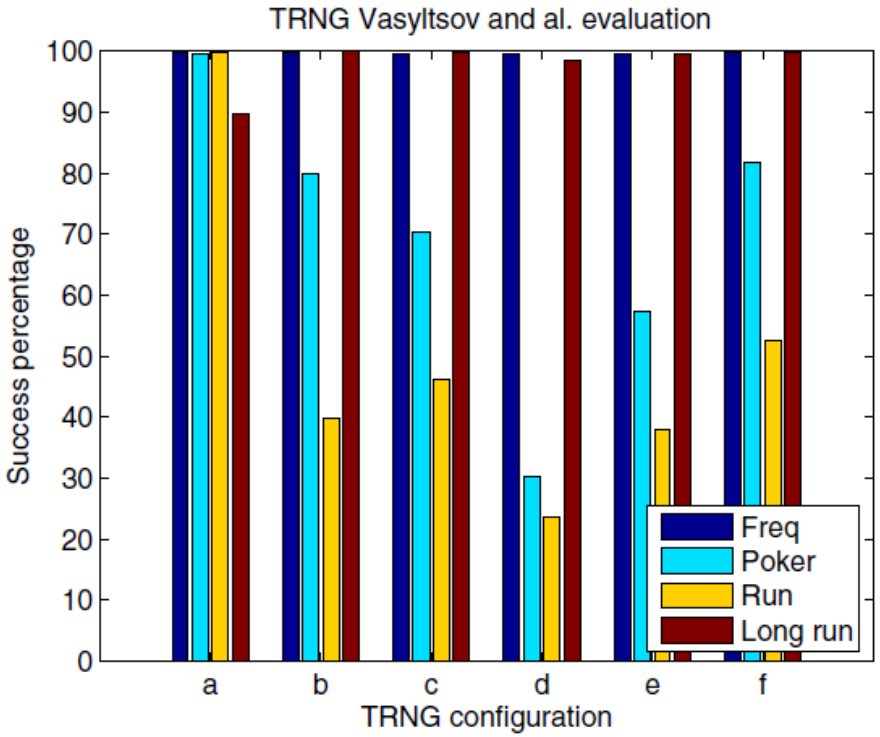
- Hardware statistical Tests
  - Ausgabe der Testresultate
  - Effiziente Implementierung
  - Geringe Fläche
  - Ausreichende Entfernung zu TRNG

- FIPS 140-2
  - Frequenz Test
  - Poker Test
  - Run Test
  - Long Run Test
  - 500 Testläufe

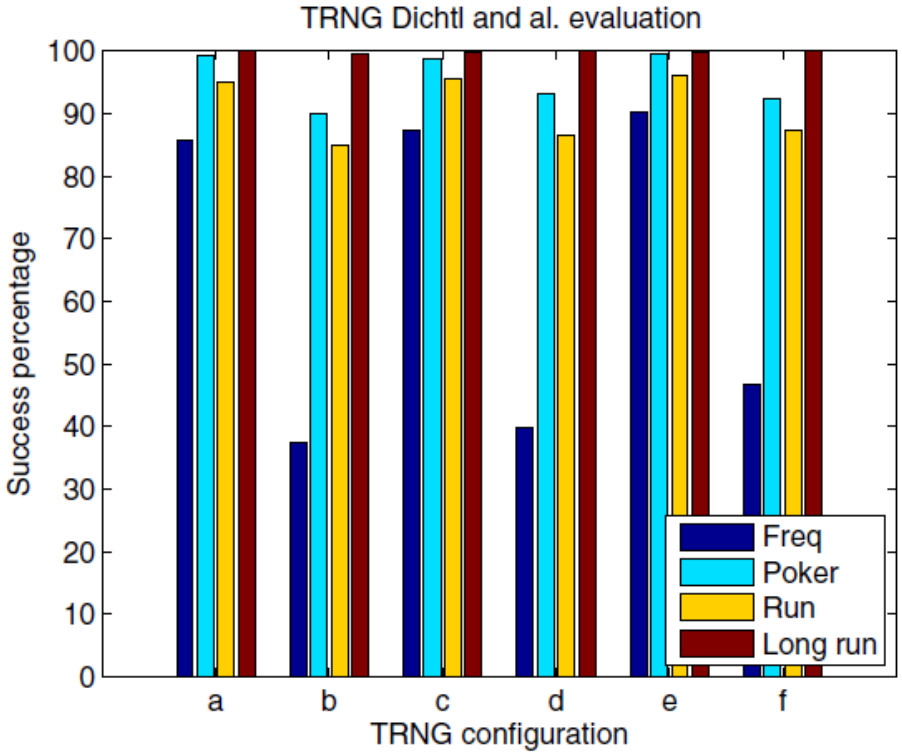
TRNG 1


TRNG Sunar and al. evaluation
Success percentage
100
90
80
70
60
50
40
30
20
10
0
a
b
c
d
e
f
TRNG configuration
Freq
Poker
Run
Long run

TRNG 2


TRNG Vasyltsov and al. evaluation
Success percentage
100
90
80
70
60
50
40
30
20
10
0
a
b
c
d
e
f
TRNG configuration
Freq
Poker
Run
Long run

TRNG 3


TRNG Dichtl and al. evaluation
Success percentage
100
90
80
70
60
50
40
30
20
10
0
a
b
c
d
e
f
TRNG configuration
Freq
Poker
Run
Long run

TRNG	ALUT Anzahl
1	1652
2	9
3	73

TRNG	Verbrauch in mW
1	45,359
2	2,52
3	3,96

ALUT - Altera Stratix II EP2S60

Verbrauch – Actel Igloo AGL125V2

- FIPS 140-2
  - Real-time Evaluation möglich
  - Geringer Flächenbedarf
  - TRNG kann auf dem selben Chip evaluiert werden

- [1] On-the-Fly Evaluation of FPGA-Based True Random Number Generator, IEEE 2009, Renaud Santoro, Olivier Sentieys, Sébastien Roy

»Wissen schafft Brücken.«