Department of Electronics and Multimedia Communications
Faculty of Electrical Engineering and Informatics
Technical University of Košice
Park Komenského 13, 04120 Košice
Slovak Republic

New High Entropy Element for FPGA Based True Random Number Generators

Michal Varchola and Miloš Drutarovský

The 12th Workshop on Cryptographic Hardware
and Embedded Systems (CHES 2010)
UC Santa Barbara
August 20, 2010

Agenda

- **Introduction**
- New Entropy Element Design Goals
- Transition Effect Ring Oscillator (TERO)
- Mathematical Model of TERO
- Experimental Results
- Conclusions

Introduction
Random Numbers are Essential...

Session Keys

Signature Parameters

Temporary Keys

Challenges for Authentication

Zero Knowledge Protocols

Generation of Primes

Nonces

...and therefore random numbers must be independent, unpredictable, and must fulfill strict statistical properties.

True Random Number Generators (TRNGs) translate a physical phenomena (e.g. thermal noise) to the random digits.

The TRNG of insufficient quality can weaken an otherwise strong cryptographic system (see e.g. [1]).

[1] Markettos, Moore: The Frequency Injection Attack on Ring-Oscillator Based True Random Number Generators, CHES 2009

Introduction
Random Numbers are Essential...

Session Keys

Signature Parameters

Temporary Keys

Challenges for Authentication

Zero Knowledge Protocols

Generation of Primes

Nonces

...and therefore random numbers must be independent, unpredictable, and must fulfill strict statistical properties.

True Random Number Generators (TRNGs) translate a physical phenomena (e.g. thermal noise) to the random digits.

The TRNG of insufficient quality can weaken an otherwise strong cryptographic system (see e.g. [1]).

[1] Markettos, Moore: The Frequency Injection Attack on Ring-Oscillator Based True Random Number Generators, CHES 2009

Introduction
Random Numbers are Essential...

Session Keys

Signature Parameters

Temporary Keys

Challenges for Authentication

Zero Knowledge Protocols

Generation of Primes

Nonces

...and therefore random numbers must be independent, unpredictable, and must fulfill strict statistical properties.

True Random Number Generators (TRNGs) translate a physical phenomena (e.g. thermal noise) to the random digits.

The TRNG of insufficient quality can weaken an otherwise strong cryptographic system (see e.g. [1]).

[1] Markettos, Moore: The Frequency Injection Attack on Ring-Oscillator Based True Random Number Generators, CHES 2009

Introduction
Random Numbers are Essential...

Session Keys

Signature Parameters

Temporary Keys

Challenges for Authentication

Zero Knowledge Protocols

Generation of Primes

Nonces

...and therefore random numbers must be independent, unpredictable, and must fulfill strict statistical properties.

True Random Number Generators (TRNGs) translate a physical phenomena (e.g. thermal noise) to the random digits.

The TRNG of insufficient quality can weaken an otherwise strong cryptographic system (see e.g. [1]).

[1] Markettos, Moore: The Frequency Injection **Attack on Ring-Oscillator** Based True Random Number Generators, CHES 2009

Introduction
Why **True** Random Number Generators?

"Any one who considers arithmetical methods
of producing random digits is, of course, in a state of sin.
For, as has been pointed out several times, there is no
such thing as a random number –
there are only methods to produce random numbers,
and a strict arithmetic procedure of course
is not such a method."

John Von Neumann

Introduction
Why **True** Random Number Generators?

"Any one who considers arithmetical methods
of producing random digits is, of course, in a state of sin.
For, as has been pointed out several times, there is no
such thing as a random number –
there are only methods to produce random numbers,
and a strict arithmetic procedure of course
is not such a method."

John Von Neumann

The Research Challenge:

To discover such a random source and extraction method,
which can be reliably synthesized in modern electronic devices
such as Field Programmable Gate Arrays (FPGAs),
where cryptographic systems are usually implemeted.

Introduction
FPGA-based TRNG Randomness Sources & Designs

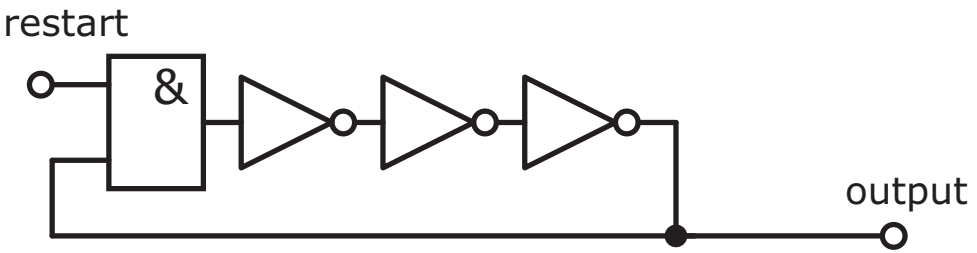
Timing Jitter:

- of Ring Oscillators (**ROs**):
  - Two **ROs** accompanied with LFSRs (Tkacik; CHES 2002; **compromised** by Dichtl)
  - Fibonacci and Galois **ROs** Combined by XOR (Golic; Tran. on Comp. 2006)
  - 114 **ROs** combined by XOR (Sunar; Tran. on Comp.; **compromised** by Dichtl)
  - 20 **ROs** combined by XOR - the modification of Sunar's 114 ROs design (Wold, Tan; Int. J. of Reconfig. Comp. 2009; **compromised** by Fischer)
  - The general frequency injection **RO attack** (Markettos, Moore; CHES 2009)
- of PLLs' output (Fischer & Drutarovsky, CHES 2002)

Metastability:

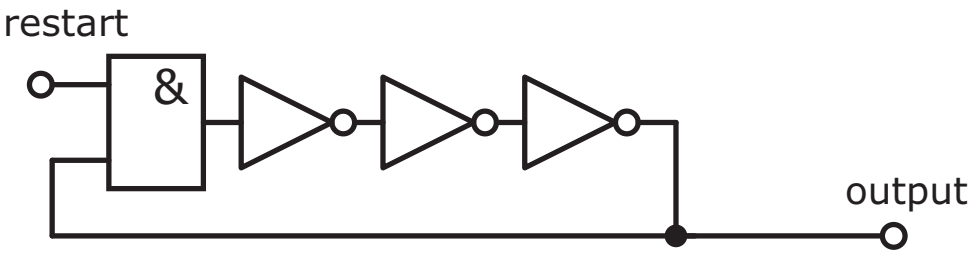
- Metastable Ring Oscillator (Vasyltsov et.al.; CHES 2008)
  - Authors mentioned difficulties realated to the implementation in FPGA hardware

Introduction
Ring Oscillator Randomness Extraction Method

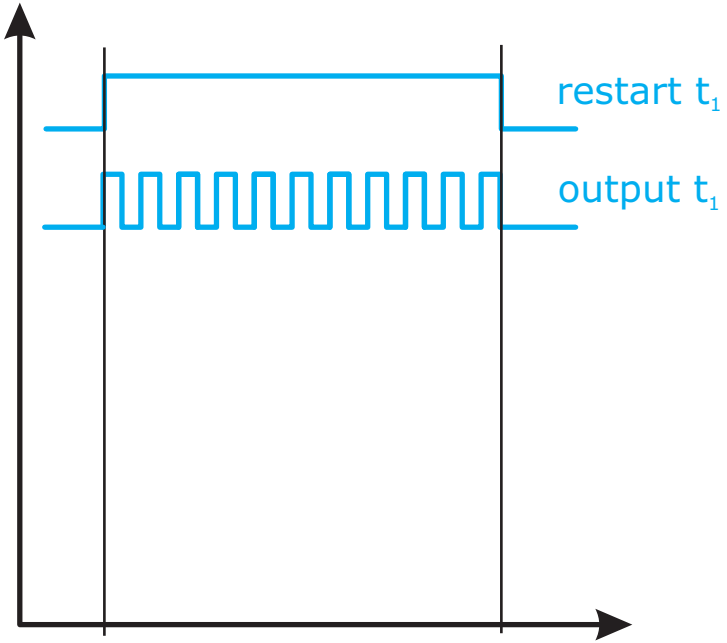


Basic RO circuitry

Introduction
Ring Oscillator Randomness Extraction Method



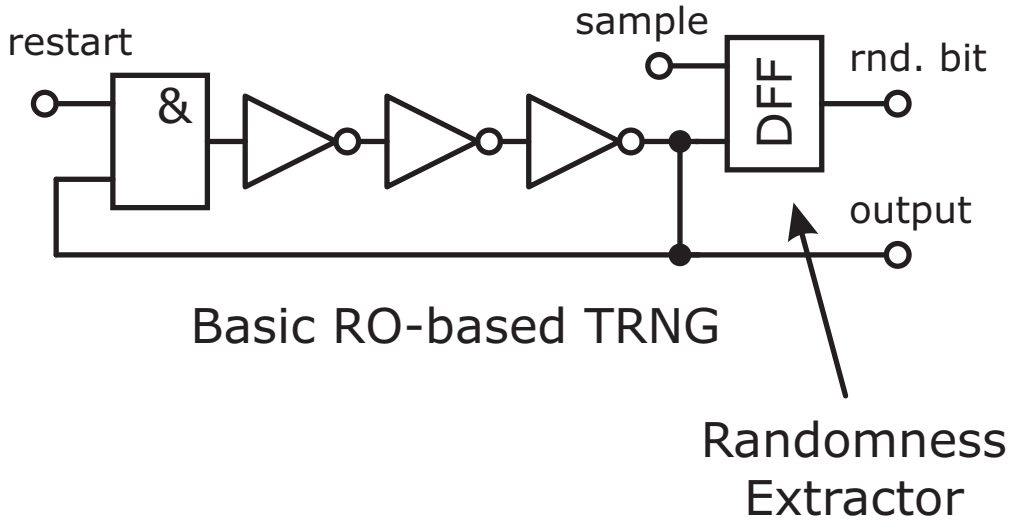
Basic RO circuitry

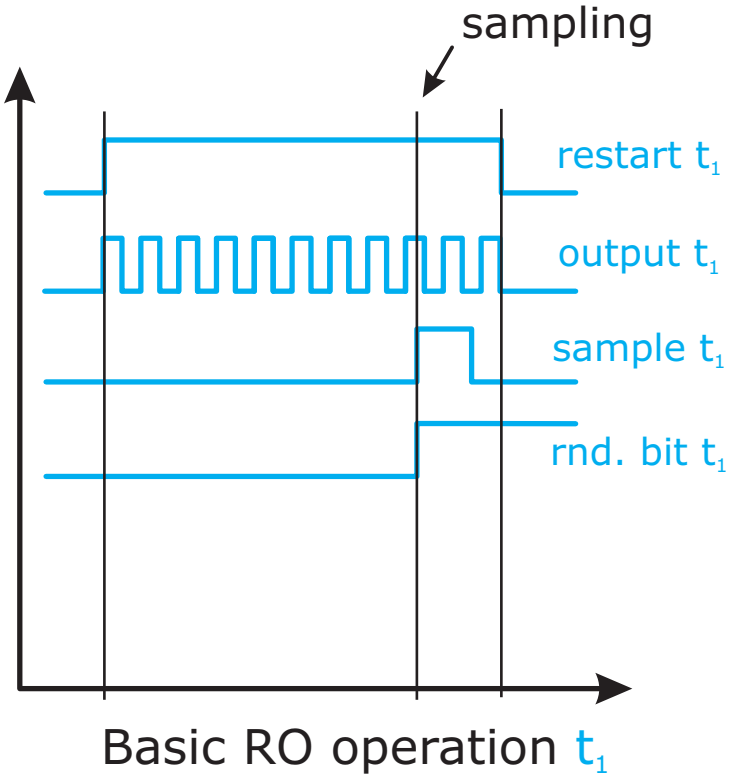


Basic RO operation t_1

Introduction

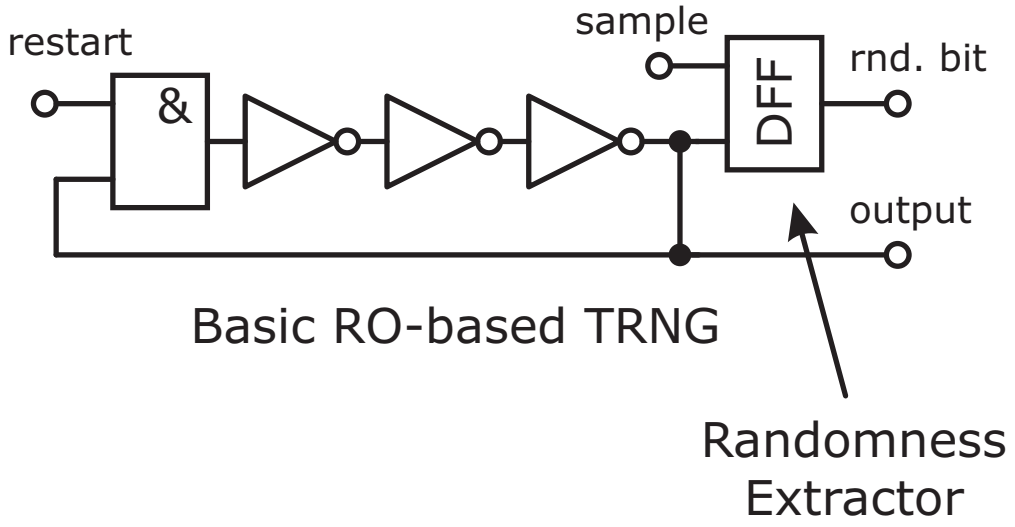
Ring Oscillator Randomness Extraction Method



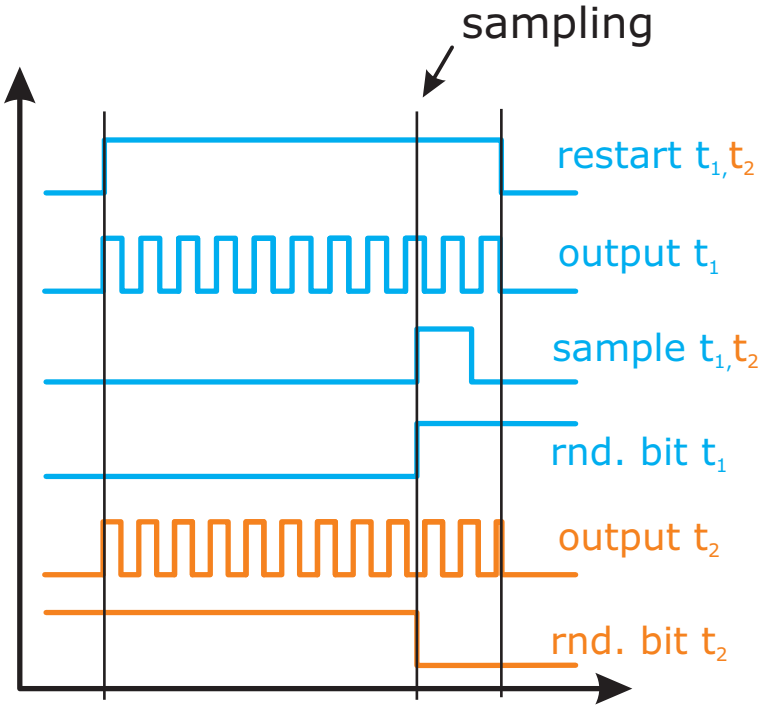


Introduction

Ring Oscillator Randomness Extraction Method

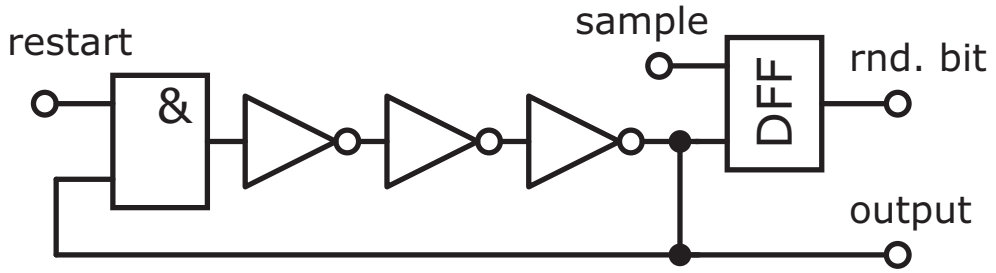


Basic RO-based TRNG

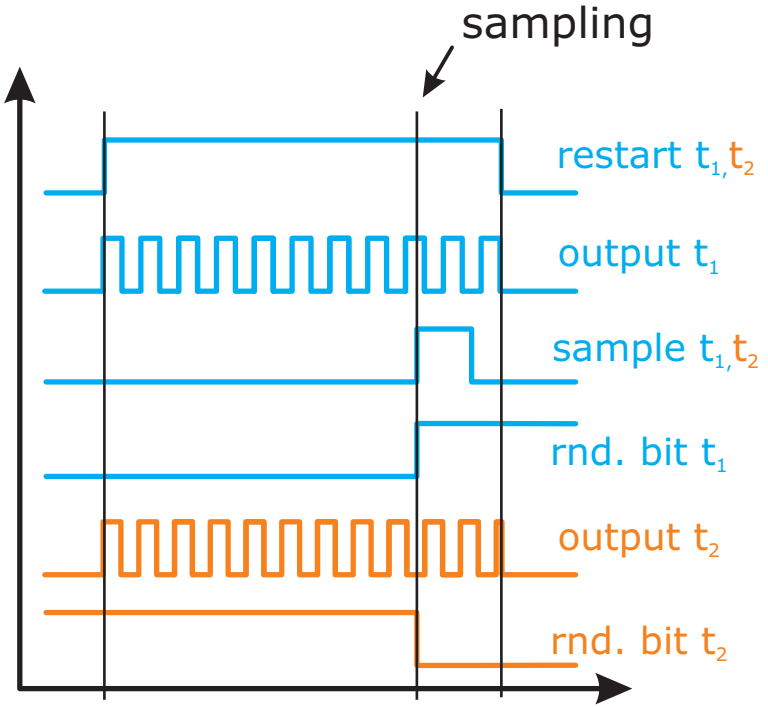


Basic RO operation t_1, t_2

Introduction
Ring Oscillator Randomness Extraction Method



Basic RO-based TRNG

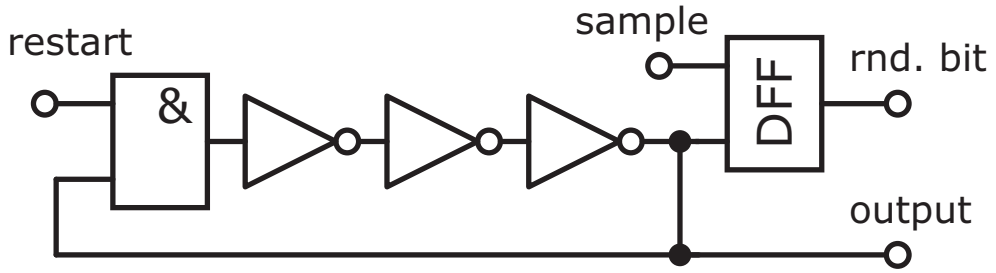


Basic RO operation t_1, t_2

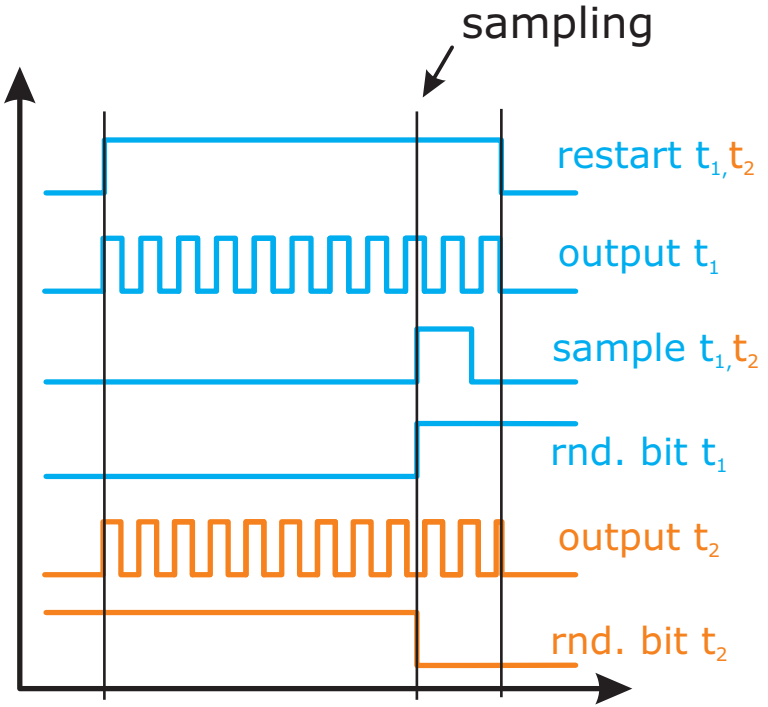
Pros of the Popular **ROs**:

- Employs standard logic cells
- Easy synthesis in FPGAs and ASICs

Introduction
Ring Oscillator Randomness Extraction Method



Basic RO-based TRNG



Basic RO operation t_1, t_2

Pros of the Popular **ROs**:

- Employs standard logic cells
- Easy synthesis in FPGAs and ASICs

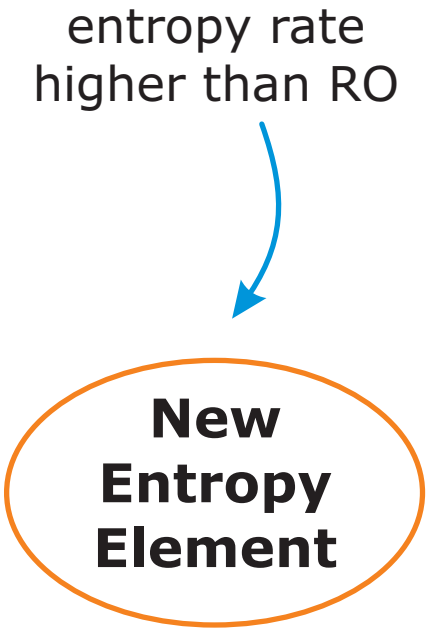
Cons of the Popular **ROs**:

- Low entropy rate (acquired from internal noise processes in RO electronic components)
- Strong dependence on working conditions and external perturbation
- RO can synchronize on parallel operating ROs or on perturbation

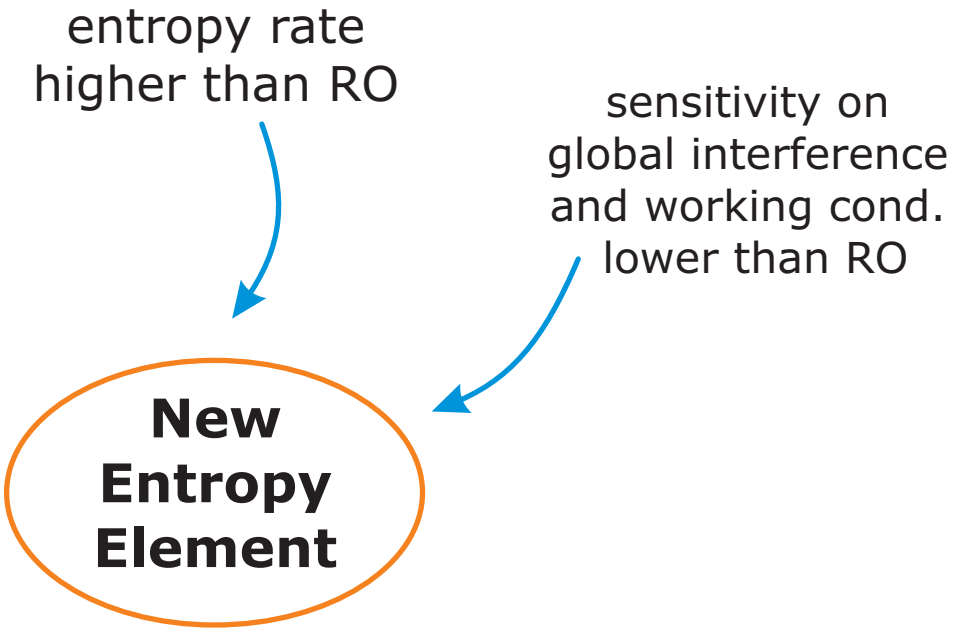
Agenda

- Introduction
- **New Entropy Element Design Goals**
- Transition Effect Ring Oscillator (TERO)
- Mathematical Model of TERO
- Experimental Results
- Conclusions

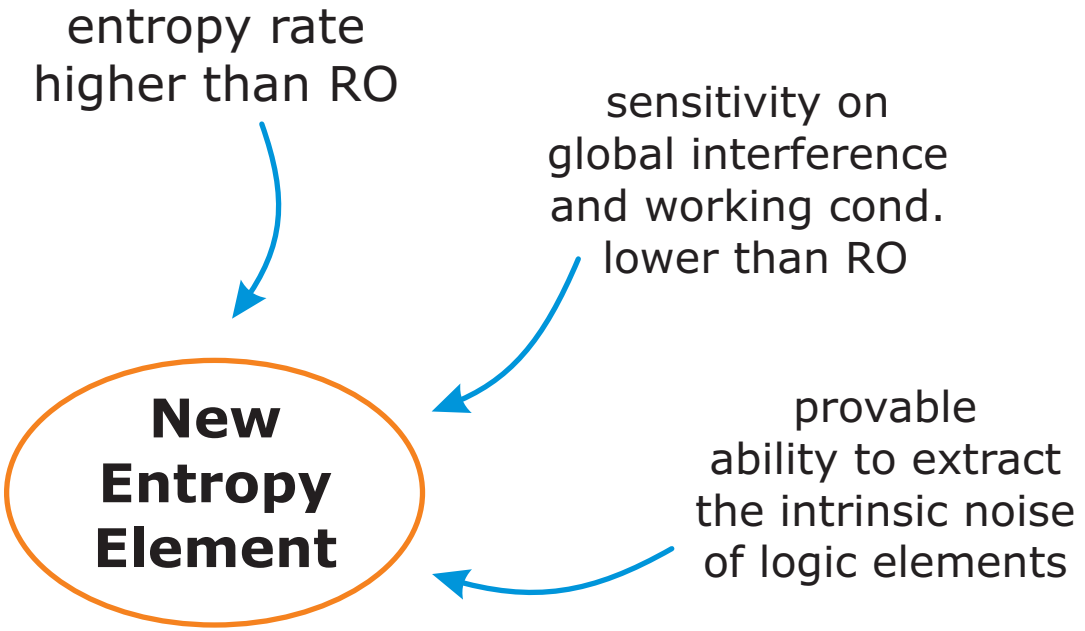
New Entropy Element Design Goals



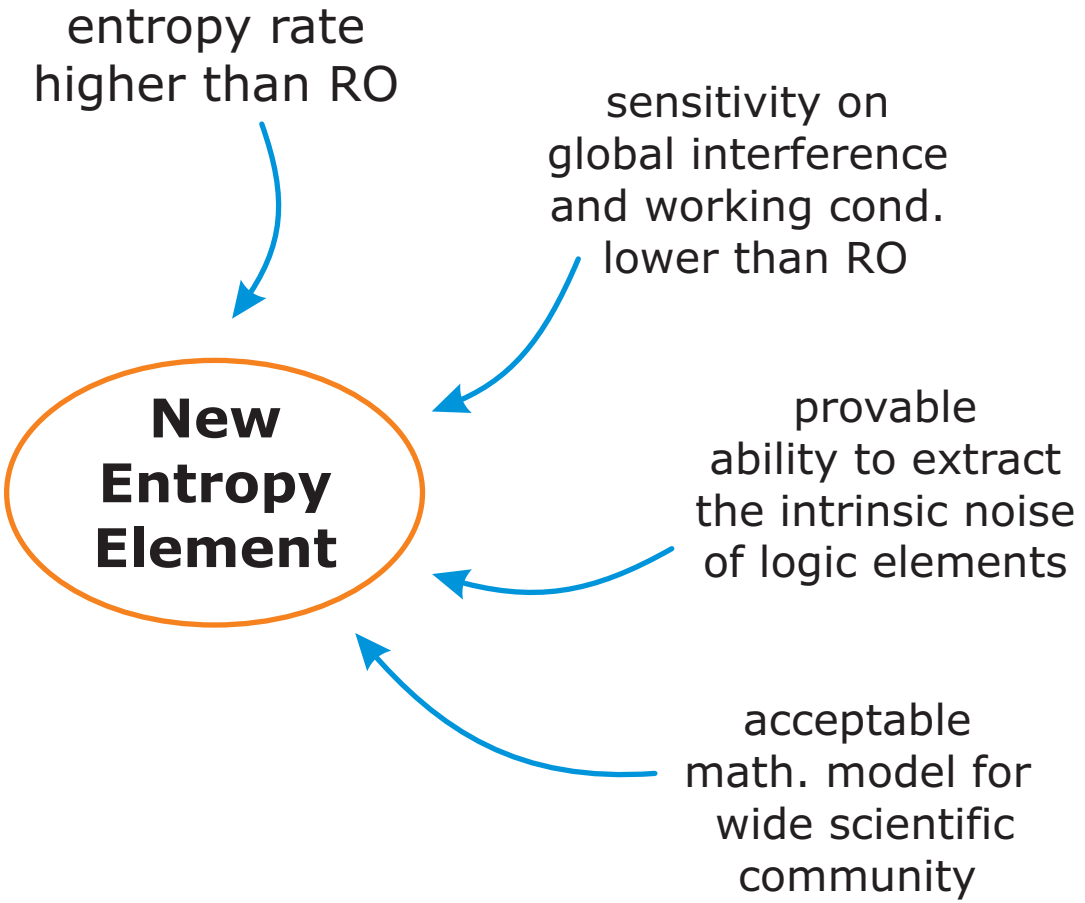
New Entropy Element Design Goals



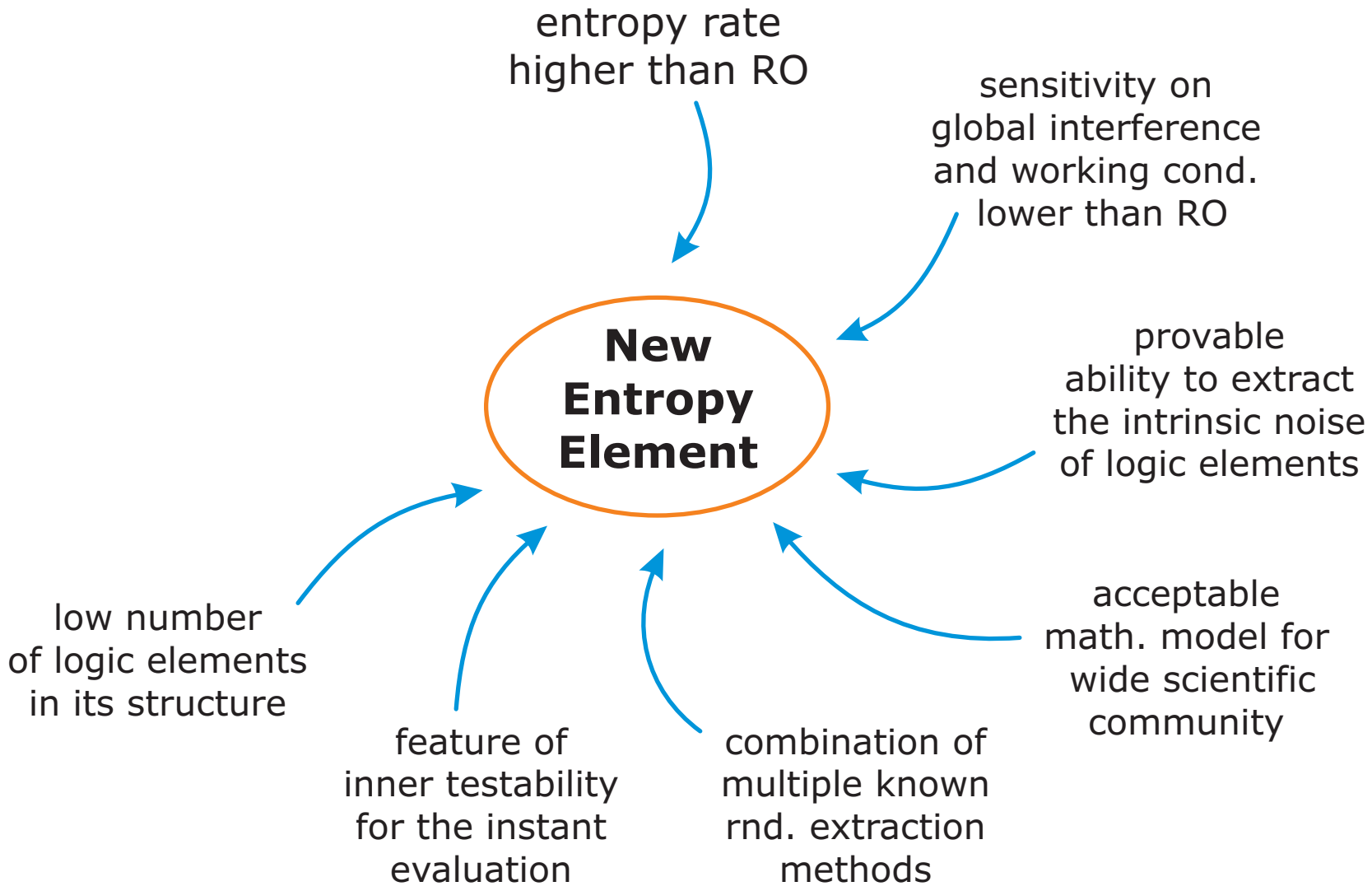
New Entropy Element Design Goals



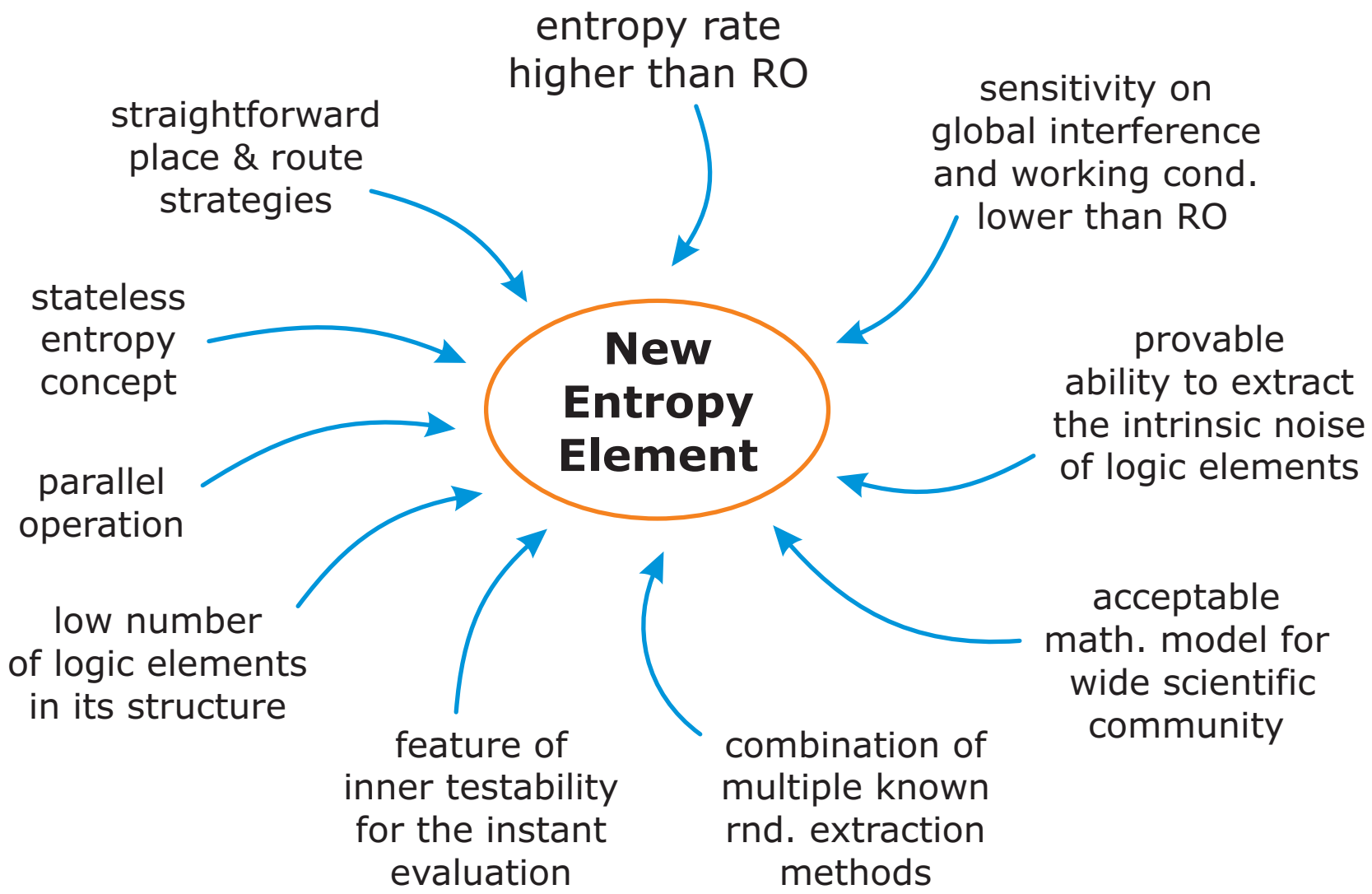
New Entropy Element Design Goals



New Entropy Element Design Goals



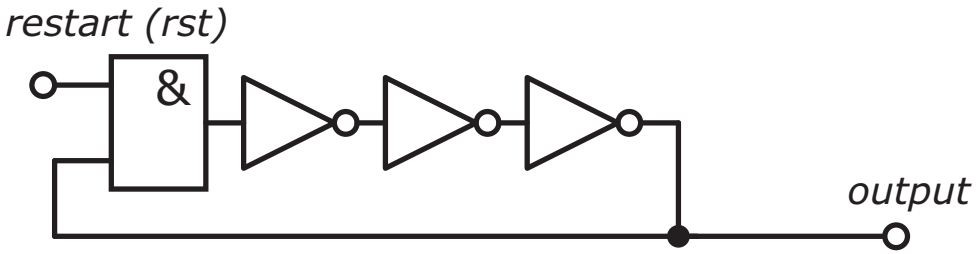
New Entropy Element Design Goals



Agenda

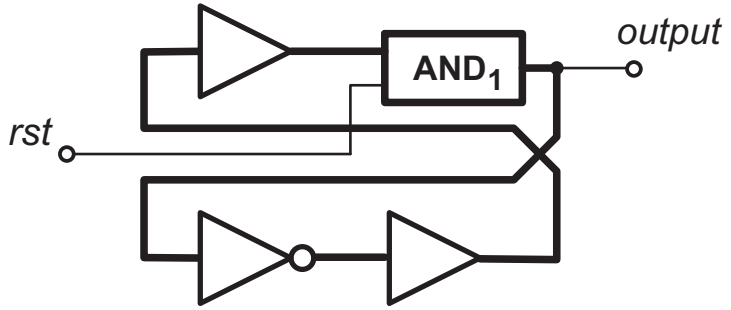
- Introduction
- New Entropy Element Design Goals
- **Transition Effect Ring Oscillator (TERO)**
- Mathematical Model of TERO
- Experimental Results
- Conclusions

Transition Effect Ring Oscillator (TERO)
TERO Circuitry and Operation in FPGA Hardware



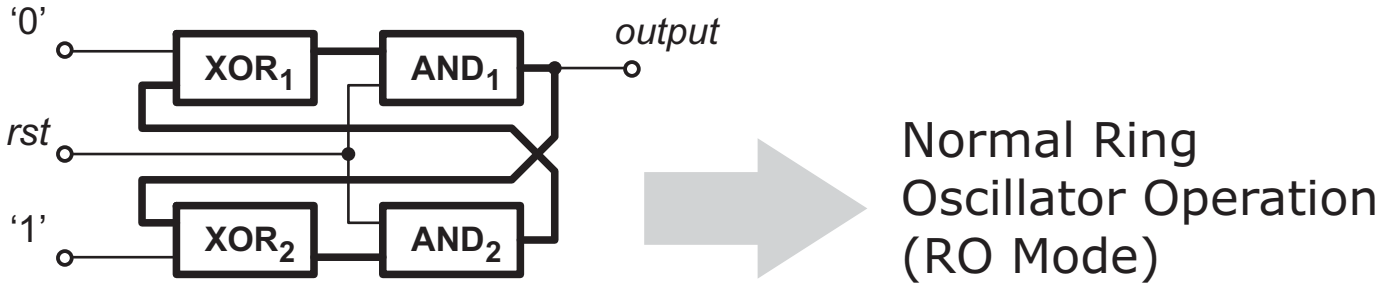
Starting from simple RO...

Transition Effect Ring Oscillator (TERO)
TERO Circuitry and Operation in FPGA Hardware



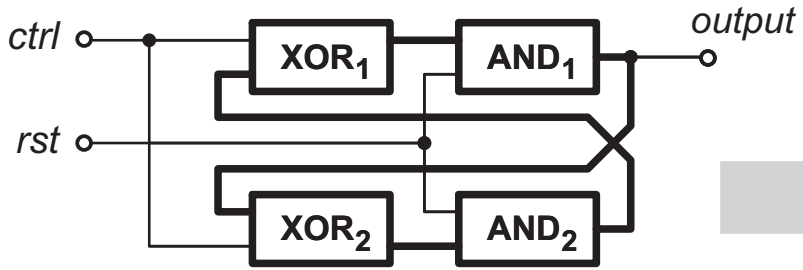
...two inverters are replaced by buffers, still the same circuit behavior...

Transition Effect Ring Oscillator (TERO)
TERO Circuitry and Operation in FPGA Hardware



...buffer and inverter are replaced by XORs, which act as buffer and inverter, second buffer is replaced by AND (in order to have the loop symmetric)...

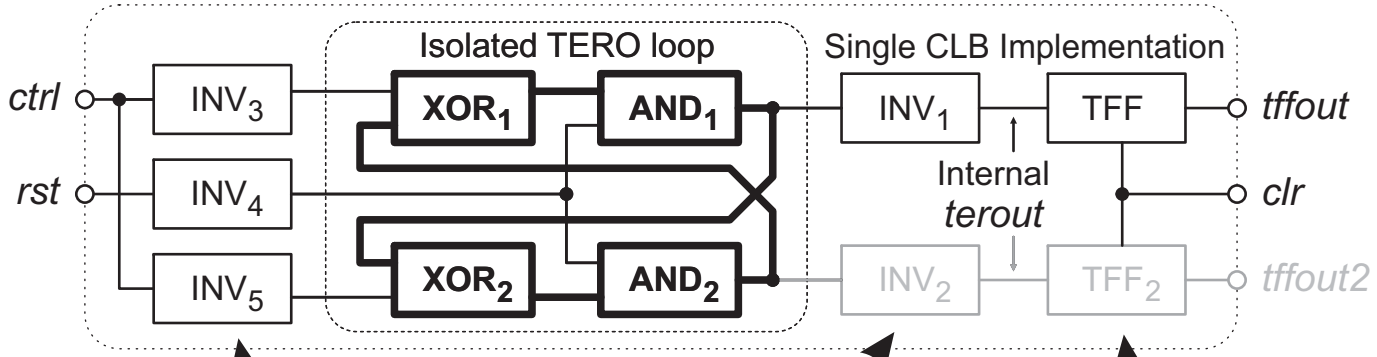
Transition Effect Ring Oscillator (TERO)
TERO Circuitry and Operation in FPGA Hardware



Transition Effect Ring Oscillator Operation (TERO Mode)

...both XORs can be switched from inverter to buffer logic function simultaneously what can cause oscillations in the circuit if the feedback path is long enough ...

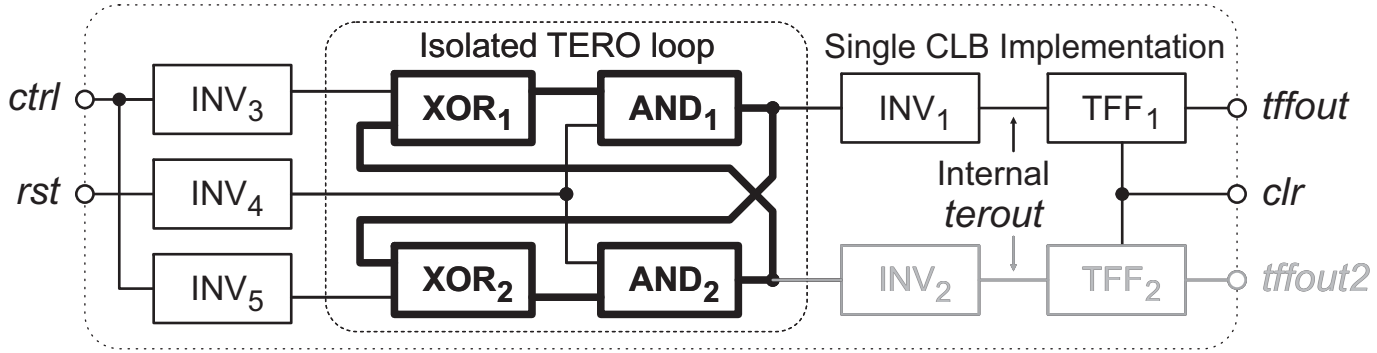
Transition Effect Ring Oscillator (TERO)
TERO Circuitry and Operation in FPGA Hardware

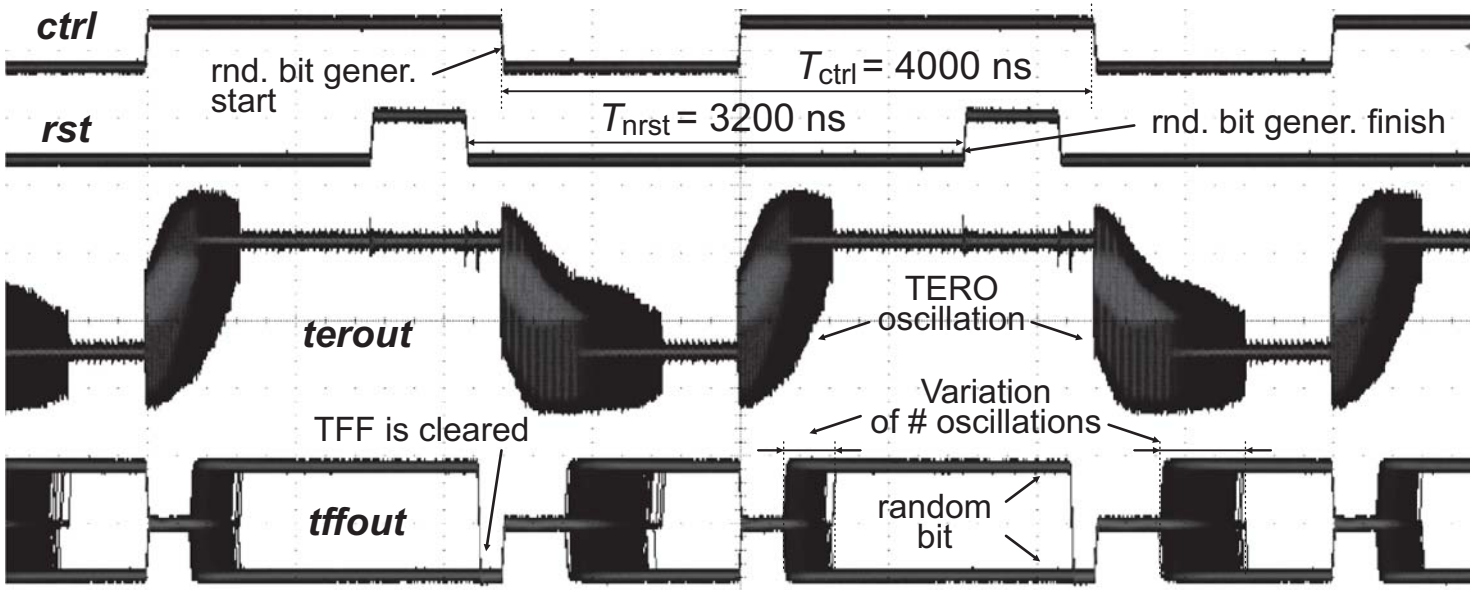


Neighboring Logic Isolation
(in order to prevent routing of internal TERO loop signals outside the CLB)

Randomness Extractor
(TFF resolves whether TERO made even or odd number of oscillations)

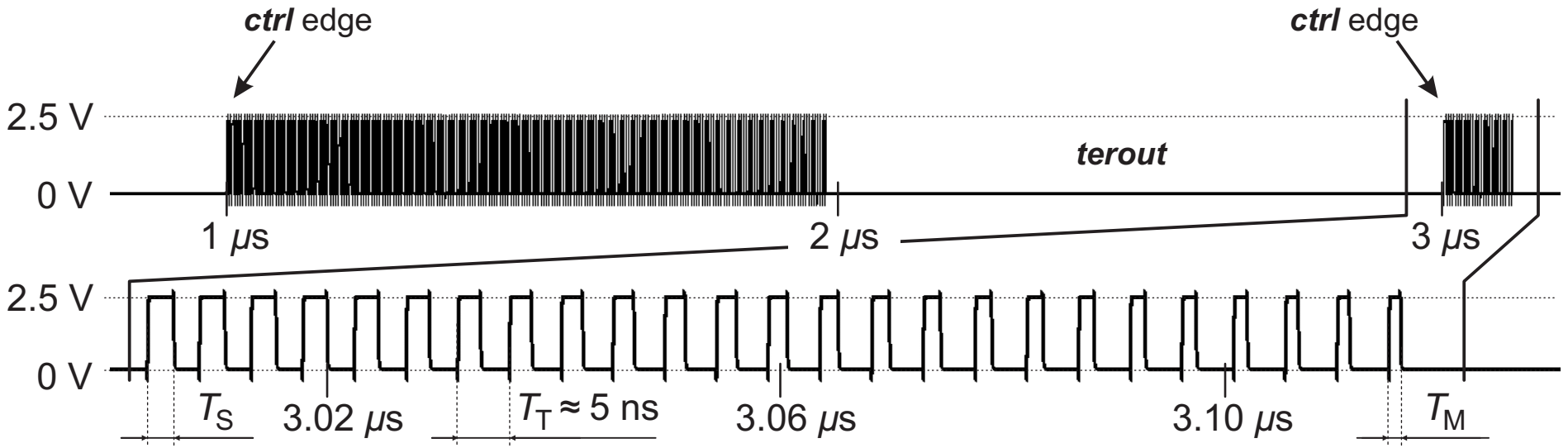
Transition Effect Ring Oscillator (TERO)
TERO Circuitry and Operation in FPGA Hardware





Single CLB Implementation in Xilinx Spartan 3E FPGA and the Oscilloscope Screenshot

Transition Effect Ring Oscillator (TERO)
LT Spice TERO Circuitry Simulation Result

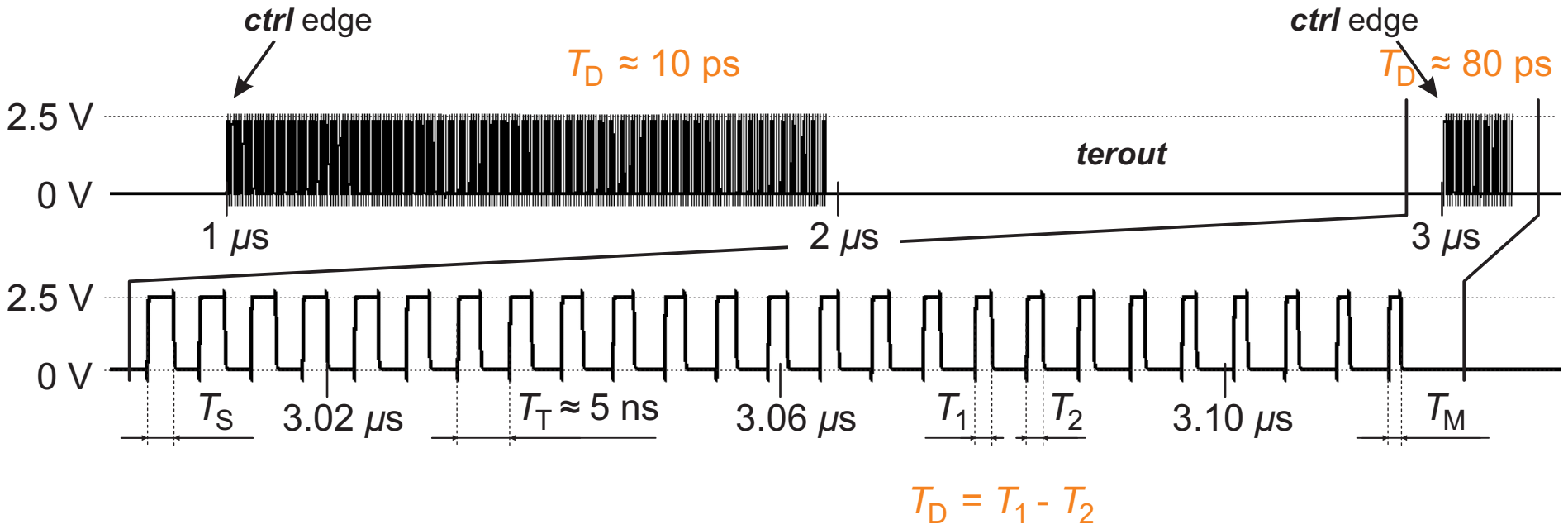


T_S - width of pulse when the oscillations are started

T_T - period of a single TERO oscillation

T_M - width of pulse when the oscillations disappear

Transition Effect Ring Oscillator (TERO)
LT Spice TERO Circuitry Simulation Result



The shortening of raised pulse plays a crucial role...

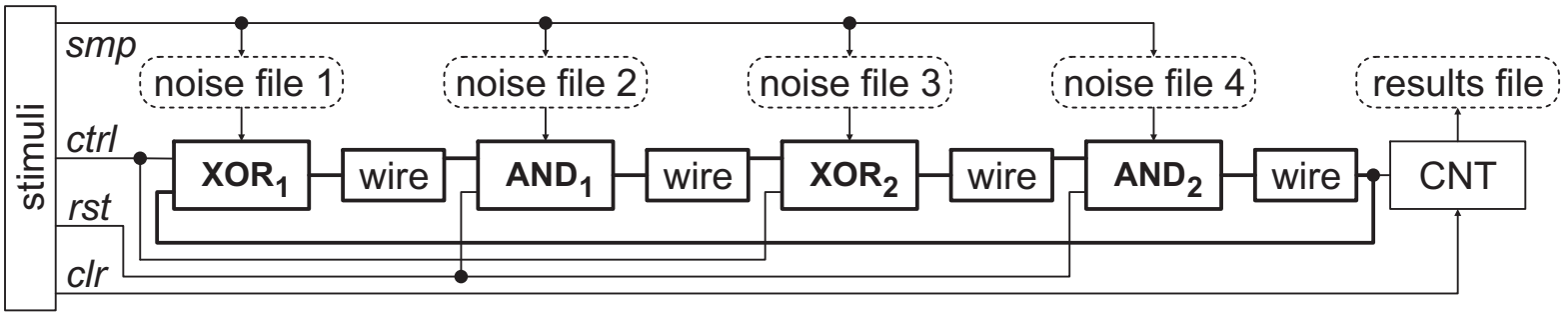
T_S - width of pulse when the oscillations are started

T_T - period of a single TERO oscillation

T_M - width of pulse when the oscillations disappear

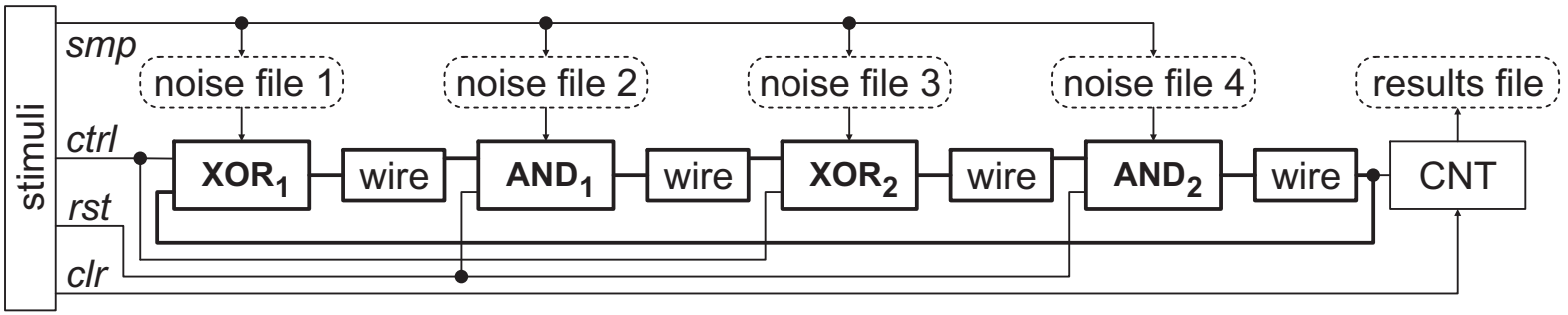
T_D - each oscillation (average) pulse shortening factor

Transition Effect Ring Oscillator (TERO)
TERO vs. RO comparison using VHDL Macro-Model

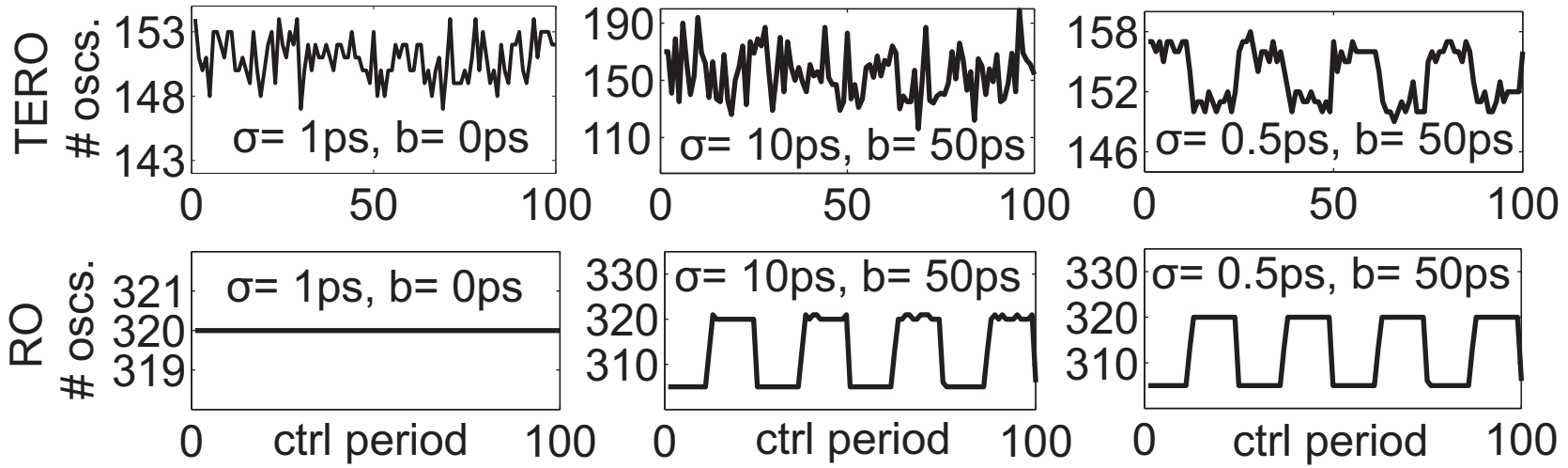


VHDL Macro-Model of TERO (and RO - when ctrl = '1' for XOR_1 and ctrl = '0' for XOR_2)

Transition Effect Ring Oscillator (TERO)
TERO vs. RO comparison using VHDL Macro-Model



VHDL Macro-Model of TERO (and RO - when ctrl = '1' for XOR_1 and ctrl = '0' for XOR_2)



The ModelSim simulation results of the VHDL structure for both TERO and RO modes

Agenda

- Introduction
- New Entropy Element Design Goals
- Transition Effect Ring Oscillator (TERO)
- **Mathematical Model of TERO**
- Experimental Results
- Conclusions

Mathematical Model of TERO

"Remember that all models are wrong;
the practical question is how wrong do they
have to be to not be useful."

George E. P. Box

Mathematical Model of TERO

"Remember that all models are wrong;
the practical question is how wrong do they
have to be to not be useful."

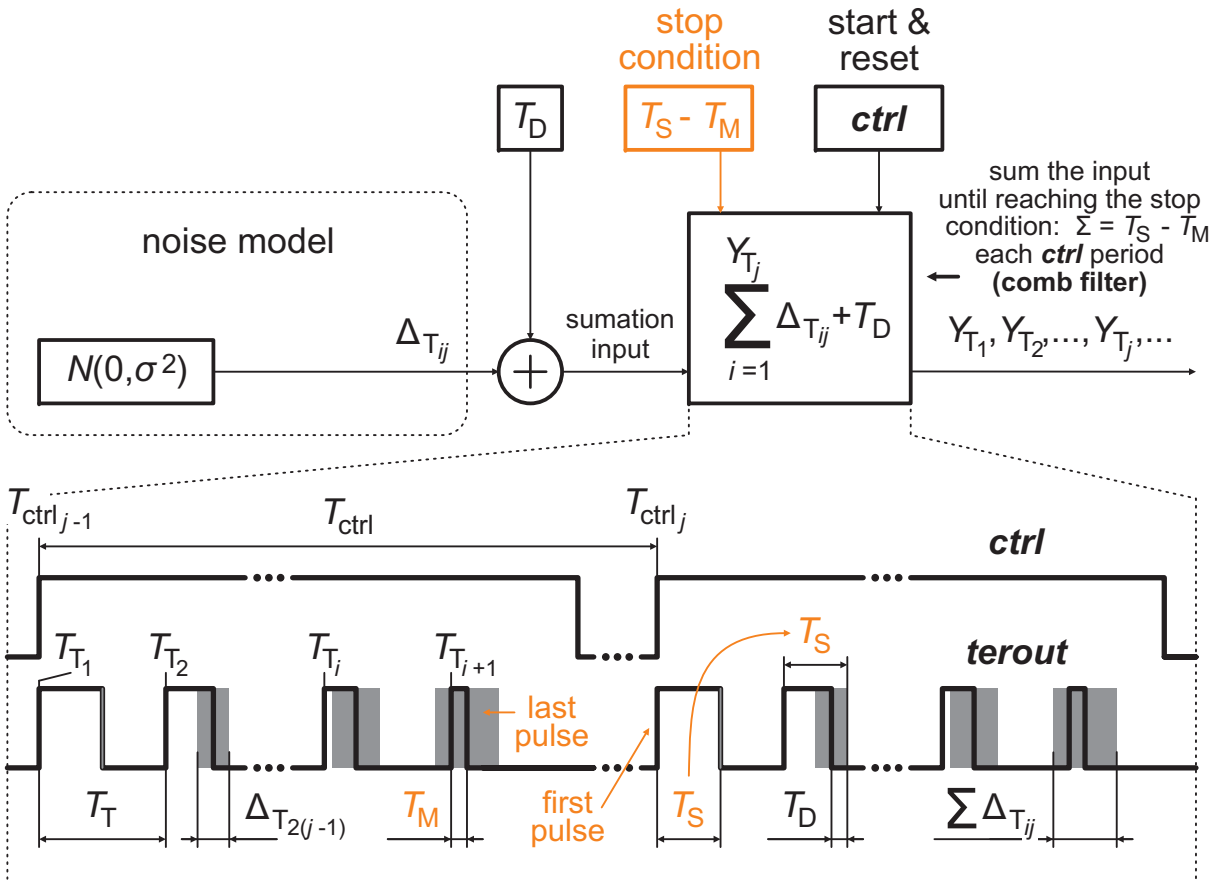
George E. P. Box

We need the useful mathematical model in order to:

- show that "randomness" relies on the physical phenomena
- determine how much "randomness" is available
- fulfill TRNG evaluation criteria
- persuade a community on the reliability of a random number generation method

Mathematical Model of TERO

TERO Mathematical Model Definition

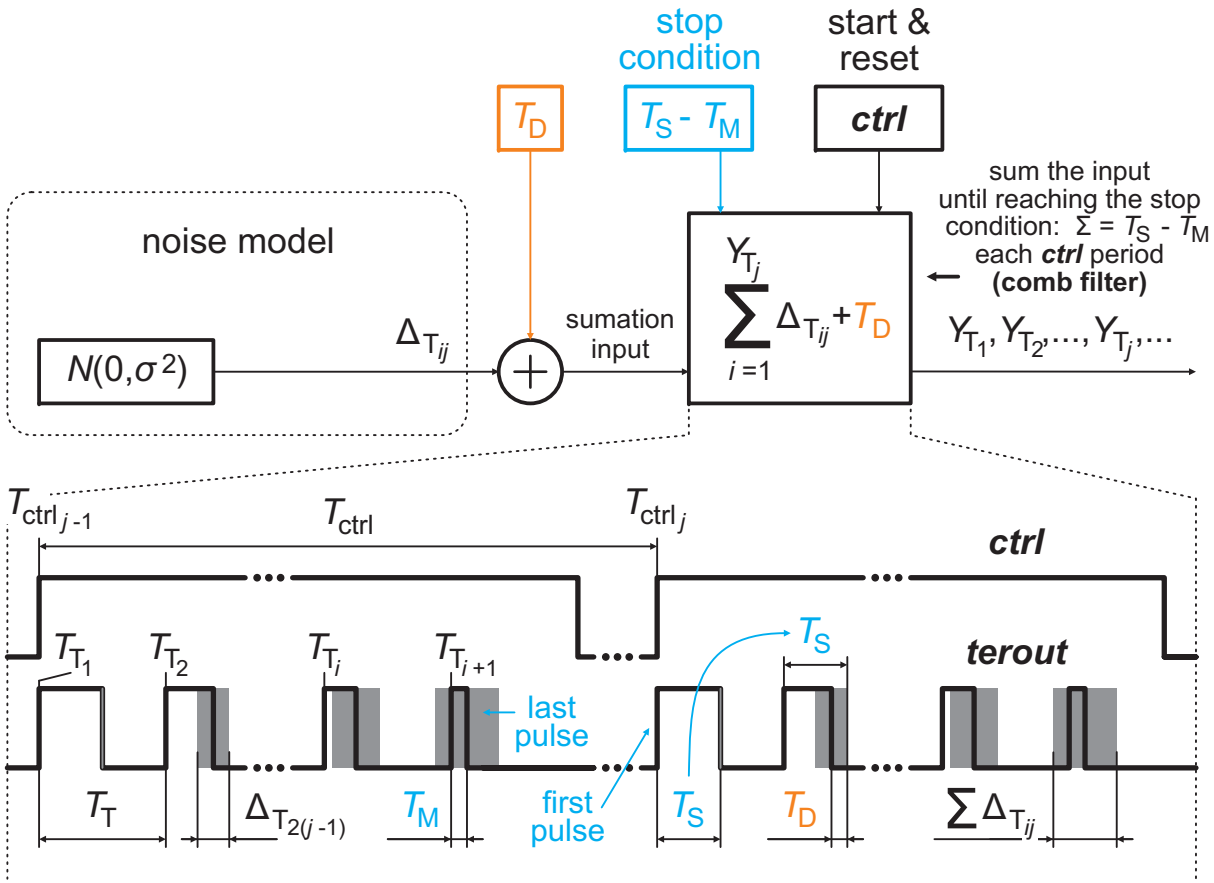


$$T_S - T_M = \sum_{i=1}^{Y_{T_j}} (\Delta_{T_{ij}} + T_D) = T_D \cdot Y_{T_j} + \sum_{i=1}^{Y_{T_j}} \Delta_{T_{ij}}$$

- T_T - period of a single TERO oscillation
- T_S - width of pulse when the oscillations are started
- T_M - width of pulse when the oscillations disappear
- T_D - each oscillation (average) pulse shortening factor
- $\Delta_{T_{ij}}$ - period jitter or instability of shortening factor
- Y_{T_j} - number of oscillations done each j-th ctrl period

Mathematical Model of TERO

TERO Mathematical Model Definition

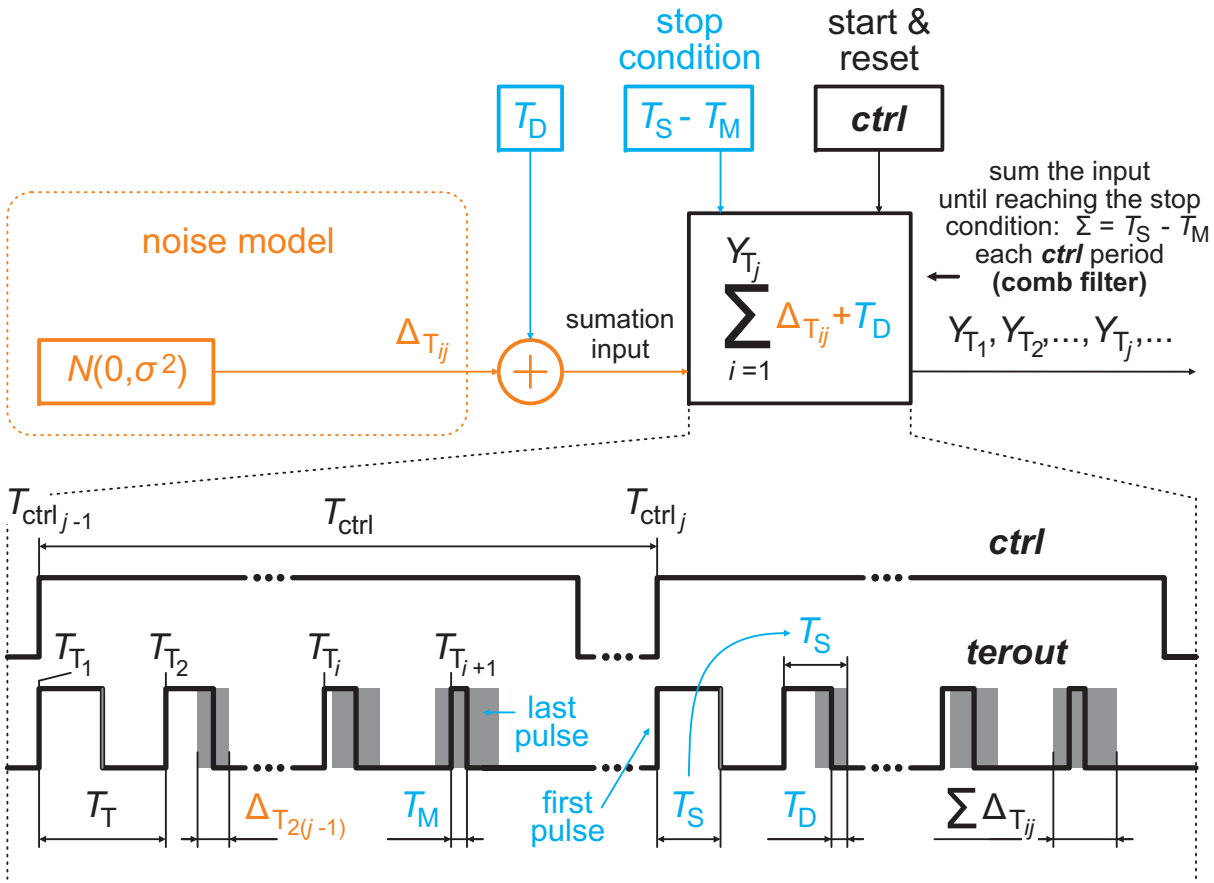


$$T_S - T_M = \sum_{i=1}^{Y_{T_j}} (\Delta_{T_{ij}} + T_D) = T_D \cdot Y_{T_j} + \sum_{i=1}^{Y_{T_j}} \Delta_{T_{ij}}$$

- T_T - period of a single TERO oscillation
- T_S - width of pulse when the oscillations are started
- T_M - width of pulse when the oscillations disappear
- T_D - each oscillation (average) pulse shortening factor
- $\Delta_{T_{ij}}$ - period jitter or instability of shortening factor
- Y_{T_j} - number of oscillations done each *j*-th ctrl period

Mathematical Model of TERO

TERO Mathematical Model Definition



$$T_S - T_M = \sum_{i=1}^{Y_{T_j}} (\Delta_{T_{ij}} + T_D) = T_D \cdot Y_{T_j} + \sum_{i=1}^{Y_{T_j}} \Delta_{T_{ij}}$$

T_T - period of a single TERO oscillation

T_S - width of pulse when the oscillations are started

T_M - width of pulse when the oscillations disappear

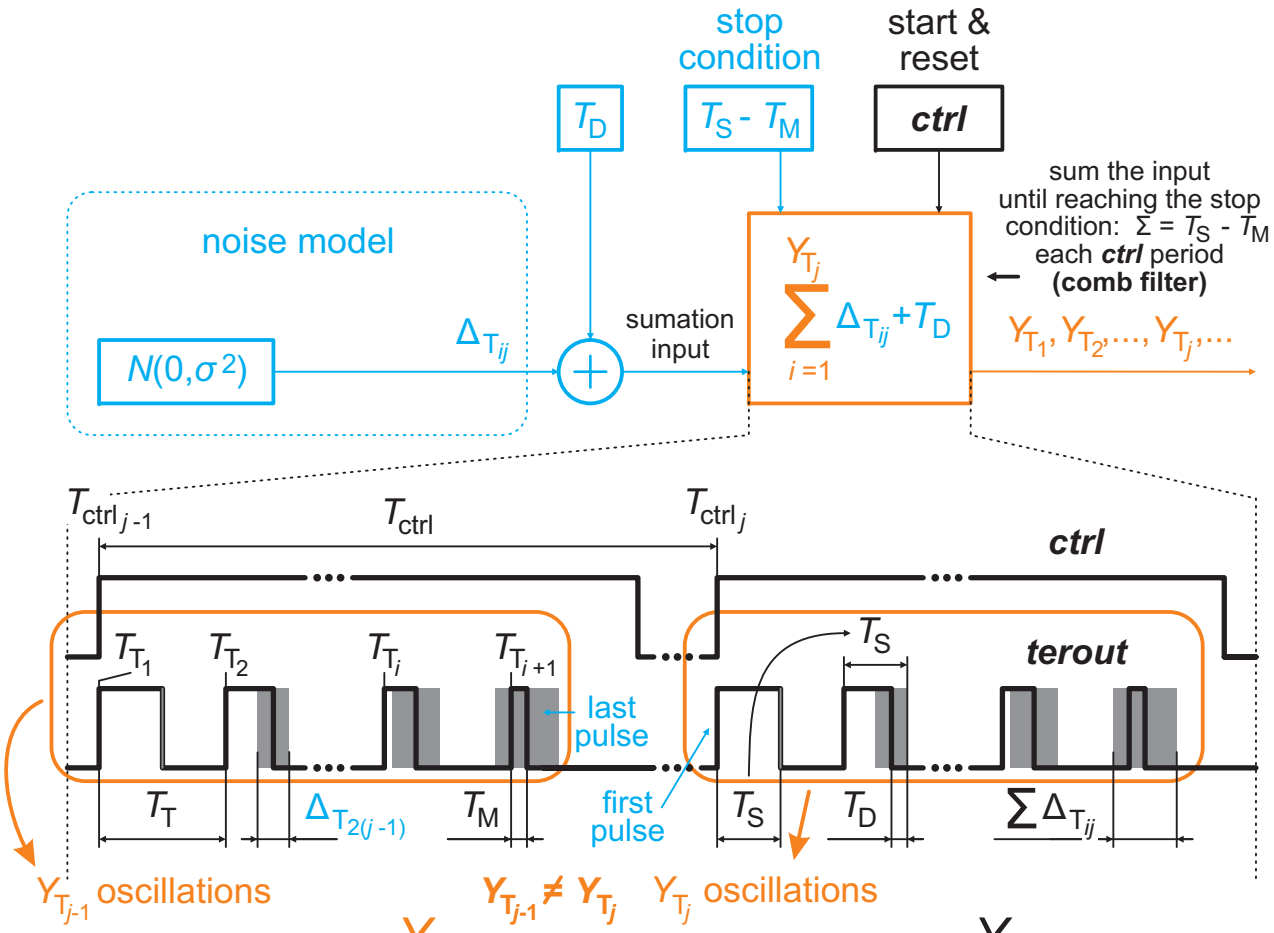
T_D - each oscillation (average) pulse shortening factor

$\Delta_{T_{ij}}$ - period jitter or instability of shortening factor

Y_{T_j} - number of oscillations done each j-th ctrl period

Mathematical Model of TERO

TERO Mathematical Model Definition

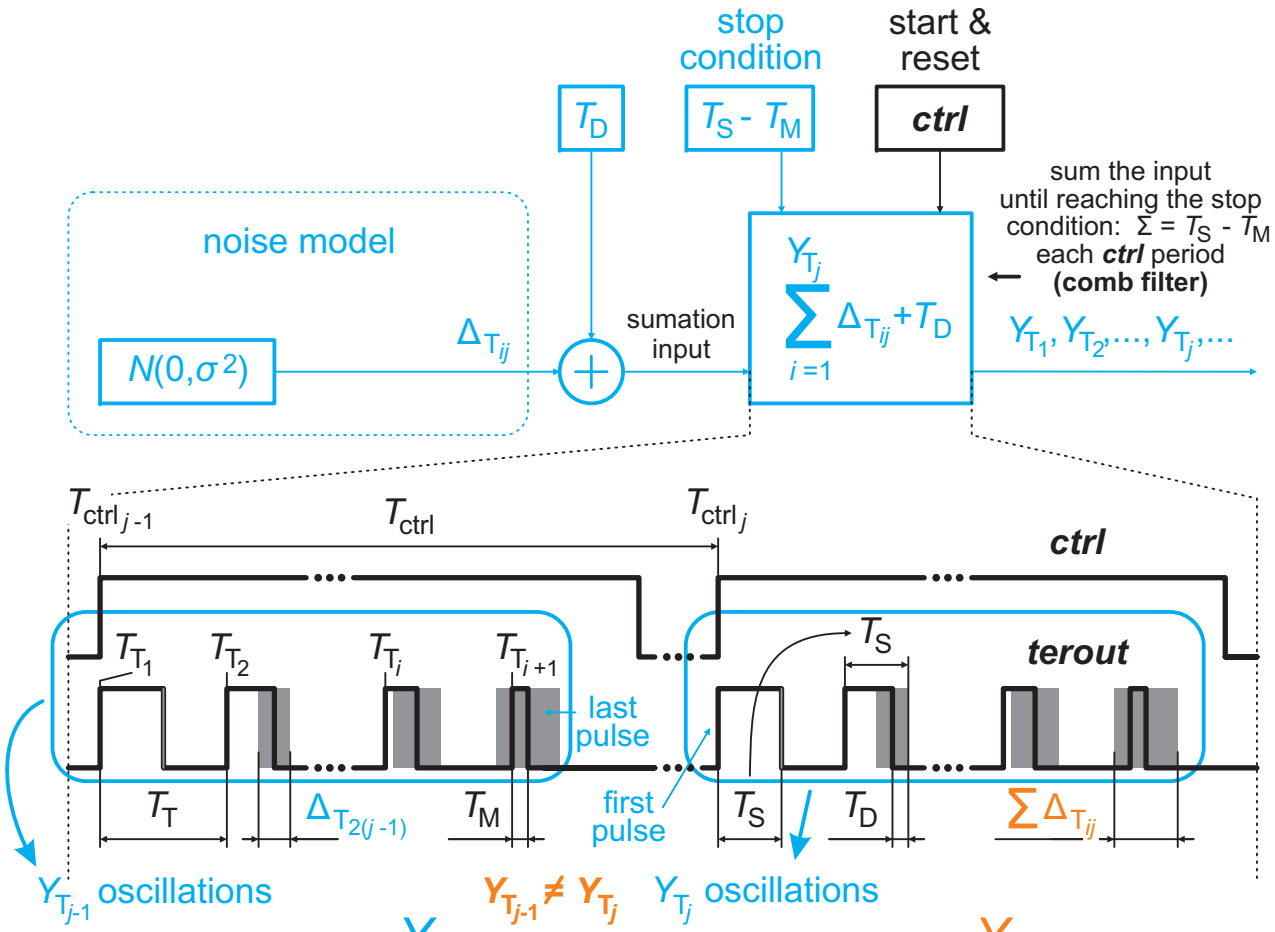


$$T_S - T_M = \sum_{i=1}^{Y_{T_j}} (\Delta_{T_{ij}} + T_D) = T_D \cdot Y_{T_j} + \sum_{i=1}^{Y_{T_j}} \Delta_{T_{ij}}$$

- T_T - period of a single TERO oscillation
- T_S - width of pulse when the oscillations are started
- T_M - width of pulse when the oscillations disappear
- T_D - each oscillation (average) pulse shortening factor
- $\Delta_{T_{ij}}$ - period jitter or instability of shortening factor
- Y_{T_j} - number of oscillations done each j-th ctrl period

Mathematical Model of TERO

TERO Mathematical Model Definition



$$T_S - T_M = \sum_{i=1}^{Y_{T_j}} (\Delta_{T_{ij}} + T_D) = T_D \cdot Y_{T_j} + \sum_{i=1}^{Y_{T_j}} \Delta_{T_{ij}}$$

- T_T - period of a single TERO oscillation
- T_S - width of pulse when the oscillations are started
- T_M - width of pulse when the oscillations disappear
- T_D - each oscillation (average) pulse shortening factor
- $\Delta_{T_{ij}}$ - period jitter or instability of shortening factor
- Y_{T_j} - number of oscillations done each j-th ctrl period

Mathematical Model of TERO

TERO Mathematical Model Practical Impact

mean value of number of oscs. in **TERO mode**

$$\overline{Y_T} \approx \frac{T_S - T_M}{T_D}$$

std. deviation of number of oscs. in **TERO mode**

$$\sigma_{Y_T} \approx \frac{\sigma}{T_D}\sqrt{\overline{Y_T}}$$

where σ is std. deviation of a period jitter

Mathematical Model of TERO

TERO Mathematical Model Practical Impact

mean value of number of oscs. in **TERO mode**

$$\overline{Y_T} \approx \frac{T_S - T_M}{T_D}$$

std. deviation of number of oscs. in **TERO mode**

$$\sigma_{Y_T} \approx \frac{\sigma}{T_D}\sqrt{\overline{Y_T}}$$

where σ is std. deviation of a period jitter

mean value of number of oscs. in **RO mode**

$$\overline{Y_R} \approx \frac{T_{nrst}}{2T_T}$$

where T_{nrst} is time when RO is oscillating

std. deviation of number of oscs. in **RO mode**

$$\sigma_{Y_R} \approx \frac{\sigma}{2T_T}\sqrt{\overline{Y_R}}$$

Mathematical Model of TERO

TERO Mathematical Model Practical Impact

mean value of number of oscs. in **TERO mode**

$$\overline{Y_T} \approx \frac{T_S - T_M}{T_D}$$

std. deviation of number of oscs. in **TERO mode**

$$\sigma_{Y_T} \approx \frac{\sigma}{T_D}\sqrt{\overline{Y_T}}$$

where σ is std. deviation of a period jitter

~ ps ~ ns

mean value of number of oscs. in **RO mode**

$$\overline{Y_R} \approx \frac{T_{nrst}}{2T_T}$$

where T_{nrst} is time when RO is oscillating

std. deviation of number of oscs. in **RO mode**

$$\sigma_{Y_R} \approx \frac{\sigma}{2T_T}\sqrt{\overline{Y_R}}$$

Mathematical Model of TERO

TERO Mathematical Model Practical Impact

mean value of number of oscs. in **TERO mode**

$$\overline{Y_T} \approx \frac{T_S - T_M}{T_D}$$

std. deviation of number of oscs. in **TERO mode**

$$\sigma_{Y_T} \approx \frac{\sigma}{T_D}\sqrt{\overline{Y_T}}$$

where σ is std. deviation of a period jitter

~ ps ~ ns

mean value of number of oscs. in **RO mode**

$$\overline{Y_R} \approx \frac{T_{nrst}}{2T_T}$$

where T_{nrst} is time when RO is oscillating

std. deviation of number of oscs. in **RO mode**

$$\sigma_{Y_R} \approx \frac{\sigma}{2T_T}\sqrt{\overline{Y_R}}$$

$$\frac{\sigma_{Y_T}}{\sigma_{Y_R}} \approx \frac{2T_T}{T_D}\sqrt{\frac{2T_T(T_S - T_M)}{T_D\,T_{nrst}}} \approx$$

≈ 100 ~ 500 !!!

Mathematical Model of TERO

TERO Mathematical Model Practical Impact

mean value of number of oscs. in **TERO mode**

$$\overline{Y_T} \approx \frac{T_S - T_M}{T_D}$$

std. deviation of number of oscs. in **TERO mode**

$$\sigma_{Y_T} \approx \frac{\sigma}{T_D}\sqrt{\overline{Y_T}}$$

where σ is std. deviation of a period jitter

~ ps ~ ns

mean value of number of oscs. in **RO mode**

$$\overline{Y_R} \approx \frac{T_{nrst}}{2T_T}$$

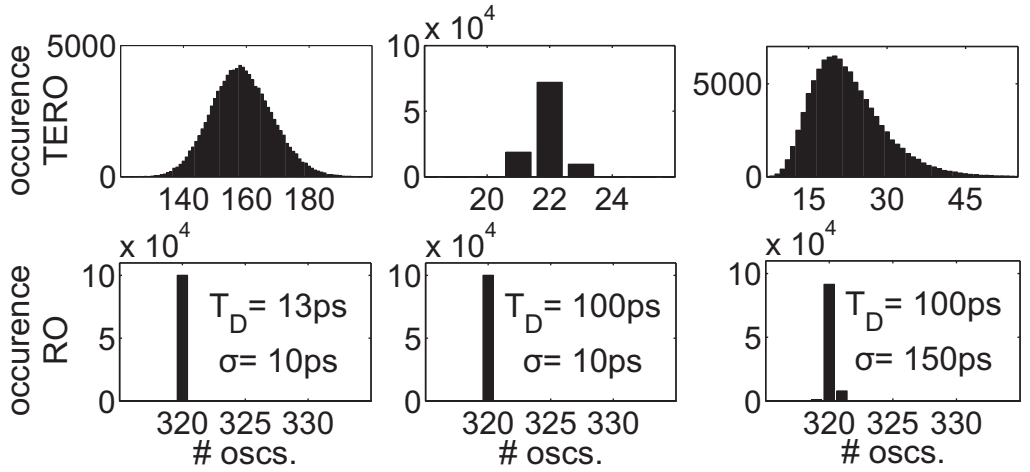
where T_{nrst} is time when RO is oscillating

std. deviation of number of oscs. in **RO mode**

$$\sigma_{Y_R} \approx \frac{\sigma}{2T_T}\sqrt{\overline{Y_R}}$$

$$\frac{\sigma_{Y_T}}{\sigma_{Y_R}} \approx \frac{2T_T}{T_D}\sqrt{\frac{2T_T(T_S - T_M)}{T_D\, T_{nrst}}} \approx$$

≈ 100 ~ 500 !!!

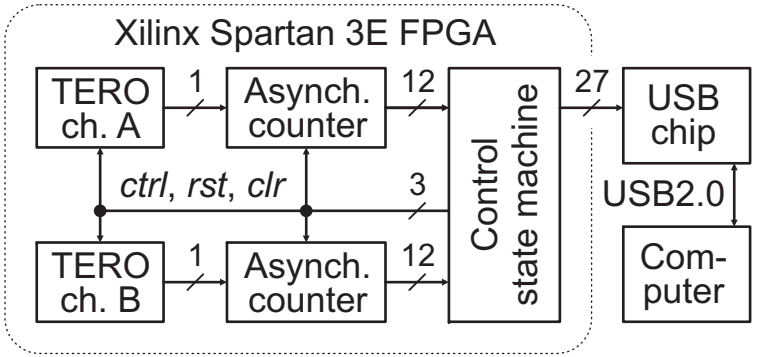


Matlab simulation of TERO and RO math. models

Agenda

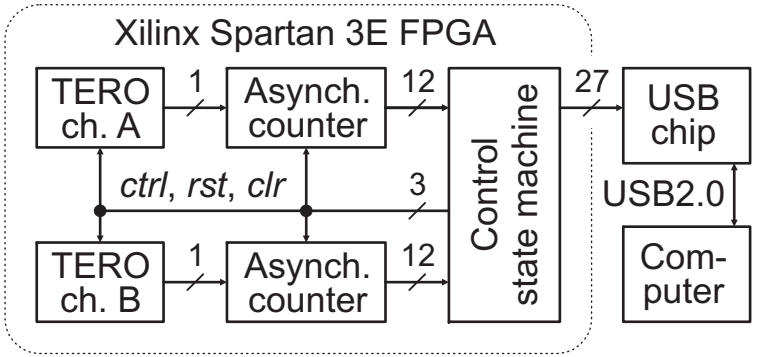
- Introduction
- New Entropy Element Design Goals
- Transition Effect Ring Oscillator (TERO)
- Mathematical Model of TERO
- **Experimental Results**
- Conclusions

Experimental Results
Synthesis of the Evaluation Platform #1

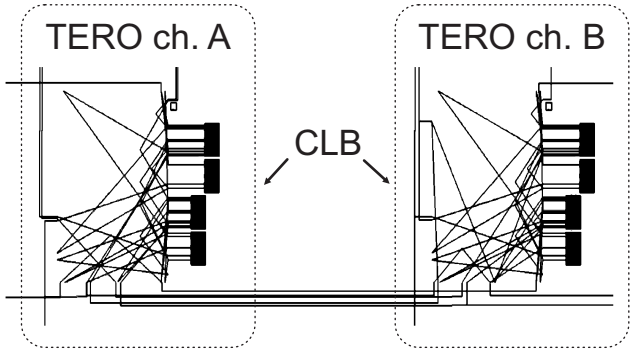


Evaluation Platform implemented in Xilinx Spartan 3E FPGA

Experimental Results
Synthesis of the Evaluation Platform #1

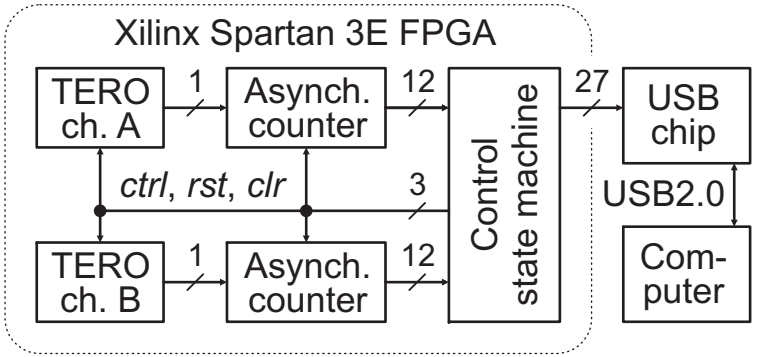


Evaluation Platform implemented in Xilinx Spartan 3E FPGA

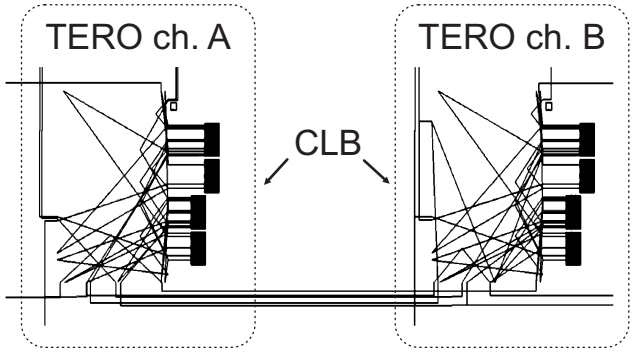


TERO Place & Route detail,
where each channel is implemented
in separated CLB

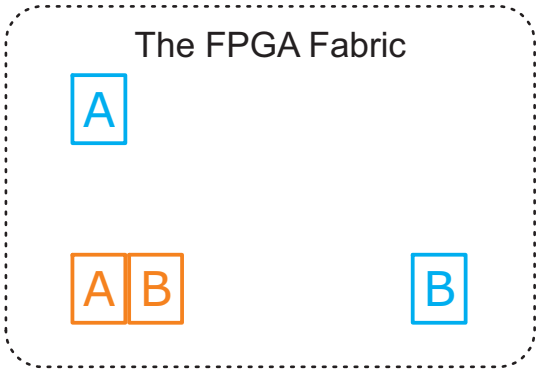
Experimental Results
Synthesis of the Evaluation Platform #1



Evaluation Platform implemented in Xilinx Spartan 3E FPGA

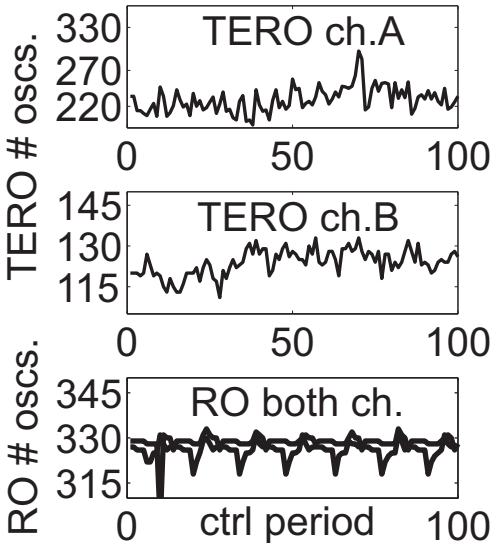


TERO Place & Route detail,
where each channel is implemented
in separated CLB



Two mutual TERO compositions:
Next and Diagonal used in
practical experiments

Experimental Results
Results of the Evaluation Platform #1 (1 of 2)



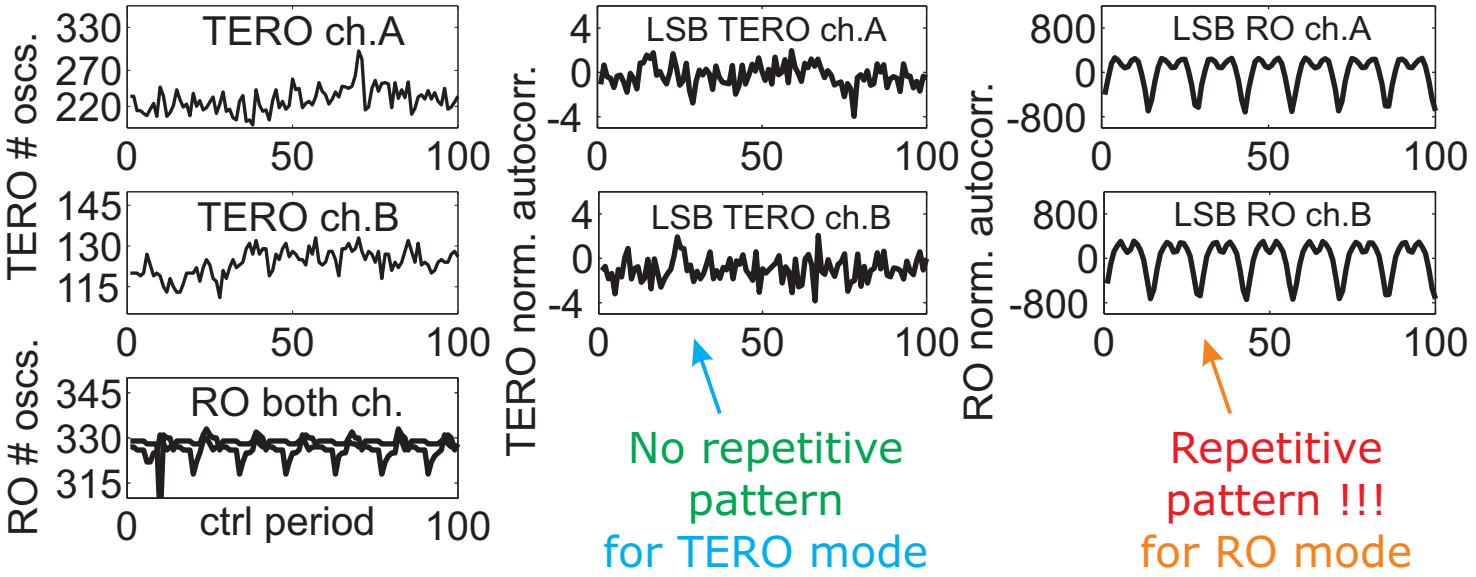
TERO mode:
- higher variance
- uncorrelated

RO mode:
- lower variance
- correlated !!!

The **comparison** of number of oscillations for both **TERO** and **RO** **modes**

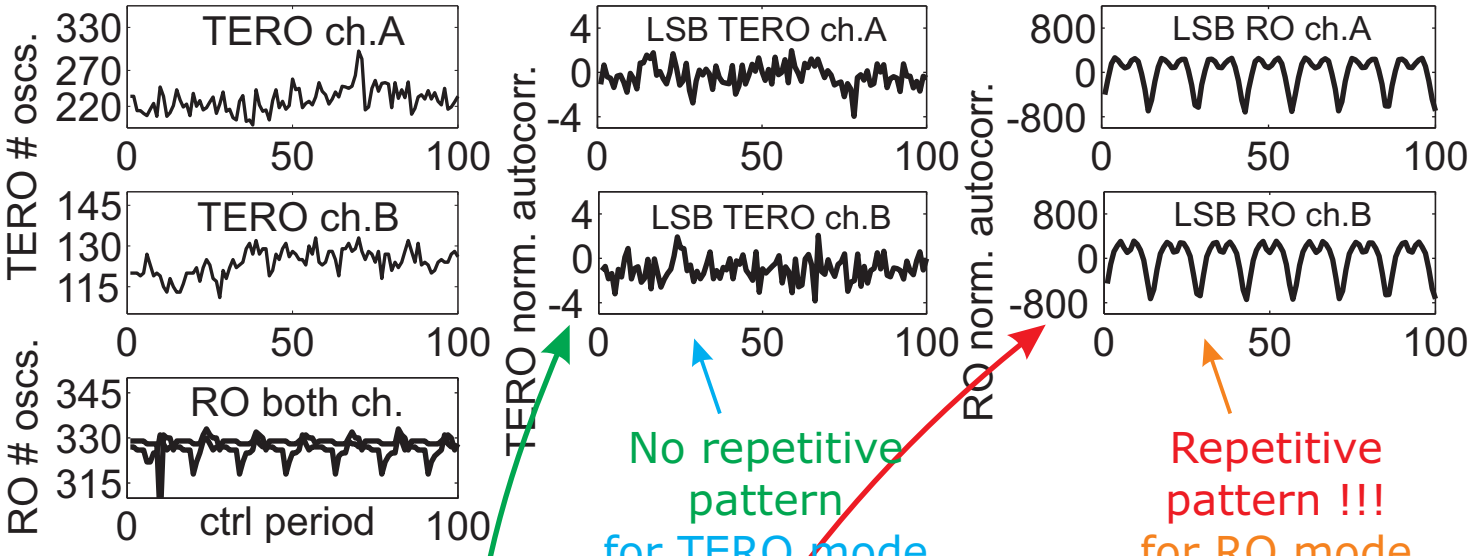
Experimental Results

Results of the Evaluation Platform #1 (1 of 2)



The **comparison** of normalized autocorrelation of number of oscillations (LSB) for both **TERO** and **RO modes**

Experimental Results
Results of the Evaluation Platform #1 (1 of 2)



The **comparison** of normalized autocorrelation of number of oscillations (LSB) for both **TERO** and **RO modes**

Normalized autocorrellation ***X*** is expressed as:

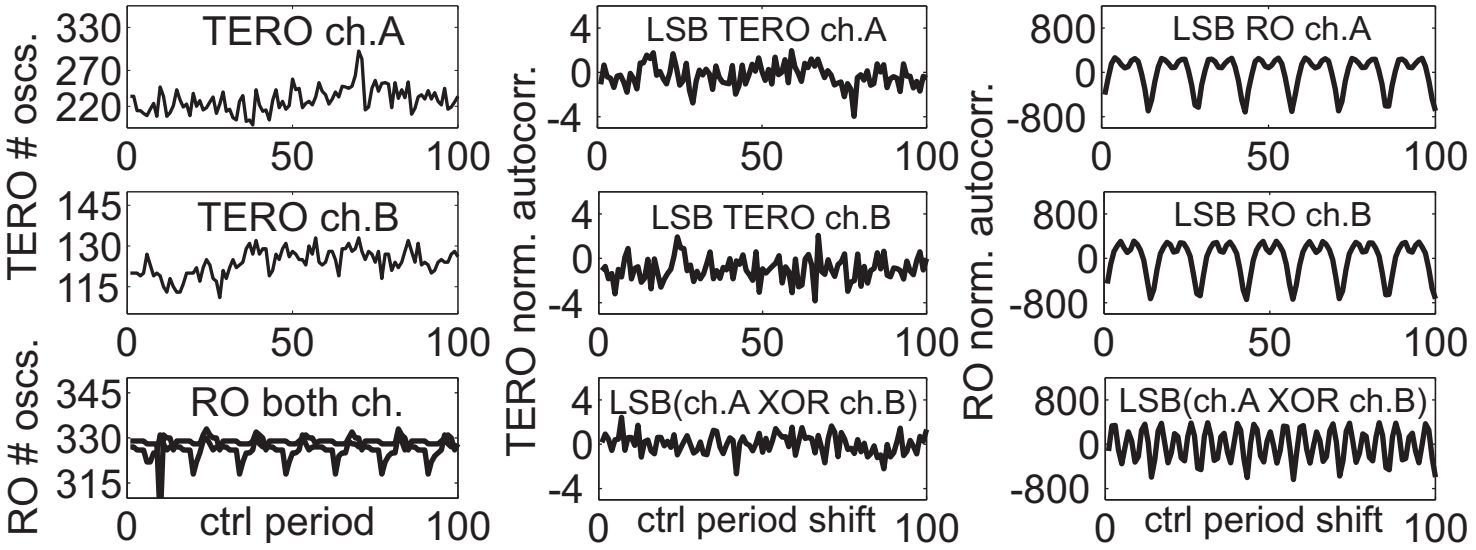
$$X = 2\left(\sum_{i=1}^{n-d-1}(s_i \oplus s_{i+d}) - \frac{n-d}{2}\right) / \sqrt{n-d}$$

X - should approximately follow $N(0,1)$
- should fall into 3σ interval: <-3,3>

s - random bit sequence
d - number of shifts ($1 \le d \le 100$)
n - number of bits (n = 1Mbit)

Experimental Results

Results of the Evaluation Platform #1 (1 of 2)



XOR combination of A and B
TERO and RO channels

Experimental Results
Results of the Evaluation Platform #1 (2 of 2)

TEST	Source	Next(TERO)	Diag.(TERO)	Next(RO)	Diag.(RO)
Mean	LSB A / LSB B	0.51/0.48	0.51/0.48	0.47/0.44	0.55/0.46
Value	LSB(A XOR B)	0.5002	0.4999	0.4539	0.7926
Normalized cross-correlation (for shift=0)	LSB (A,B)	0.4160	-0.0917	-94.3378	599.3945
NIST / FIPS	Only LSB A	F / P	F / F	- / F	- / F
Statistical	Only LSB B	F / F	F / F	- / F	- / F
tests result	LSB(A XOR B)	P / P	P / P	- / F	- / F

Experimental Results
Results of the Evaluation Platform #1 (2 of 2)

mean value improved by XOR combination

mean value worsened by XOR combination !!!

TEST	Source	Next(TERO)	Diag.(TERO)	Next(RO)	Diag.(RO)
Mean Value	LSB A / LSB B LSB(A xor B)	0.51/0.48 0.5002	0.51/0.48 0.4999	0.47/0.44 0.4539	0.55/0.46 0.7926
Normalized cross-correlation (for shift=0)	LSB (A,B)	0.4160	-0.0917	-94.3378	599.3945
NIST / FIPS Statistical tests result	Only LSB A	F / P	F / F	- / F	- / F
	Only LSB B	F / F	F / F	- / F	- / F
	LSB(A xor B)	P / P	P / P	- / F	- / F

Experimental Results
Results of the Evaluation Platform #1 (2 of 2)

mean value improved by XOR combination

mean value worsened by XOR combination !!!

TEST	Source	Next(TERO)	Diag.(TERO)	Next(RO)	Diag.(RO)
Mean Value	LSB A / LSB B LSB(A xor B)	0.51/0.48 0.5002	0.51/0.48 0.4999	0.47/0.44 0.4539	0.55/0.46 0.7926
Normalized cross-correlation (for shift=0)	LSB (A,B)	**The outputs of TEROs are uncorelated** 0.4160	-0.0917	**The outputs of ROs are correlated !!!** -94.3378	599.3945
NIST / FIPS Statistical tests result	Only LSB A	F / P	F / F	- / F	- / F
	Only LSB B	F / F	F / F	- / F	- / F
	LSB(A xor B)	P / P	P / P	- / F	- / F

Experimental Results
Results of the Evaluation Platform #1 (2 of 2)

mean value improved by XOR combination

mean value worsened by XOR combination !!!

TEST	Source	Next(TERO)	Diag.(TERO)	Next(RO)	Diag.(RO)
Mean Value	LSB A / LSB B LSB(A xor B)	0.51/0.48 0.5002	0.51/0.48 0.4999	0.47/0.44 0.4539	0.55/0.46 0.7926
Normalized cross-correlation (for shift=0)	LSB (A,B)	**The outputs of TEROs are uncorelated** 0.4160	-0.0917	**The outputs of ROs are correlated !!!** -94.3378	599.3945
NIST / FIPS Statistical tests result	Only LSB A	F / P	F / F	- / F	- / F
	Only LSB B	F / F	F / F	- / F	- / F
	LSB(A xor B)	P / P	P / P	- / F	- / F

NIST 800-22 and FIPS 140-2 results improved by XOR combination

FIPS 140-2 tests fail completely !!!

Experimental Results
Results of the Evaluation Platform #1 (2 of 2)

mean value improved by XOR combination

mean value worsened by XOR combination !!!

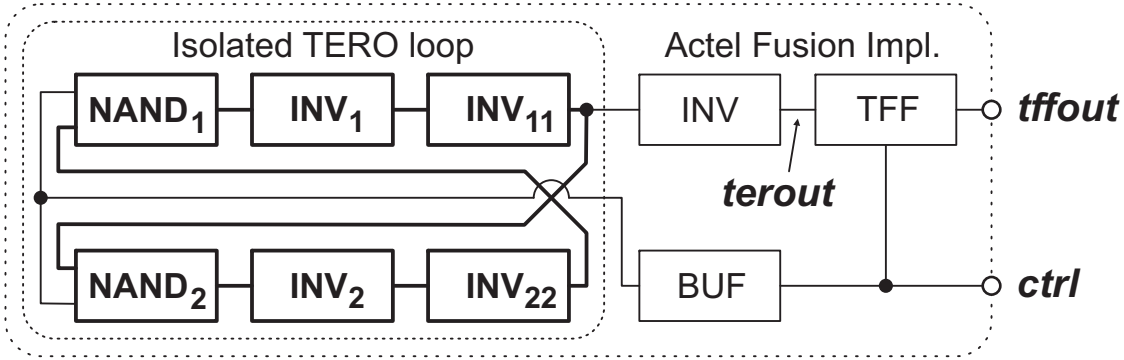
TEST	Source	Next(TERO)	Diag.(TERO)	Next(RO)	Diag.(RO)
Mean Value	LSB A / LSB B LSB(A xor B)	0.51/0.48 0.5002	0.51/0.48 0.4999	0.47/0.44 0.4539	0.55/0.46 0.7926
Normalized cross-correlation (for shift=0)	LSB (A,B)	**The outputs of TEROs are uncorelated** 0.4160	-0.0917	**The outputs of ROs are correlated !!!** -94.3378	599.3945
NIST / FIPS Statistical tests result	Only LSB A	F / P	F / F	- / F	- / F
	Only LSB B	F / F	F / F	- / F	- / F
	LSB(A xor B)	P / P	P / P	- / F	- / F

Random sequences are independent (with high probability)

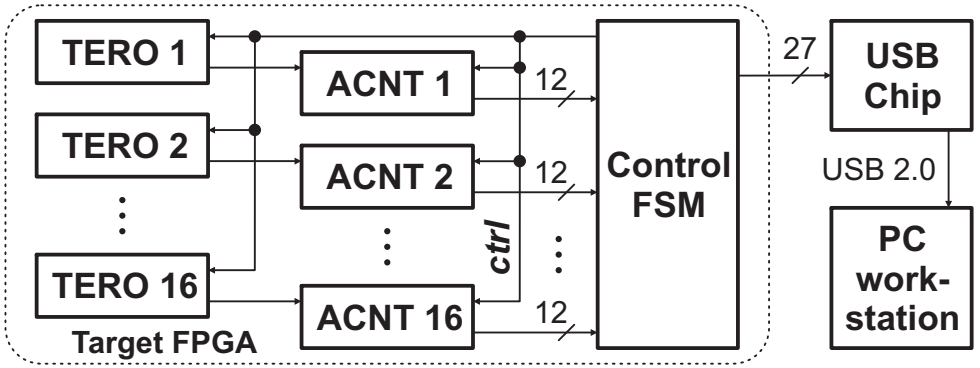
NIST 800-22 and FIPS 140-2 results improved by XOR combination

FIPS 140-2 tests fail completely !!!

Experimental Results
Synthesis of the Evaluation Platform #2



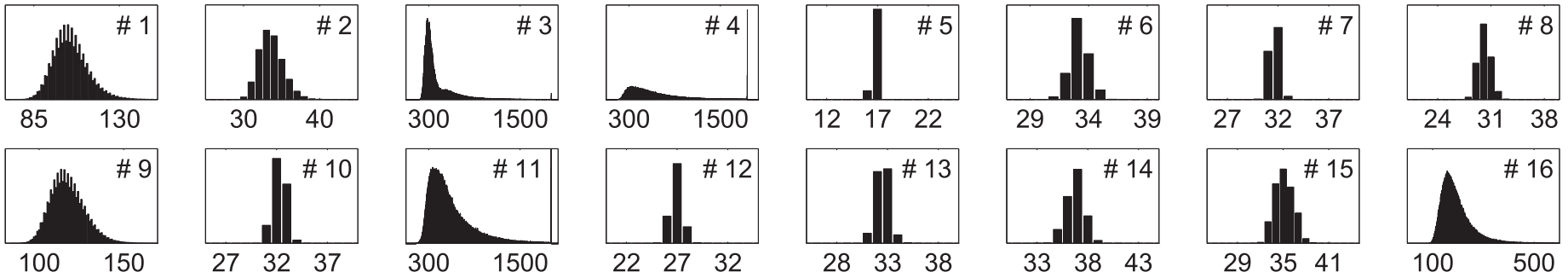
TERO structure adapted for Actel Fusion FPGA



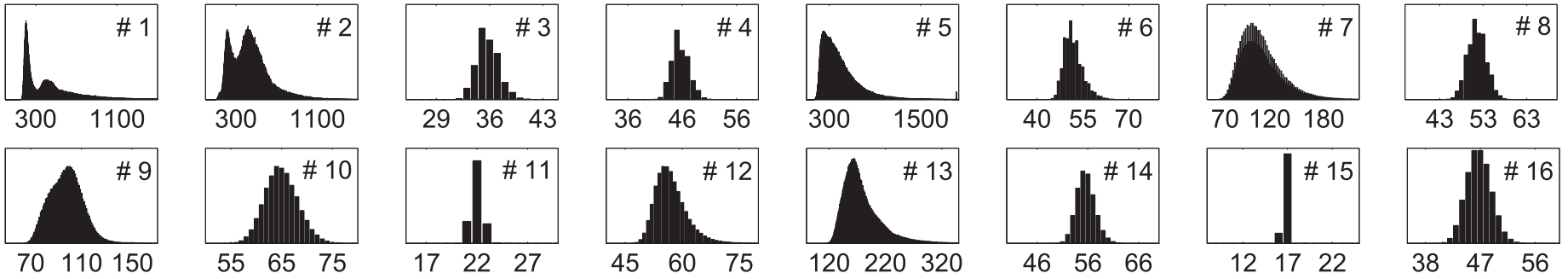
Evaluation Platform implemented in Actel Fusion FPGA

Experimental Results

Results of the Evaluation Platform #2 (1 of 2)

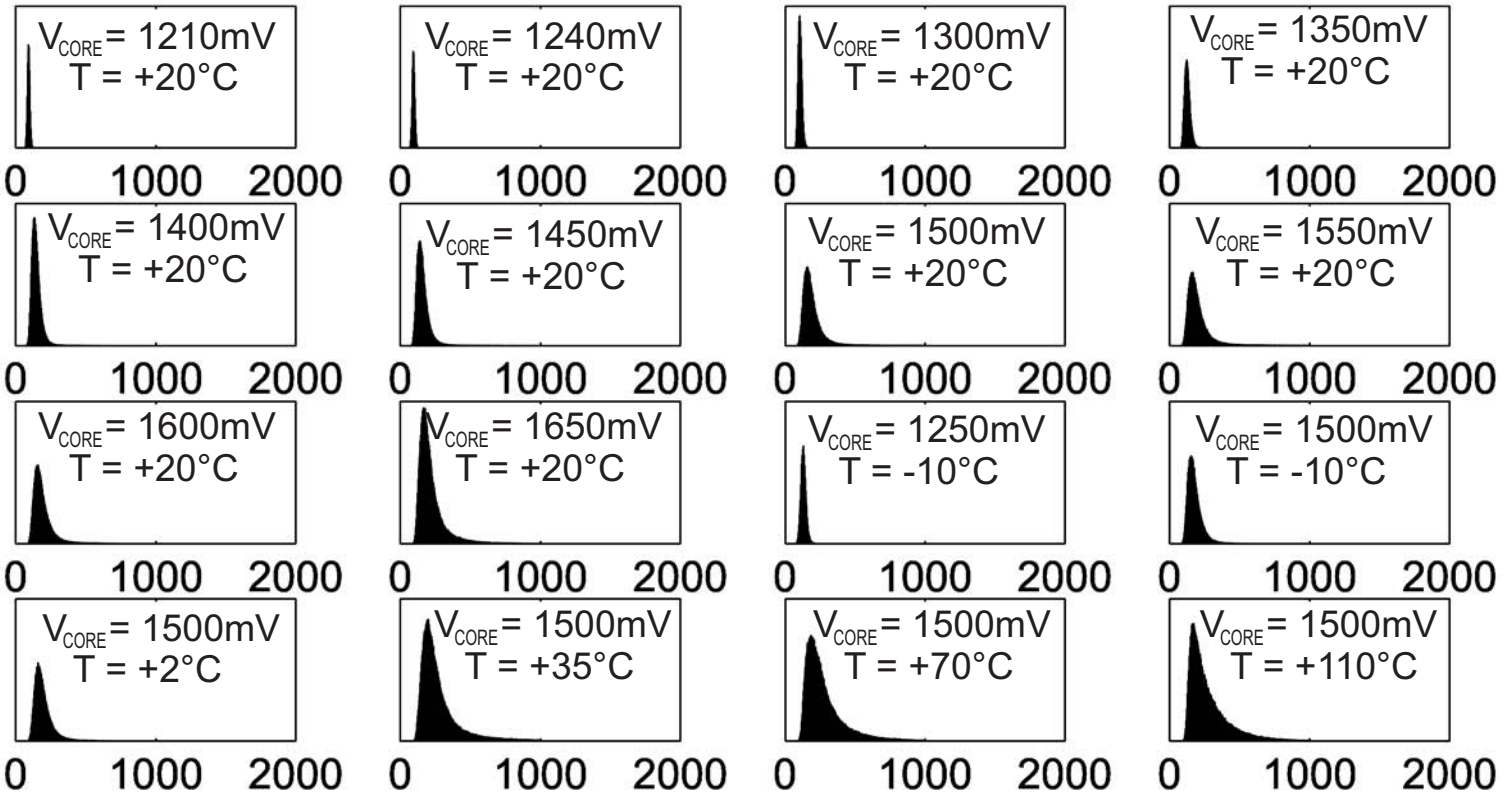


Histograms of number of TERO oscillations of all 16 TERO channels; Placement #1



Histograms of number of TERO oscillations of all 16 TERO channels; Placement #2

Experimental Results
Results of the Evaluation Platform #2 (2 of 2)



Histograms of number of TERO oscillations of a single TERO channel under variously violated working conditions

Agenda

- Introduction
- New Entropy Element Design Goals
- Transition Effect Ring Oscillator (TERO)
- Mathematical Model of TERO
- Experimental Results
- **Conclusions**

Conclusion

- New entropy element (TERO) introduced
- High sensitivity to random processes inside FPGA logic cells, while rejecting global perturbation
- Inner testability - counting of number of oscillations
- Basic mathematical model was introduced
- Two XOR-combined TERO channels can pass the NIST 800-22 statistical tests
- Speed from 100kpbs to 250 kbps per single TRNG
- Stateless entropy concept
- Performance of TEROs cluster appears to be independent from the position in FPGA and from implementation in another identical FPGA board, and from working conditions

Conclusion

- New entropy element (TERO) introduced
- High sensitivity to random processes inside FPGA logic cells, while rejecting global perturbation
- Inner testability - counting of number of oscillations
- Basic mathematical model was introduced
- Two XOR-combined TERO channels can pass the NIST 800-22 statistical tests
- Speed from 100kpbs to 250 kbps per single TRNG
- Stateless entropy concept
- Performance of TEROs cluster appears to be independent from the position in FPGA and from implementation in another identical FPGA board, and from working conditions

Conclusion

- New entropy element (TERO) introduced
- High sensitivity to random processes inside FPGA logic cells, while rejecting global perturbation
- Inner testability - counting of number of oscillations
- Basic mathematical model was introduced
- Two XOR-combined TERO channels can pass the NIST 800-22 statistical tests
- Speed from 100kpbs to 250 kbps per single TRNG
- Stateless entropy concept
- Performance of TEROs cluster appears to be independent from the position in FPGA and from implementation in another identical FPGA board, and from working conditions

Conclusion

- New entropy element (TERO) introduced
- High sensitivity to random processes inside FPGA logic cells, while rejecting global perturbation
- Inner testability - counting of number of oscillations
- Basic mathematical model was introduced
- Two XOR-combined TERO channels can pass the NIST 800-22 statistical tests
- Speed from 100kpbs to 250 kbps per single TRNG
- Stateless entropy concept
- Performance of TEROs cluster appears to be independent from the position in FPGA and from implementation in another identical FPGA board, and from working conditions

Conclusion

- New entropy element (TERO) introduced
- High sensitivity to random processes inside FPGA logic cells, while rejecting global perturbation
- Inner testability - counting of number of oscillations
- Basic mathematical model was introduced
- Two XOR-combined TERO channels can pass the NIST 800-22 statistical tests
- Speed from 100kpbs to 250 kbps per single TRNG
- Stateless entropy concept
- Performance of TEROs cluster appears to be independent from the position in FPGA and from implementation in another identical FPGA board, and from working conditions

Conclusion

- New entropy element (TERO) introduced
- High sensitivity to random processes inside FPGA logic cells, while rejecting global perturbation
- Inner testability - counting of number of oscillations
- Basic mathematical model was introduced
- Two XOR-combined TERO channels can pass the NIST 800-22 statistical tests
- Speed from 100kpbs to 250 kbps per single TRNG
- Stateless entropy concept
- Performance of TEROs cluster appears to be independent from the position in FPGA and from implementation in another identical FPGA board, and from working conditions

Conclusion

- New entropy element (TERO) introduced
- High sensitivity to random processes inside FPGA logic cells, while rejecting global perturbation
- Inner testability - counting of number of oscillations
- Basic mathematical model was introduced
- Two XOR-combined TERO channels can pass the NIST 800-22 statistical tests
- Speed from 100kpbs to 250 kbps per single TRNG
- Stateless entropy concept
- Performance of TEROs cluster appears to be independent from the position in FPGA and from implementation in another identical FPGA board, and from working conditions

Conclusion

- New entropy element (TERO) introduced
- High sensitivity to random processes inside FPGA logic cells, while rejecting global perturbation
- Inner testability - counting of number of oscillations
- Basic mathematical model was introduced
- Two XOR-combined TERO channels can pass the NIST 800-22 statistical tests
- Speed from 100kpbs to 250 kbps per single TRNG
- Stateless entropy concept
- Performance of TEROs cluster appears to be independent from the position in FPGA and from implementation in another identical FPGA board, and from working conditions

Acknowledgment

"We would like to thank

Actel University Program

for a donation of 10 Actel Fusion

FPGA evaluation boards,

which enabled us to

confirm the TERO principle using

number of identical FPGA boards."

Thank You
for the Attention