Technical university of Kosice, Slovakia
Department of Electronics and Multimedia Communication

New FPGA based TRNG Principle Using Transition Effect with Built-In Malfunction Detection

Michal Varchola, Milos Drutarovsky

CryptArchi 2009
Prague, June 24-27

Agenda

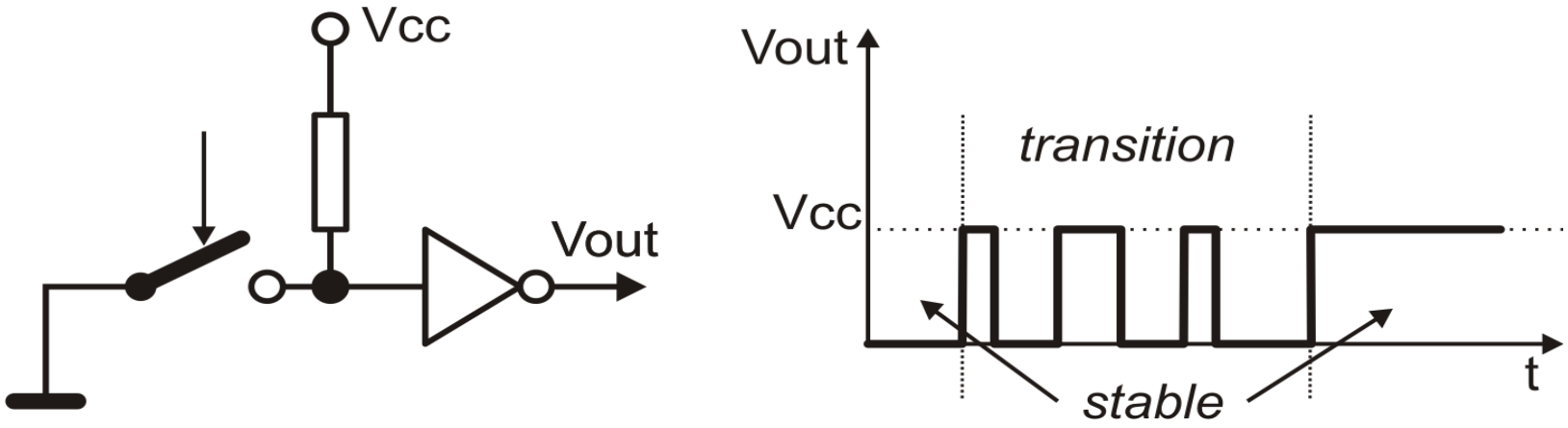
- TRNG State of the Art
- Transition Effect
- A Roadmap to the Transition Effect in the FPGA
  - Modified Ring Oscillator
  - Transition Effect Ring Oscillator
- TRNG Based on the Transition Effect
- Transition Effect TRNG Experimental Results
- Conclusion
- Future Work

TRNG State of the Art

- TRNGs based on the Jitter of the Ring Oscillators
- TRNGs based on the Jitter of the PLLs
- TRNGs based on Metastability
- *TRNGs based on Transtion Effect*

Transition Effect

- one of the first challenge of an embedded designer:

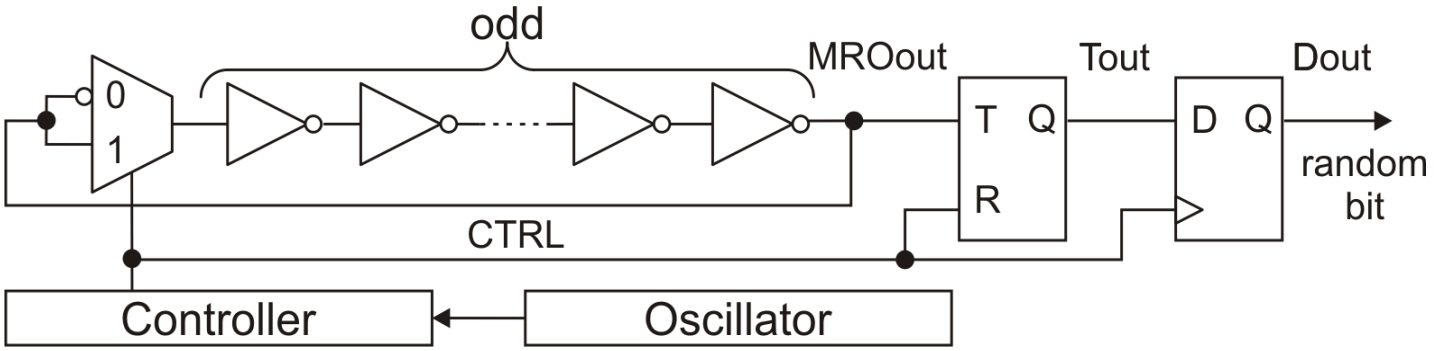


Transition effect:

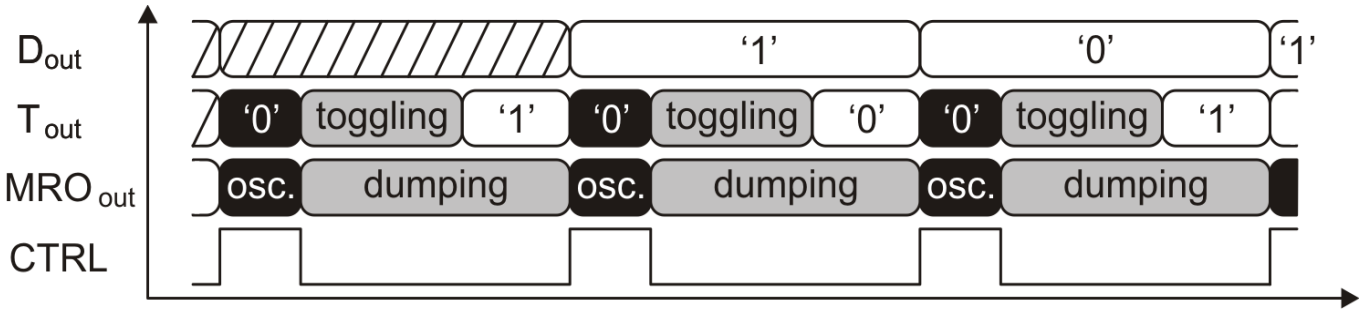
- An undetermined behavior of the circuit between two stable deterministic states
- Perhaps, a good source of randomness, but how to use it inside FPGA?

A Roadmap to the Transition Effect in the FPGA

- Modified Ring Oscillator (MRO) – Schematic Diagram and Timing



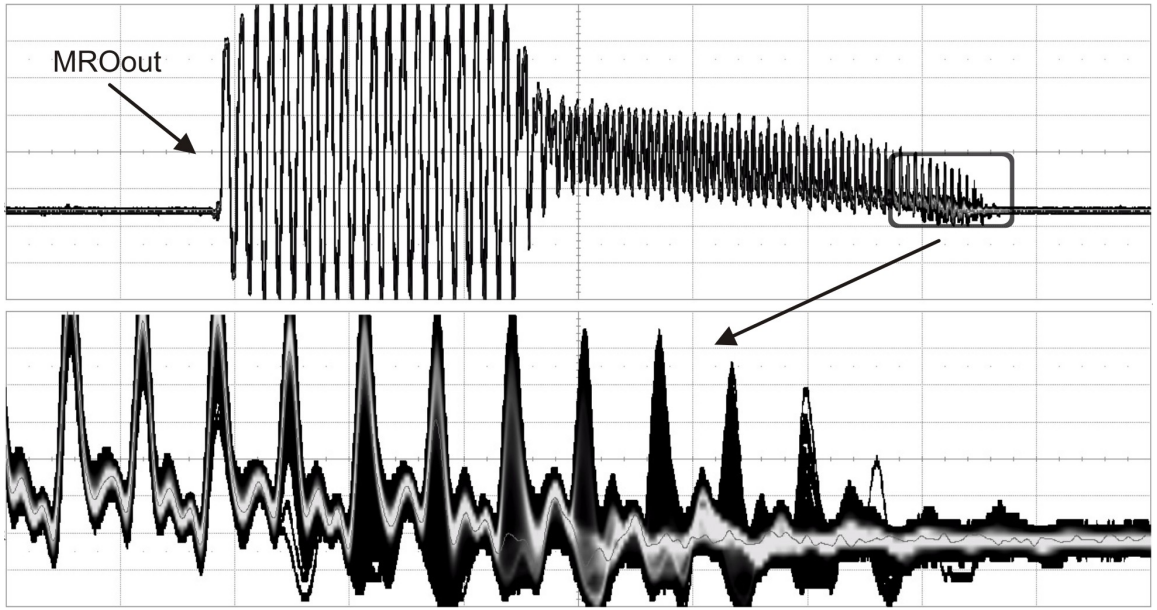
A MRO with a 1-bit randomness extractor

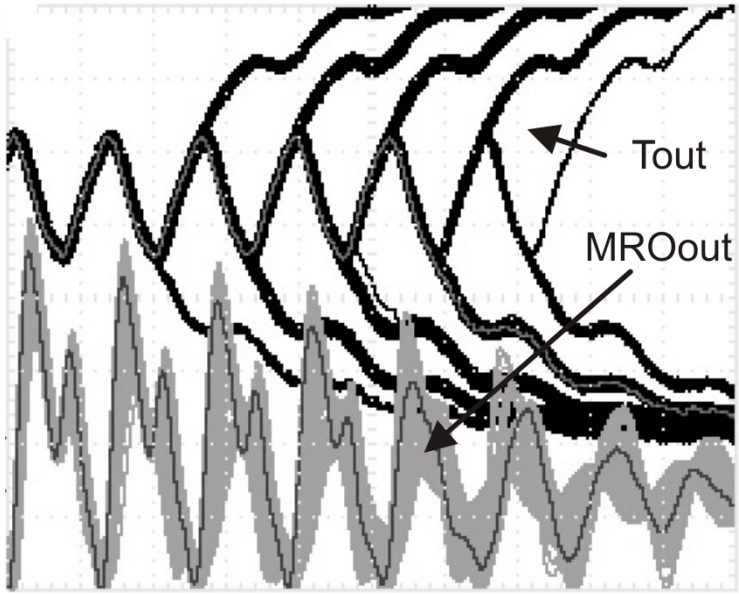


Timing of 1-bit randomness extraction using MRO as the source of randomness

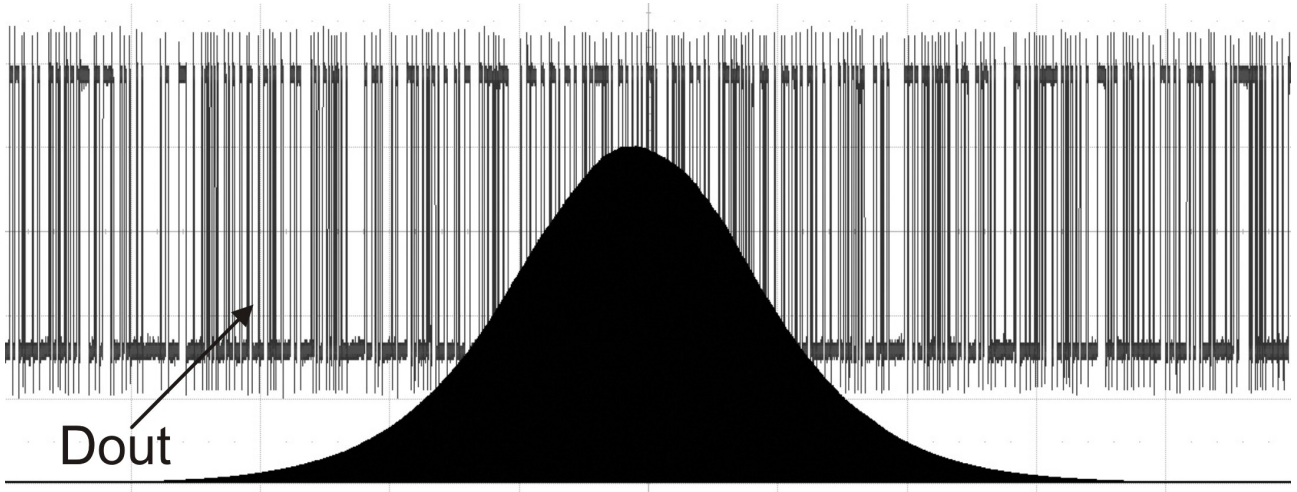
A Roadmap to the Transition Effect in the FPGA

- Modified Ring Oscillator – Oscilloscope Screenshots





Output signal of MRO during one cycle of the control signal and randomness extraction by a T-flip-flop



Histogram of averaged output random bits measured by the LeCroy oscilloscope

A Roadmap to the Transition Effect in the FPGA

- Modified Ring Oscillator – Verdict, Pros and Cons

Transition Effect:

- Oscillation mode (deterministic oscillation)
- Dumping mode (various number of oscillation)
- Stable after the oscillation disappears

Pros:

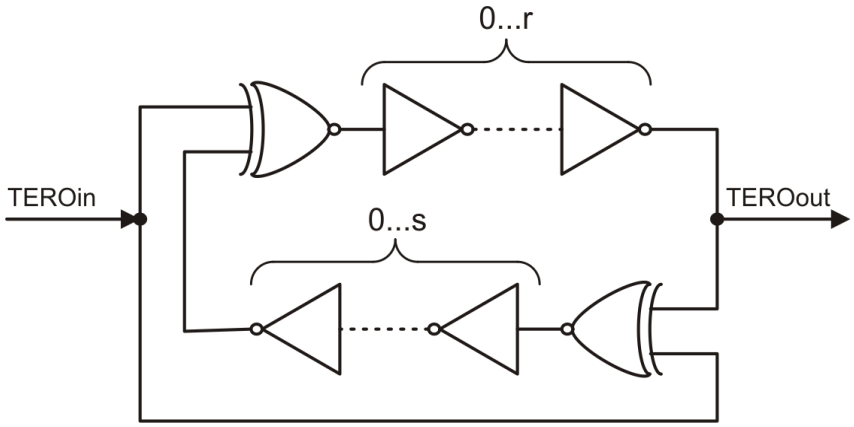
- Possibility of the synthesis for FPGA (tested for Actel Fusion FPGA)
- Small
- Possibility of malfunction detection by counting the number of oscillation in one period of control signal

Cons:

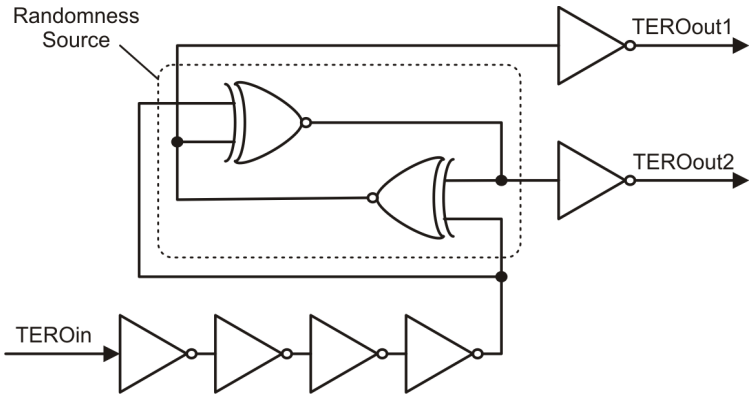
- Extremely dependent on the working conditions – source of randomness can stop even completely
- Place and Route dependent

A Roadmap to the Transition Effect in the FPGA

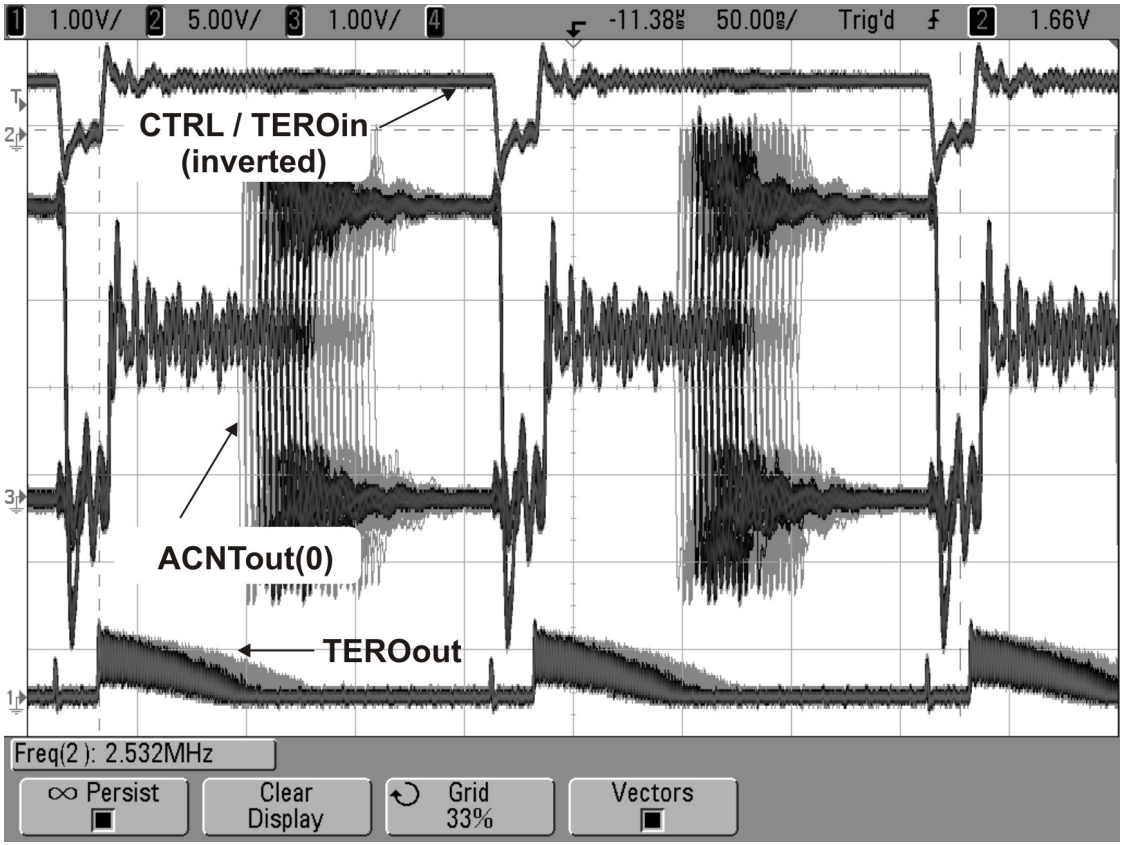
- Transition Effect Ring Oscillator (TERO) – Basic principle



General circuitry of the TERO



Used circuitry of the TERO for the experiments



Output of the TERO in two periods of the control signal and 1-bit randomness extraction by the first stage of an asynchronous counter

A Roadmap to the Transition Effect in FPGA

- Transition Effect Ring Oscillator – Verdict, Pros and Cons

Transition Effect:

- Stable
- Oscillation Dumping (various number of oscillation)
- Stable

Pros:

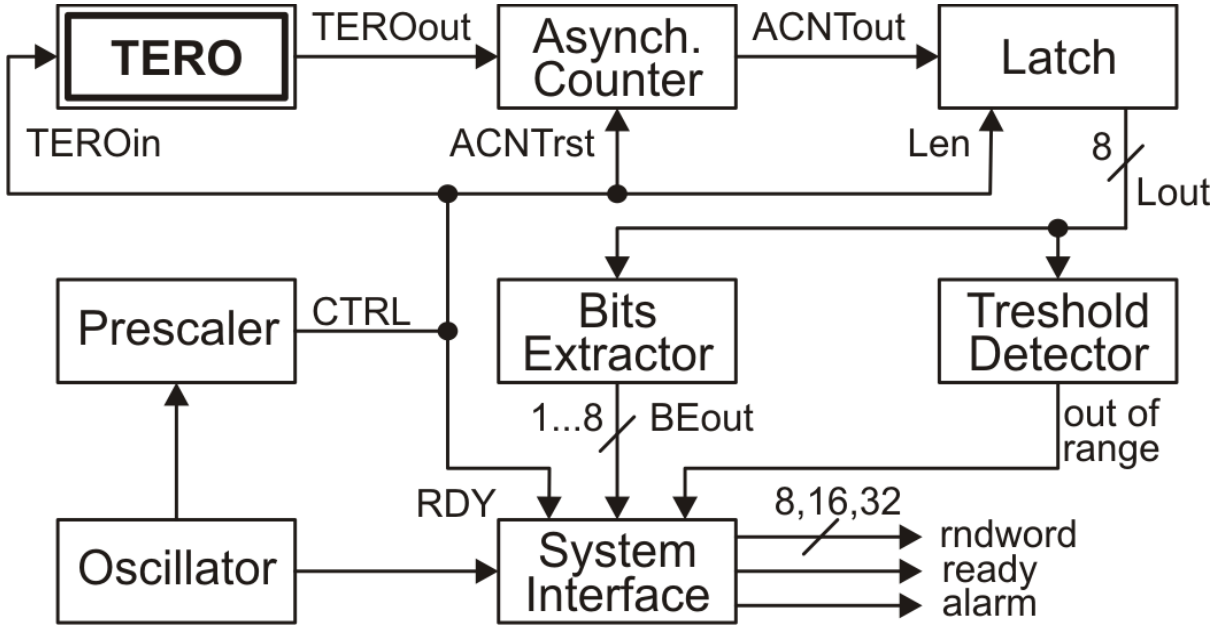
- Possibility of the synthesis for FPGA (tested for Xilinx Spartan 3E)
- Very small
- Possibility of malfunction detection by counting the number of oscillation in one period of the control signal
- Supressed working condition dependence
- Fast

Cons:

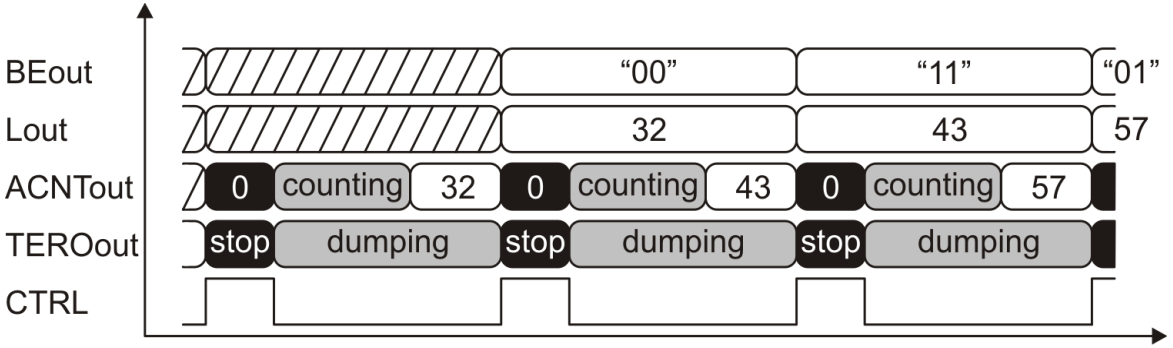
- Place and Route dependent

TRNG Based on the Transition Effect

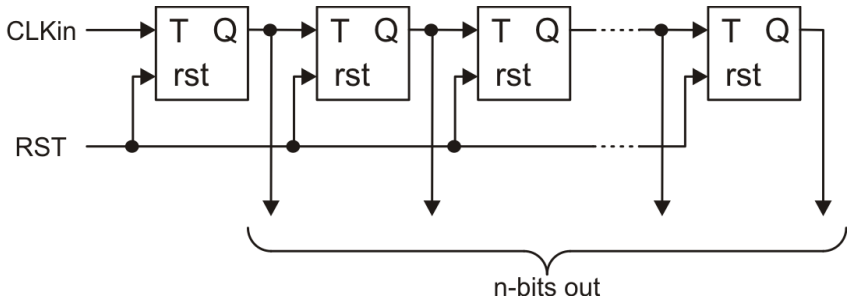
- Block Diagram and Timing



Block diagram of the TRNG based on the TERO with Malfunction Detection



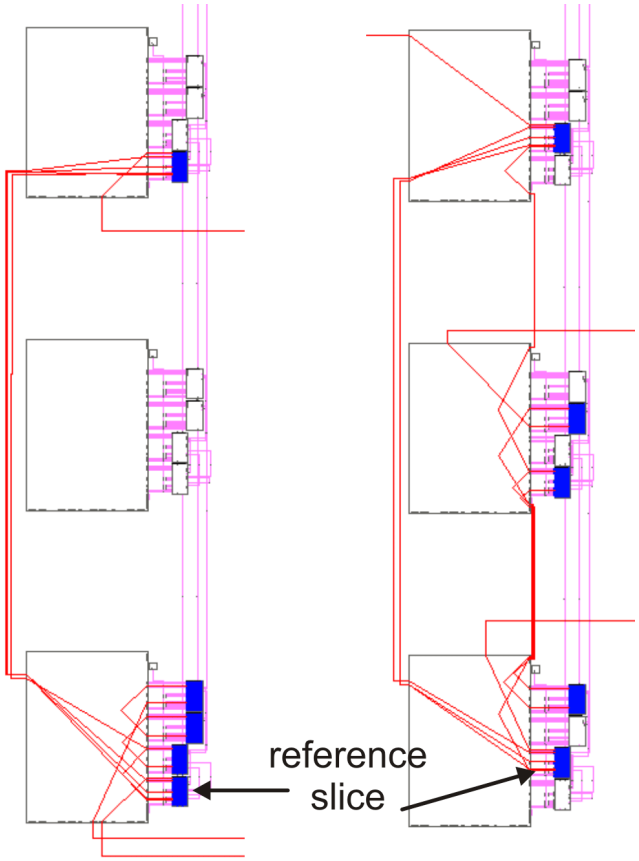
Timing of the TRNG based on the TERO



Asynchronous counter as a randomness extractor

Transition Effect TRNG Experimental Results

- Manual Place and Route (P&R), FIPS 140 Tests results



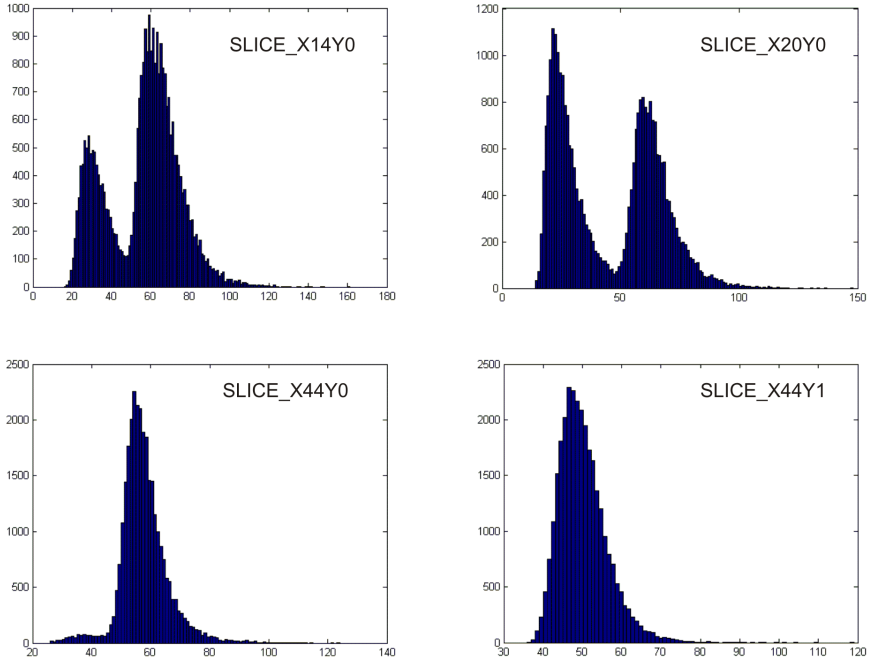
Two different manual P&R of the TERO in the Spartan 3E FPGA fabric;
Left: X14Y0, X20Y2, X44Y0, X48Y2
Right: X44Y1

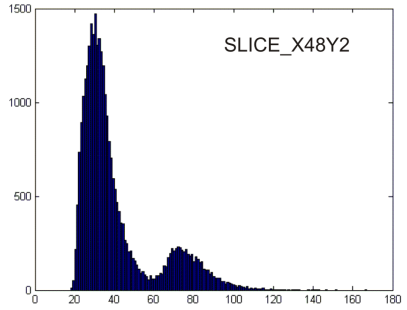
Core Voltage	X14Y0	X20Y2	X44Y0	X44Y1	X48Y2
1020 mV	FFFF	FPPP	PPPF	PPPP	PPPP
1080 mV	FFPP	FPPP	PPFF	PPPP	PPPP
1140 mV	FPPP	PPPP	PPFF	PPPP	PPPP
1200 mV	PPPP	PPPF	PPPF	PPPF	PPPP
1260 mV	PPPP	PPPF	PPPF	PPFF	PPPF
1320 mV	PPPF	PPPF	PPPF	PPFF	PPPF
1380 mV	PPPF	PPPF	PFFF	PFFF	PPPF
1440 mV	PPFF	PPFF	PPPF	FFFF	PPFF

Results of FIPS 140 tests for various P&R for 1,2,3 and 4 extracted bits from the counter values during one period of the control signal (Vcore = 1200mV, $V_{core_{min}}$ = 1140mV, $V_{core_{max}}$ = 1260mV)

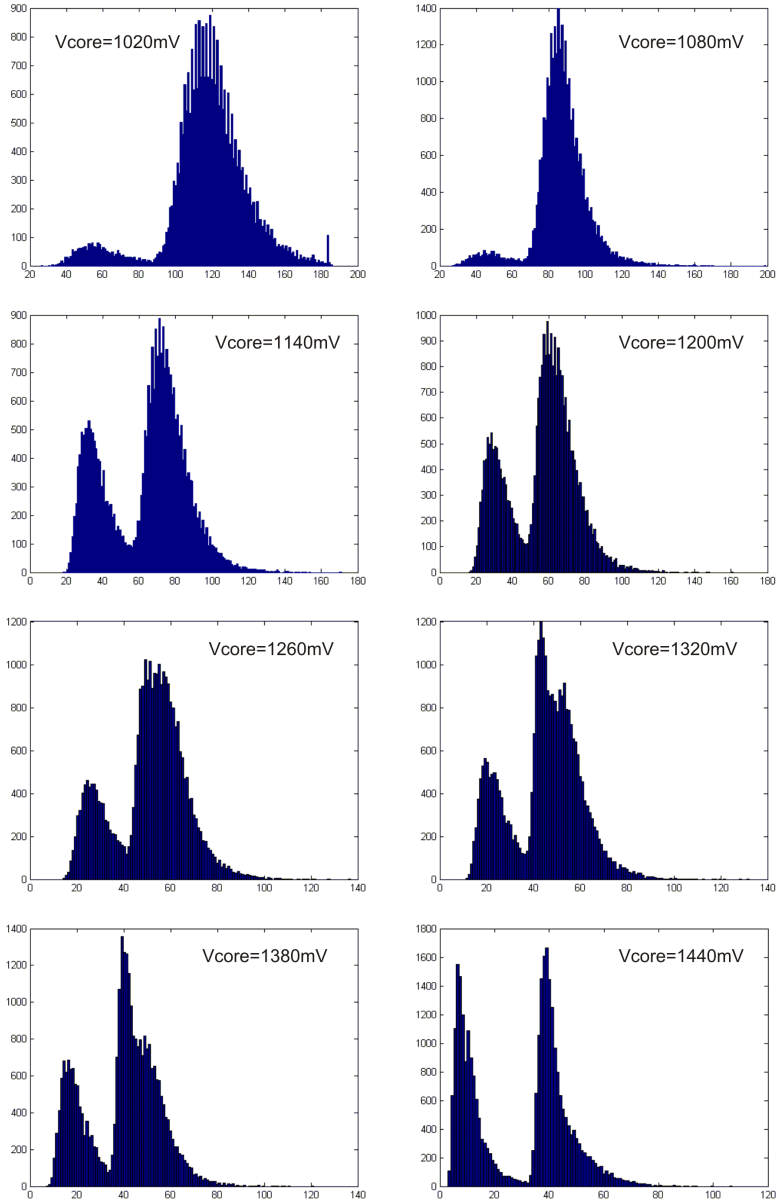
Transition Effect TRNG Experimental Results

- Manual Place and Route, Oscillations count values





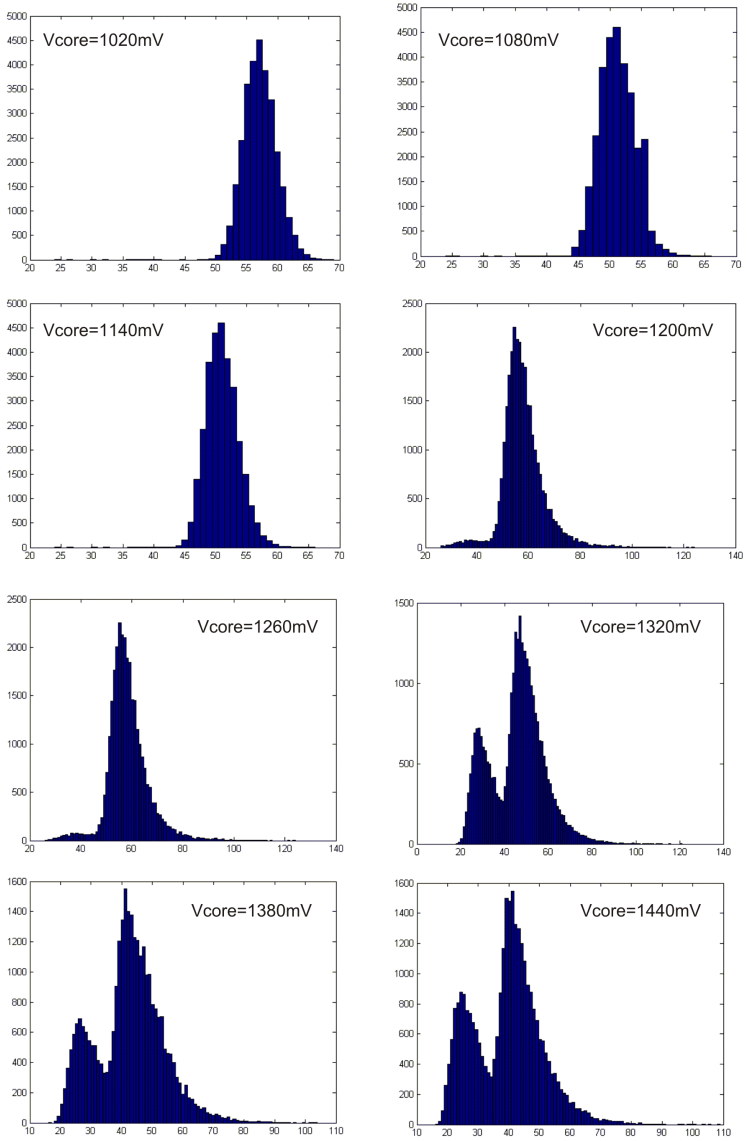
Vcore = 1200mV



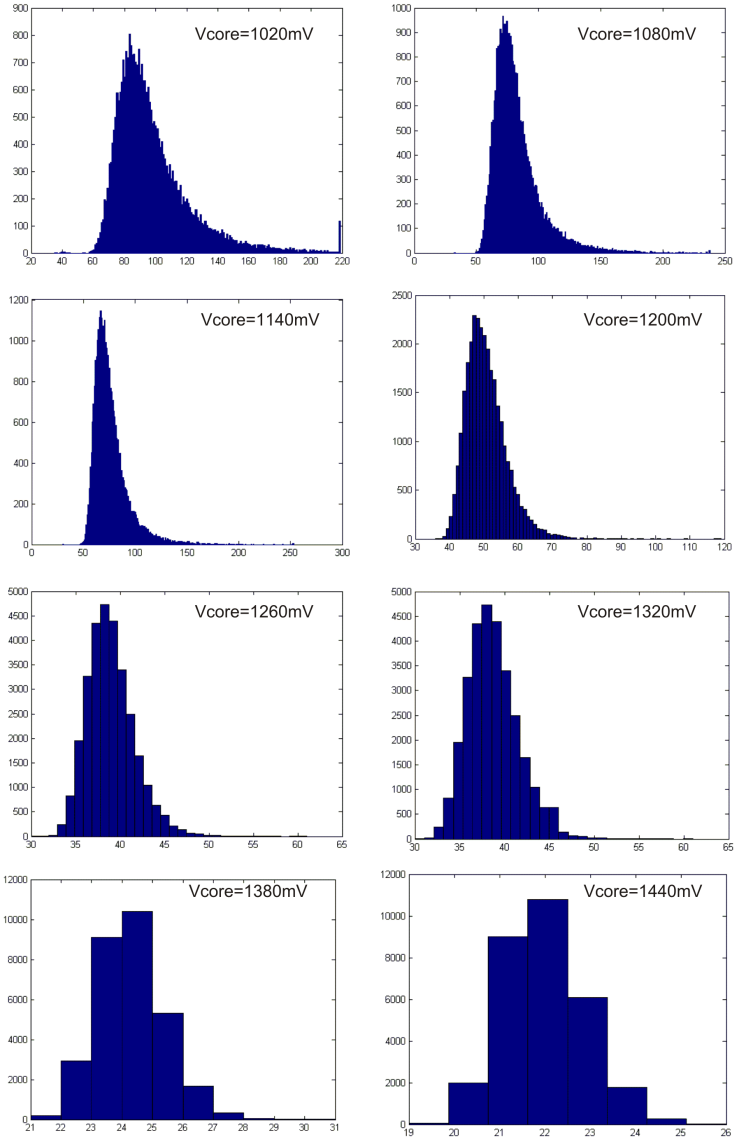
X14Y0

Transition Effect TRNG Experimental Results

- Manual Place and Route, Oscillations count values



X44Y0



X44Y1

Transition Effect TRNG Conclusion

- **TERO** as new source of randomness in FPGAs
- **Low area:** only two LUTs configured as XNORs represent source of the randomness
- **High speed:** High dispersion of counter values provides extraction of several bites what results up to 10 Mbps speed in the shown example
- **Increased security I:** Stateless design without memory – each random bit is generated from the same conditions
- **Increased security II:** Each generated bit can be evaulated easily by testing if the number of the oscilations done fits into the treshold region; If generated bit does not fulfill required criteria, it will be thrown away and an alarm can be issued
- **Supressed** working condition dependence
- **Manual** Place & Route is still **necessary**

Transition Effect TRNG Future Work

- Stochastic model definition
- Practical Transition Effect TRNG design

Thank You for the Attention
Questions?