Multiple output bits ROPUF design for TRNG

Filip Kodýtek, Róbert Lórencz, Jiří Buček and Simona Buchovecká

Czech Technical University in Prague

Faculty of Information Technology

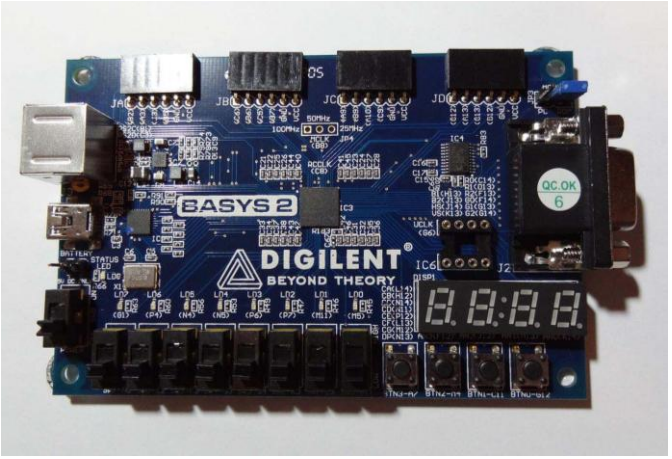
CryptArchi, Montpellier, 2016

Outline

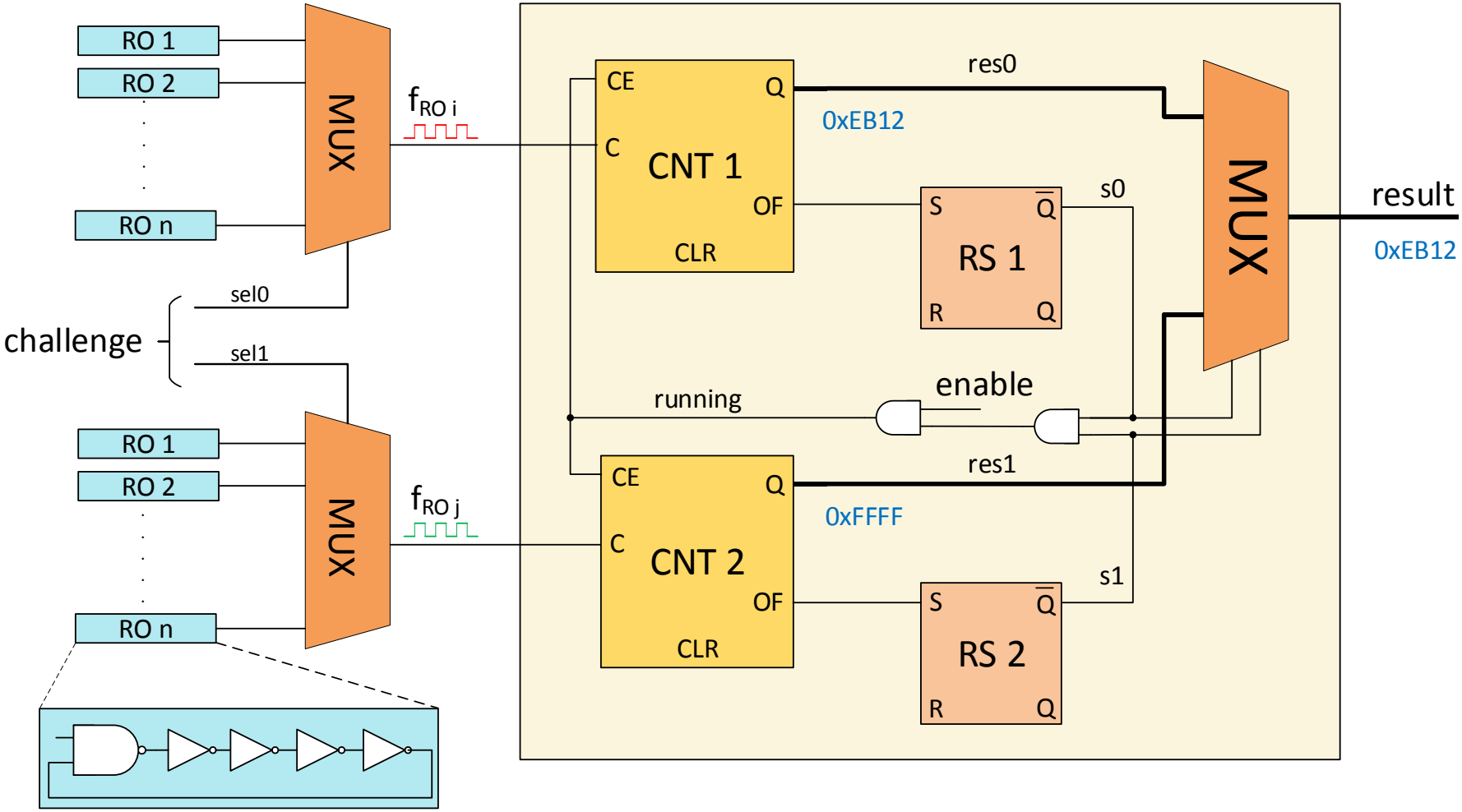
- Recapitulation of the ROPUF
  - Statistical properties for PUF
  - Influence of supply voltage variations
- Temperature influence measurement
- Approaches to RO frequency processing using counters
- ROPUF Circuit as True Random Number Generator
- Statistical testing of generated TRNGs
- Output generation process proposition
- Conclusion

PUF and TRNG

- Ring oscillator based design
  - The PUF or TRNG output is generated from RO pairs
  - Multiple output bits from each pair of ROs
    - obtained from counter values
    - Different positions selected for PUF and TRNG
  - Same design can be used for device identification and random number generation
    - Potential for key generation
- Experimental platform
  - Digilent Basys2
    (with Spartan3E-100 CP132)

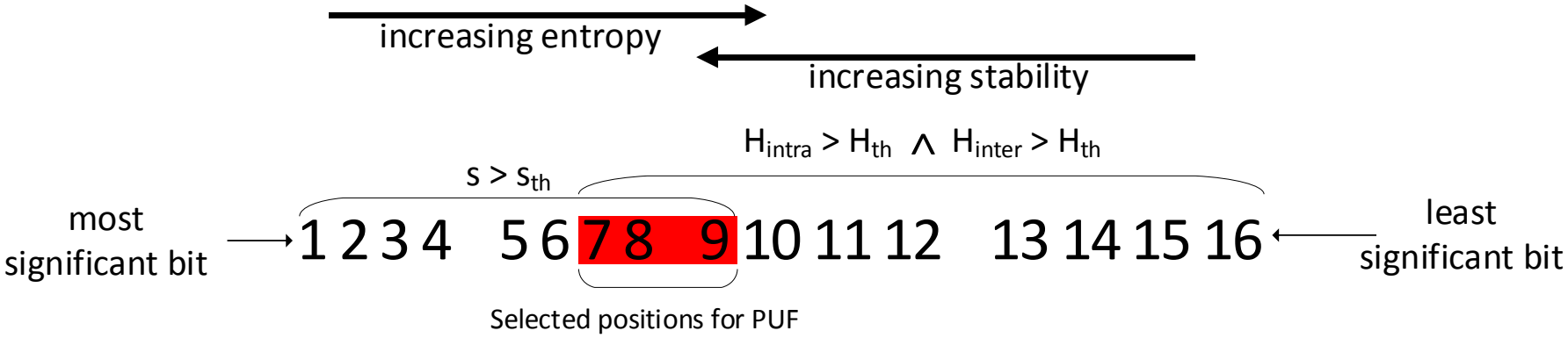


The circuit used for measurements



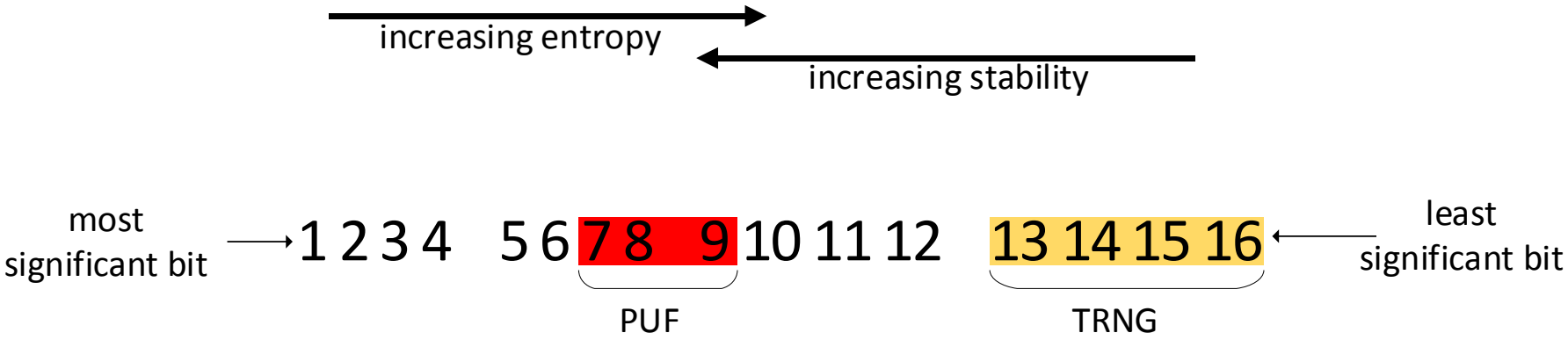
Processing the counter values

- Counter values represented in binary code
- Appropriately selected part of these values can be used directly for PUF – based on their entropy and stability
- For PUF, we need to select positions, where both the entropy and stability are high
- s_{th} and H_{th} – threshold values of required stability and entropy



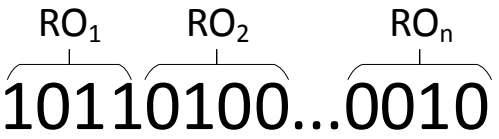
Processing the counter values

- Counter values represented in binary code
- Appropriately selected part of these values can be used directly for PUF or TRNG – based on their entropy and stability
- For PUF, we need to select positions, where both the entropy and stability are high
- s_{th} and H_{th} – threshold values of required stability and entropy
- For TRNG, we need positions with high entropy



Statistical evaluation of the PUF outputs

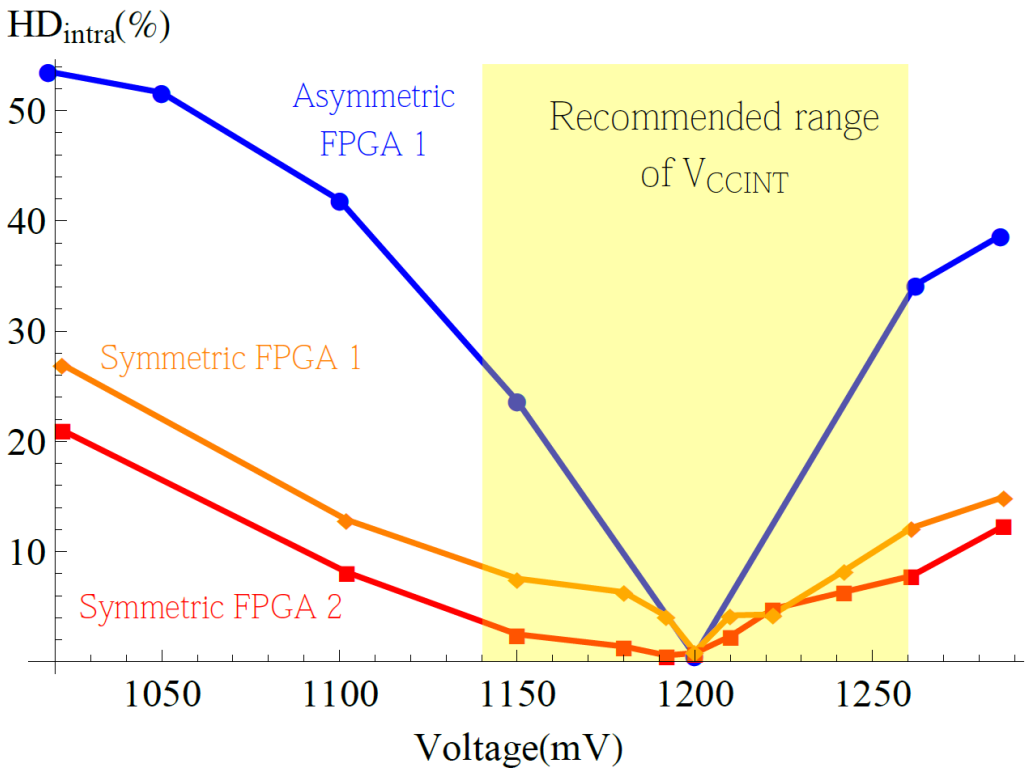
- Results for 450 pairs of ROs
- We can select more bits with almost the same error rate
- Gray code applied to selected positions



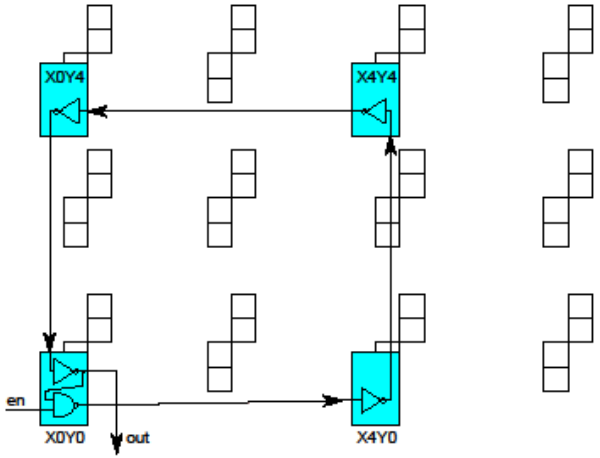
Positions	7-8	7-9	7-10	8-9
w	2	3	4	2
BER	0.80%	1.08%	1.65%	1.62%
HD_{intra}	1.19%	1.60%	2.45%	2.40%
HD_{intra} interval	<0%, 2.78%>	<0.52%, 3.70%>	<0.78%, 5.33%>	<0.78%, 5.56%>
HD_{inter}	47.44%	48.3%	48.74%	49.97%
HD_{inter} interval	<35.89%, 60.33%>	<39.48%, 57.11%>	<41.61%, 56.39%>	<45.67%, 56.11%>

Placement of ROs vs voltage variation

- Comparison of HD_{intra} vs supply voltage for positions 7-8
  - asymmetric ROs (150 pairs)
  - symmetric ROs (50 pairs)

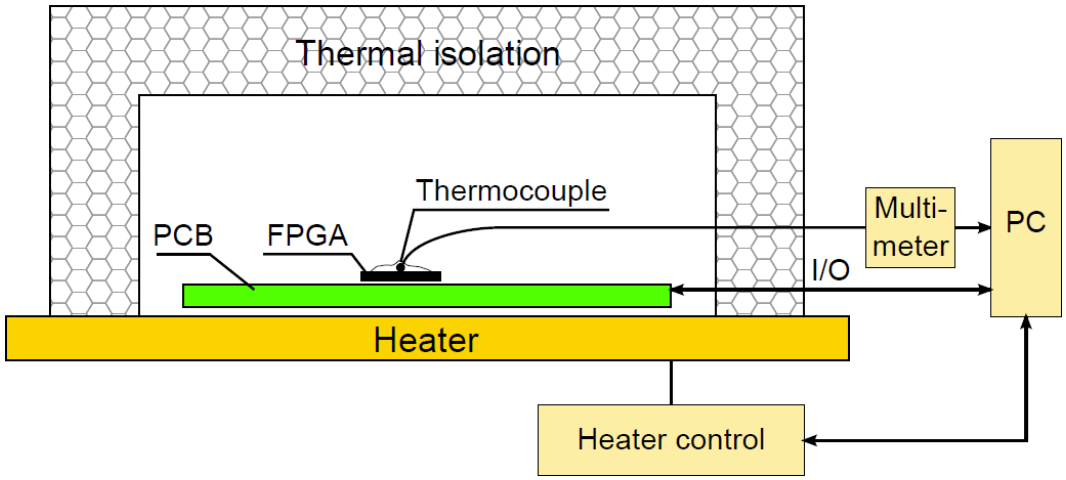


Symmetric RO placement



Temperature influence measurement

- FPGA board was placed on a heated platform with thermal isolation
- Measured for cca 33 to 70 °C
- Before each measurement, temperature was allowed to stabilize, temperature was increased in steps of cca 10 °C



Influence of temperature – results

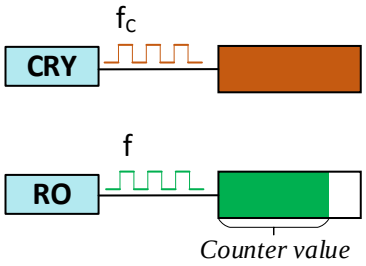
- Asymmetric vs symmetric ROs, 3 FPGAs
- HD_{intra} for 150 asymmetric / 50 symmetric RO pairs
- Selected positions 7 – 8 at different temperatures

Asymmetric ROs					
FPGA 1		FPGA 2		FPGA 3	
Temperature [°C]	HD_{intra} [%]	Temperature [°C]	HD_{intra} [%]	Temperature [°C]	HD_{intra} [%]
36.7 → 41.2	2.67	38.4 → 42.3	2.67	37.7 → 41.8	1.0
36.7 → 51.8	7.67	38.4 → 50.1	6.67	37.7 → 50.9	5.0
36.7 → 60.4	9.33	38.4 → 60.3	9.33	37.7 → 61.3	7.0
36.7 → 71.1	11.33	38.4 → 69.9	12.67	37.7 → 70.1	12.0
Symmetric ROs					
FPGA 1		FPGA 2		FPGA 3	
Temperature [°C]	HD_{intra} [%]	Temperature [°C]	HD_{intra} [%]	Temperature [°C]	HD_{intra} [%]
33.0 → 42.4	2.67	34.4 → 40.9	1.67	34.5 → 41.1	3.67
33.0 → 50.5	3.67	34.4 → 50.5	3.0	34.5 → 51.4	6.0
33.0 → 60.6	3.67	34.4 → 60.8	4.67	34.5 → 60.6	7.0
33.0 → 71.0	4.67	34.4 → 70.2	5.33	34.5 → 70.4	7.33

- Symmetric are better (1.67 to 7.33 % of HD_{intra})

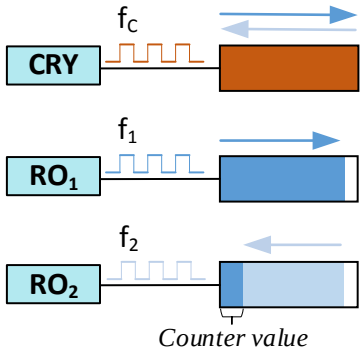
Approaches to RO frequency processing using counters

Crystal reference



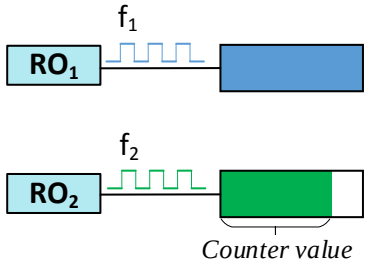
$$Counter\ value = \frac{\varphi(f)}{f_C} \times 2^{16}$$

Frequency difference



$$Counter\ value = \varphi(f_1 - f_2) \times \frac{1}{f_C} \times 2^{16}$$

Frequency ratio



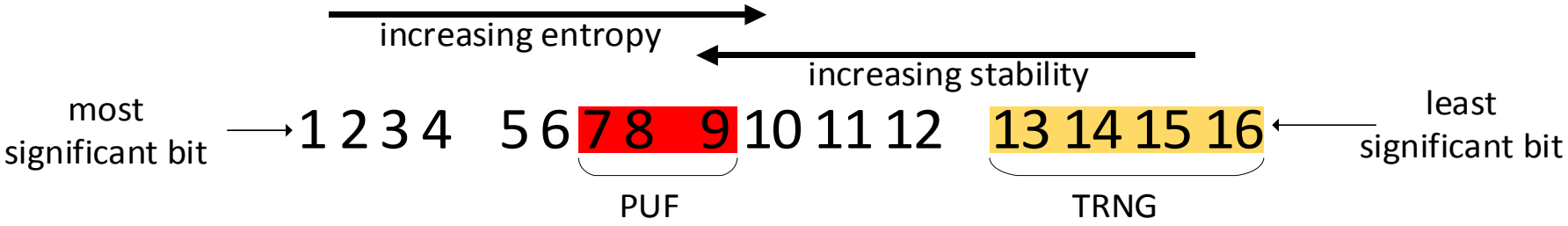
$$Counter\ value = \varphi\left(\frac{f_2}{f_1}\right) \times 2^{16}$$

	Temperature			Supply voltage
	FPGA 1	FPGA 2	FPGA 3	FPGA 1
	$\frac{\Delta\varphi}{\varphi_{max}}$ [%]	$\frac{\Delta\varphi}{\varphi_{max}}$ [%]	$\frac{\Delta\varphi}{\varphi_{max}}$ [%]	$\frac{\Delta\varphi}{\varphi_{max}}$ [%]
crystal	3.42	3.01	2.97	22.18
subtraction	4.08	4.29	3.78	33.21
ratio	0.27	0.16	0.14	2.41

Frequency ratio partially eliminates temperature and voltage variations

ROPUF Circuit as True Random Number Generator

- So far, we selected suitable positions for PUF
- Are there any positions suitable for TRNG?
- How to select RO pairs for TRNG?
- How to combine them into TRNG output?
- Postprocessing needed?



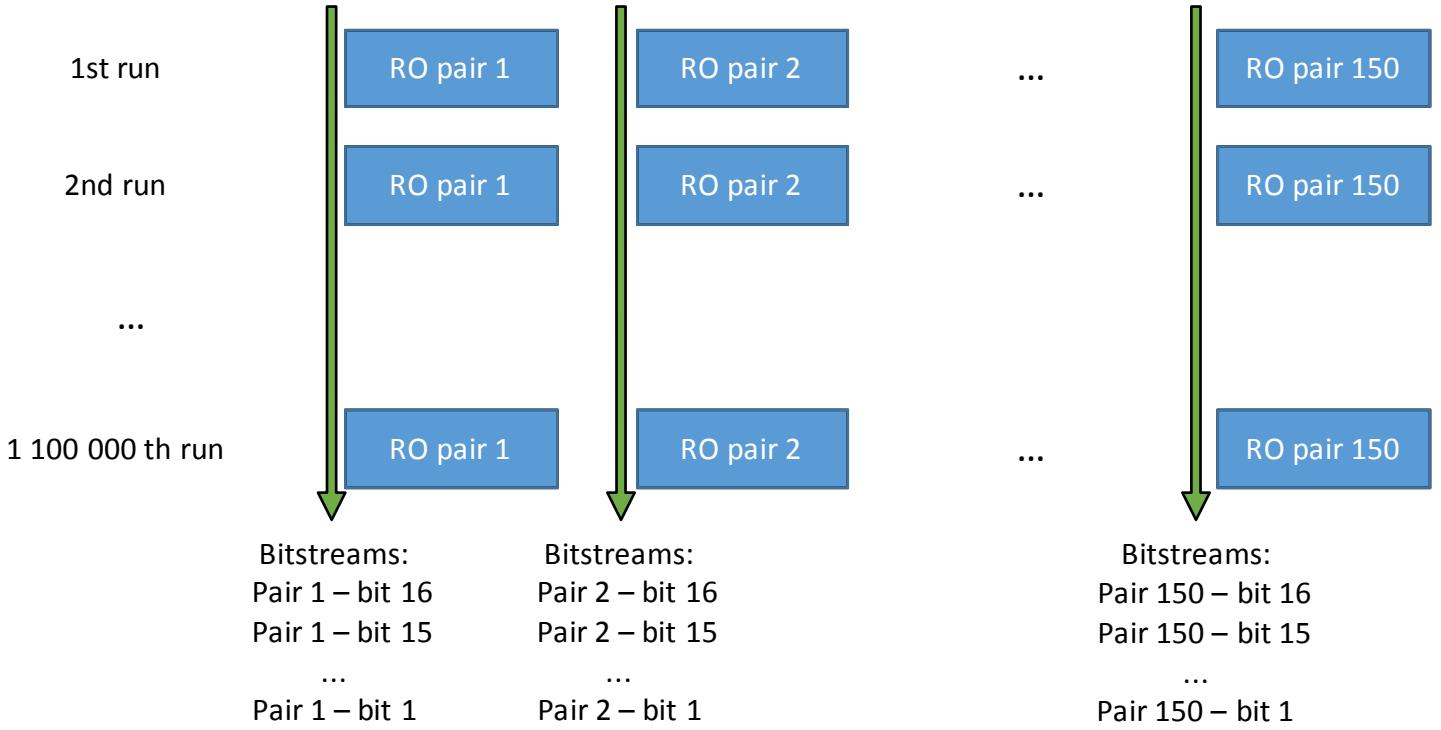
Statistical testing of generated TRNGs

- 150 RO pairs x 1 100 000 runs tested

- Performed tests:
  - Individual RO pairs output
  - Concatenated RO pairs output
  - Post processed bit stream
    - Von Neumann
    - XOR

Individual RO pairs tests

- Single bits from every RO pair examined
- We consider every RO pair as unique source entropy
- 150 x 16 bit streams tested



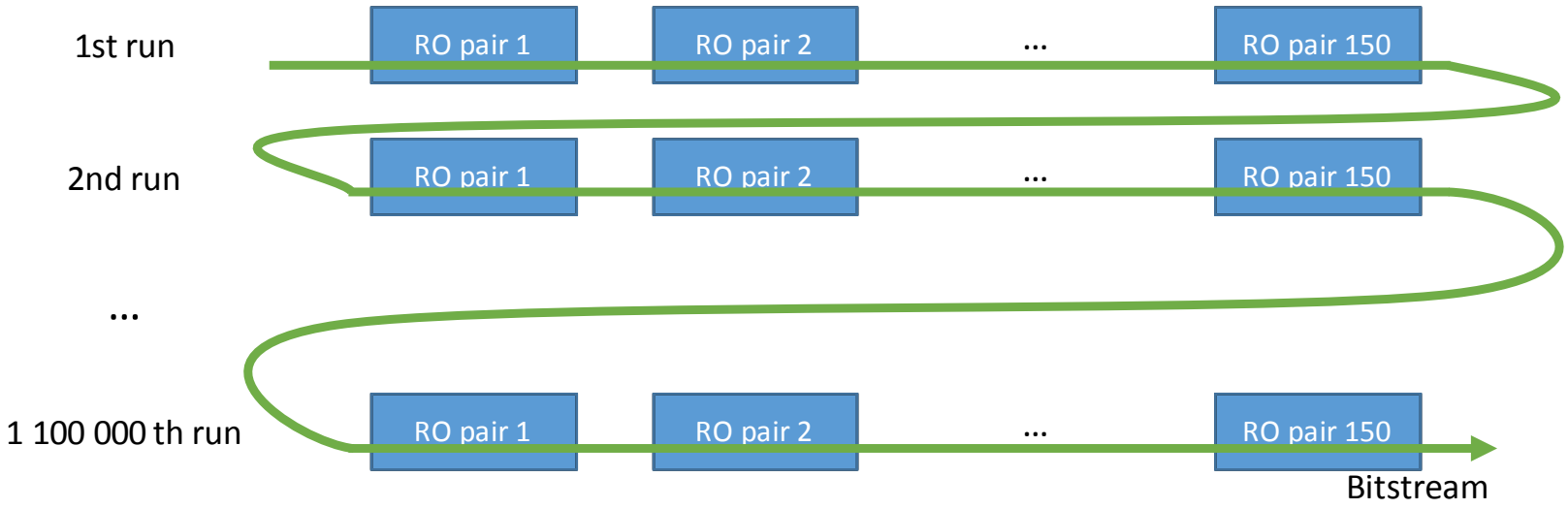
Individual RO pairs tests - results

- Some RO pairs generated only few unique values; therefore we excluded them from further testing – the cause is examined
- Table summarizes the resulting values of the NIST tests (median values from 142 pairs tests are shown in the table)

TEST	Bit 16	Bit 15	Bit 14	Bit 13
Frequency	97/100	99/100	99/100	98/100
BlockFreq.	99/100	99/100	99/100	97/100
CumSum I	97/100	99/100	99/100	98/100
CumSum II	97/100	99/100	99/100	98/100
Runs	99/100	99/100	99/100	97/100
LongestRun	99/100	99/100	99/100	98/100
ApproxEntropy	99/100	99/100	99/100	98/100

Concatenated RO pairs outputs tests

- Initial tests shown that each RO pair can be used as a source of an entropy
- Single bits 16–13 shown satisfactory characteristics – we concatenated them into single stream to get higher rate of generated bits



Concatenated RO pairs outputs tests – results

- Table summarizes the resulting values of the NIST tests for concatenated bit stream consisting from bits 16 to 13 from 142 RO pairs
- If the test failed for the distribution of p-values (yellow cells)

TEST	Bit 16	Bit 15	Bit 14	Bit 13
Frequency	0/100	24/100	82/100	69/100
BlockFreq.	99/100	98/100	99/100	98/100
CumSum I	0/100	31/100	83/100	69/100
CumSum II	0/100	25/100	87/100	70/100
Runs	0/100	83/100	95/100	94/100
LongestRun	99/100	99/100	98/100	100/100
Rank	100/100	99/100	99/100	98/100
FFT	97/100	96/100	99/100	100 /100
NonOverlapping template	85-100 /100	96 -100 /100	96 -100 /100	96 -100 /100
Overlapping template	96/100	97/100	97/100	99/100
Universal	97/100	98/100	97/100	98/100
ApproxEntropy	89/100	100 /100	98/100	100 /100
Random Excursions	4/4	18/18	51-52 /52	34-35 /35
Random ExcursionVariants	4/4	17-18 /18	51-52 /52	34-35 /35
Serial I	99/100	99/100	99/100	99/100
Serial II	99/100	100 /100	97/100	100 /100
Linear Complexity	100 /100	99/100	98/100	99/100

Post processing generated bit stream

- Tested bit stream performed well in most of the tests, but uniform distribution of 0’s and 1’s is not satisfactory
- This may happen, when dealing with physical TRNG
- Further post processing to enhance the properties of generated bit stream
  - Von Neumann corrector
  - XOR corrector

Von Neumann corrector

TEST/Results	Bit 16	Bit 15	Bit 14	Bit 13
Frequency	99/100	100/100	99/100	100/100
BlockFreq.	99/100	100/100	98/100	100/100
CumSum I	100/100	100/100	99/100	100/100
CumSum II	98/100	100/100	99/100	100/100
Runs	97/100	99/100	99/100	98/100
LongestRun	99/100	100/100	98/100	100/100
ApproxEntropy	100/100	98/100	100/100	99/100

- Results are satisfying, but the bit stream is shortened by approx. 75 %

XOR corrector

TEST/Results	Bit 16	Bit 15	Bit 14	Bit 13
Frequency	99/100	100/100	99/100	100/100
BlockFreq.	100/100	100/100	100/100	99/100
CumSum I	100/100	99/100	99/100	100/100
CumSum II	100/100	100/100	100/100	99/100
Runs	98/100	99/100	99/100	99/100
LongestRun	97/100	100/100	99/100	98/100
ApproxEntropy	99/100	99/100	100/100	98/100

- Results are satisfying, and the bit stream is shortened by approx. 50 % only

Concatenated bits

- Multiple bits concatenated
  - Bits 15 – 13 from each RO pair
  - 142 RO pairs
  - 1 100 000 runs
- XOR corrector
- 3x more bits than individual
- Passes NIST suite tests
- For each run,
  142x3/2 bits of TRNG

TEST	Results	
	Bits 16-13	Bits 15-13
Frequency	82/100	98/100
BlockFreq.	99/100	100/100
CumSum I	85/100	99/100
CumSum II	83/100	97/100
Runs	96/100	100/100
LongestRun	99/100	99/100
Rank	99/100	99/100
FFT	100/100	98/100
NonOverlapping template	98-100/100	97-100/100
Overlapping template	99/100	100/100
Universal	99/100	100/100
ApproxEntropy	98/100	100/100
Random Excursions	43-44/100	55/55
Random ExcursionVariants	43-44/100	55/55
Serial I	100/100	100/100
Serial II	98/100	98/100
Linear Complexity	98/100	97/100

Conclusion

- Influence of voltage and temperature
  - Better statistical properties when using symmetric ROs
- Comparison of different approaches for frequency processing using counter values
  - Frequency ratio provides better results
- ROPUF circuit can be used for TRNG generation – up to 142x3/2 random bits can be gained in one run (XOR corrector is needed)
- Future work: Issues of aging & tamper resistance (both for PUF & TRNG), TRNG testing and health monitoring

Thank you for your attention