LABORATOIRE Hubert CURIEN
UMR • CNRS • 5516 • ST-ETIENNE

Embedded testing of the source of randomness in FPGAs

Clock jitter evaluation and measurements

Viktor Fischer, Florent Bernard, Alain Aubert, Nathalie Bochard
(fischer, florent.bernard, alain.aubert, Nathalie.Bochard)@univ-st-etienne.fr
Laboratoire Hubert Curien
UMR 5516 CNRS Université Jean Monnet, Saint-Etienne, France

Outline

- Introduction
- Clock jitter as a source of randomness
  - definitions and measurements
- Embedded measurement of the clock jitter in ring oscillators
- Embedded measurement of the clock jitter in PLLs
- Conclusions

Introduction (1/3)

- Use of RNGs in cryptography
  - Generation of cryptographic keys (symmetric, public, private) – needs special security requirements
  - Generation of initialization vectors
  - Generation of nonces
  - Generation of padding values
  - Counter-measures against side-channel attacks
- Required characteristics of RNGs in cryptography
  - Good statistical parameters of the output numbers
  - Unpredictability of the output
  - (Inner) testability
  - (Provable) security – robustness, – resistance against attacks

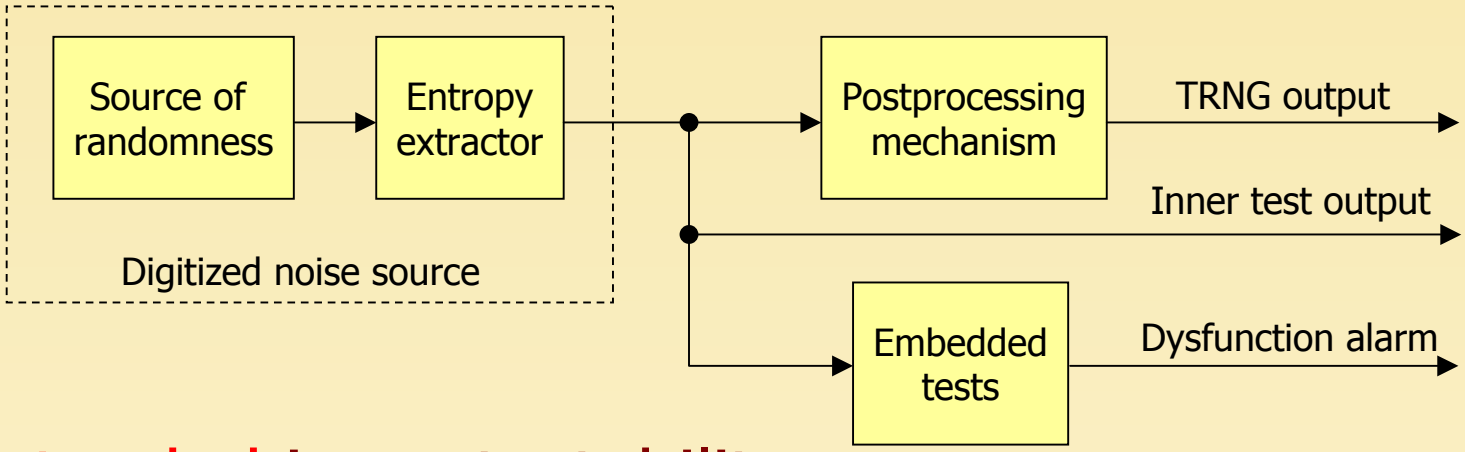
} New security requirements

Introduction (2/3)

- Testing TRNG output
  - Tests designed for PRNGs (NIST Test Suite, DIEHARD) are commonly used → the entropy is not evaluated
  - If these tests do not pass, the sampling frequency can be reduced or post-processing methods can be used
  - New tests were proposed specifically for TRNGs by BSI (AIS31) – entropy testing
  - New paradigm: the designers should provide
    - Mathematical model of the principle (if it exists) and/or
    - RNG-specific test (before post-processing) and testing methodology

Introduction (3/3)

- Inner testability
  - Possibility to test the source of randomness (entropy) before a post-processing operation



- Extended inner testability
  - Enables to evaluate better the entropy: the test is equal to zero if the signal does not contain any entropy (e.g. deterministic signal)

Sources of randomness in FPGAs

- Delay variation of logic elements
  - Depending on physical processes and working conditions - supply voltage (fast fluctuations possible), temperature (slow variations)
  - Used in designs based on ring oscillators
- "Analogue" features of flip-flops
  - E. g. metastability - low entropy can be expected
- Jitter of clock signals
  - Free-running oscillators (e.g. RC oscillator in Actel Fusion FPGA)
  - On-chip PLL (or DLL) clock synthesizers in FPGAs

Jitter as a source of randomness (1/5)

- Jitter
  - a short-term variation of an event from its ideal position in time
- Jitter measurements
  - Phase jitter
  - Period jitter
  - Cycle-to-cycle jitter
  - Timing jitter and time-interval error (TIE)

  } Different measurements of the same jitter

  - Tracking jitter - only for PLLs and DLLs
- Jitter components
  - Random (Gaussian) jitter
  - Deterministic jitter

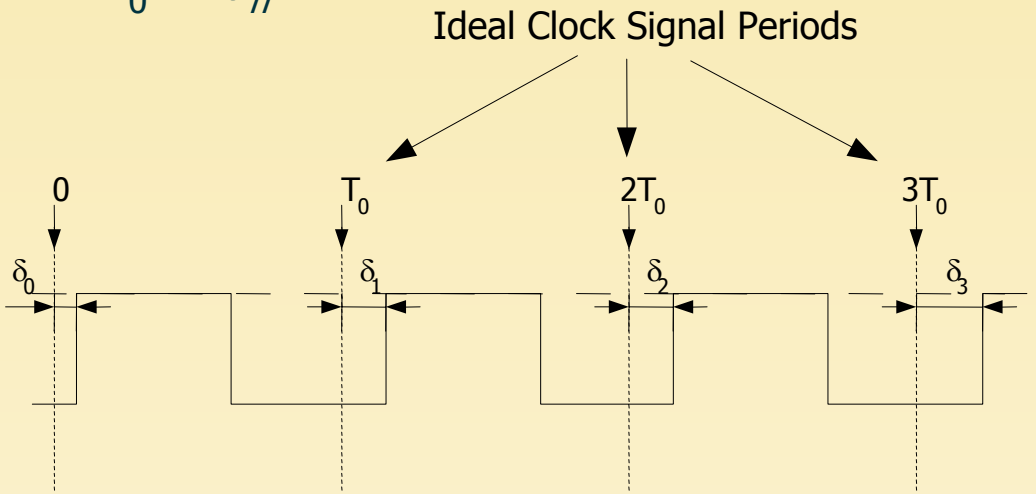
Jitter as a source of randomness (2/5)

- Phase jitter δ_n
  - phase advance of the observed clock from an ideal clock with period T_0 made in discrete time intervals nT_0

Cycle occurrences of a noisy clock signal:

$$t_n = nT_0 + \delta(nT_0) = nT_0 + \delta_n$$

$$\delta_n = t_n - nT_0$$

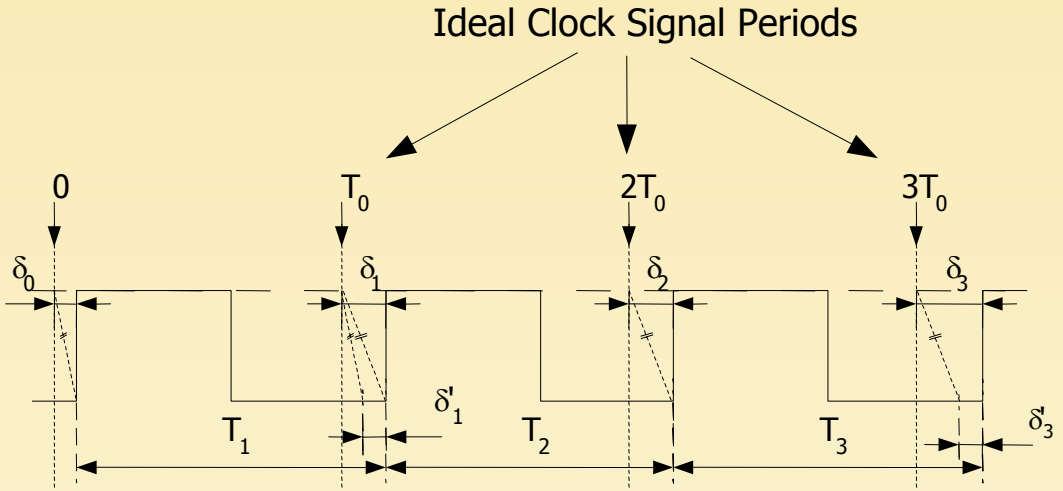


Jitter as a source of randomness (3/5)

- Period jitter δ'_n
  - the difference between measured adjacent clock periods and the ideal clock period T_0

The first difference function of the phase jitter

$$\delta'_n = \underbrace{(t_n - t_{n-1})}_{T_n} - T_0 = \delta_n - \delta_{n-1}$$

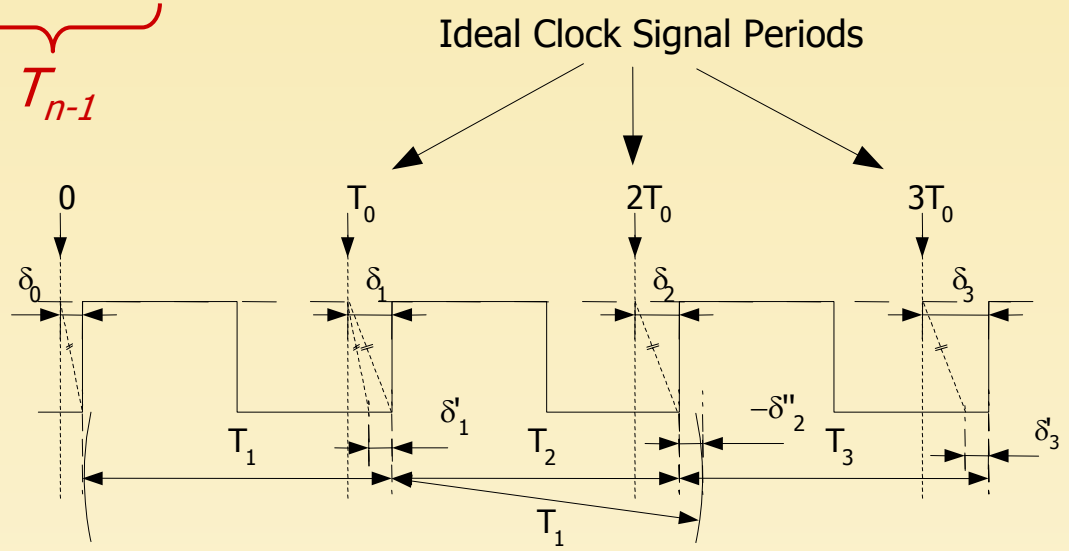


Jitter as a source of randomness (4/5)

- Cycle-to-cycle jitter δ''_n
  - the difference between between successive clock periods

The first difference function of the period jitter, the second order function of the phase jitter

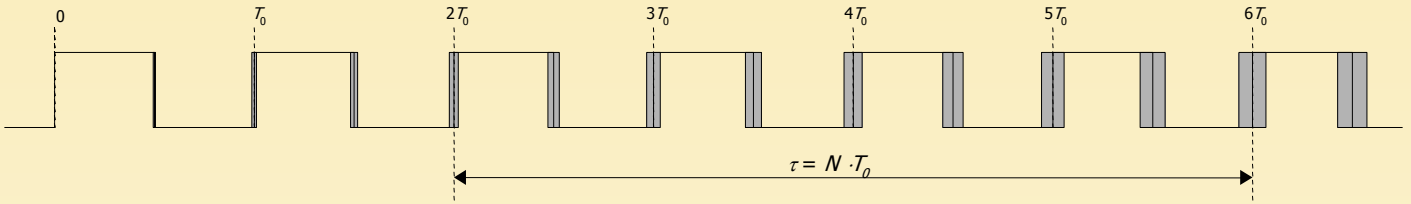
$$\delta''_n = \underbrace{(t_n - t_{n-1})}_{T_n} - \underbrace{(t_{n-1} - t_{n-2})}_{T_{n-1}} = \delta'_n - \delta'_{n-1}$$



Jitter as a source of randomness (5/5)

- Timing jitter
  - The mean square average value of a time-interval error (TIE)
- Time-interval error - TIE
  - The difference between two clock edges separated by an ideal edge delay of N clock periods
    = A measure of the timing error accumulated during the interval τ

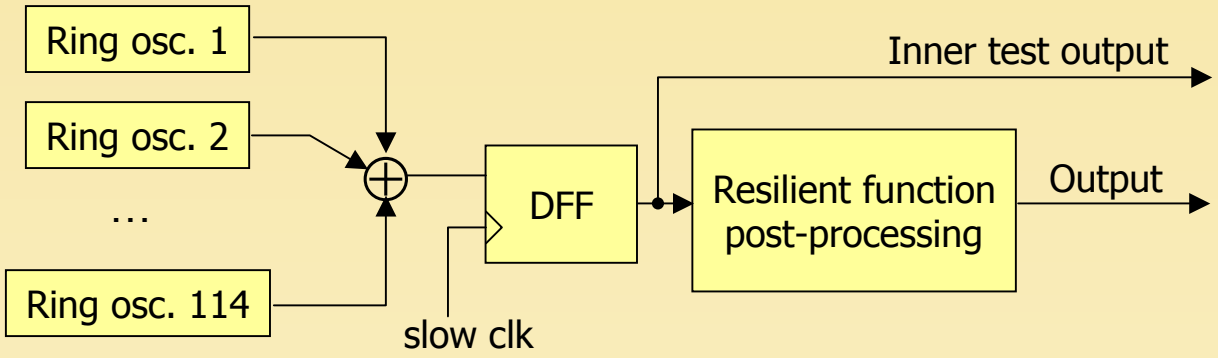
$$\mathrm{TIE}(t, \tau) = \delta(t + \tau) + \delta(t), \text{ where } \tau = N \cdot T_0$$



Note: If $t = 0$ and $\delta(t) = 0$, TIE = Phase jitter!

Example of a RO-based TRNG

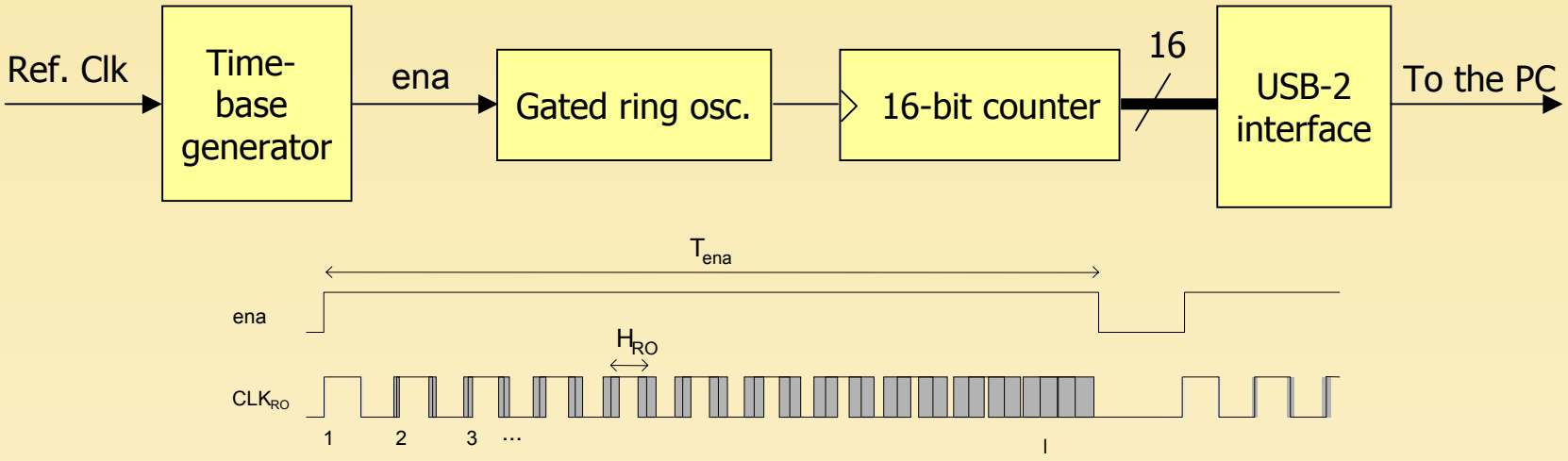
- TRNG of Sunar et al. [IEEE TC 2007]



  - Source of randomness - jitter accumulated during one period clk
  - Many independent (?) ring oscillators are used to increase entropy
  - "Provable security" based on deep probability analysis
  - Sophisticated post-processing – fault resilient function
  - Aimed for FPGAs
  - Inner tests feasible (but not extended inner tests)

Embedded measurement of the jitter in ring oscillators (1/2)

- The method



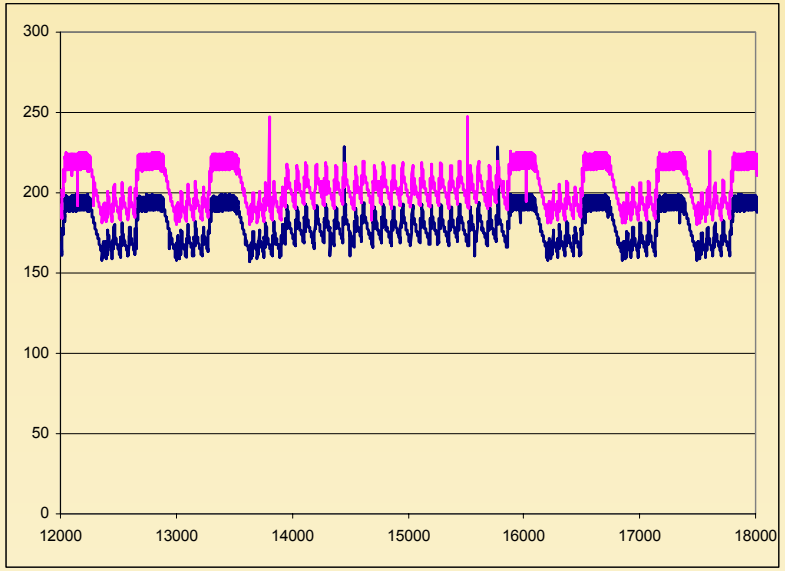
Results in HW - Actel Fusion EB:

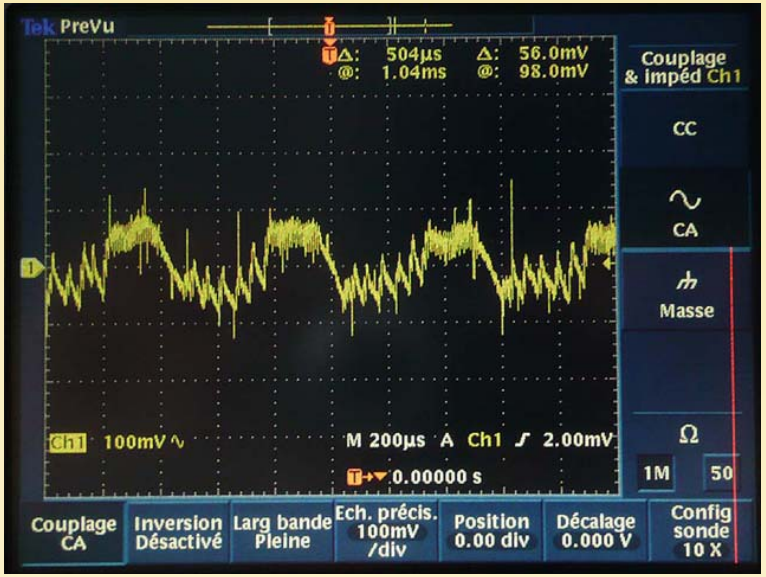
- 7-element RO, f = 96 MHz, time base - 10.000 periods on 30 MHz
- Gaussian random jitter with standard deviation σ = 33 ps/gate

Embedded measurement of the jitter in ring oscillators (2/2)

Results in HW - Altera Stratix II NIOS II EB:

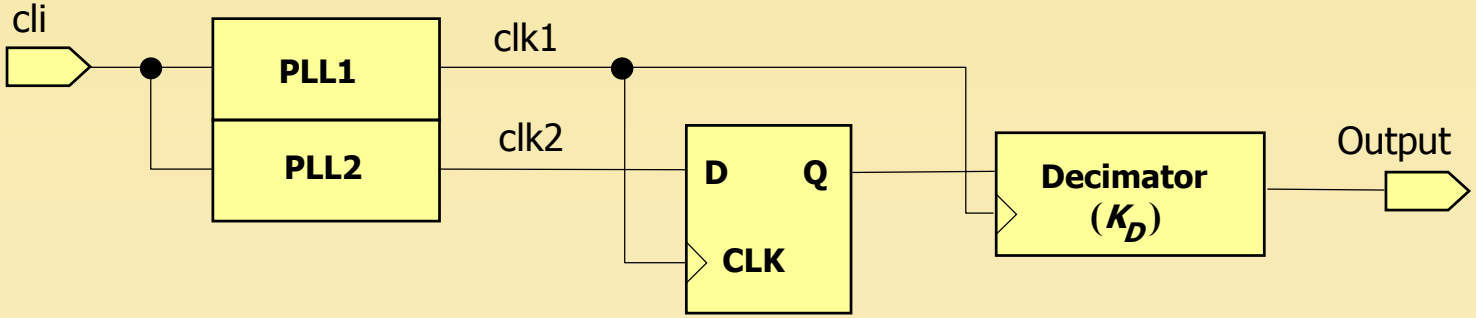
- 7-element RO, f = 196 MHz, time base - 100 periods on 50 MHz
- Huge deterministic jitter detected - switching power supply noise





Example of a PLL-based TRNG

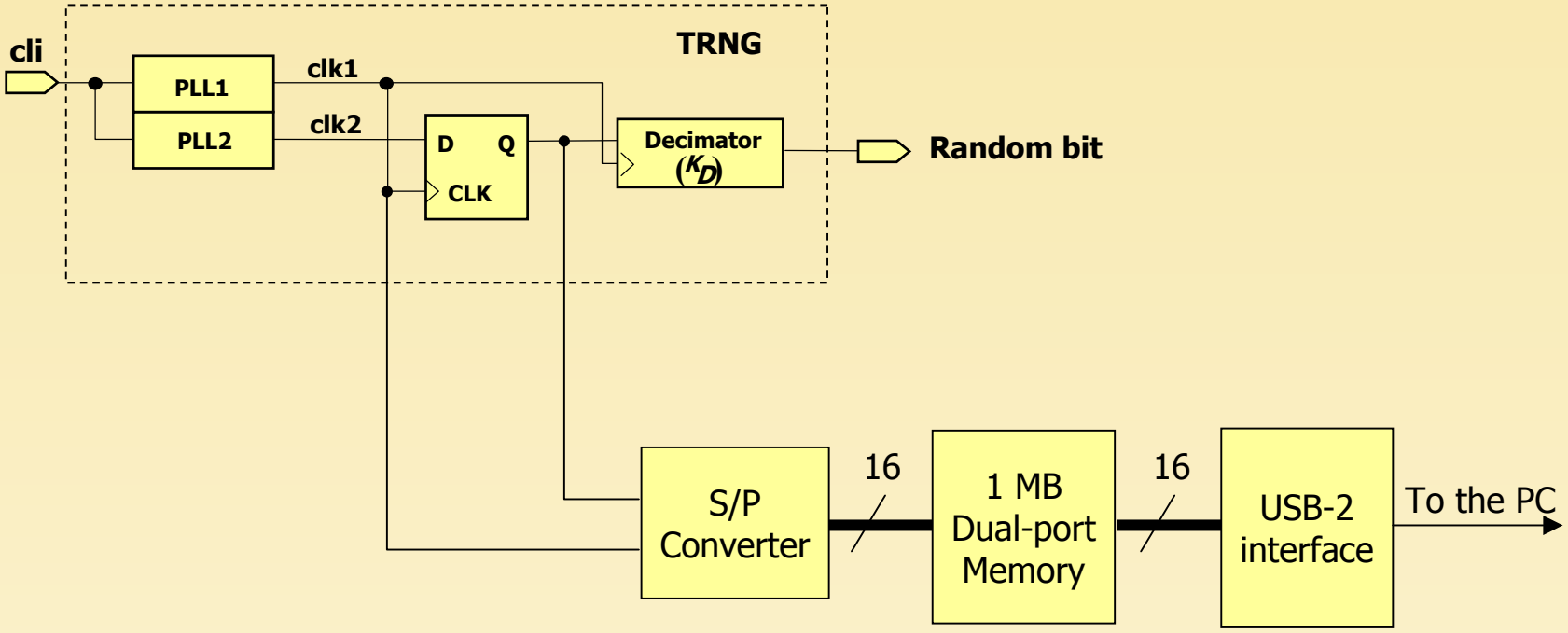
- TRNG of Fischer & Drutarovsky [CHES 2002]



  - One or two PLLs generate frequency-related clocks $f_2 = f_1 \cdot K_M/K_D$
  - Source of randomness - tracking jitter
  - Entropy extraction by a DFF and decimator – one random bit per K_D periods of clk1
  - No post-processing needed (depending on K_M and K_D)
  - Easy to implement in FPGAs (containing PLLs)
  - Extended inner tests feasible

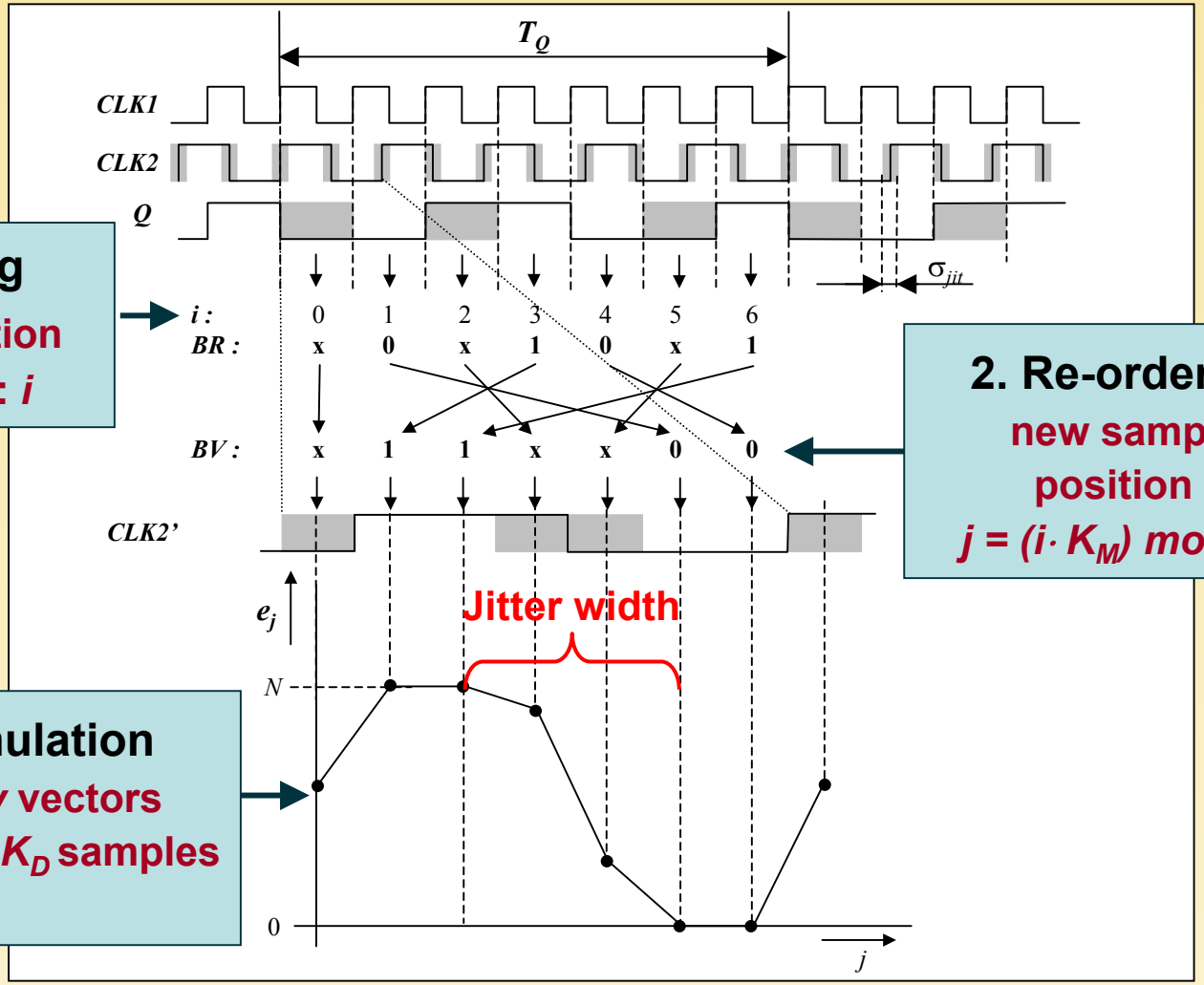
Embedded measurement of the jitter in PLLs (1/4)

- The method



Embedded measurement of the jitter in PLLs (2/4)

$K_M = 5$
$K_D = 7$



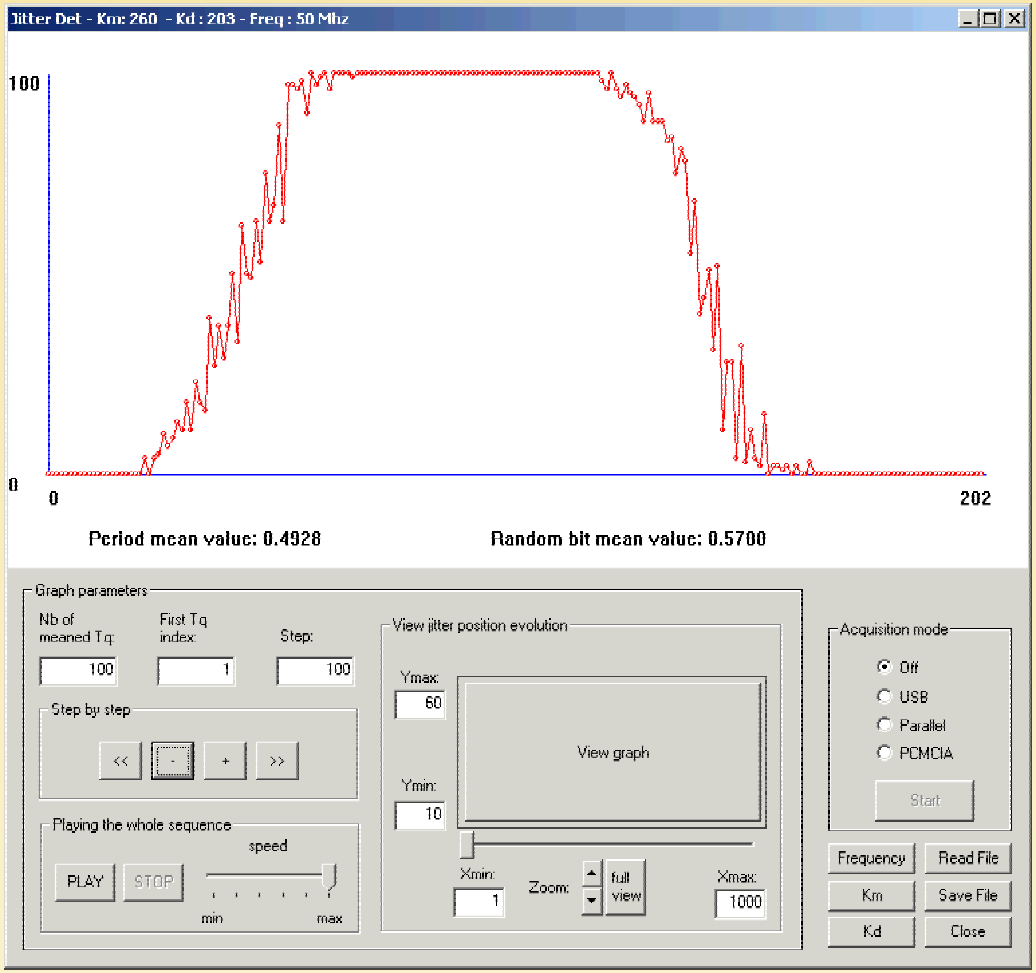
1. Sampling
original position of a sample : *i*

2. Re-ordering
new sample position :
$j = (i \cdot K_M) \bmod K_D$

3. Accumulation
of *N binary* vectors composed of K_D samples

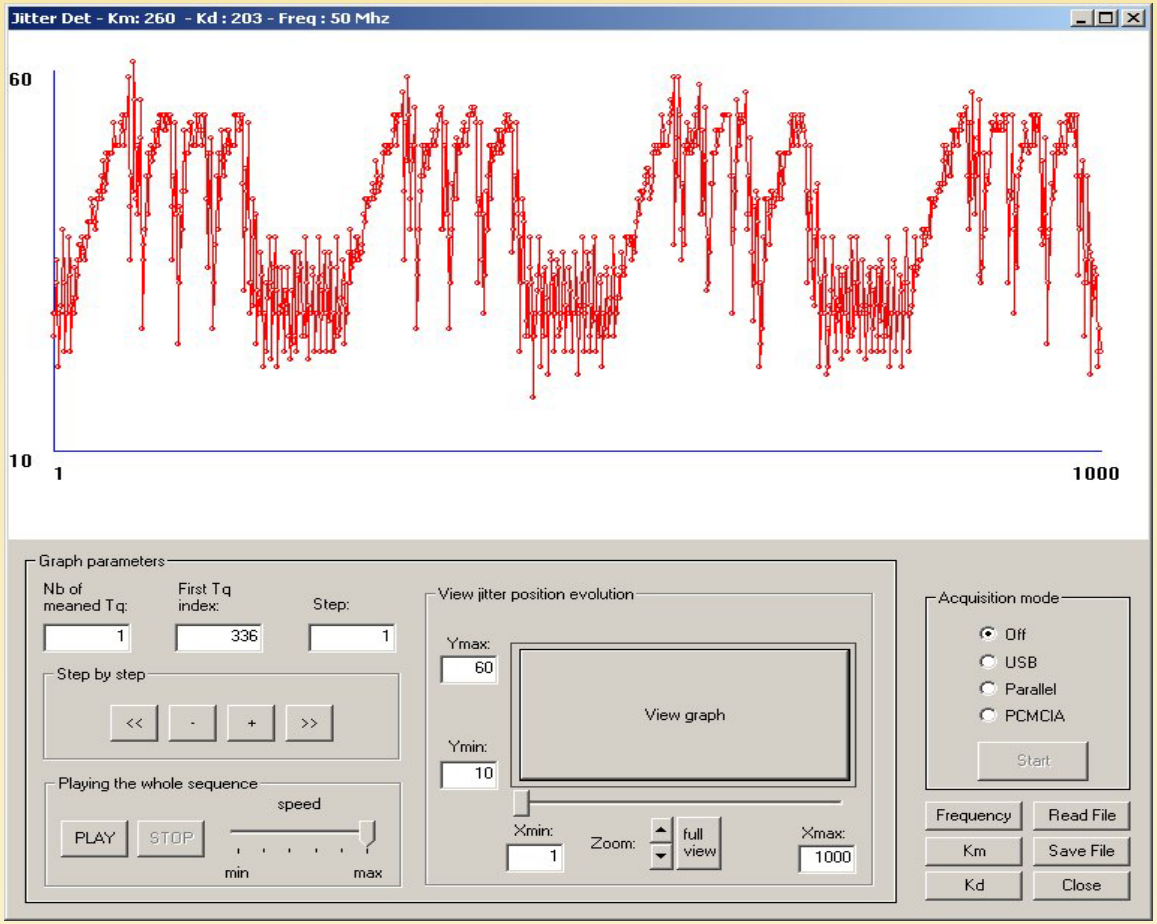
Embedded measurement of the jitter in PLLs (3/4)

- **Dynamic restitution of a CLK2 clock period mean value over 100 periods T_q**
- **Note: the clock jitter corresponds to the width of the rising/falling edge**
- **Board: Altera Stratix II EB**
- **Generator coefficients:**
  K_M=260
  K_D=203



Embedded measurement of the jitter in PLLs (4/4)

- **Evolution of the CLK2 clock rising edge**
- **Board: Altera Stratix II EB**
- **Generator coefficients:**
  K_M=260
  K_D=203
- **Tq = 260 * TCLK1 = = 203 * TCLK2 = 1.4 us**
- **So the time interval depicted is: 1000 * Tq = 1.4 ms**



Conclusions

- Security of the RNG can be increased using embedded online tests of the source of randomness
- Two online tests have been proposed for two different kinds of jitter
  - timing jitter used in RO-based TRNG
  - tracking jitter employed in PLL-based TRNG
- Both kind of test were able to detect deterministic jitter, which could be used to manipulate TRNG output
- Next step - TRNG output manipulation by introducing a deterministic jitter to the clock signal