Viktor Fischer

Université Jean Monnet,
Saint-Etienne, France
fischer@univ-st-etienne.fr

Miloš Drutarovský

Technical University of Košice,
Slovakia
Milos.Drutarovsky@tuke.sk

True Random Number Generator Embedded in Reconfigurable Hardware

Introduction

Motivation

- Embedded cryptographic system in reconfigurable hardware - system in a programmable chip (SOPC) solution

Offering

- Higher security
- Lower price
- Adaptability

Problem

- Missing cryptographic primitive in programmable logic applications - True Random Number Generator (TRNG)

Source of randomness

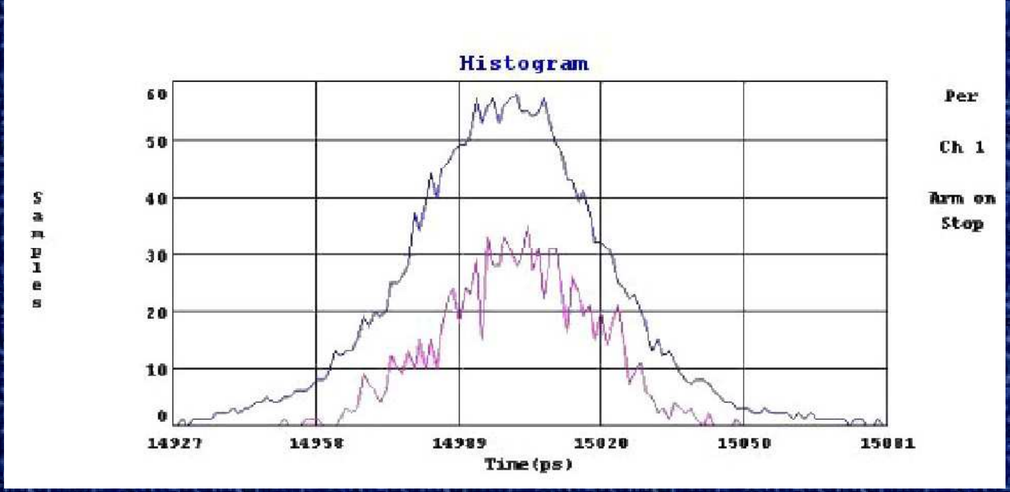
Problem

Field Programmable Logic Device (FPLD) - suitable especially for pseudo-random number generators (logic circuitry), usually the source of randomness is missing

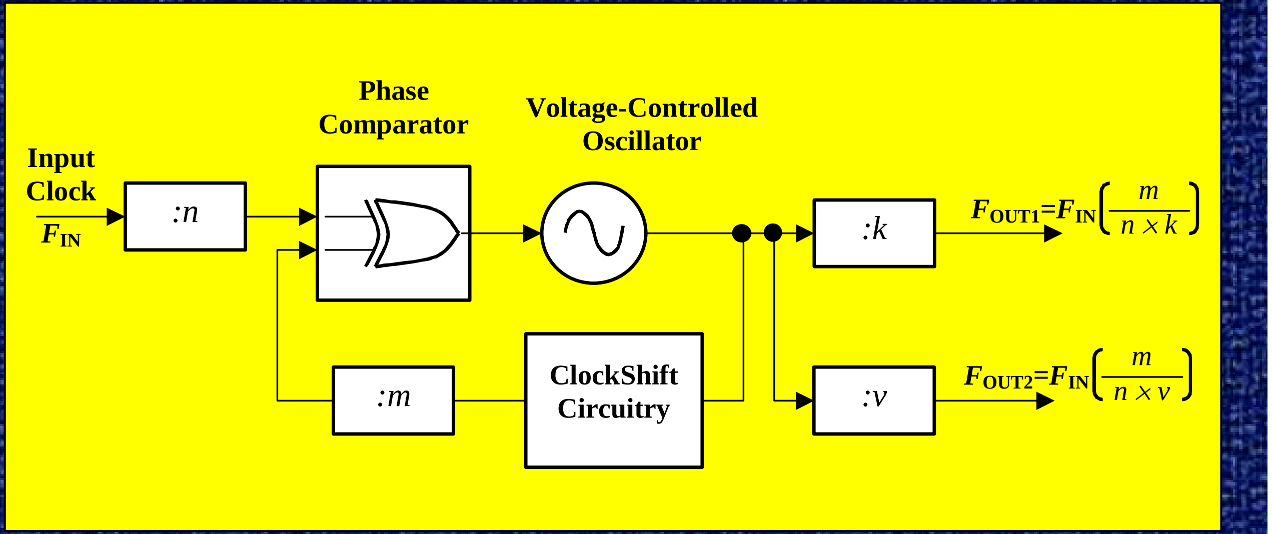
Solution

Analog part of recent FPLD - a PLL used usually for the clock synthesis - introduces very small random jitter

Jitter parameters



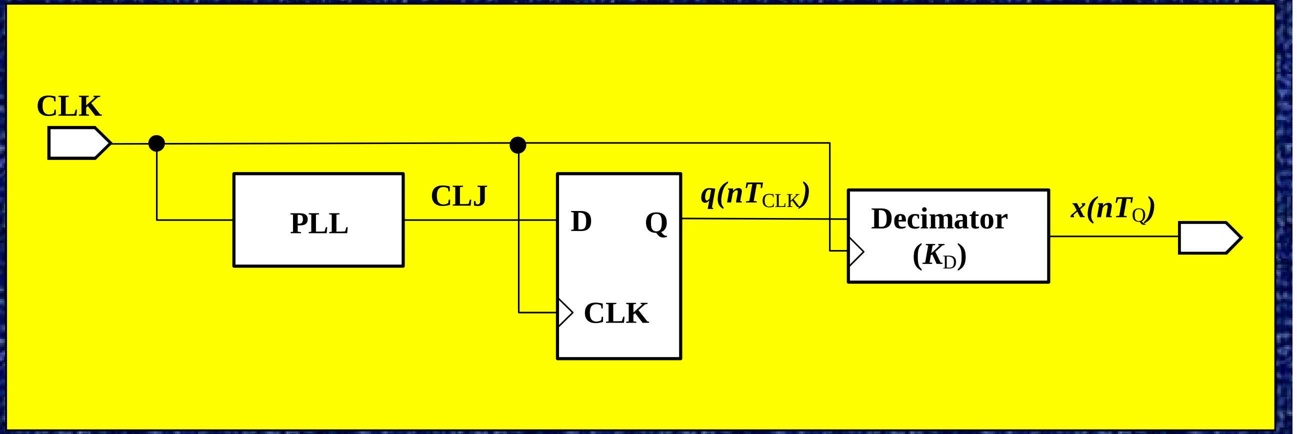
Analog PLL in Altera FPLD


Input Clock
F_{IN}
Phase Comparator
Voltage-Controlled Oscillator
:n
:k
:m
:v
ClockShift Circuitry
$F_{OUT1}=F_{IN}\left(\frac{m}{n \times k}\right)$
$F_{OUT2}=F_{IN}\left(\frac{m}{n \times v}\right)$

Parameters

- Analog PLL with high multiplication and division factors (up to 160)
- Used for high-speed clock generation (typically up to 200 MHz)
- Instability reduced to a minimum - clock jitter 1-sigma value: ~ 15 ps (very good for a clock synthesis, less good for a TRNG implementation)

TRNG principle



Principle

- Summation modulo 2 of the synthesized clock signal (CLJ) sampled in the fixed clock intervals (CLK) during the period T_Q
- If $F_{CLJ} = F_{CLK} K_M / K_D$ and K_M and K_D are relative primes

then

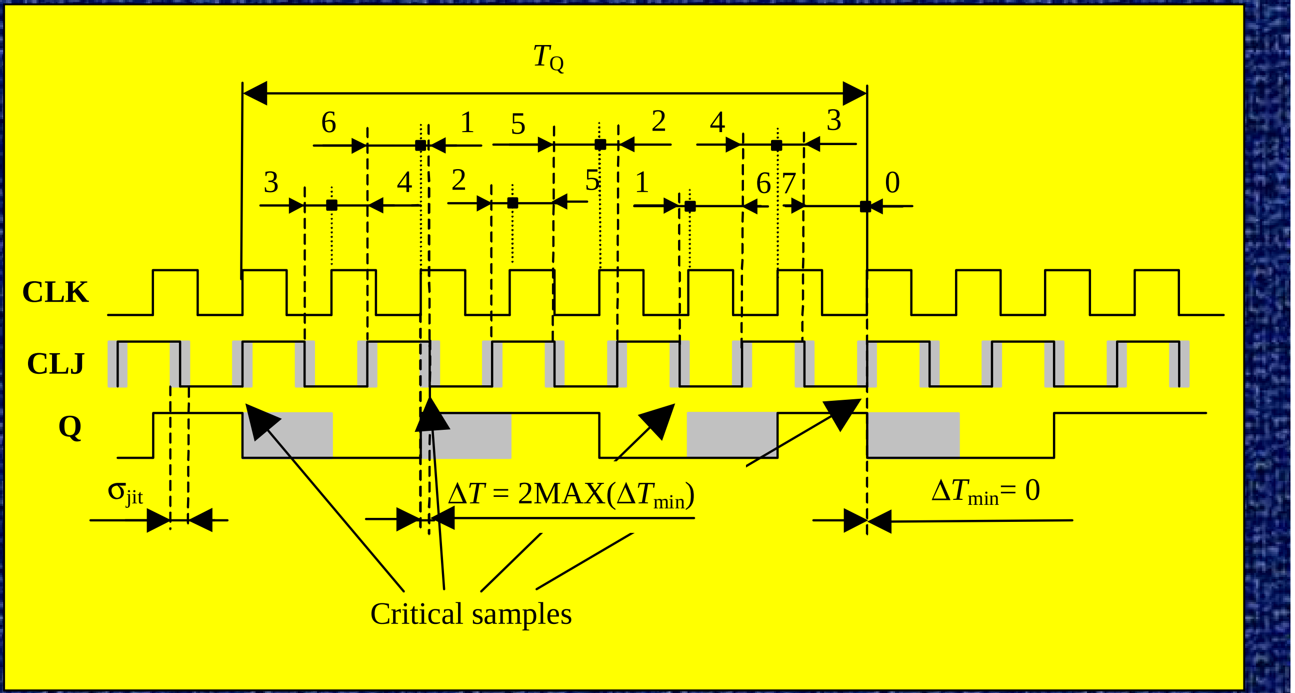
$$T_Q = K_D T_{CLK} = K_M T_{CLJ}$$

Example of the clock relationship

$K_M = 5$

$K_D = 7$

$F_{CLJ} < F_{CLK}$



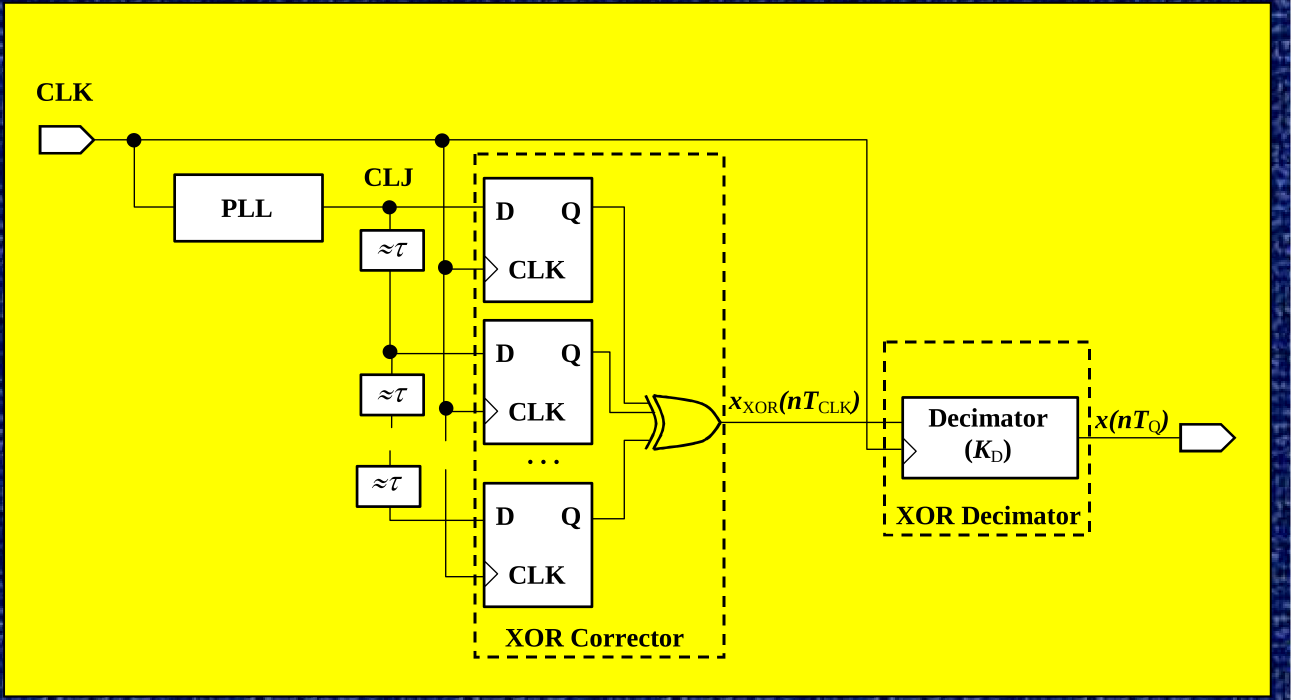
Note

- Sampling of the signal CLJ in K_D discrete positions (phases)

Condition for the jitter detection

$$\sigma_{jit} > T_{CLJ} /4\, K_D = T_{CLK} /4\, K_M$$

TRNG realization



XOR corrector

- Increases the probability of CLK and CLJ edge zones overlapping during the T_Q period

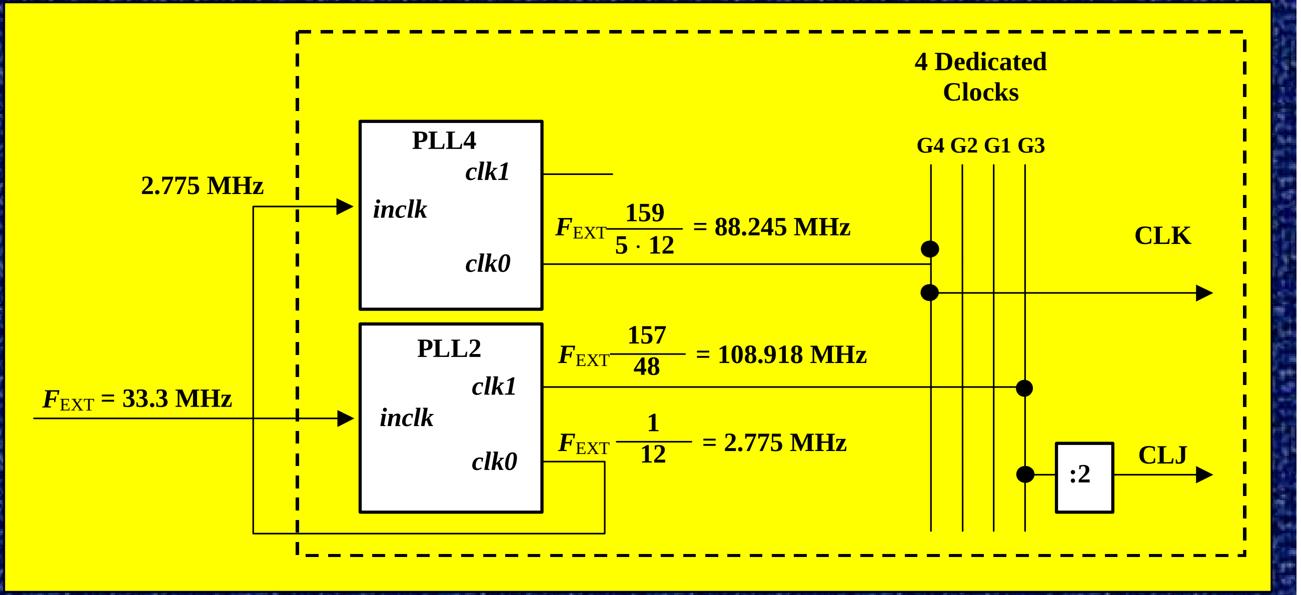
XOR decimator

- Removes deterministic part of the signal with the T_Q period

Hardware testing equipment

Altera NIOS development board based on APEX20K200-2X device

PLLs configuration


4 Dedicated Clocks
G4 G2 G1 G3
PLL4
clk1
inclk
clk0
2.775 MHz
$F_{EXT}\frac{159}{5 \cdot 12} = 88.245$ MHz
CLK
PLL2
clk1
inclk
clk0
$F_{EXT}\frac{157}{48} = 108.918$ MHz
$F_{EXT} = 33.3$ MHz
$F_{EXT}\frac{1}{12} = 2.775$ MHz
:2
CLJ

Parameters

- $K_M = 785$, $K_D = 1272$, $T_{CLK}/4K_M = 7.2$ ps $< \sigma_{jit}$

Implemented blocks

- TRNG
- 4 kB FIFO and I/O control logic

Hardware implementation

Description language

- AHDL
- VHDL

Difficulties

- Simulation of the jitter and simulation of the TRNG performance is impossible
- Placement and routing results are very important

Development tools

- Quartus II, version 2.0

Requirements

Device	TRNG only				TRNG + FIFO			
	LCs #	LCs %	ESBs #	ESBs %	LCs #	LCs %	ESBs #	ESBs %
EP20K200EFC484-2X	48	0.6	0	0	121	1.5	4	7.7

Tests results

Mean values for 1-Gigabit records

Record	1	2	3	4	5
Board	A	B	B	B	B
Mean	0.500001	0.500109	0.500001	0.50012	0.50012

Conclusion

For very long records some small bias can be noticed, this bias should be negligible for cryptographic applications and it can be further reduced

NIST test suite

Frequency, Block-Freq., Cusum, Runs, Long-Run, Rank, FFT, Periodic-Template, Universal, Apen, Serial, Lempel-Ziv, Linear-Complexity

Conclusion

All the tests have passed with some small deviation for some FFT tests

Conclusions

We have proposed a new method for the true random number generator implementation in reconfigurable hardware:

- the principle of randomness extraction is very reliable (independ on voltage and temperature fluctuation)
- since no external component is needed, it seems to be very difficult to manipulate the generator output values
- the principle is adaptable to all devices using analog PLL with sufficiently high K_M and K_D and relatively high jitter (all recent Altera FPLDs, some other FPLDs, ASICs, etc.)

Perspectives

- Intensive testing in cooperation with other (specialized) organizations
- Improvement of the characteristics of the XOR corrector to reduce the bias
- Exact measurement of the jitter in different conditions
- Design of the complete IP block including on-line FIPS tests
- Improvement of the strategy of the choice of multiplication and division factors