Modeling and securing RO-based TRNG in FPGAs

Jitter accumulation from local and global sources

Boyan Valtchanov, Viktor Fischer, Florent Bernard, Alain Aubert, Nathalie Bochard
(boyan.valtchanov,fischer, florent.bernard, alain.aubert, Nathalie.Bochard)@univ-st-etienne.fr

Laboratoire Hubert Curien UMR 5516 CNRS
Université Jean Monnet, Saint-Etienne, France

Outline

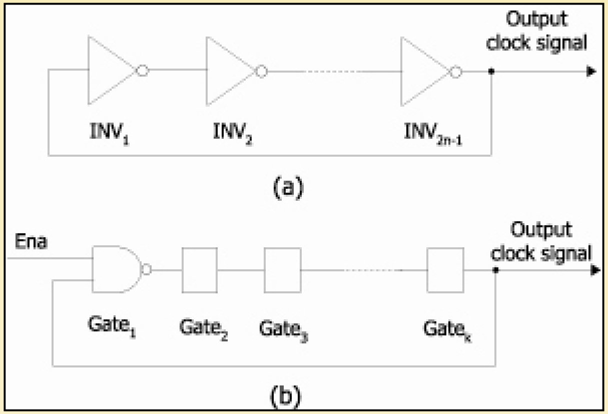
- Introduction
- Jitter in RO-generated clocks
- Modeling jitter accumulation in VHDL using behavioral model of RO
- Reduction of global jitter accumulation in RO-based TRNG
- Discussion
- Conclusions

Introduction (1/2)

- Data security in cryptography based on the confidentiality of encryption keys
- Keys generated using TRNG inside the chip
- Flexible security (reconfiguration of obsolete crypto protocols and their implementation) needs reconfigurable hardware
- Problem: source of “true” randomness in digital devices like FPGAs

Introduction (2/2)

- Commonly used sources of randomness in FPGAs
  - Timing jitter in PLL-generated clock
  - More frequently: Timing jitter in RO-generated clock
- Ring oscillators
  - Free-running oscillators propagating rising and falling edges of the clock signal in two half-periods



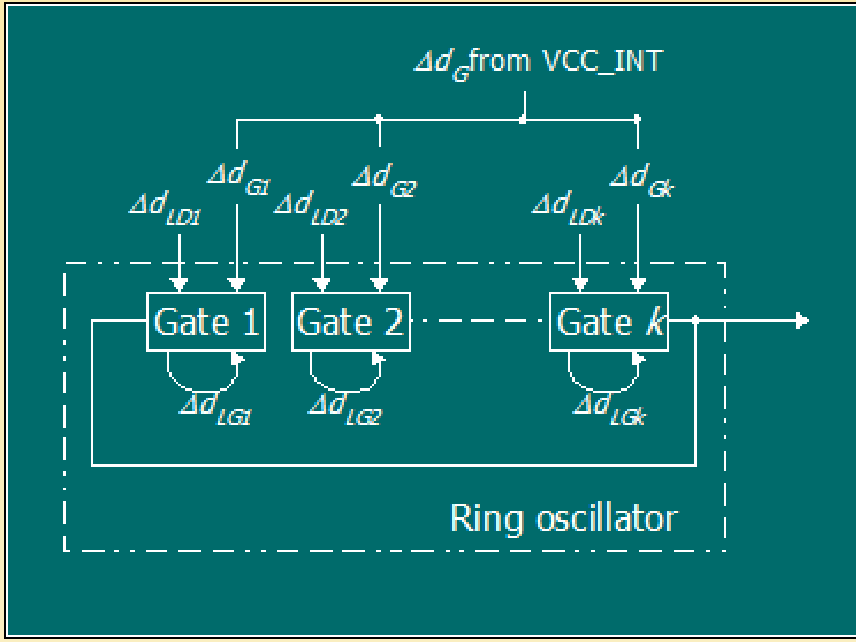
$$H_j = \sum_{i=1}^{k} d_{i,j},$$

H: Half period

d: elementary gate delay

Jitter in RO-generated clocks

- Model of jitter sources in RO
  - Global sources
    - Random
    - Deterministic
  - Local sources
    - Random
    - Deterministic



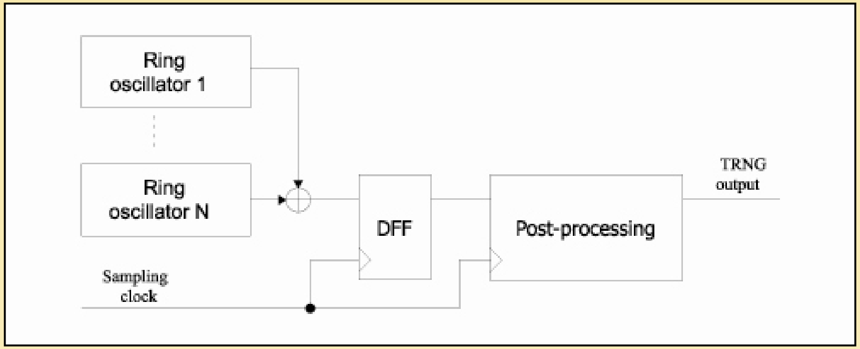
- Delay of gate i in half period j

$$\boxed{d_{i,j} = D_i + \Delta d_{i,j} = D_i + \Delta d_{Li,j} + \Delta d_{Gi,j},}$$

D: Constant part of the gate delay

Jitter accumulation in RO-based TRNG (1/4)

- Ring oscillator-based TRNG general structure
  - The jitter is accumulated during one period of the sampling clock



- Half period j of RO-generated clock

$$H_j = \sum_{i=1}^{k} D_i + \Delta H_{LGaccj} + \Delta H_{GDaccj},$$

ΔH_{LGacc}: Local Gaussian accumulated jitter

ΔH_{GDacc}: Global Deterministic accumulated jitter

Jitter accumulation in RO-based TRNG (2/4)

- Total jitter accumulated after l periods

$$\Delta T_{tot} = \sum_{j=1}^{2l} \Delta H_{LGaccj} + \sum_{j=1}^{2l} \Delta H_{GDaccj},$$

- Accumulated global deterministic jitter

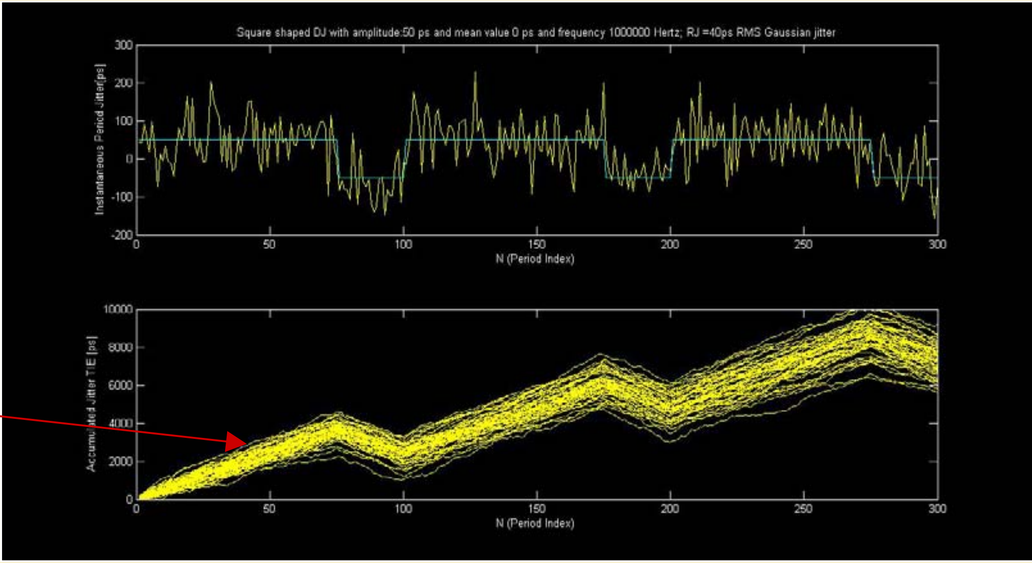
$$\sum_{j=1}^{2l} \Delta H_{GD_{accj}} = \sum_{j=1}^{2l} \sum_{i=1}^{k} K_i \Delta d_{GDj}$$

- Accumulated local Gaussian jitter

$$\sigma_{tot} = \sqrt{\sum_{j=1}^{2l} \sigma_{acc}^2} = \sqrt{2kl}\sigma.$$

Jitter accumulation in RO-based TRNG (3/4)

- Simulation of jitter accumulation in Matlab



Global jitter accumulates faster

- generated signals:
  - Global Gaussian jitter independent for each gate:
    Rectangular shape (duty cycle 75/25), 50 ps in amplitude, 0 mean value
  - Global deterministic jitter common for all gates
    Gaussian pdf with σ = 40 ps and mean 0 ps

Jitter accumulation in RO-based TRNG (4/4)

- Conclusions
  - Total jitter accumulated in RO during l periods
  - Random normal variable with mean

$$\boxed{\left(\sum_{i=1}^{k} K_i\right)\left(\sum_{j=1}^{2l} \Delta d_{GDj}\right)}$$

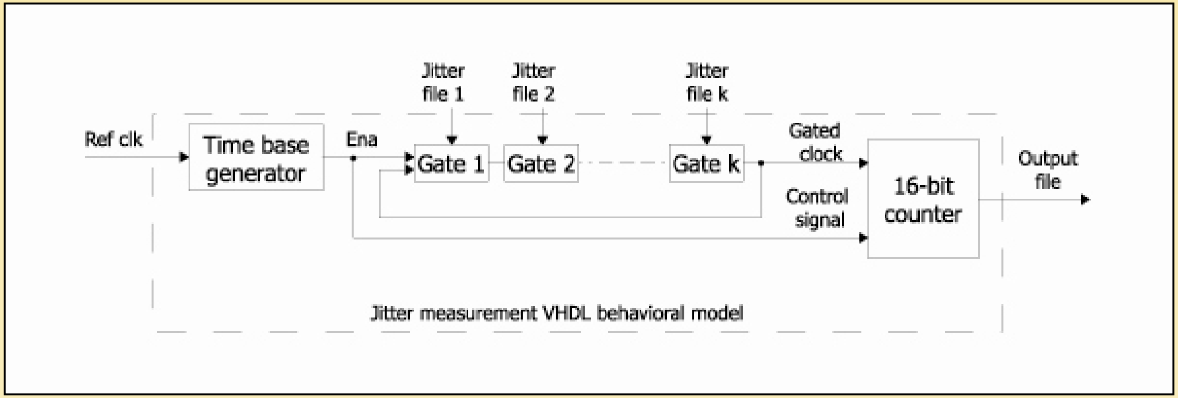
  - And standard deviation

$$\boxed{\sqrt{2kl}\sigma}$$

- If *Δ* d_{GDj} is assumed to be constant, the global deterministic jitter accumulates with l linearly
- The local Gaussian jitter accumulates always as sqrt(l)

Modeling jitter accumulation in VHDL using behavioral model of RO (1/2)

- VHDL behavioral model



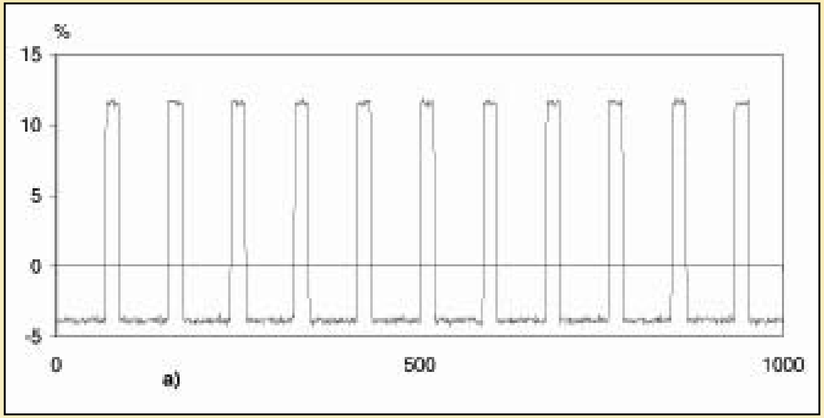
- Delays of individual gates composed of
  - Gaussian component (independent for each gate)
  - Deterministic component (the same shape with a similar, but not the same amplitude for all gates)
- Delays are generated in Matlab and read by the VHDL model during simulation

Modeling jitter accumulation in VHDL using behavioral model of RO (2/2)

- Simulation data
  - Individual Gaussian components: Normal distribution (0, σ=30ps)
  - Global deterministic components: Square shape 75/25, amplitude 40 ps

- VHDL simulation results

Counter output values in time



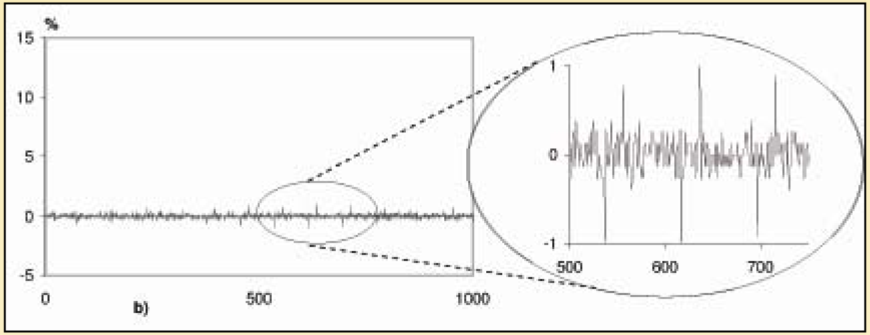
- Conclusion: the deterministic signal dominates the shape of the counter values and Gaussian jitter is very small

Reducing global deterministic jitter in the accumulated jitter (1/2)

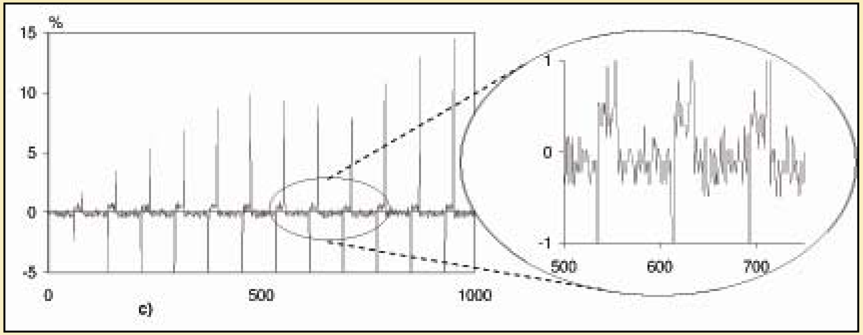
- Idea:
  - The reference clock signal is generated inside FPGA using another RO
  - Both clock signal will depend on the same global deterministic jitter
  - The deterministic jitters accumulated in both ring oscillators will compensate each other in the final jitter measurement
  - The relative accumulated jitter will depend only on the local Gaussian jitter

Reducing global deterministic jitter in the accumulated jitter (2/2)

- Simulation conditions
  - Global deterministic jitter is the same for all gates (difficult to obtain in reality) (left)
  - Global deterministic jitter is slightly different in size in individual gates (right)
- Simulation results



Deterministic part is removed



Deterministic part is reduced

Evaluation of jitter accumulation in the uncontrolled RO (as in TRNG) (1/2)

- Problem
  - Does the jitter accumulate in RO-based TRNG and gated RO used in our embedded jitter measurement circuitry in the same way?
- Principle remains the same
  - The jitter accumulates during several periods of (reference) clock
- Difference
  - In the measurement, the RO’s clock phase is reset at the beginning of the measurement interval

Evaluation of jitter accumulation in the uncontrolled RO (as in TRNG) (2/2)

- Idea

  Make the jitter measurement methode as close as possible to the TRNG structure:

  - Time base generator is used only to reset the counters but not the ring oscillators (free running oscillators)

- Simulation
  - The same simulation project was used as before, but the ENA signal for the RO was set to '1'

- Simulation results
  - Very close to those obtained for gated ROs

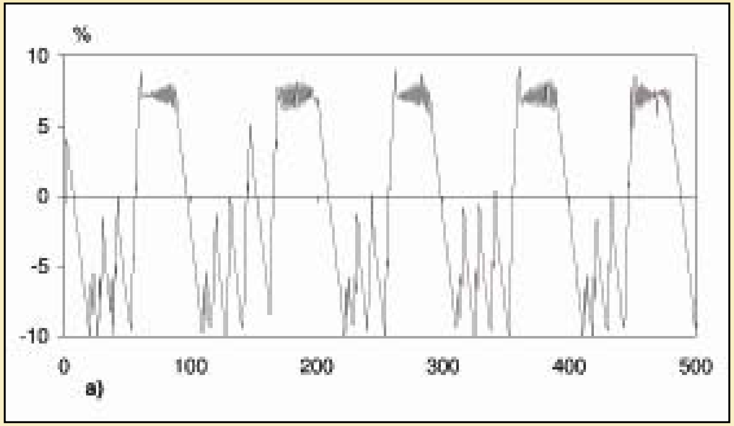
Reduction of global deterministic jitter accumulation in hardware (1/3)

- Hardware employed

  Altera Stratix II NIOS II Evaluation board

- Configuration of the measurement circuitry
  - 7-element ring oscillator
  - 25 MHz fixed reference clock
  - 100 reference clock periods in one measurement interval

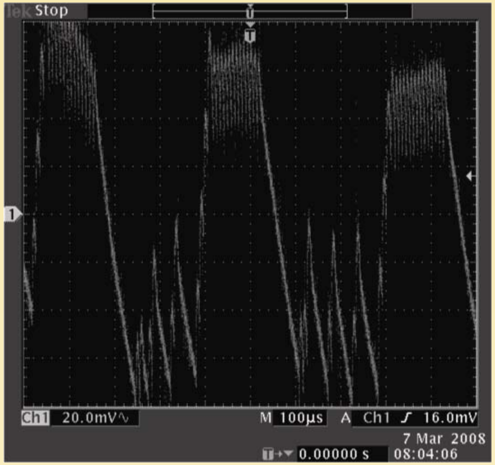
- Results

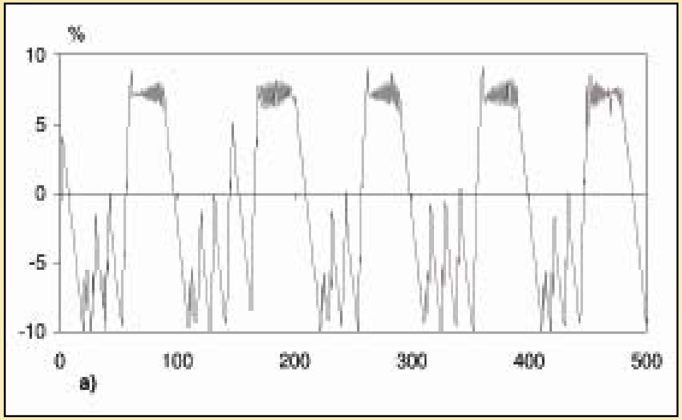


Evolution of counter values in time

Reduction of global deterministic jitter accumulation in hardware (2/3)

- Signal superimposed on the VCC_INT power supply in Altera Stratix II NIOS II EB





Plot of VCC_INT using oscilloscope

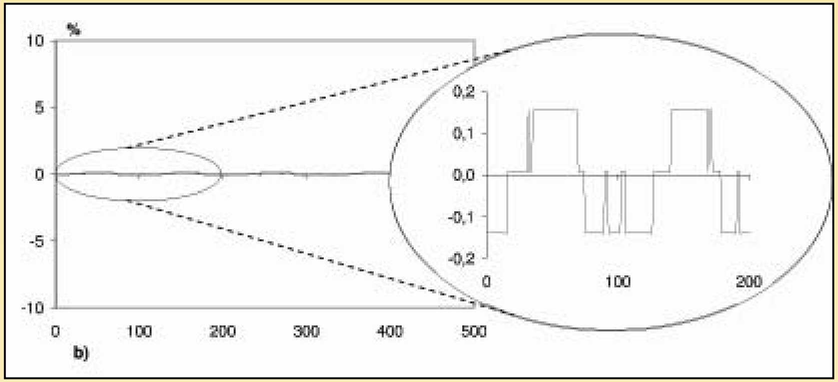
100 mV of AC component over 1.2V DC!

Embedded measurement (counter values)

Reduction of global deterministic jitter accumulation in hardware (3/3)

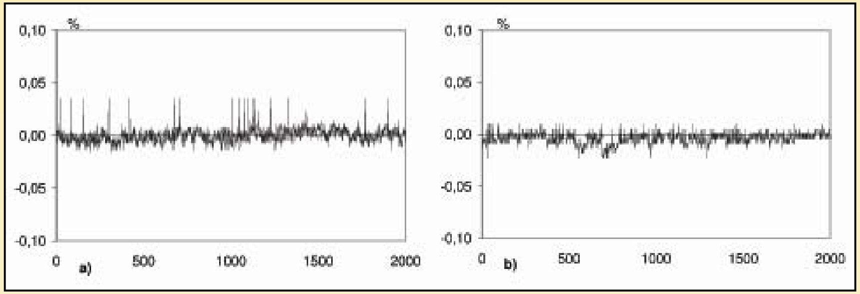
- Results with reduced global deterministic jitter

  (7-element RO was used to generate the reference clock)



- Results without deterministic jitter

  (10.000 reference clock periods instead of 100)



Discussion

- Accumulated jitter depends more on global (deterministic) than on local (random) jitter sources
- Global deterministic jitter can be manipulated, so the generated bitstream could be manipulated, too
- Solution:
  - The use of local reference clock signal generated by a ring oscillator
  - All ROs should be implemented in the same way
  - All ROs should be located close to each other

Conclusions

- Enhanced model of jitter accumulation in ring oscillators was proposed
- The model permits to show that the global jitter accumulates faster than the local (Gaussian) jitter
- This potential weakness can be reduced using a ring oscillator to generate TRNG sampling clock
- Without any special design constraints, the deterministic jitter could be reduced in real FPGA by as much as five orders of magnitude