A Novel Security Technique to Generate Truly Random and Highly Reliable Reconfigurable ROPUF-based Cryptographic Keys

Electrical Engineering and Computer Science (EECS) Department

The University of Toledo

By

Fathi Amsaad

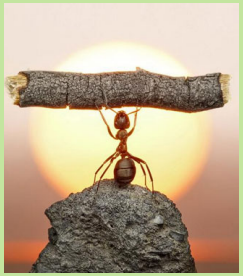
Research Advisor
Dr. Mohamed Niamat

Co-Authors
Atul Prasad Deb Nath, and Chayanika Roy Chaudhuri

Presentation Outline

- [x] Motivation
- [x] Background
- [x] Problem Statement
- [x] Proposed Solution
- [x] Implementation
- [x] Experimental Results
- [x] NIST Randomness Test
- [x] Conclusion

Motivation



CH-46 Helicopter

C-17 Sea

P-8A Transport

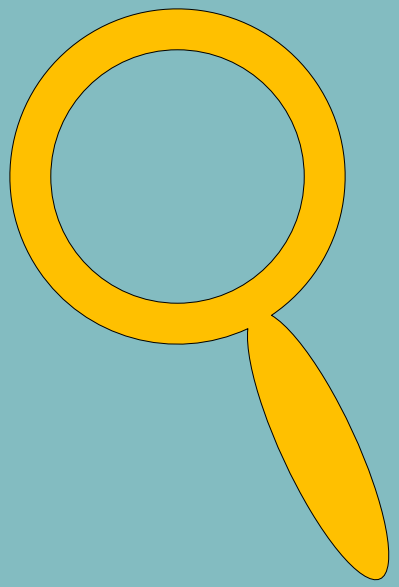
F-16 Fighter

- Supply chain counterfeited components
- Threatening both military and commercial systems
  - Vendors sell old military chips as new
  - About $1.4 billion is lost on repairable weapon*
  - With 10 % increase every year*
  - More than $250 billion is lost in revenue**
  - Around 750,000 jobs are lost a year**

*The Aerospace Industrial Association (AIA), USA : One DoD official in John Reed's article

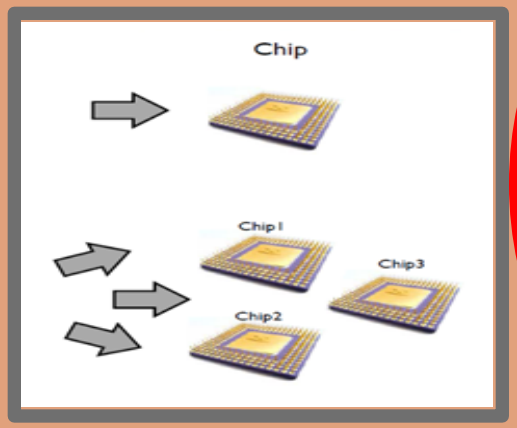
**Anti-Counterfeiting Bureau (ACB), USA :International Anti-Counterfeiting Bureau, "Intellectual Property Theft", 2011

Motivation Cont'd- Scope

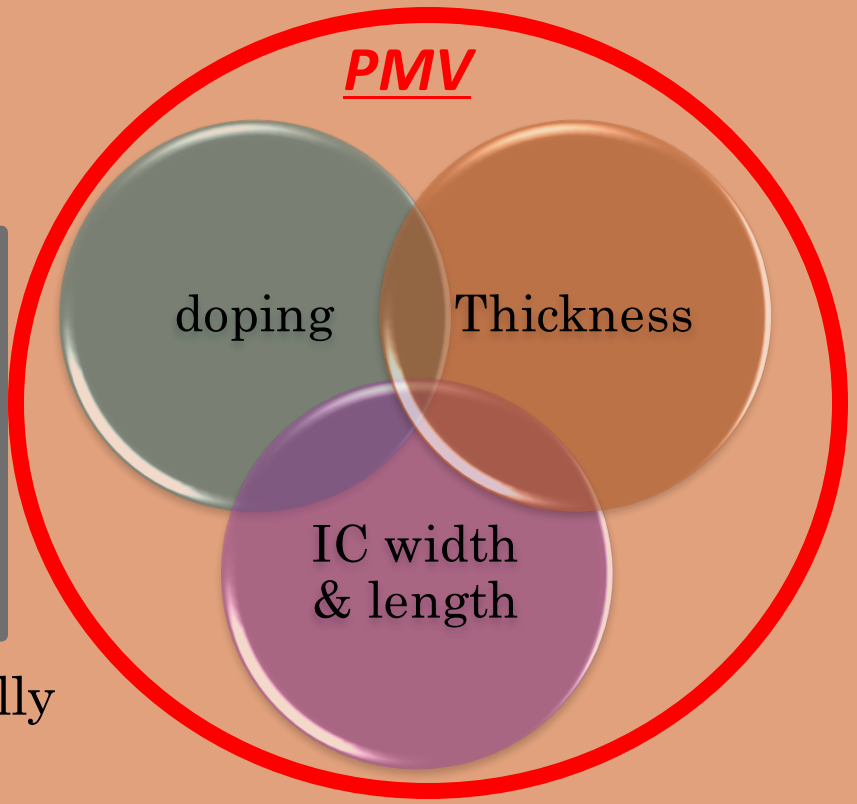


- The scope of this investigation covers a spectrum of random manufacturing process variations (MPV) that is inherently unclonable
- Optimizing MPV of Integrated Circuits or ICs, PUF can generate truly random cryptographic keys

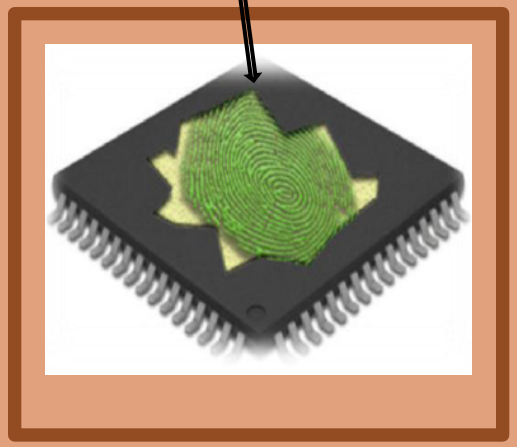
Background



Identical functionally

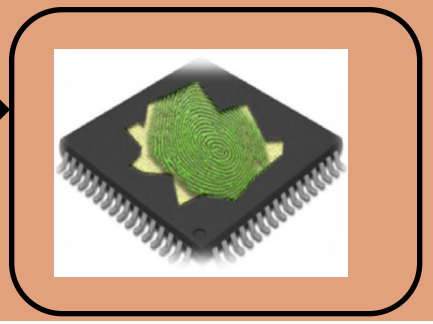


PUF Circuit



Silicon Chip

n-bit challenge



PMV delay

k-bit response

$$\gamma : \{0,1\}^n \longrightarrow \{0,1\}^k$$

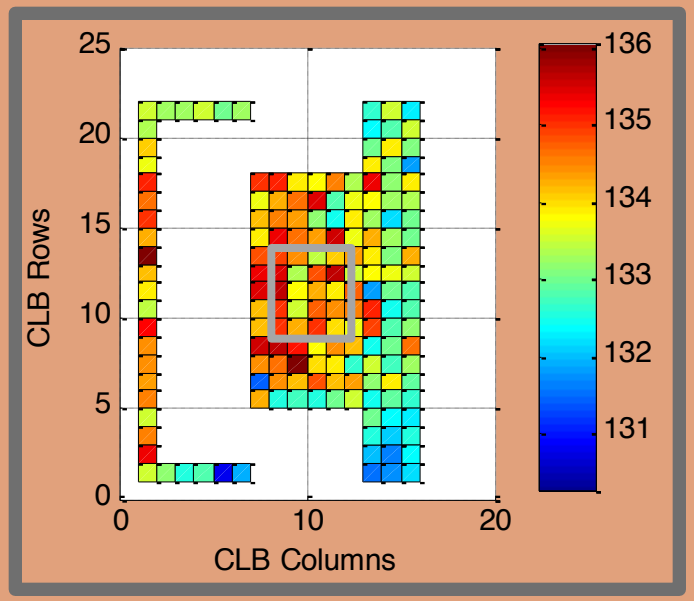
Background - Process Manufacturing Variations (PMV)

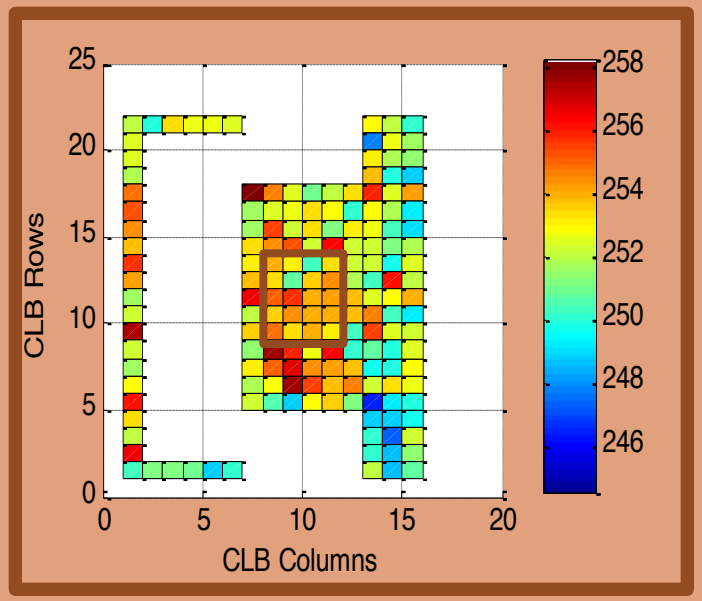
- An extremely small delay (invisible)
- Caused by differences in fabrication
- Inherited on a silicon chip
- Magnified using PUF circuitry
- Unique chip IDs are extracted
- Stochastic (random) & systematic

Problem Statement

- Systematic Process Variations are not statistically random by nature
- Negatively impacts PUF performance in terms of uniqueness, reliability, and randomness
- Leads to major hardware security threats

Problem Statement - Cont'd



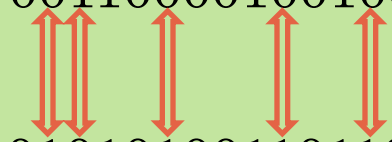


FPGA Seven Stages Layout

FPGA three Stages Layout

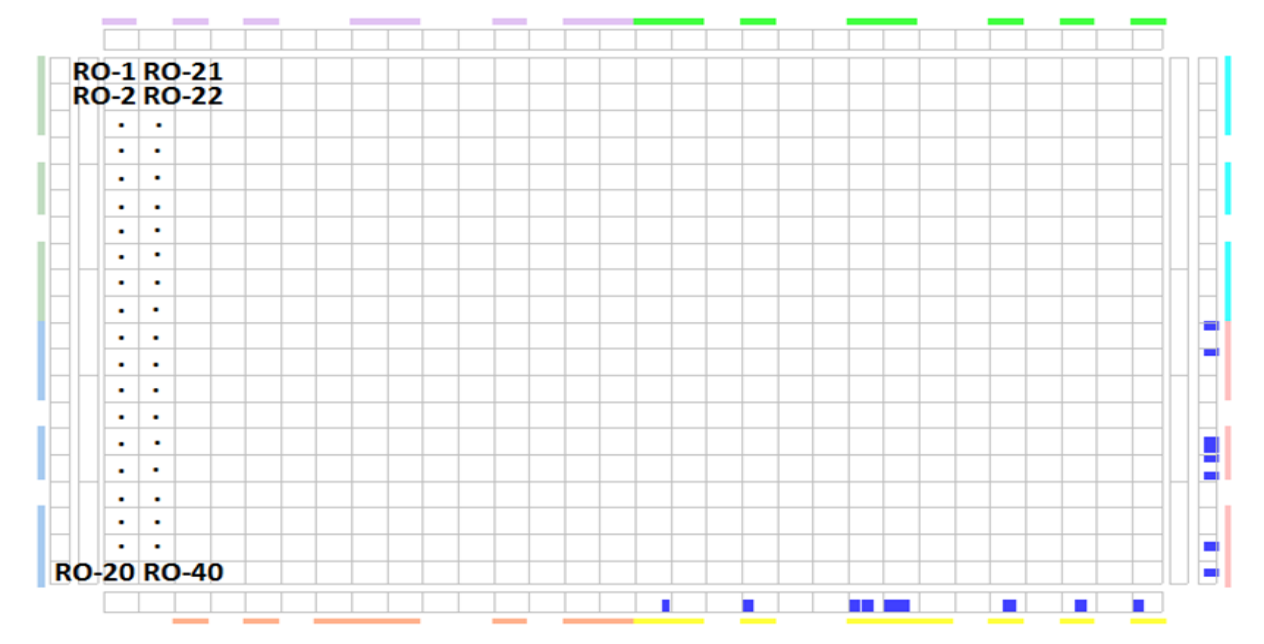
Problem Statement - Cont'd

- RO-1 to RO-20 the response A is
- 00110000100100100101

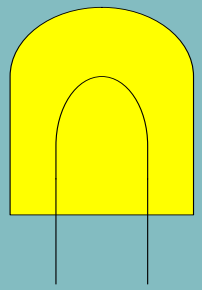


01010100110110100101

- RO-21 to RO-40 the response B is as above
- Hamming Distance = 5, Hamming Distance percentage = 25%



Proposed Solution



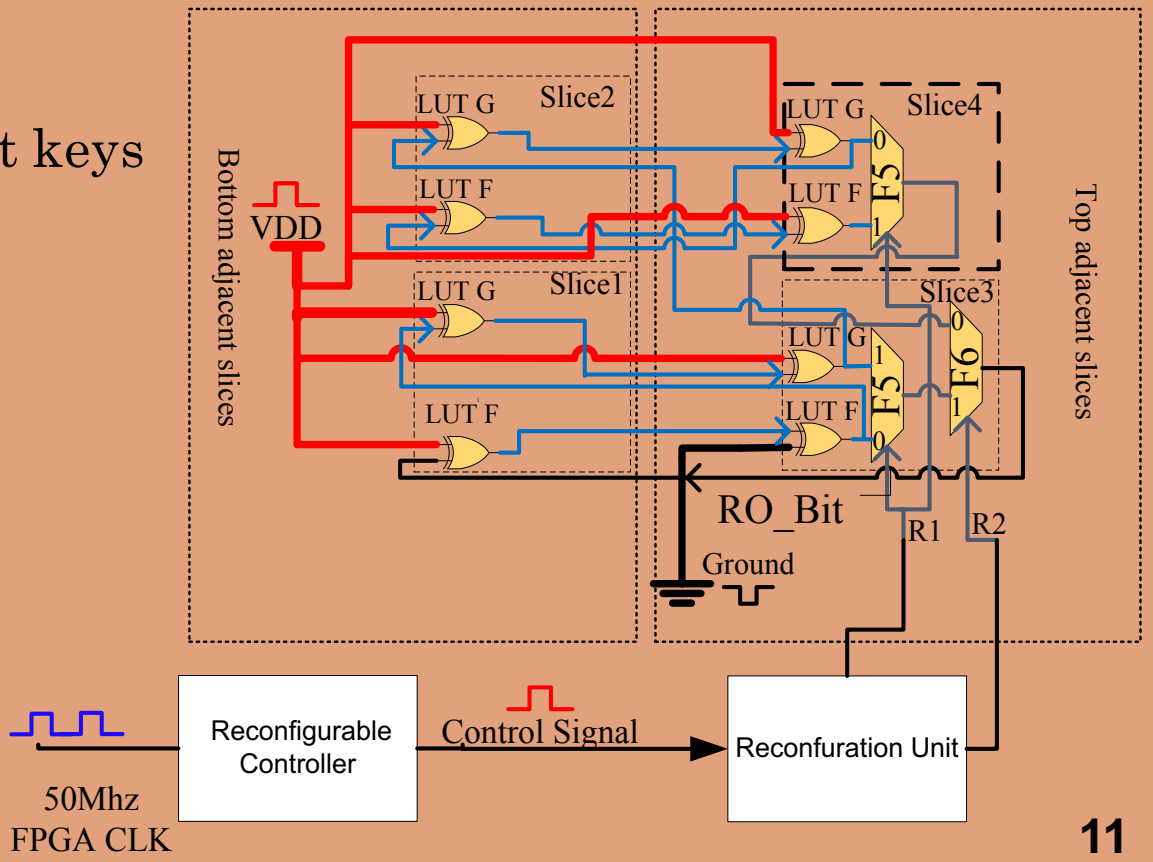
- A novel Reconfigurable Ring Oscillator (RO) PUF design for updated secret key extractions
- A security technique to nullify the effects of spatial systematic variations on PUF outputs

- Central Limit Theorem (CLT) states that data samples should be approximately normally distributed to verify true randomness

- Transformation of RO frequencies to statistically normal frequencies using log-normal and square root

Proposed Reconfigurable RO PUF

- Area efficient design comprises four different RO structures in one CLB
- Exploit identical nature of internal CLB routings
- Improved CRP Space
- Enables for updated secret keys



Design Implementation

- The design is implemented on the entire area of 30 Spartan 3E FPGA chips

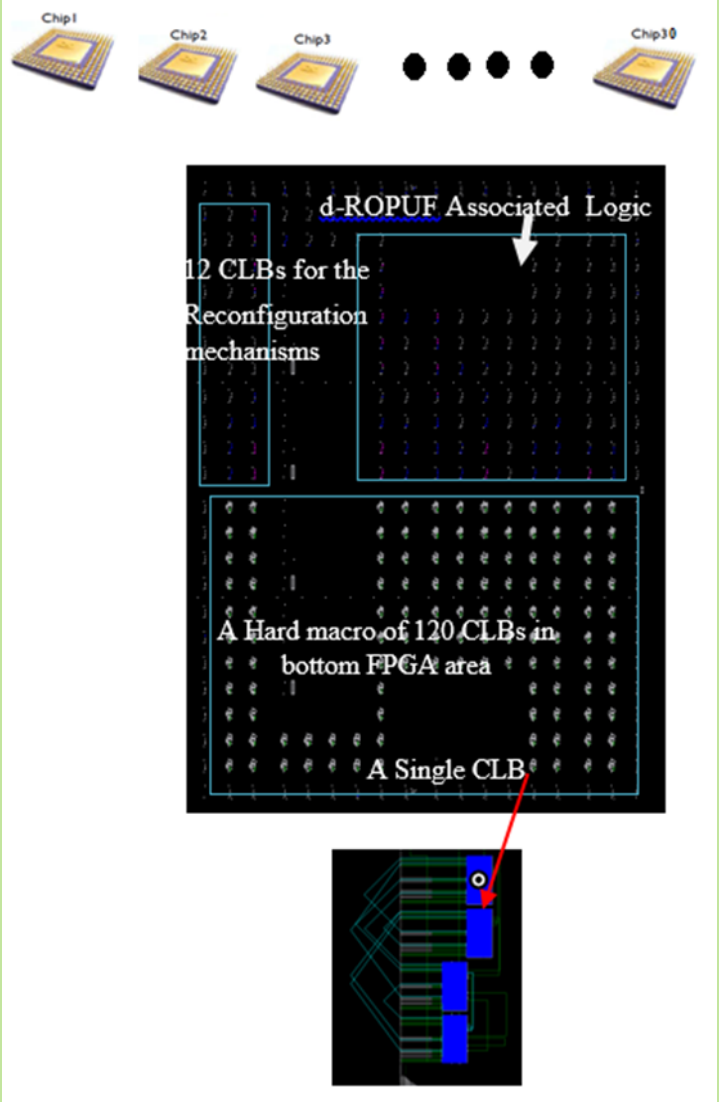
☛ FPGAs are divided into two areas (top and bottom) with 120 CLBs

☛ The RO PUF structures are mapped on 120 CLBs per area

☛ Each area will have 120 ROs (one RO per CLB)

☛ Total 240 ROs per chip (top and bottom FPGA areas)

☛ Data samples are measured for each FPGA offline with the help of Agilent logic analyzer



Existing Techniques

Polynomial regression based distiller technique

- Response bits produced by Chain-like Neighbor Coding failed to pass NIST test
- Order 2 polynomial regression or higher is required resulting in a computational overhead when applied to real hardware

Pseudorandom number (PRN) generator technique

- Response bits produced by Chain-like Neighbor Coding failed to pass the entire NIST test
- Response bits are generated based on pseudorandom numbers

Proposed Solution : Logarithmic and Absolute Diverseness Technique (LDT)

The concept here is a simple transmission technique (LDT) to transform RO frequencies to statistically normal frequencies by normalizing the extracted frequencies using log-normal and square root

Square root of the deviation of each average RO frequencies from average ROPUF structure is calculated

$$deviation_i = \sqrt{ABS(Avg\_RO_i - Avg\_ROPUF\_Structure)}$$

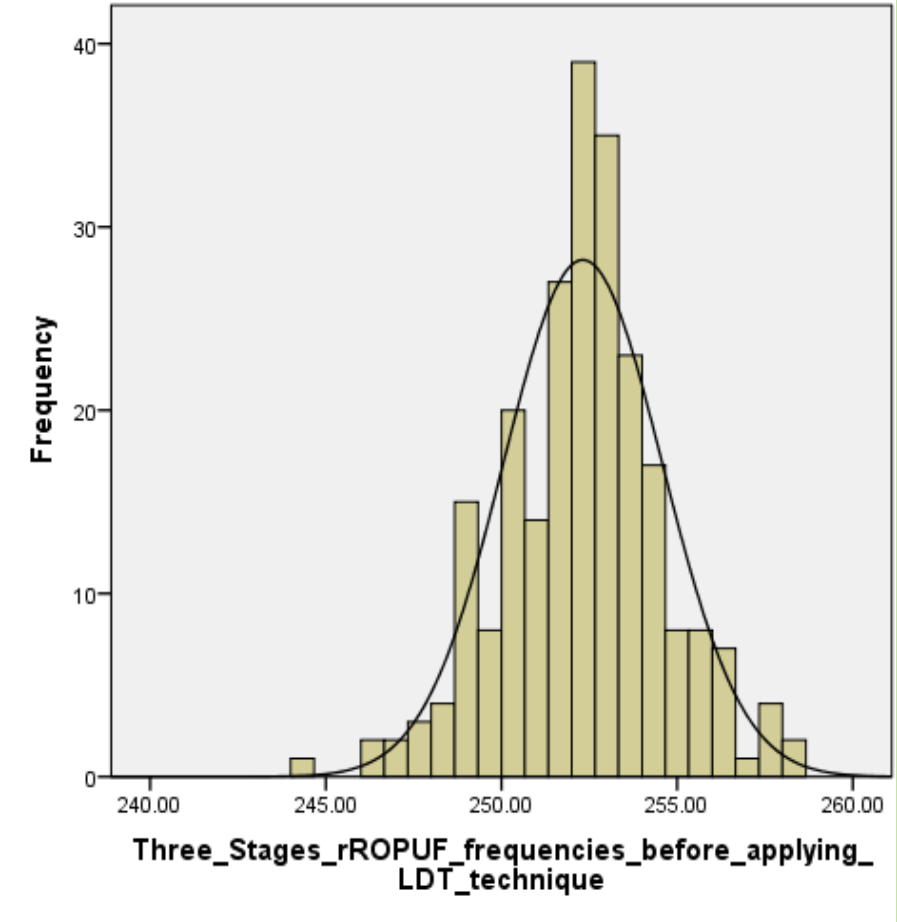
Base-10 logarithm for each of average ring oscillator frequencies is then computed

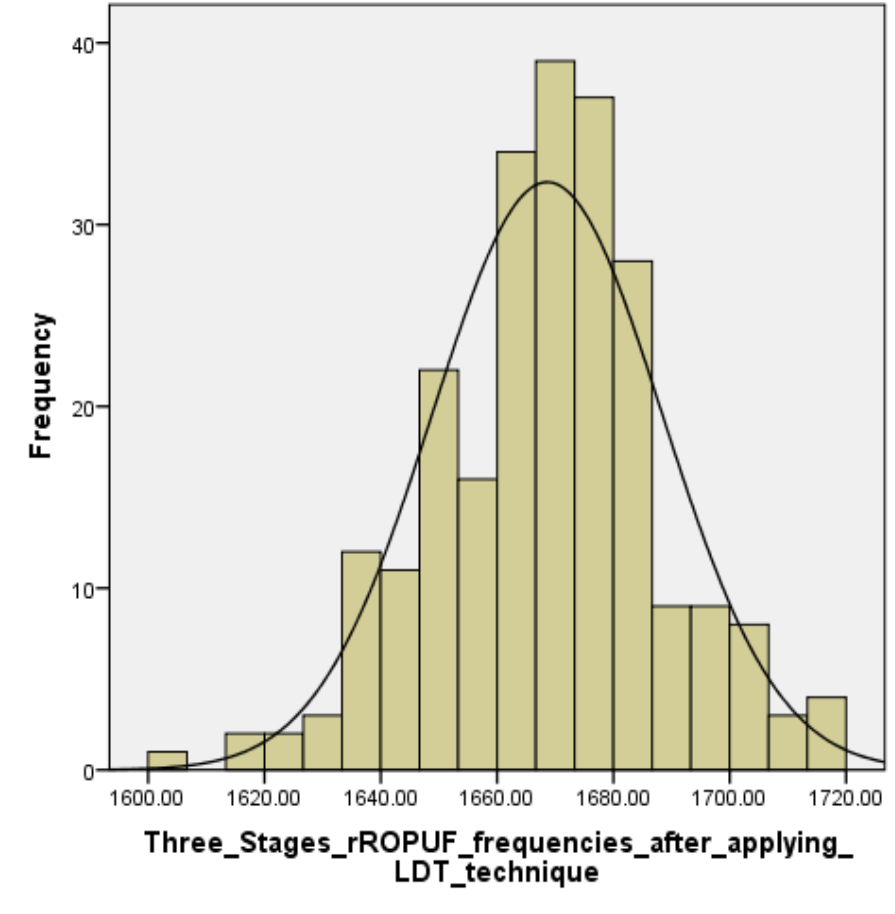
$$LG_i = LOG_{10}(ABS(Avg\_RO_i - Max(Avg\_RO_i + 1)))$$

Average RO frequencies are normalized as follows

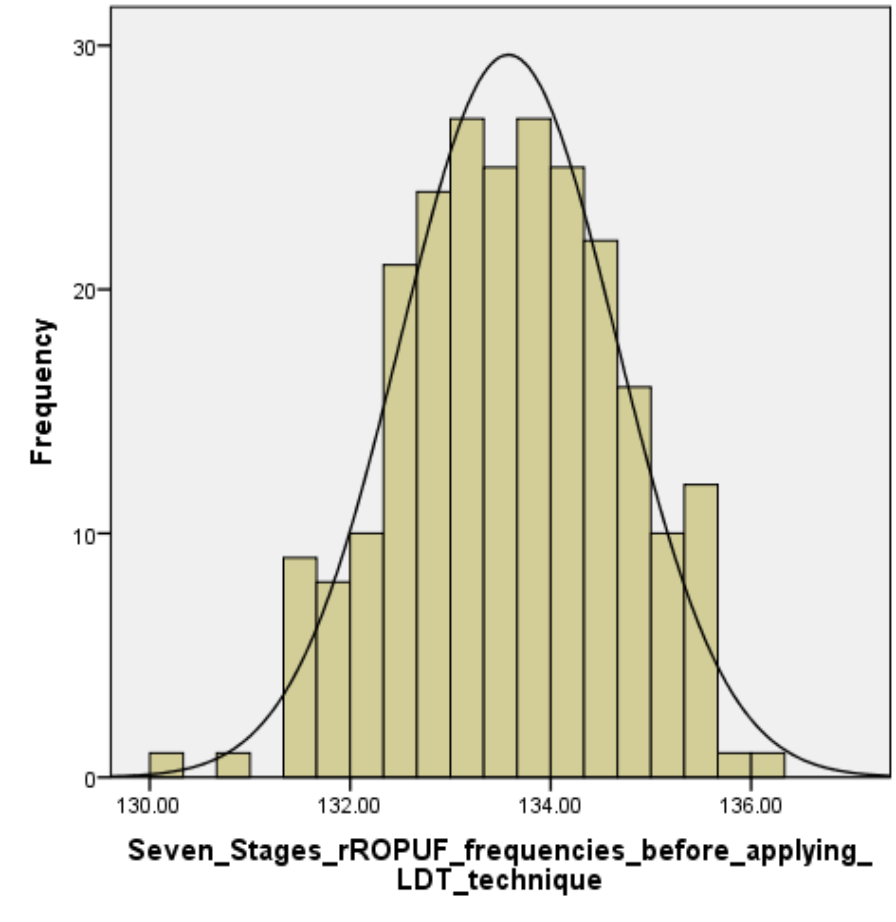
$$Normalized\_Avg\_RO_i = Avg\_RO_i \times \frac{deviation_i}{LG_i}$$

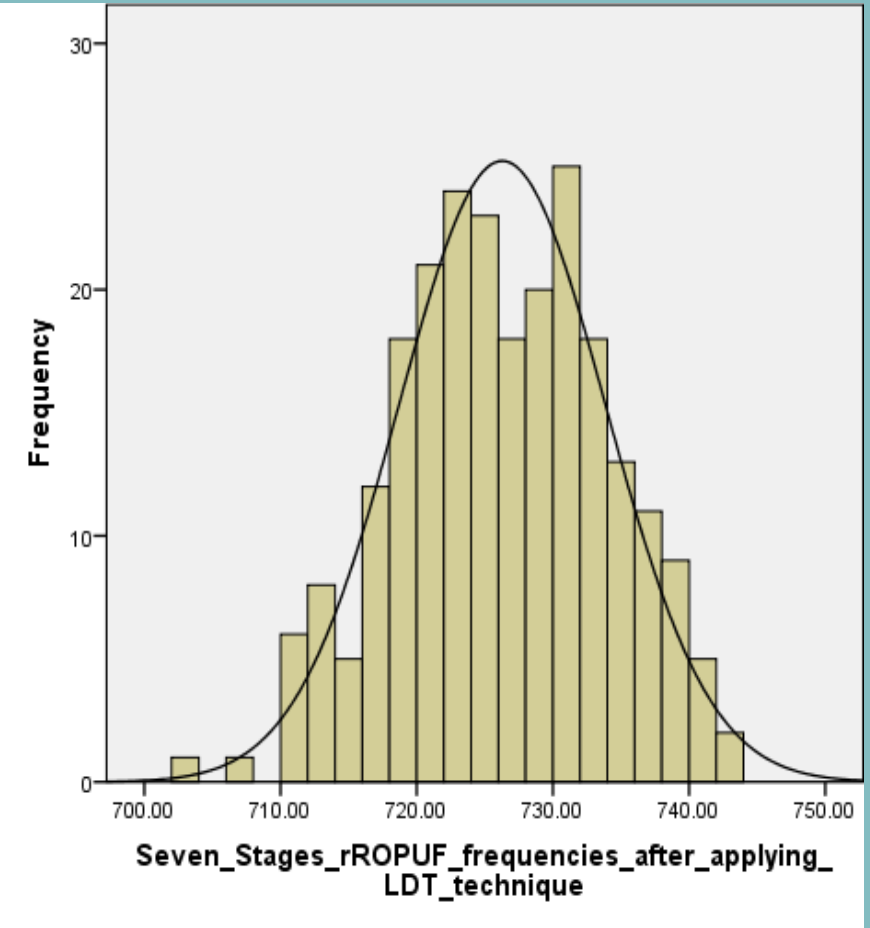
Experiential Result





Experiential Result - Cont'd

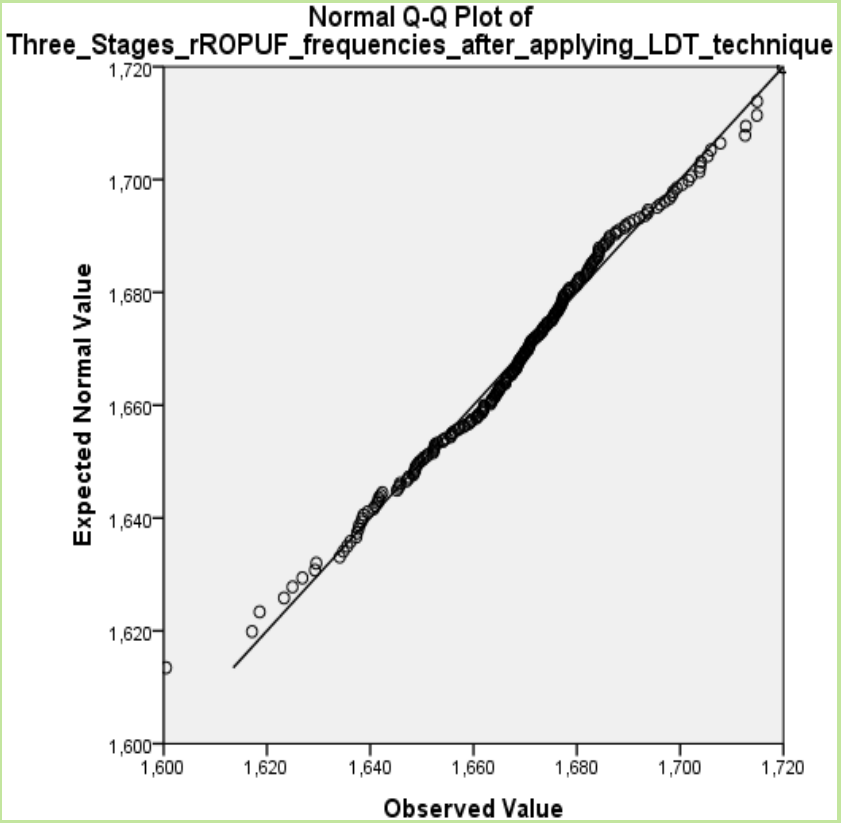


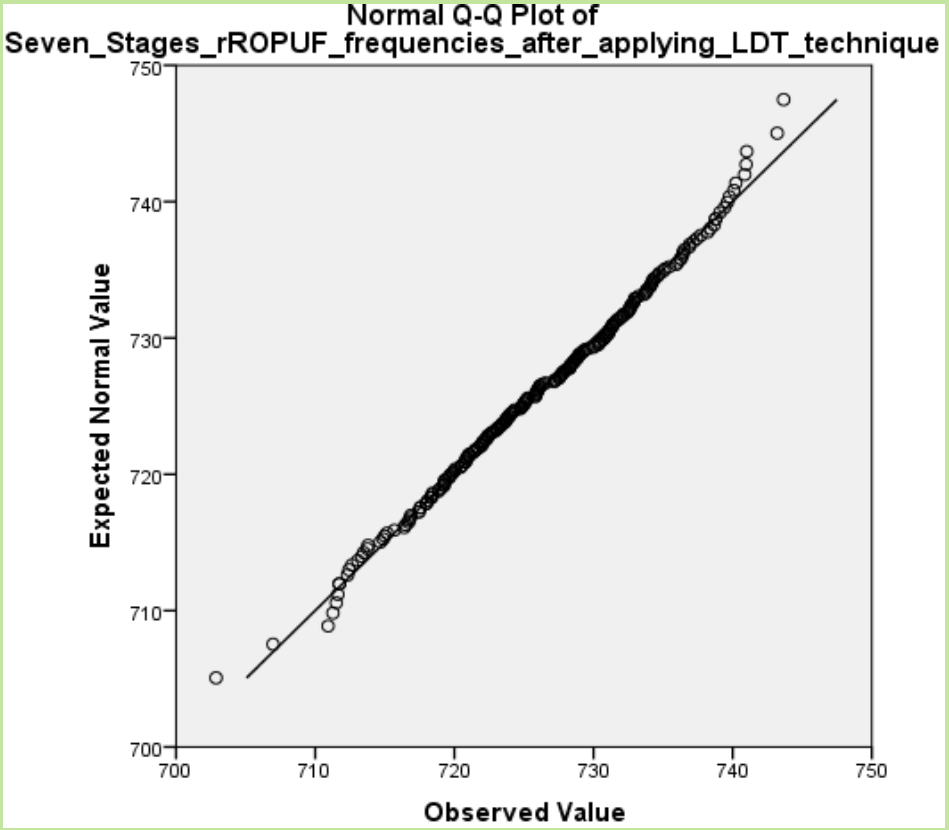


Experiential Result - Cont'd

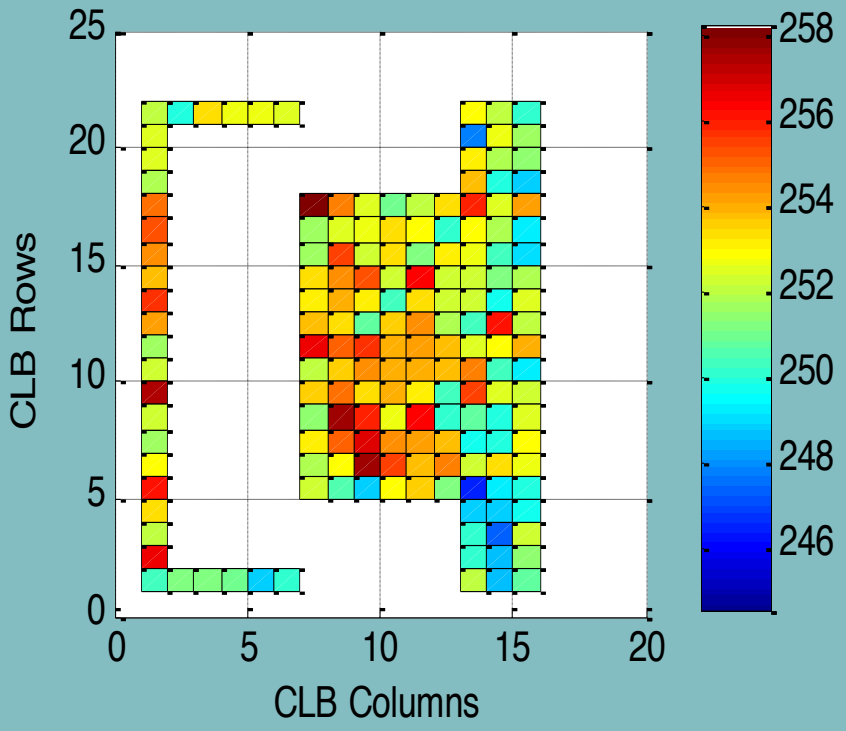
r-ROPUF parameter	Reconfigurable ROPUF Structures							
	Before applying LDT on r-ROPUF				After applying LDT on r-ROPUF			
	One Stage	Three Stage	Five Stage	Seven Stage	One Stage	Three Stage	Five Stage	Seven Stage
N	240	240	240	240	240	240	240	240
Mean	264.9	252.3	148	133.5	1779	1668	830	726
Median	264.8	252.4	148.1	133.6	1778	1669	830.6	726.0
Diversity	3.3	2.263	1.18	1.078	29.72	19.73	8.61	7.59
Variability	11.22	5.119	1.40	1.161	883.3	389.4	74.11	57.61
Skewness	0.129	-0.146	-0.164	-0.129	0.138	-0.134	-0.157	-0.122
Kurtosis	-0.606	0.494	-0.210	-0.350	-0.601	0.487	-0.216	-0.355
Range	15.69	13.72	6.62	5.80	139.3	119.5	48.13	40.78
Minimum	257.4	244.5	144.1	130.3	1713	1600	801.2	702.9
Maximum	273.1	258.2	150.7	136	1853	1720	849.3	743.7

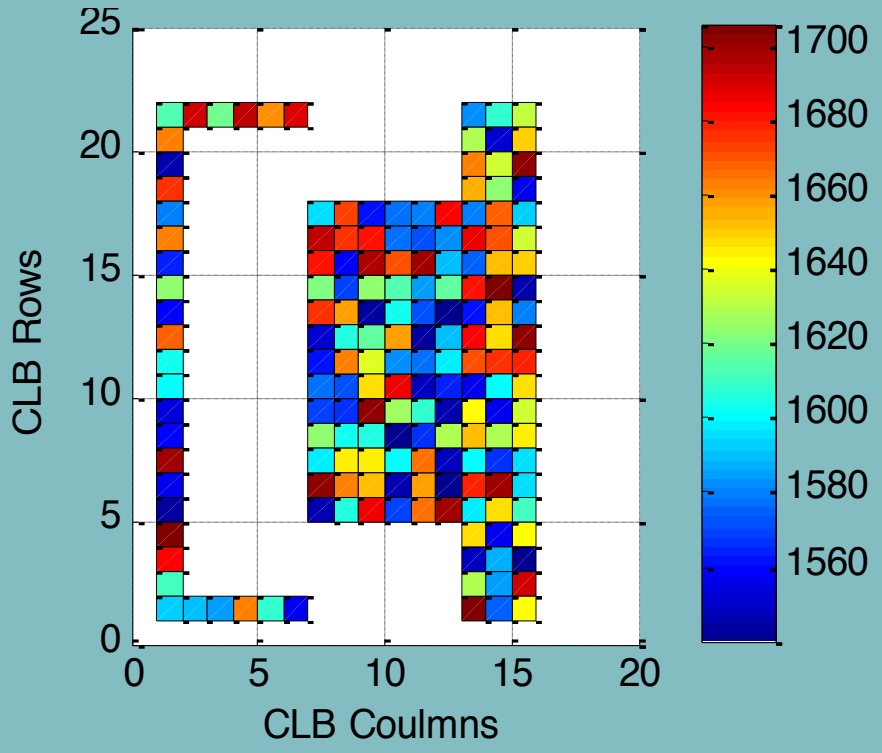
Experiential Result - Cont'd





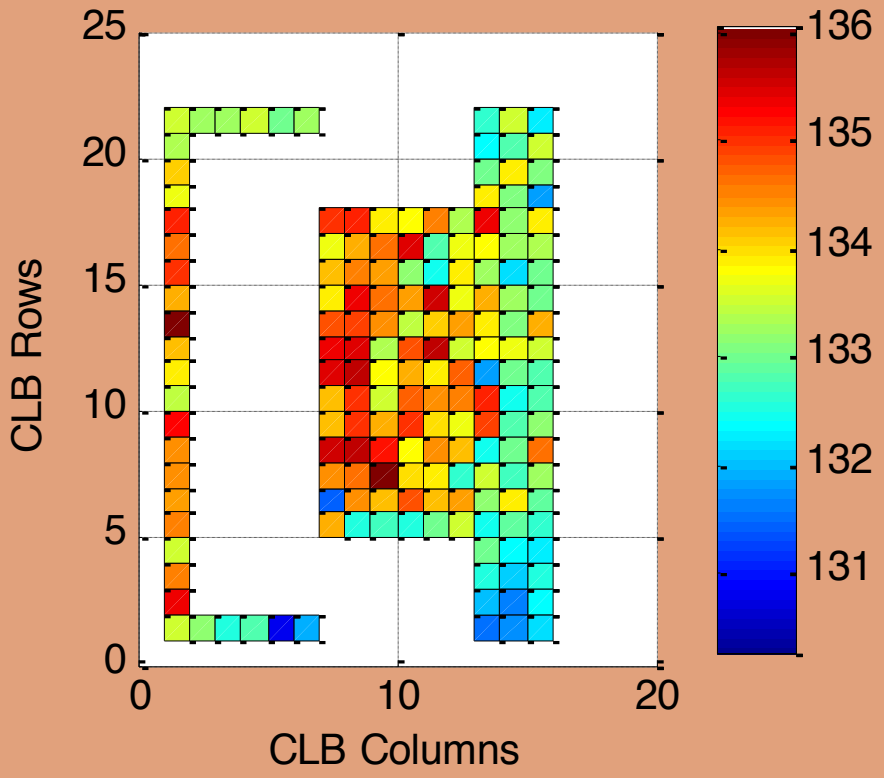
Experiential Result - Cont'd

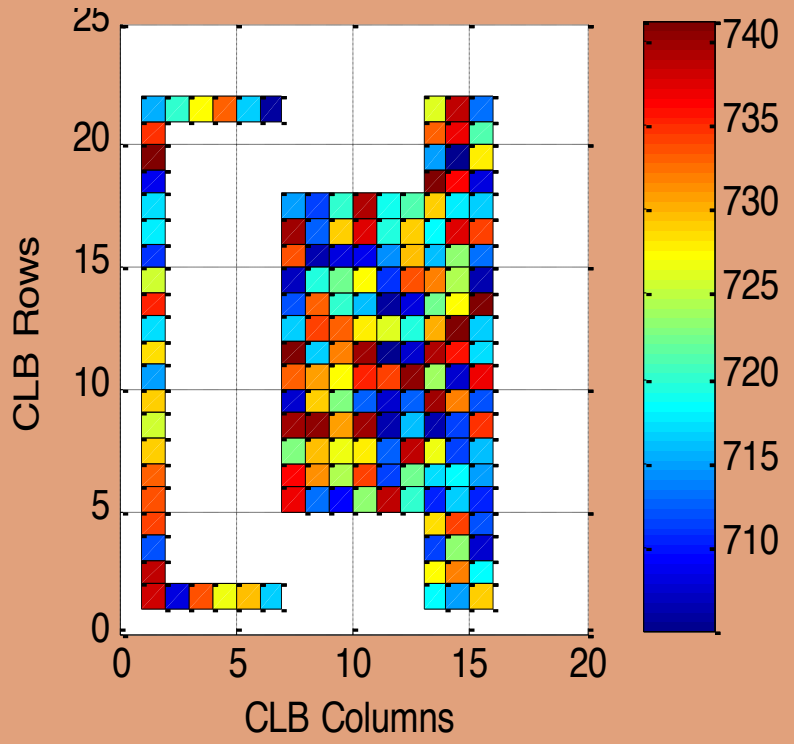




Average ROs frequencies before and after application of LDT: three stages

Experiential Result - Cont'd





Average ROs frequencies before and after application of LDT: seven stages

NIST Randomness Test

- A well known standard for measuring the randomness of statistical data
- data sequences are obtained from frequency characterization of 30 chips
- 30 different binary tested sequences (1,0) per each r-ROPUF structure
- 120 test sequences generated per r-ROPUF structure (four structures)
- 5520 responses are generated by comparing neighbor ROs in each column which generates n-1 response bits out of n RO frequencies
- For 1-out-of-8 coding, 2700 response bits are generated by a 3- bit index: 000,001,010 . . . 111 that points to the fastest RO out of 8 consecutive ROs on the same column bits for the tested sequence
- Response bits are stored on text files and tested for randomness using NIST software

NIST Randomness Test

- 9 different randomness tests are used：

  (Frequency Test, Block Frequency Test, Cumulative Sums Test (with block size m = 2 and m = 3), Runs Test, Longest Run Test, Serial Test (forward and backward) and Approximate Entropy Test are applied on the generated sequences

- Each of the 9 tests calculates the PVALUE_T using the χ^2 statistic

- The test fails if the calculated PVALUE_T of χ^2 is smaller than $0.0001 (P - VALUE_T \geq 0.0001)$

- Furthermore, the PROPORTION values should be above 90% percent or more than 27/30 samples

- If 90% of the total test sequences are significant (more than 27/30), the 'PROPORTION' of a test passes

NIST Randomness Test - Result

STATISTICAL TEST	One stages r-ROPUF Structure			
	1-out-of-8		Chain-like Neighbor Coding	
	$PVALUE_T$	PROPORTION	PVALUE	PROPORTION
Frequency	0.00021	30/30	0.00013	30/30
Block Frequency	0.00043	29/30	0.03024	27/30
Cumulative (m-2)	0.03472	28/30	0.05052	28/30
Cumulative (m-3)	0.52105	29/30	0.00331	29/30
Runs	0.00024	27/30	0.00004*	18/30*
Longest Run	0.00031	30/30	0.00052	29/30
Approximate	0.00001*	27/30	0.00054	28/30
Serial (forward)	0.00041	30/30	0.22044	30/30
Serial (backward)	0.00034	29/30	0.07035	29/30
'*' indicates a randomness failure in the applied NIST Test.				

NIST Randomness Test - Result

STATISTICAL TEST	Three stages r-ROPUF Structure			
	1-out-of-8		chain-like neighbor	
	$PVALUE_T$	PROPORTION	PVALUE	PROPORTION
Frequency	0.00032	30/30	0.00035	30/30
Block Frequency	0.05039	30/30	0.00044	30/30
Cumulative (m-2)	0.00035	29/30	0.00044	29/30
Cumulative (m-3)	0.07048	27/30	0.00041	28/30
Runs	0.00031	29/30	0.00005*	0/30*
Longest Run	0.03042	28/30	0.00048	30/30
Approximate	0.00013	27/30	0.00033	28/30
Serial (forward)	0.00050	30/30	0.00052	30/30
Serial (backward)	0.00032	29/30	0.00035	27/30
'*' indicates a randomness failure in one of the applied NIST Tests.				

NIST Randomness Test - Result

STATISTICAL TEST	Five stages r-ROPUF Structure			
	1-out-of-8		chain-like neighbor	
	$PVALUE_T$	PROPORTION	PVALUE	PROPORTION
Frequency	0.00031	29/30	0.00039	29/30
Block Frequency	0.00049	27/30	0.00035	27/30
Cumulative (m-2)	0.00037	30/30	0.06043	30/30
Cumulative (m-3)	0.00038	30/30	0.00054	30/30
Runs	0.00048	30/30	0.00001*	6/30*
Longest Run	0.00012	28/30	0.57049	30/30
Approximate	0.00000*	28/30	0.00054	30/30
Serial (forward)	0.00049	30/30	0.00047	30/30
Serial (backward)	0.00031	30/30	0.00039	28/30
'*' indicates a randomness failure in one of the applied NIST Tests.				

NIST Randomness Test - Result

STATISTICAL TEST	Seven Stages r-ROPUF Structure			
	1-out-of-8		chain-like neighbor	
	$PVALUE_T$	PROPORTION	PVALUE	PROPORTION
Frequency	0.00046	30/30	0.04043	29/30
Block Frequency	0.00031	30/30	0.00031	28/30
Cumulative (m-2)	0.06032	27/30	0.00035	30/30
Cumulative (m-3)	0.00046	30/30	0.00043	30/30
Runs	0.05036	30/30	0.00001*	0/30*
Longest Run	0.00038	28/30	0.0004	29/30
Approximate	0.00032	29/30	0.50034	29/30
Serial (forward)	0.00045	28/30	0.02031	30/30
Serial (backward)	0.00032	29/30	0.00043	29/30
'*' indicates a randomness failure in one of the applied NIST Tests.				

Conclusion

- Nullifying the negative effects of systematic variation on ROPUF response bits is a very critical process to improve the randomness of ROPUF.
- In this paper, a novel security technique named LDT is introduced using base-10 logarithm and square root of RO deviations from the global mean to increase ROPUF security in terms of randomness and reliability.
- After the application of LDT, the generated response bits successfully passed the entire NIST test using 1-out-of-8 coding.
- As for Chain-like Neighbor Coding, the resultant response bits passed almost 90% of the randomness tests.
- LDT is proven to exhibit improved security, true randomness and higher reliability on the response bits compared to earlier randomness techniques

Thanks for Listening!

Any Questions?