[1]TECHNICAL UNIVERSITY OF KOŠICE
Faculty of Electrical Engineering and Informatics
Department of Electronics and Multimedia Communications

[2]UNIVERSITÉ JEAN MONNET
Laboratoire Hubert Curien
UMR CNRS 5516, Saint Etienne, France

Evaluation of various TRNG principles implemented in Actel Fusion Flash FPGA

Michal Varchola[1], Miloš Drutarovský[1], Viktor Fischer[2]

CryptArchi 2008 Trégastel, France
June 1 - 4, 2008

Agenda

- Motivation
- Hardware Platform Overview
- PLL Based True Random Number Generator NIST-Tests Results
- Ring Oscillator Mutual Influence Evaluation
- Conclusion
- Future Work

Motivation

- Use recent modern Actel Fusion FPGA that includes following benefits for Cryptography:
  - Nonvolatile Flash FPGA fabric
  - Optional CoreMP7 – the only ARM7 soft-core processor
  - Embedded Flash and SRAM memories
  - Powerful analog front-end (ADC, MOSFET gate drivers)
  - Internal 100 MHz RC oscillator
- Implement PLL based TRNG with RC oscillator as an clock input
- Perform NIST test of implemented PLL based TRNG output
- Evaluate mutual influence of two ring oscillators

Hardware Platform Overview
Actel Fusion Flash FPGAs

CoreMP7	**–**	**M7AFS600**	**–**
Cortex-M1	**M1AFS250**	**M1AFS600**	**M1AFS1500**
System Gates	250,000	600,000	1,500,000
Tiles (D-flip-flops)	6,144	13,824	38,400
PLLs	1	2	2
Flash Memory Bits	2 M	4 M	8 M
FlashROM Bits	1 k	1 k	1 k
RAM Bits	36 k	108 k	270 k
Digital I/Os	114	172	252
Analog I/Os	24	40	40

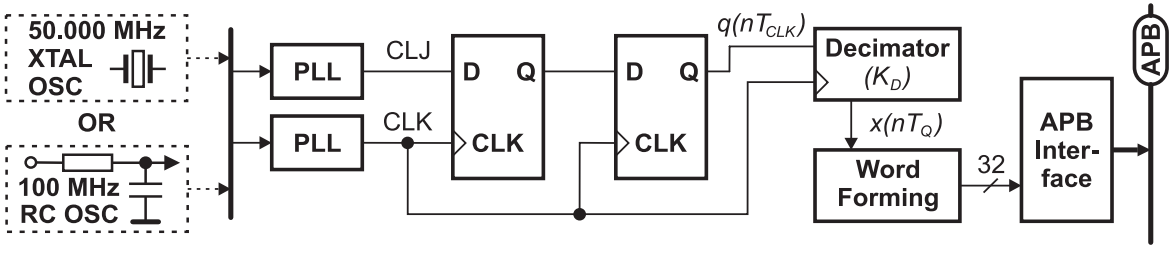
PLL based TRNG

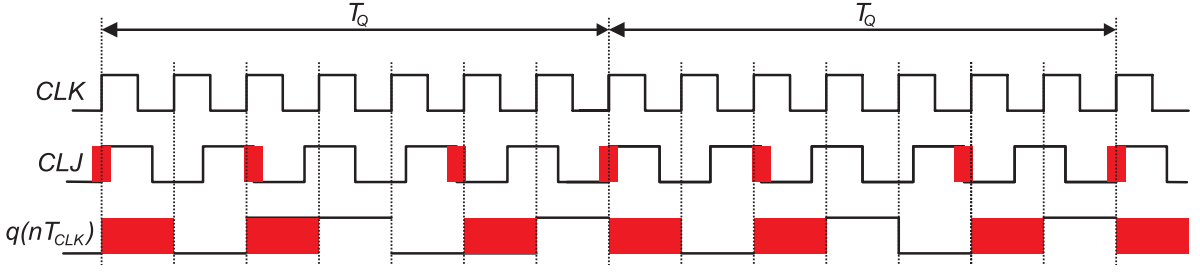
Principle of the Method

$$F_{CLJ} = \frac{M_{CLJ}}{D_{CLJ}} F_{OSC} \qquad K_D = D_{CLJ} M_{CLK} \qquad T_Q = \frac{1}{R} = K_D T_{CLK} = K_M T_{CLJ}$$

$$K_M = M_{CLJ} D_{CLK}$$

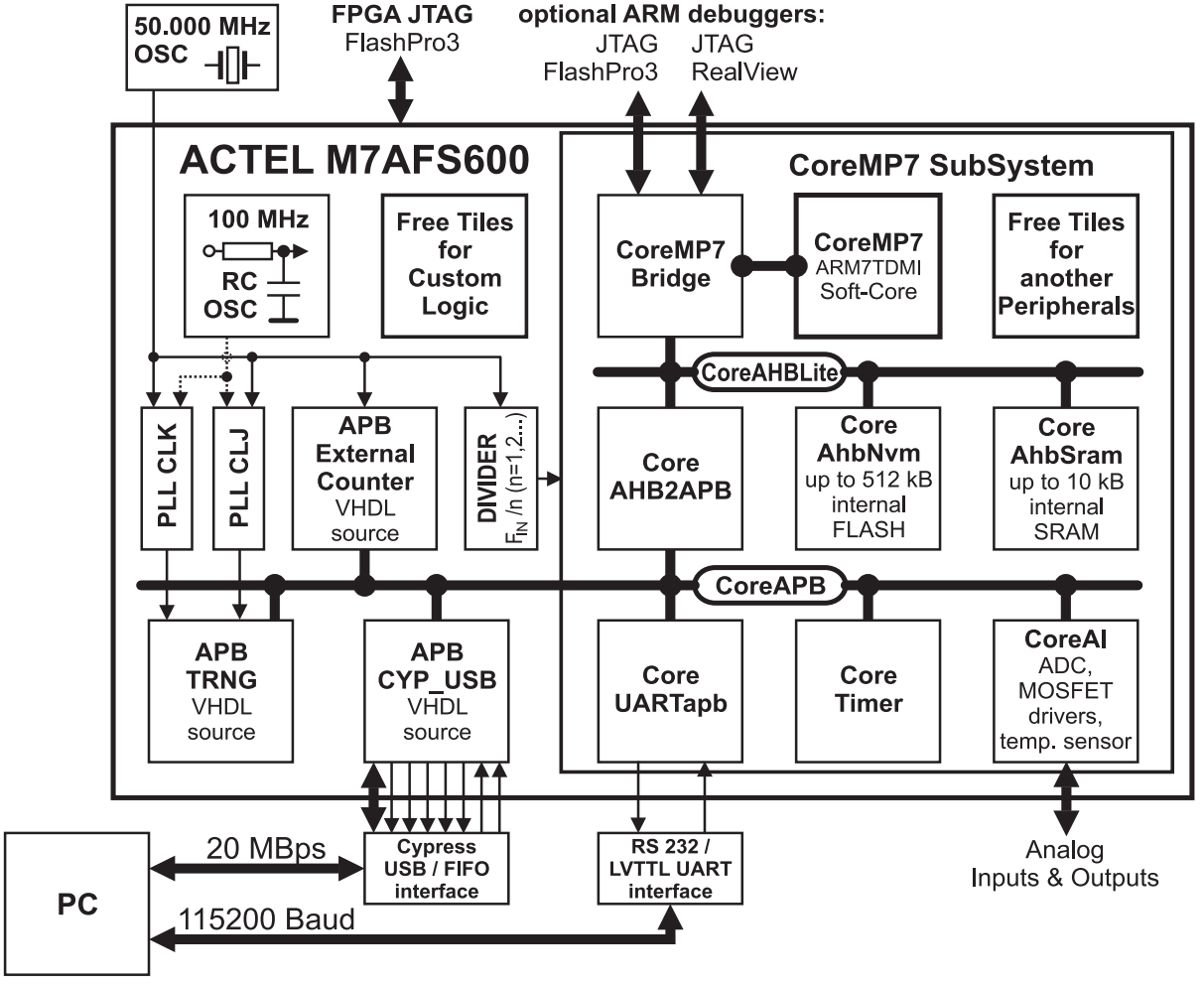
$$F_{CLK} = \frac{M_{CLK}}{D_{CLK}} F_{OSC} \qquad \sigma_{jit} \gg MAX\left(\triangle T_{\min}\right) \qquad MAX\left(\triangle T_{\min}\right) = \frac{T_{CLK}}{4K_M} GCD\left(2K_M, K_D\right)$$





PLL based TRNG

Implementation of the Measurement Method

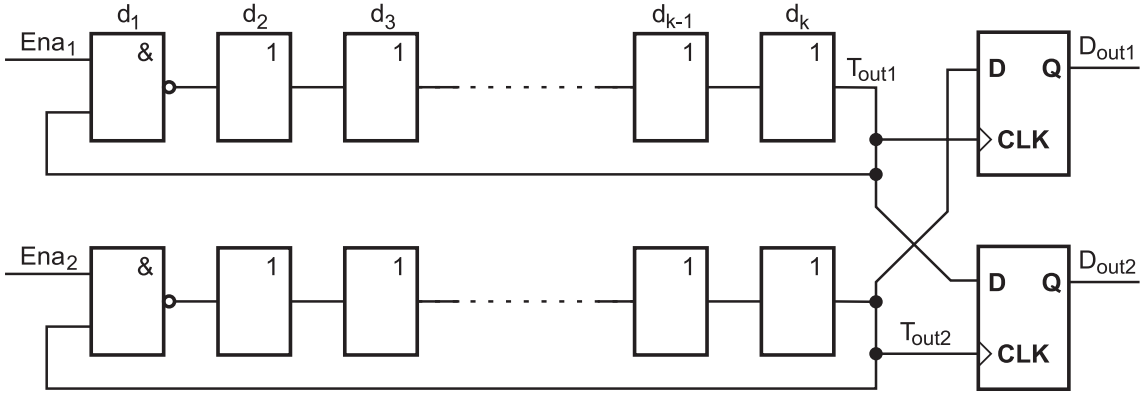


PLL based TRNG

Experimental Results - NIST Tests

Test	**40 kbps**	**1 Mbps**
Frequency	0.9940	0.0000*
Block Frequency	0.9960	0.0000*
Cumulative Sums	0.9920	0.0000*
Runs	0.9920	0.0000*
Longest Run	0.9920	0.0680*
Binary Matrix Rank	0.9900	0.9880
Discrete Fourier Transform	0.9820	0.0080*
Non-overlapping Template Matching	0.9840	0.0000*
Overlapping Template Matching	0.9920	0.0000*
Universal	0.9900	0.6200*
Approximate Entropy	0.9880	0.0000*
Random Excursion	0.9908	0.0000*
Random Excursions Variant	0.9908	0.0000*
Serial	0.9880	0.0000*
Linear Complexity	0.9920	0.9940
Result	**pass**	**not pass**

Ring Oscillator (RO)
Principle of Operation

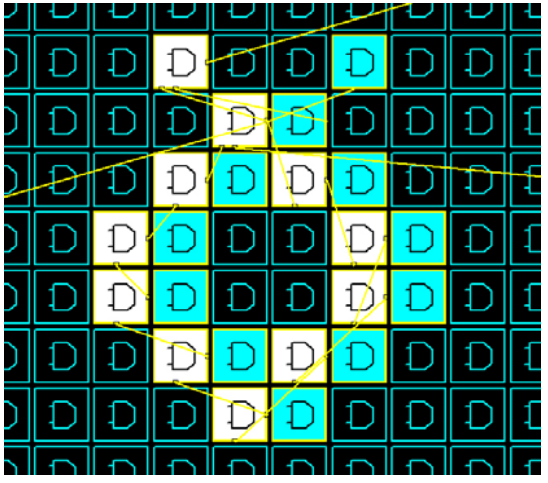


Testing Circuit for observation of influence between two ROs depending on their mutual position inside the FPGA

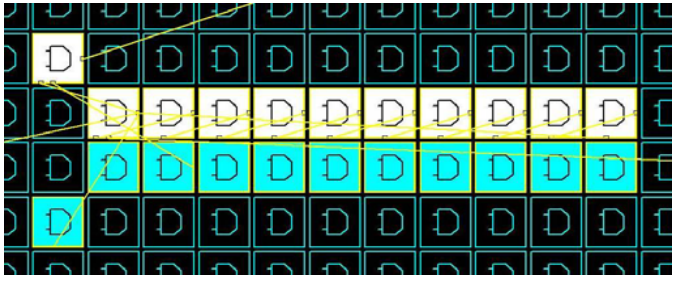
$$T_{out} = 2\sum_{i=1}^{k} d_i$$

Period of RO's output signal

Ring Oscillator (RO)
Examples of Implementation

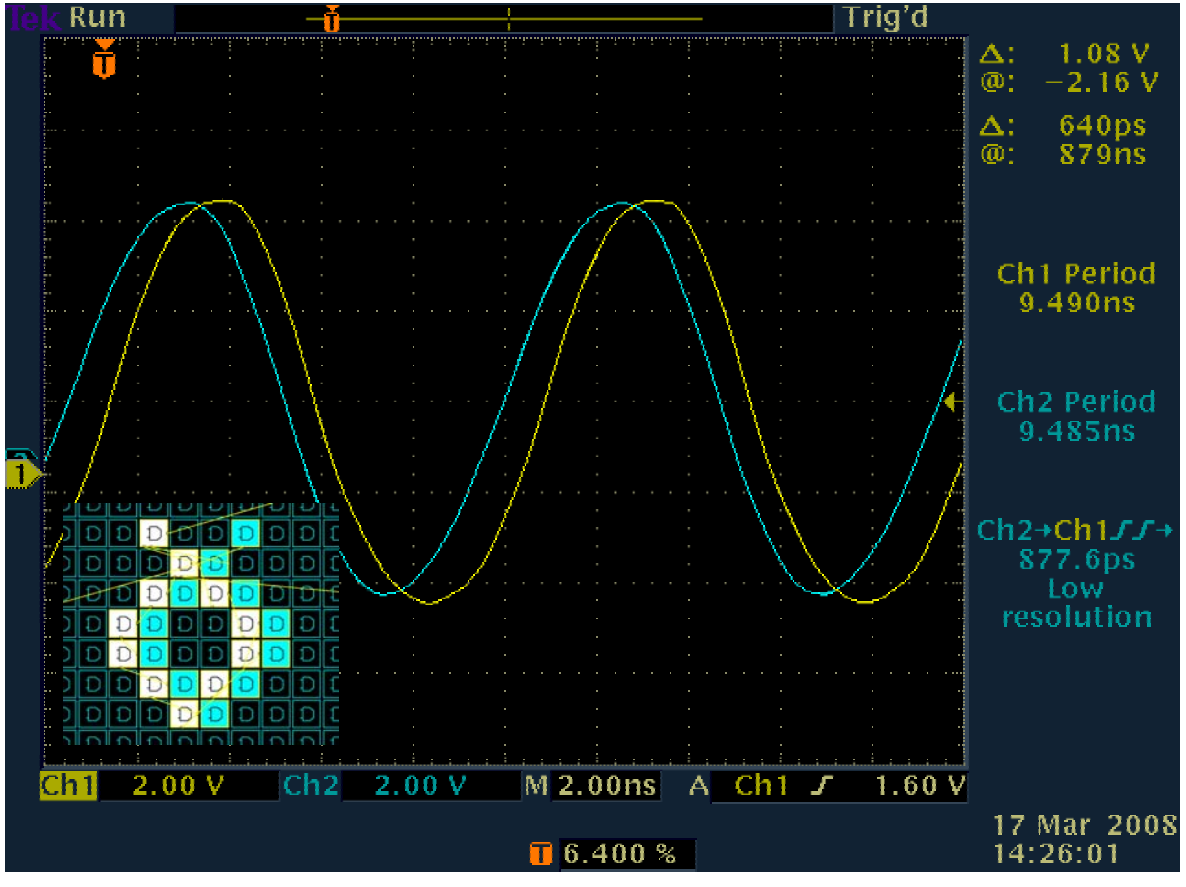


Circular layout



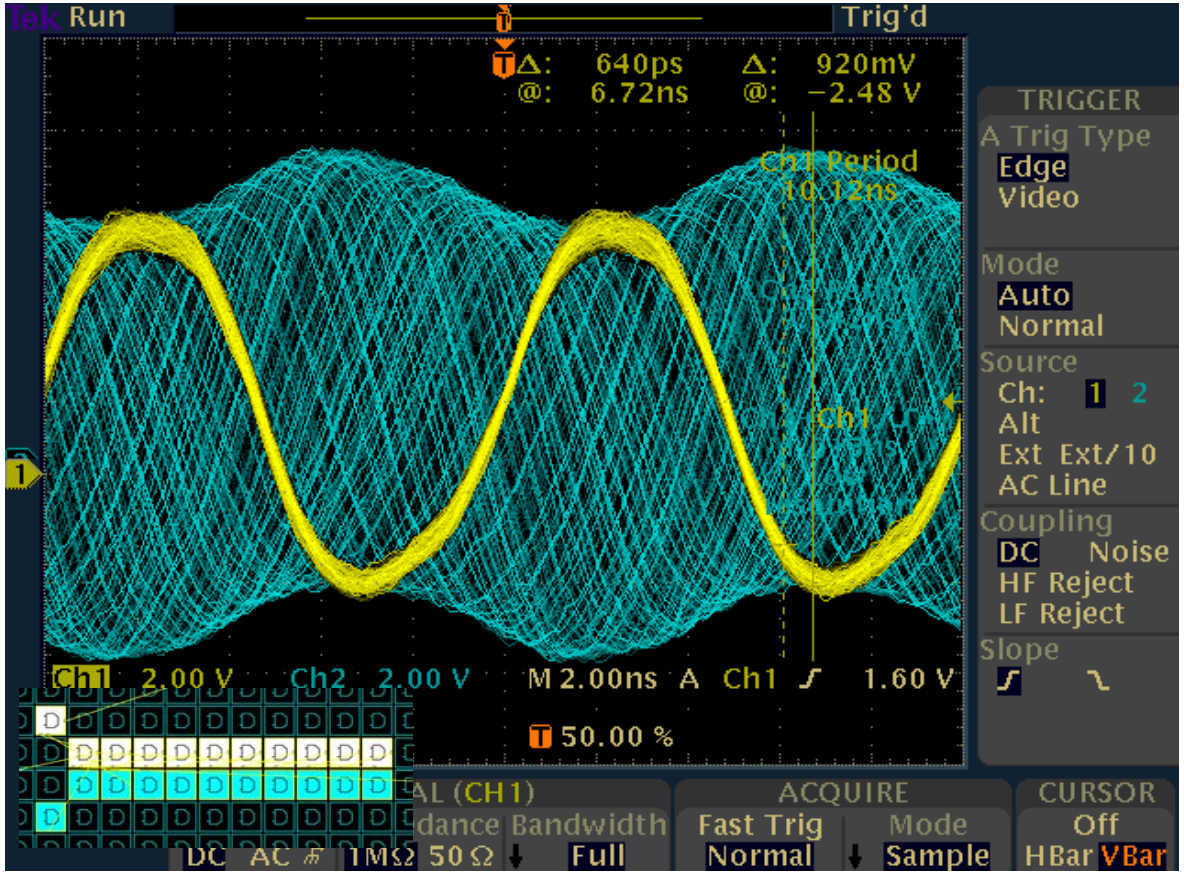
Linear layout

RO Experimental Results (1/4)
Synchronized and Unsynchronized ROs



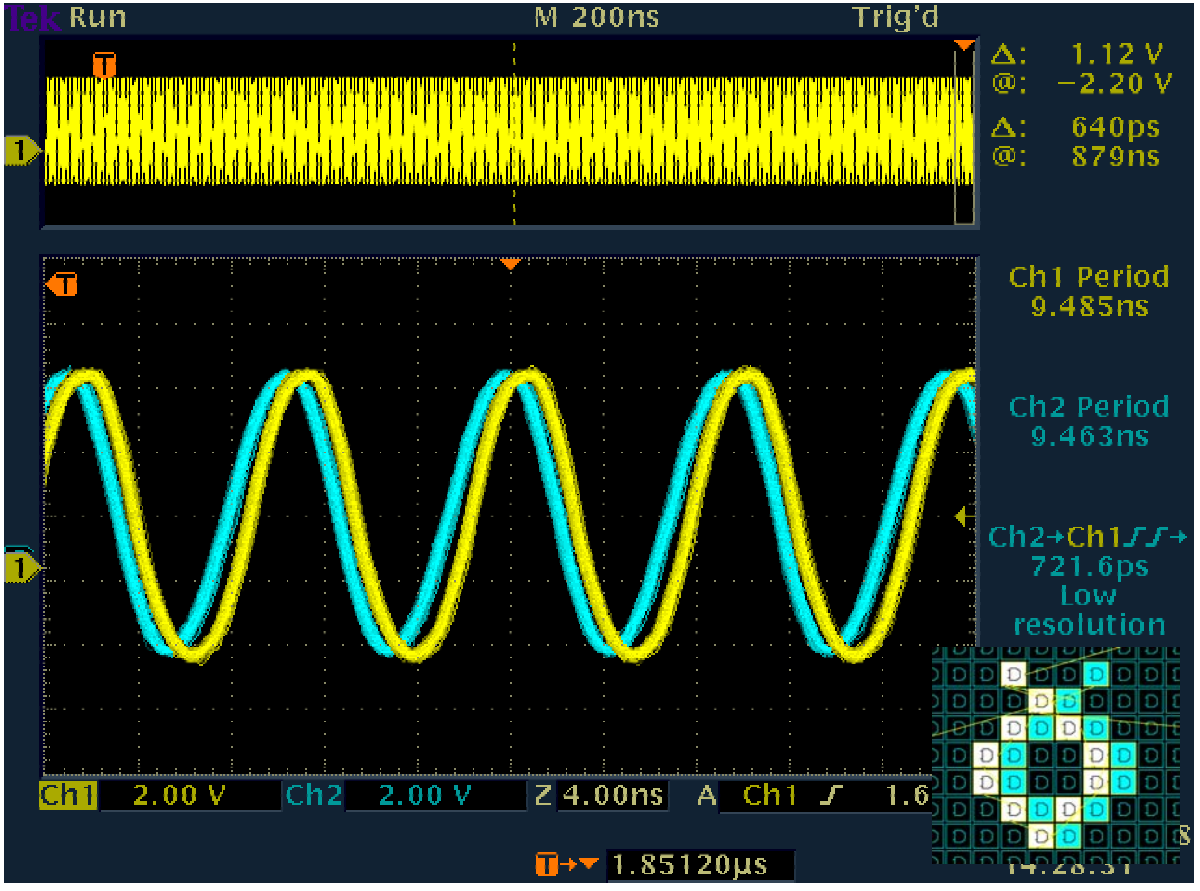
Output signals of two ROs are synchronized each other using their circular layout where trigger was set for “yellow” channel

RO Experimental Results (2/4)
Synchronized and Unsynchronized ROs



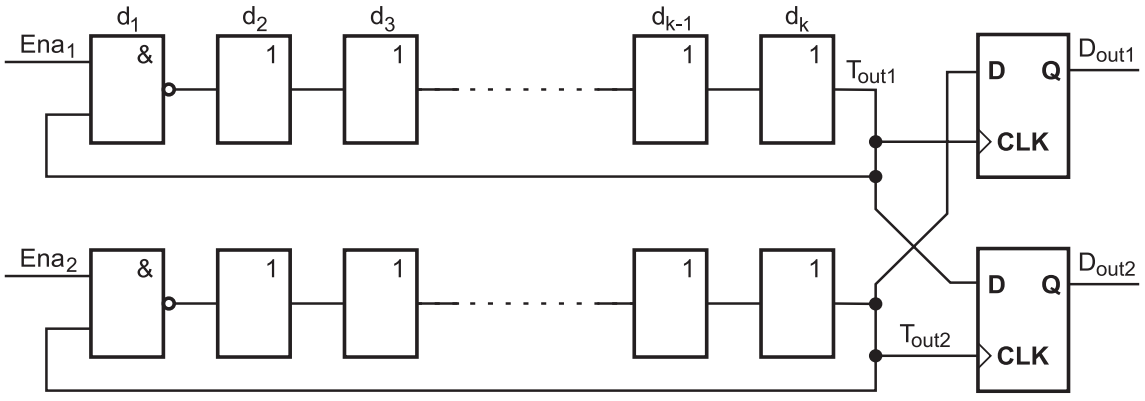
Output signals of two ROs are unsynchronized using their linear layout where trigger was set for “yellow” channel

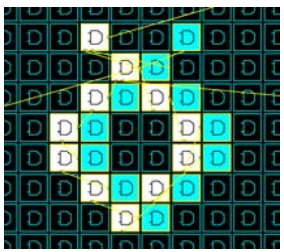
RO Experimental Results (3/4)
Waveform Development of Two Synch. ROs



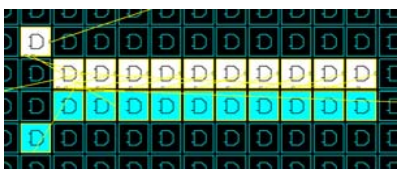
Waveform development of two ROs 1.85µs after triggering using circular layout with displayed jitter where trigger was set for “yellow” channel

RO Experimental Results (4/4)
Proof of the ROs' synchronization





D_{out1} and D_{out2} signals had constant value during test using the Circular Layout



D_{out1} and D_{out2} signals did not have constant value during test using the Linear Layout

Conclusion

- The first complex NIST tests of PLL based TRNG in Actel platform.
- Possibility of using an internal RC oscillator for the TRNG purpose to enhance security (no external TRNG component is necessary).
- Noted mutual influence of ring oscillators.
- CoreMP7 – ARM7 compatible processor core significantly decreased development time of USB communication protocol.

Future Work

- More complex analysis on:
  - Quality of generated true random numbers
  - PLL based TRNG principle
  - RO mutual influence
- On-chip countermeasures:
  - On-chip power consumption and voltage level measurement by ADC included in Fusion FPGA
  - Online testing of random source quality

Thank You for Your Attention