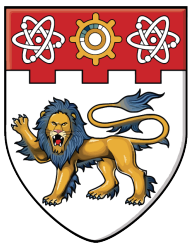
Multi-valued Arbiters for Quality Enhancement of PUF Responses on FPGA Implementation

Siarhei S. Zalivaka[1], Alexander V. Puchkov[2],
Vladimir P. Klybik[2], Alexander A. Ivaniuk[2], Chip-Hong Chang[1]

[1]School of Electrical and Electronic Engineering
Nanyang Technological University

[2]Faculty of Computer Systems and Networks
Belarusian State University of Informatics and Radioelectronics

January 28, 2016



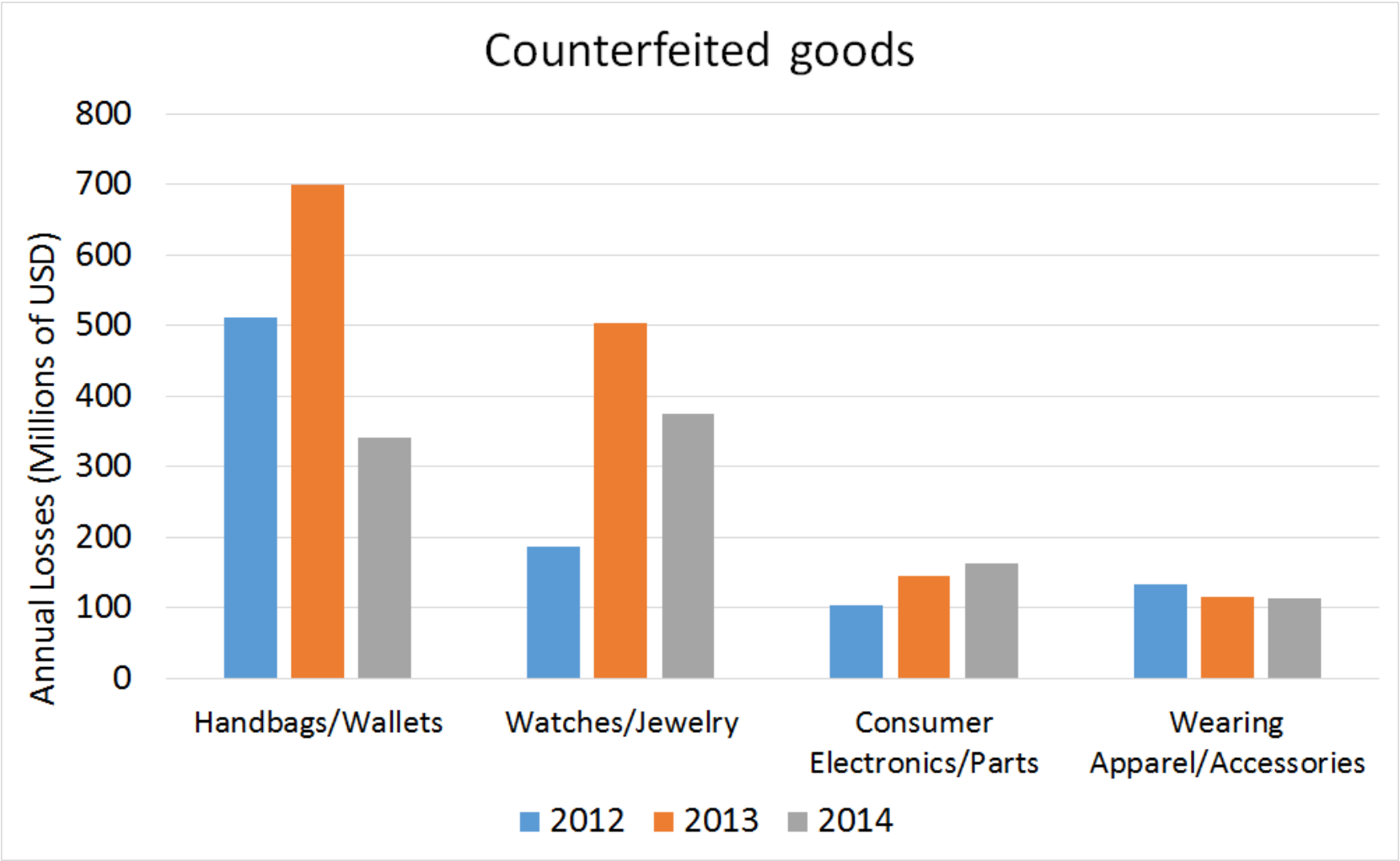
NANYANG TECHNOLOGICAL UNIVERSITY

ASIA SOUTH PACIFIC DESIGN AUTOMATION CONFERENCE

Outline

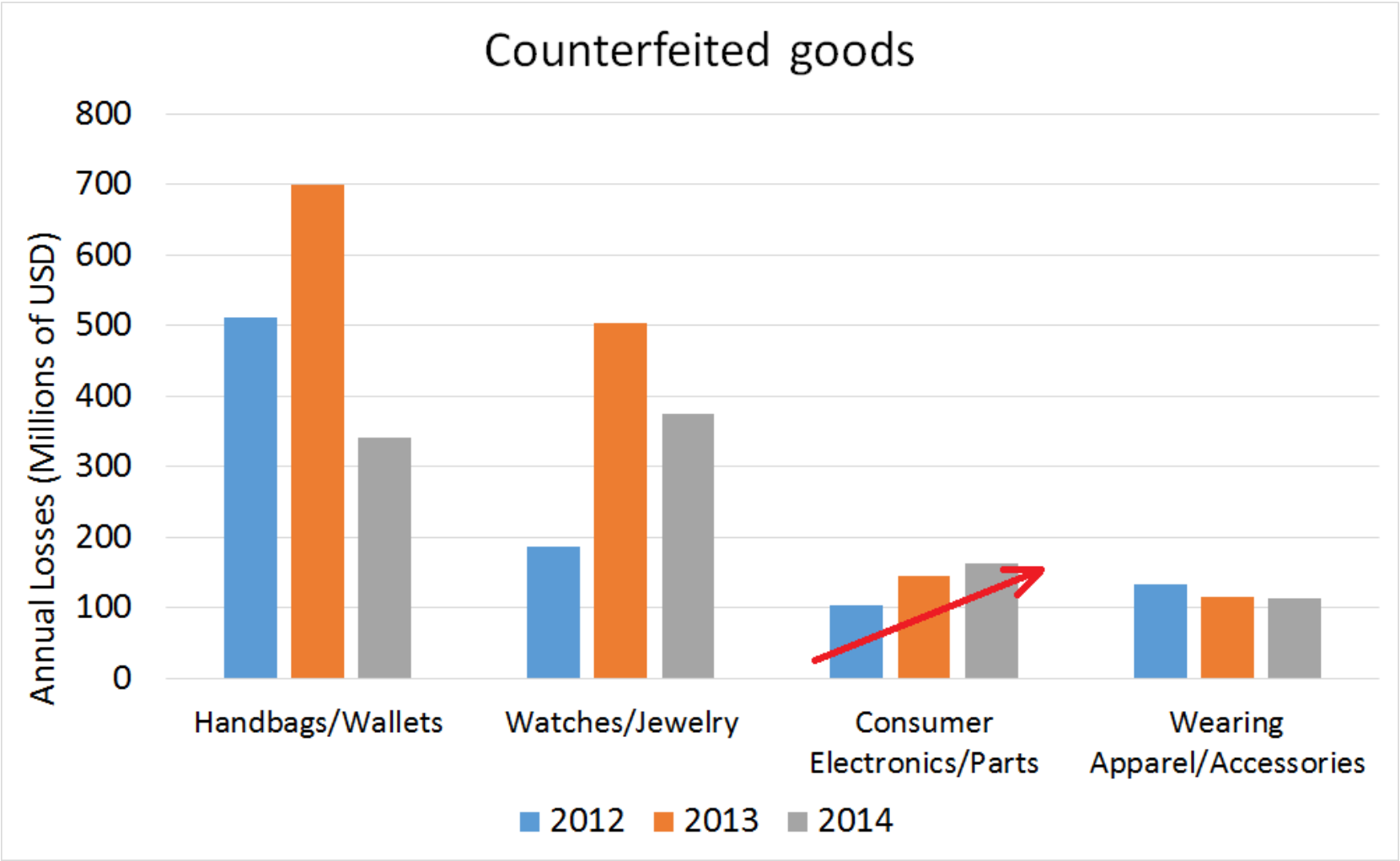
Introduction

Counterfeiting



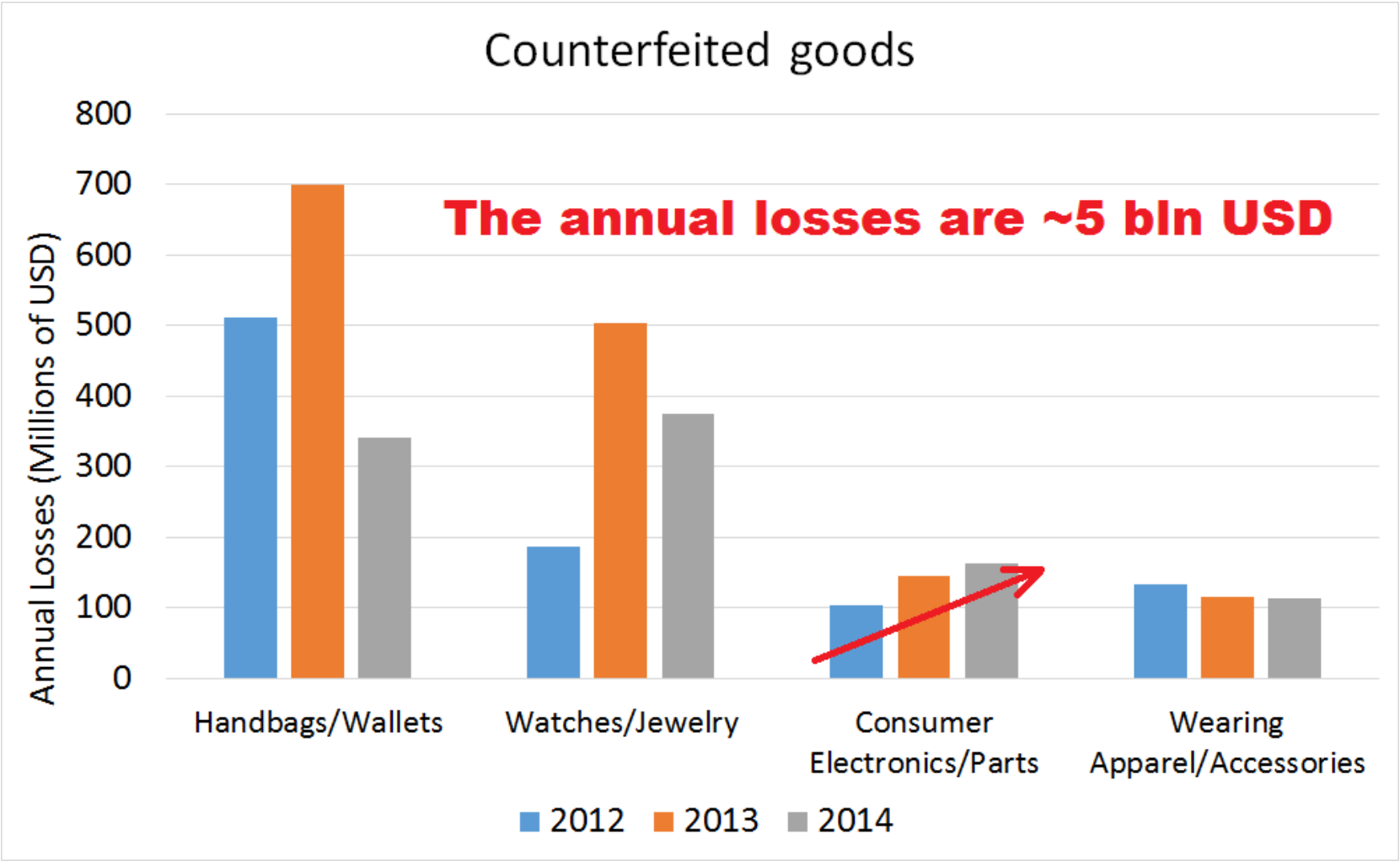
* Intellectual Property Rights Seizures Statistics Fiscal Year 2012-2014

Counterfeiting



* Intellectual Property Rights Seizures Statistics Fiscal Year 2012-2014

Counterfeiting



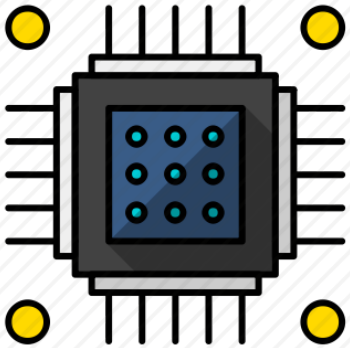
* Intellectual Property Rights Seizures Statistics Fiscal Year 2012-2014

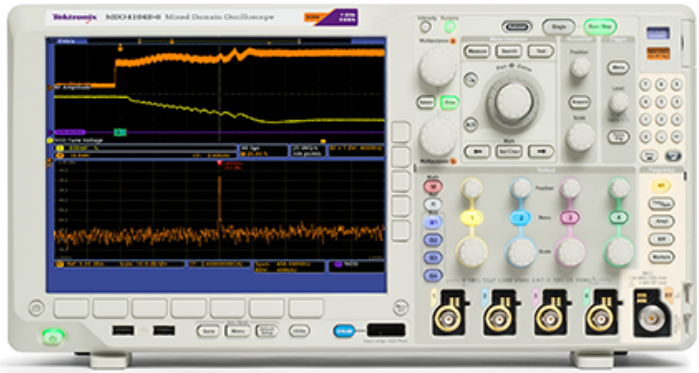
Classic

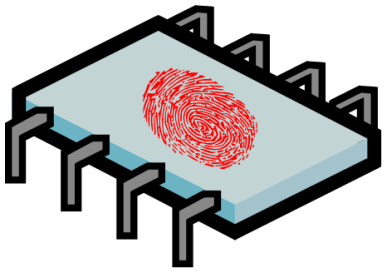
"Unique"
Physical Property

Measurement Method

Authentication
Key Generation





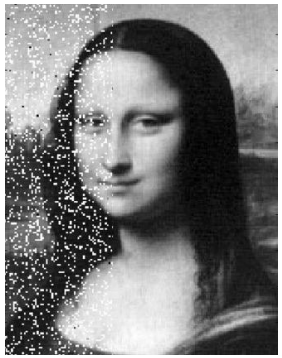


Silicon

Reliability Issues

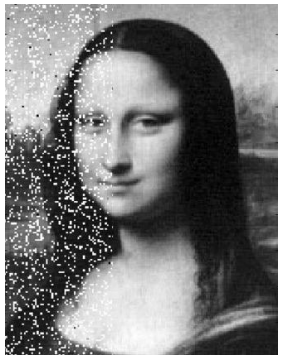
Reliability Issues

Error Correction Codes

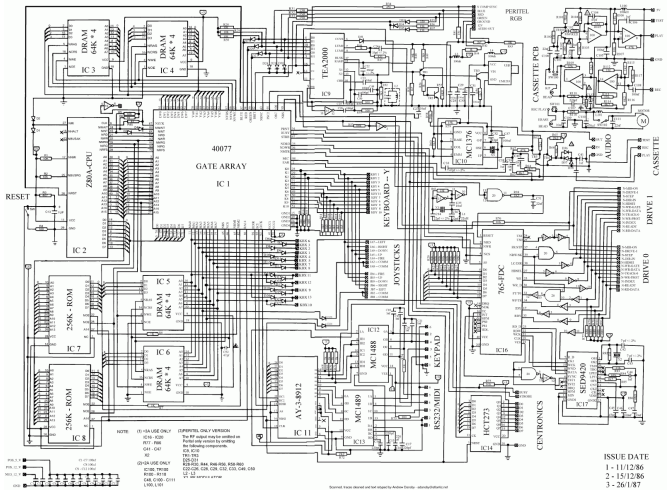


Reliability Issues

Error Correction Codes

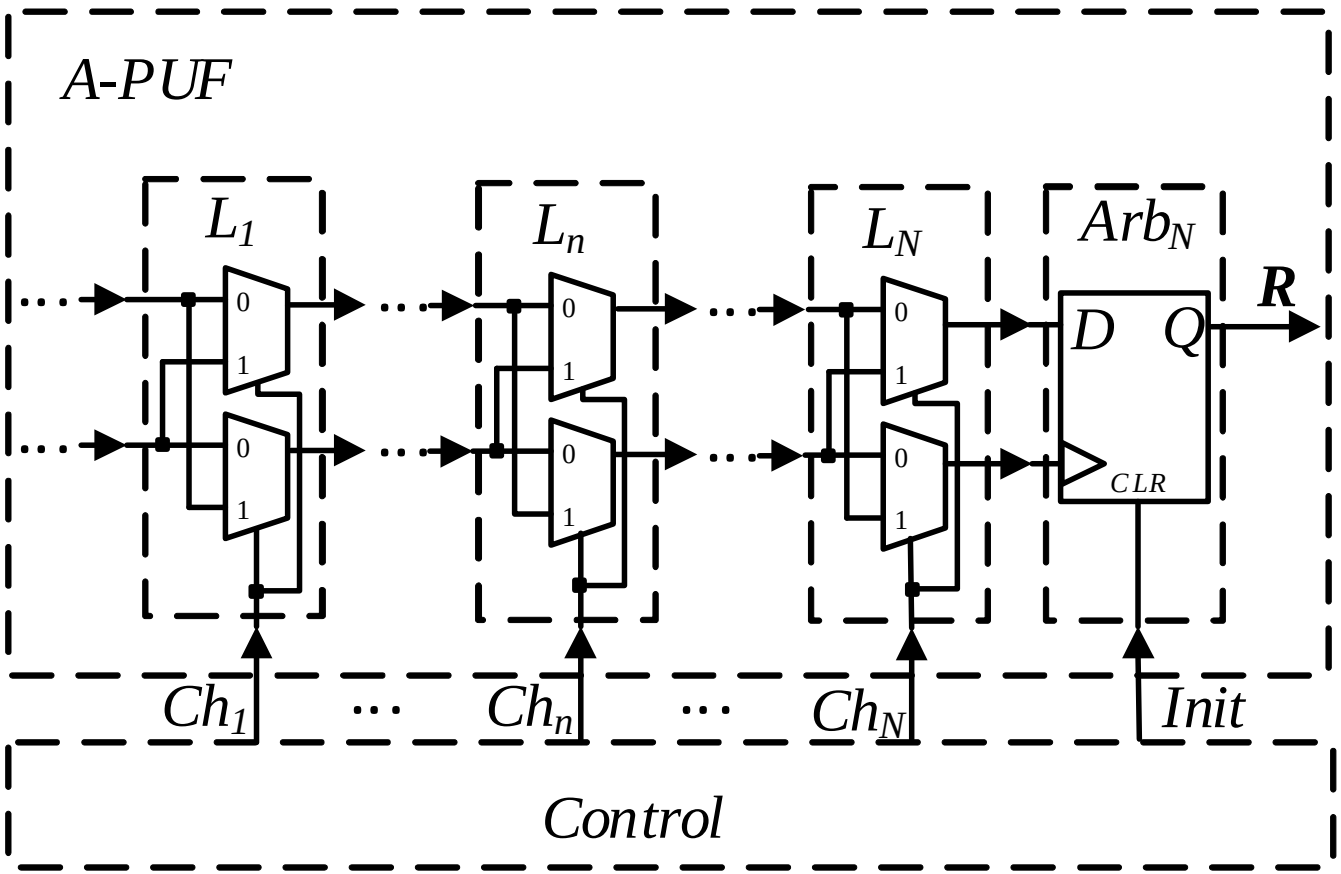


Structure Enhancement



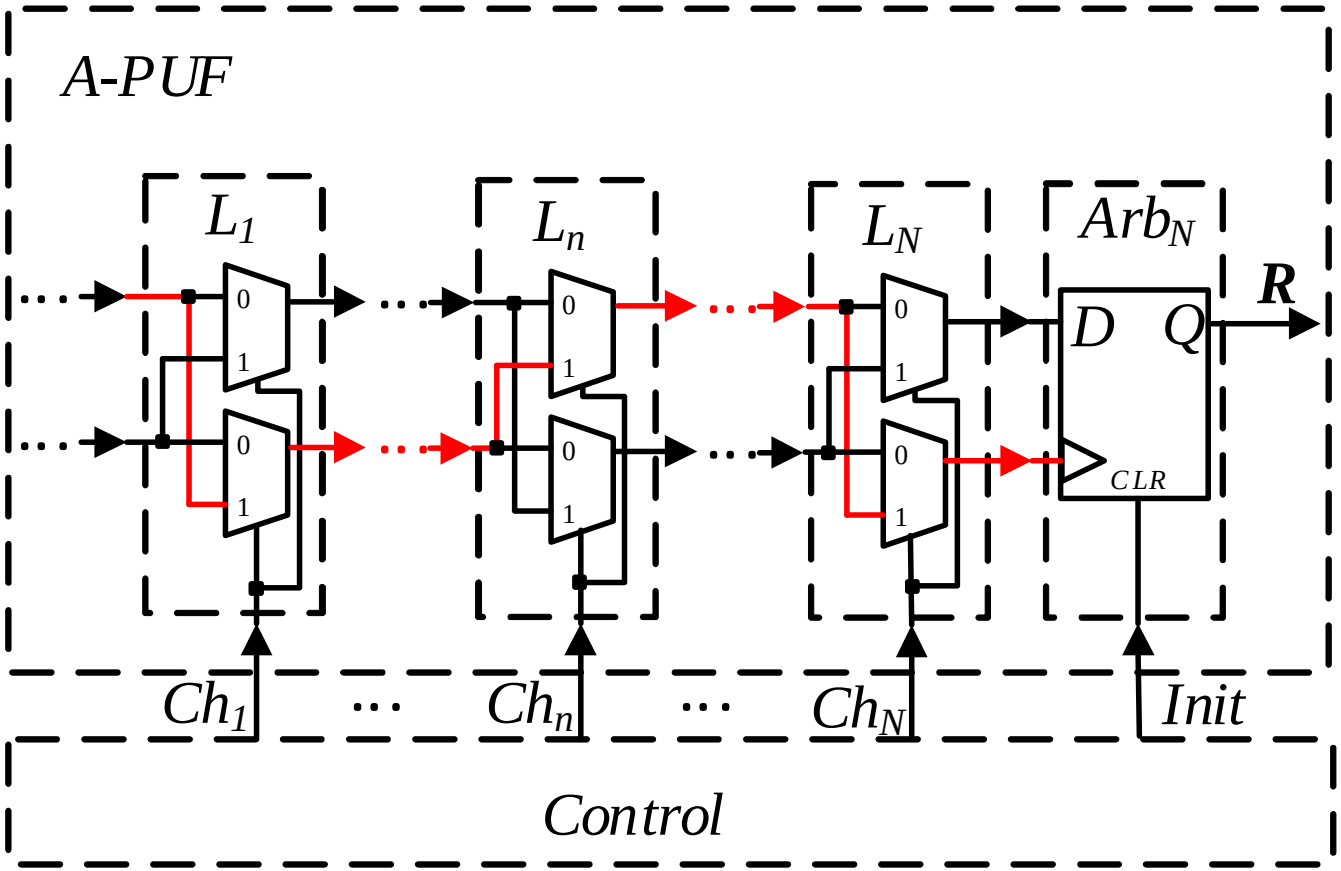
Arbiter PUF Architecture

Classical Arbiter PUF architecture



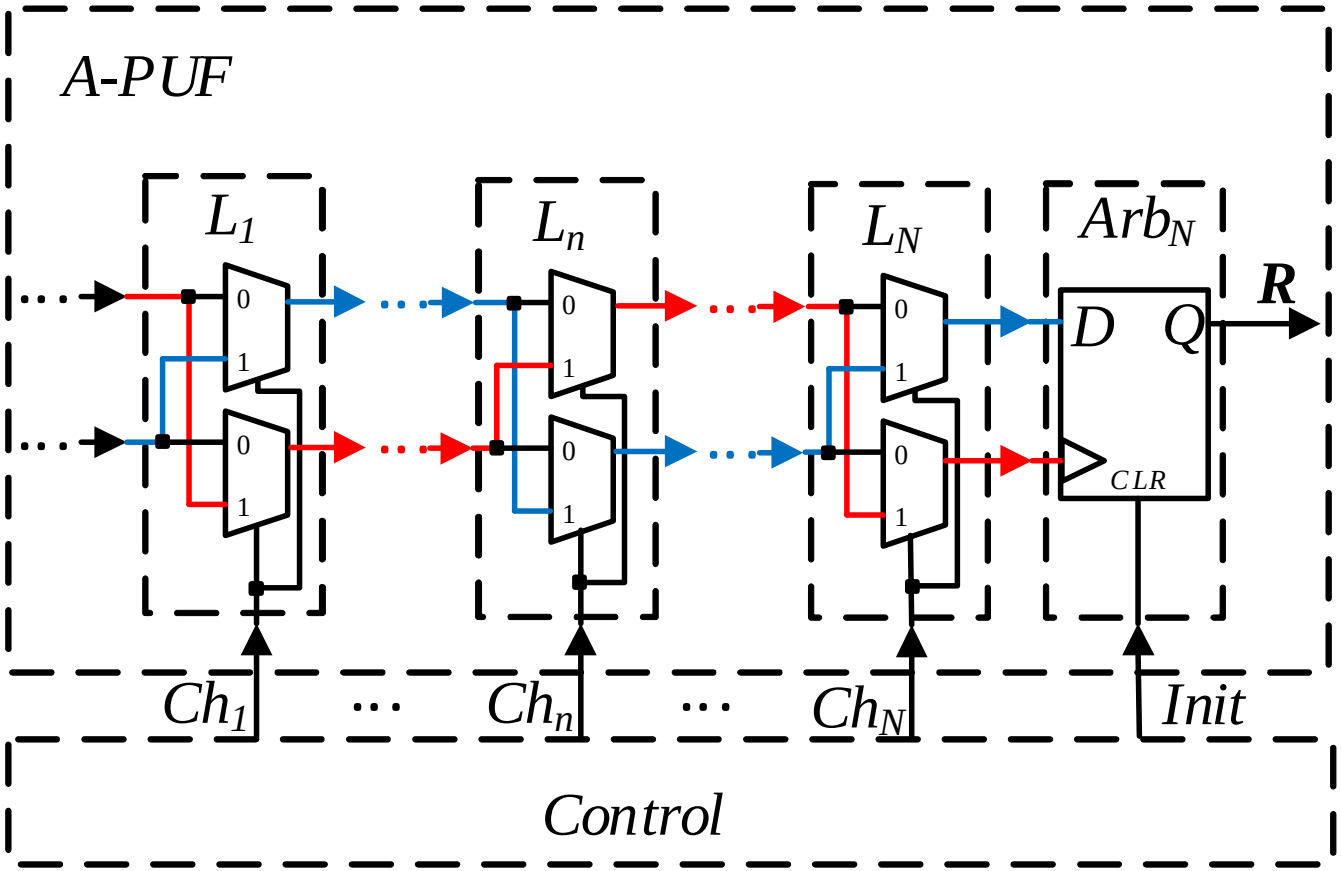
* J. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, S. Devadas "A technique to build a secret key in integrated circuits for identification and authentication applications", VLSIC'04 (Conference), June 2004.

Classical Arbiter PUF architecture



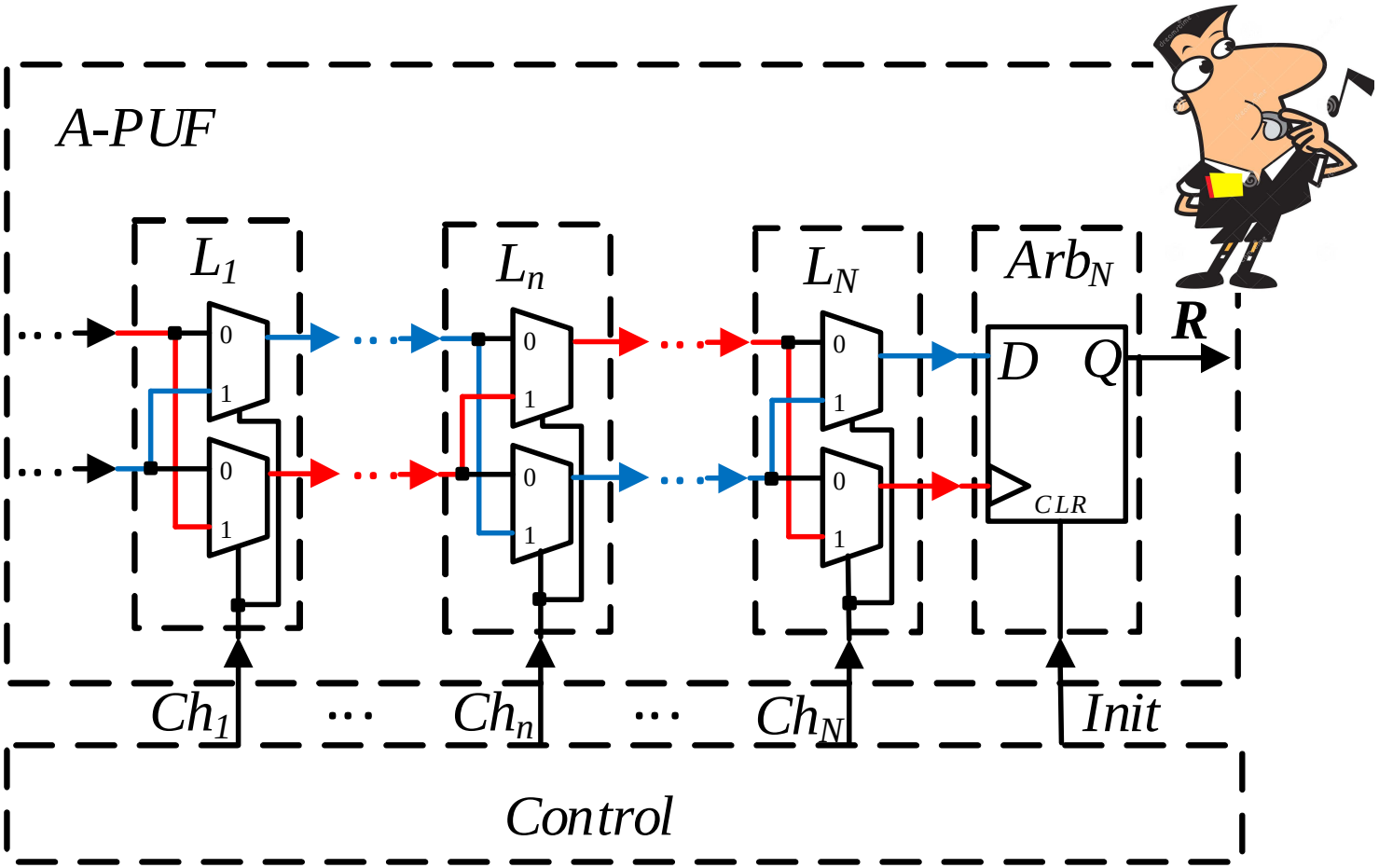
* J. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, S. Devadas "A technique to build a secret key in integrated circuits for identification and authentication applications", VLSIC'04 (Conference), June 2004.

Classical Arbiter PUF architecture



* J. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, S. Devadas "A technique to build a secret key in integrated circuits for identification and authentication applications", VLSIC'04 (Conference), June 2004.

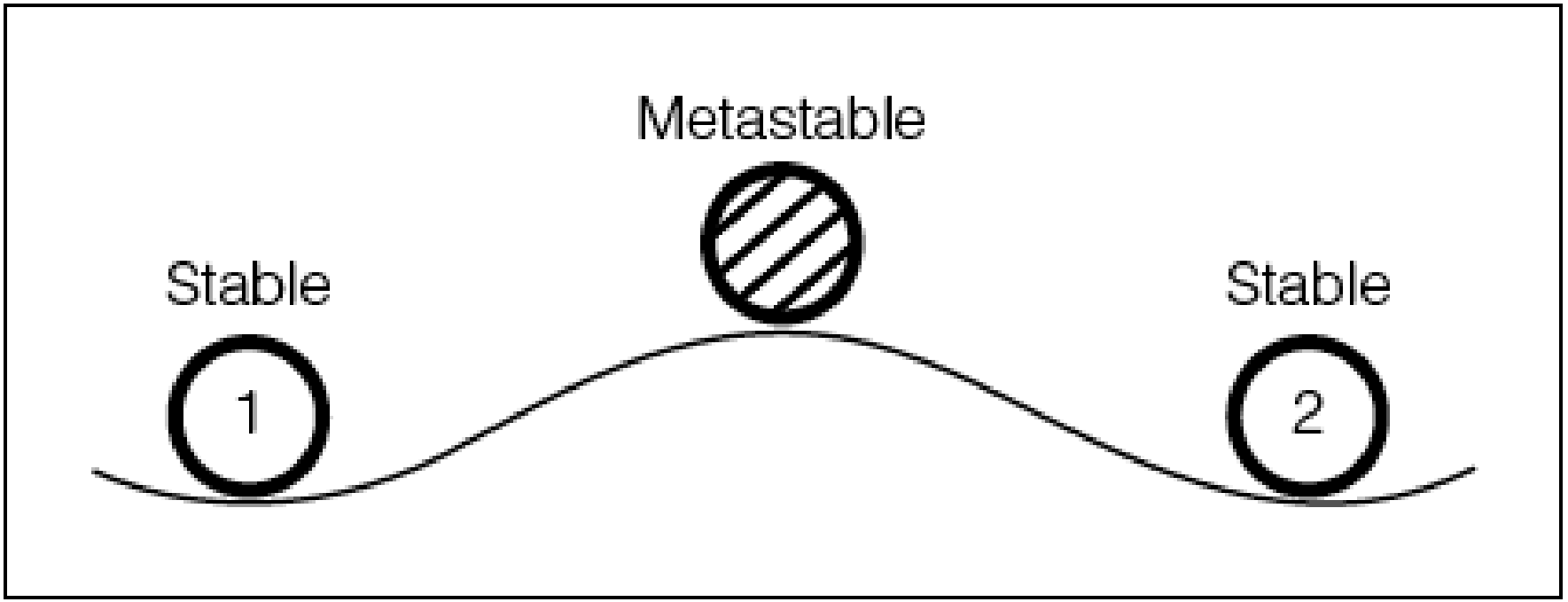
Classical Arbiter PUF architecture



Reliability is 0.5769.

* J. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, S. Devadas "A technique to build a secret key in integrated circuits for identification and authentication applications", VLSIC'04 (Conference), June 2004.

Metastability



Efforts

Big Challenge Size

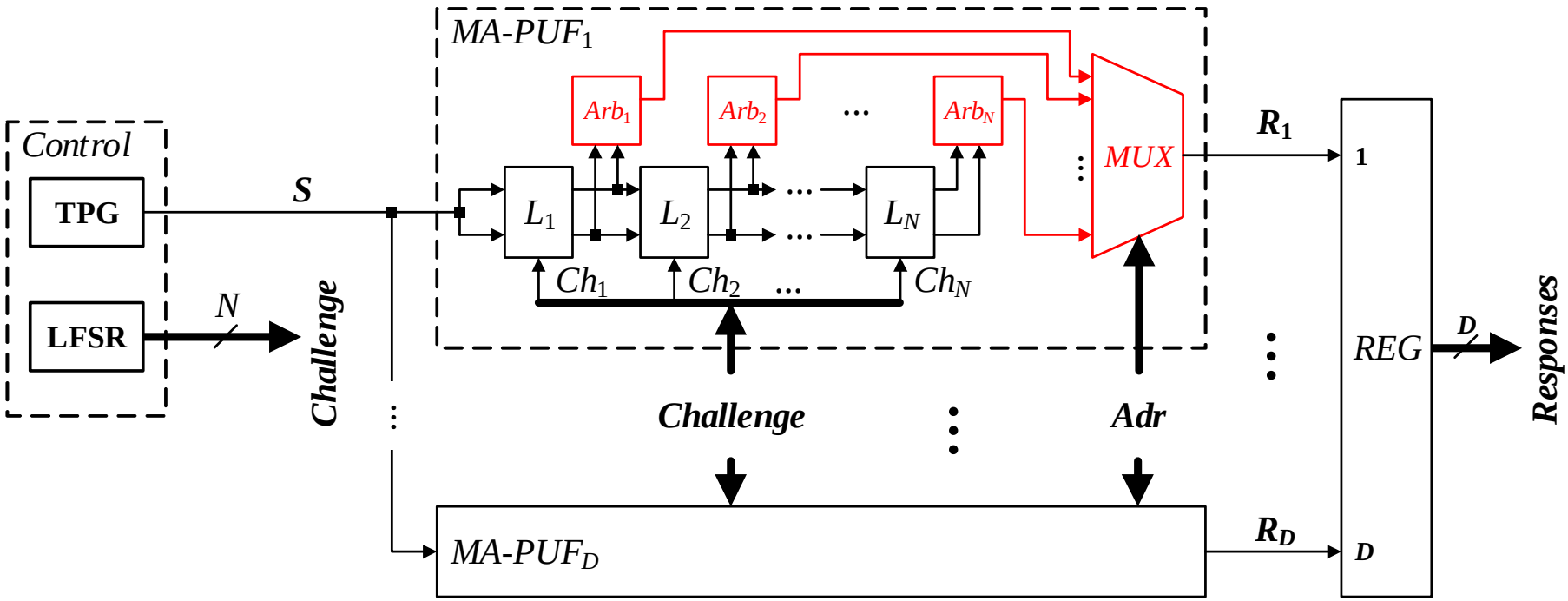
Efforts

Big Challenge Size

Only One Bit Response

Multi-Arbiter PUF with Enhanced Response Set

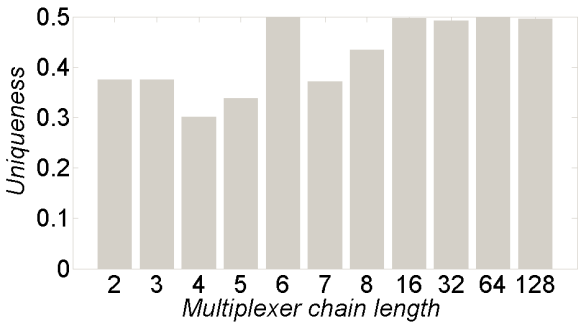
Multi-arbiter PUF Architecture



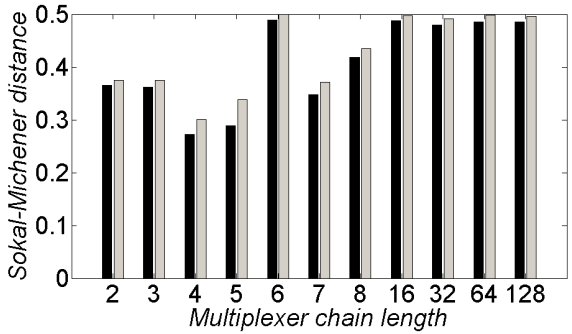
* V. P. Klybik, A. A. Ivaniuk "Use of Arbiter Physical Unclonable Function to solve identification problem of digital device", AC& CS (Journal), May 2015

Multiplexer chain length investigation

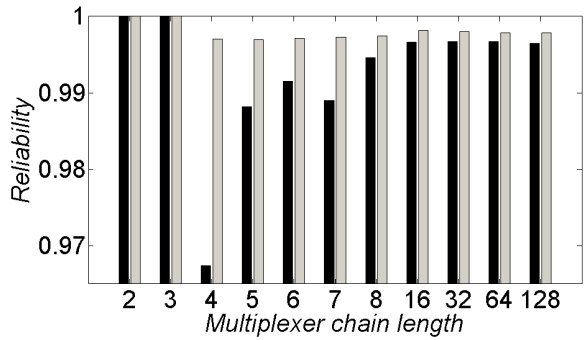
Uniqueness



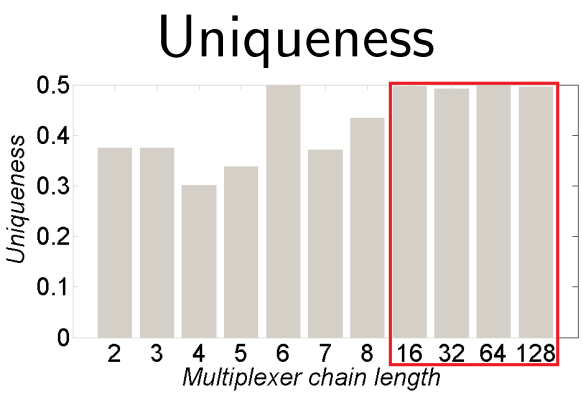
Sokal-Michener dist.

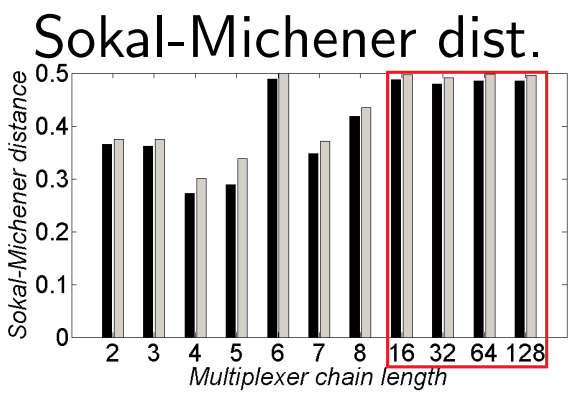


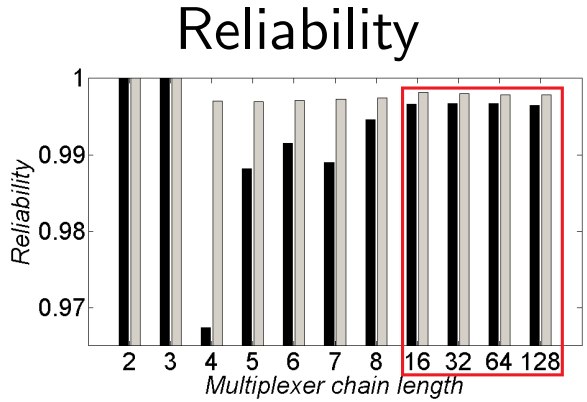
Reliability



Multiplexer chain length investigation







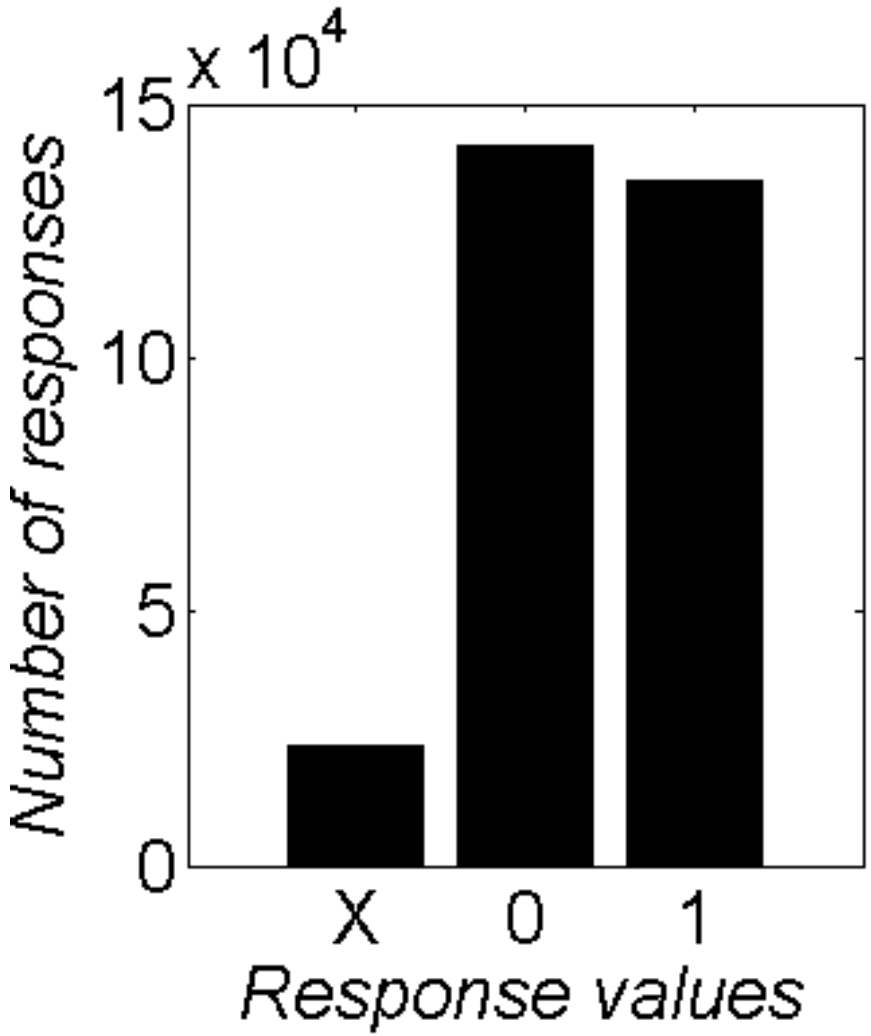
For arbiter index greater than **16**, PUF figures of merit became stable and vary within a narrow range.

* Gray colored bars represent average values,

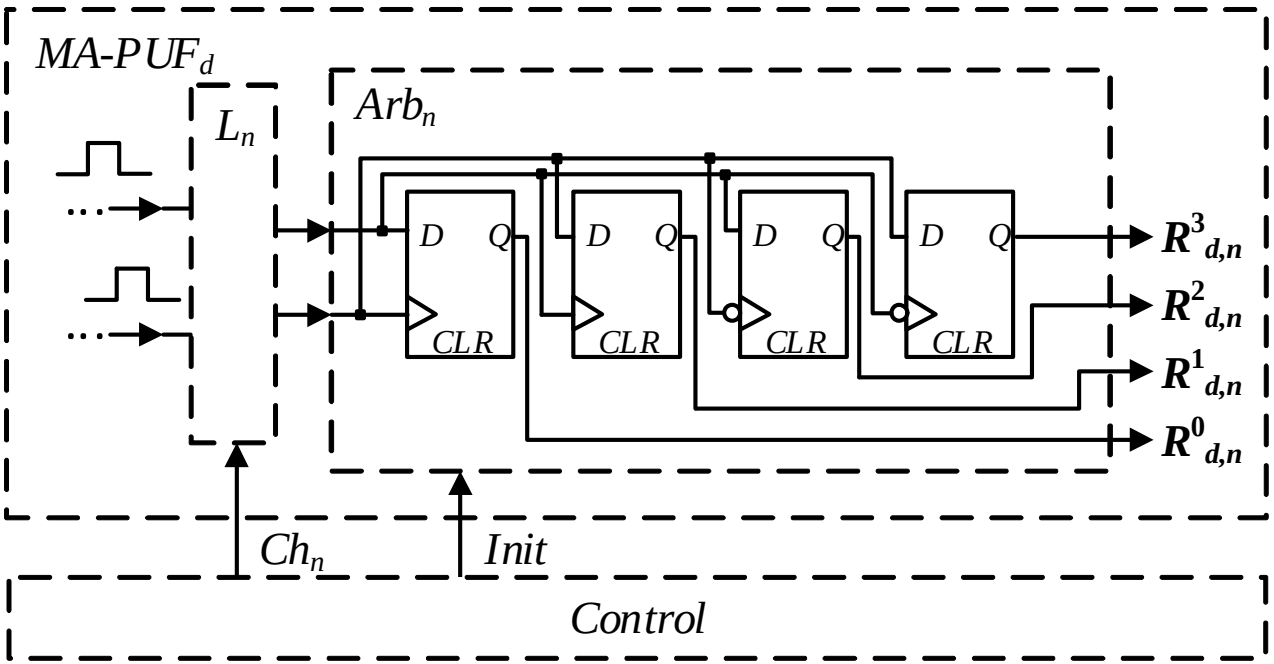
Black colored – minimal.

Metastability Detection

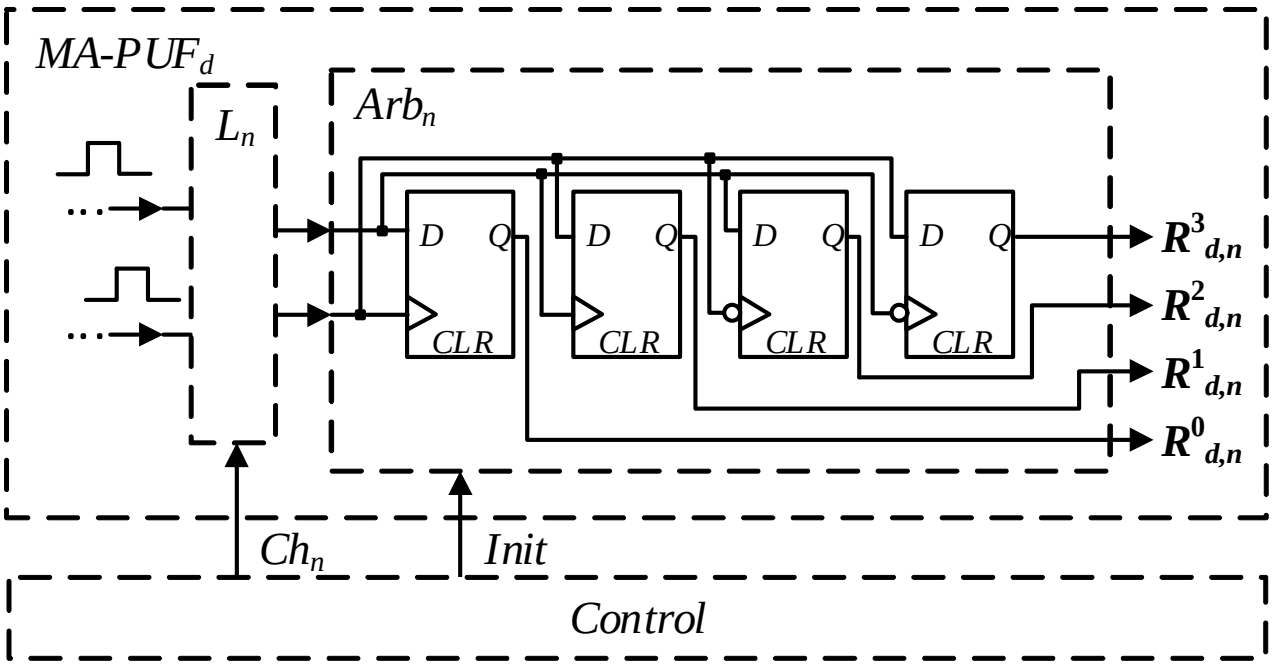
Identification of metastable arbiter bits



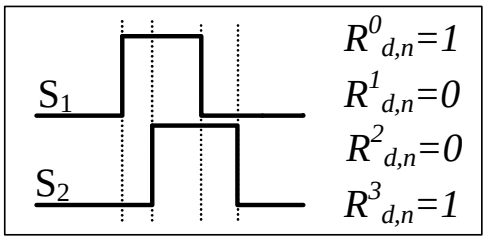
4-DFF based arbiter



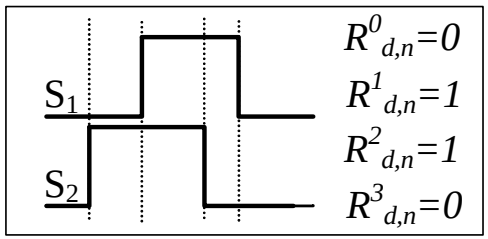
4-DFF based arbiter



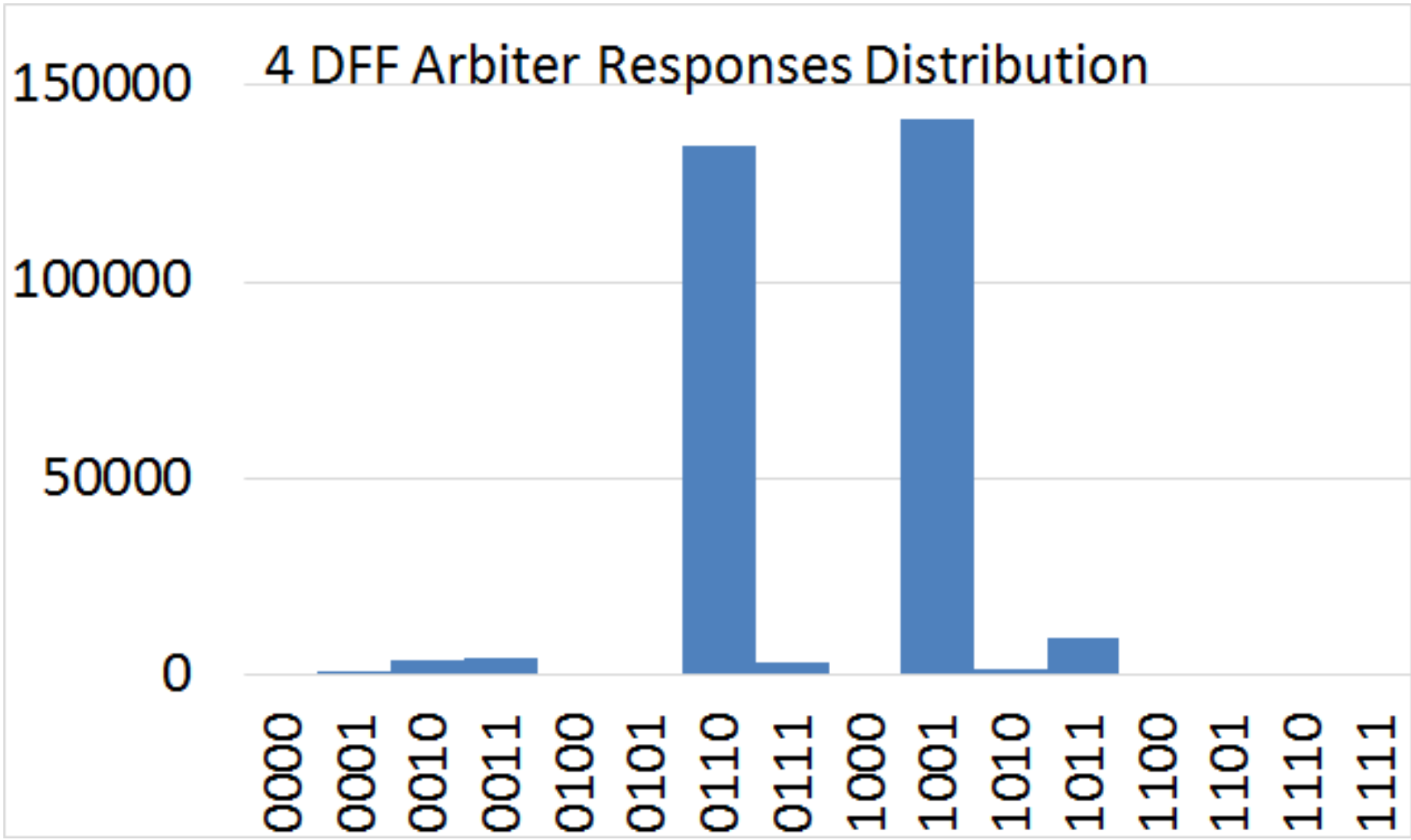
Stable zero



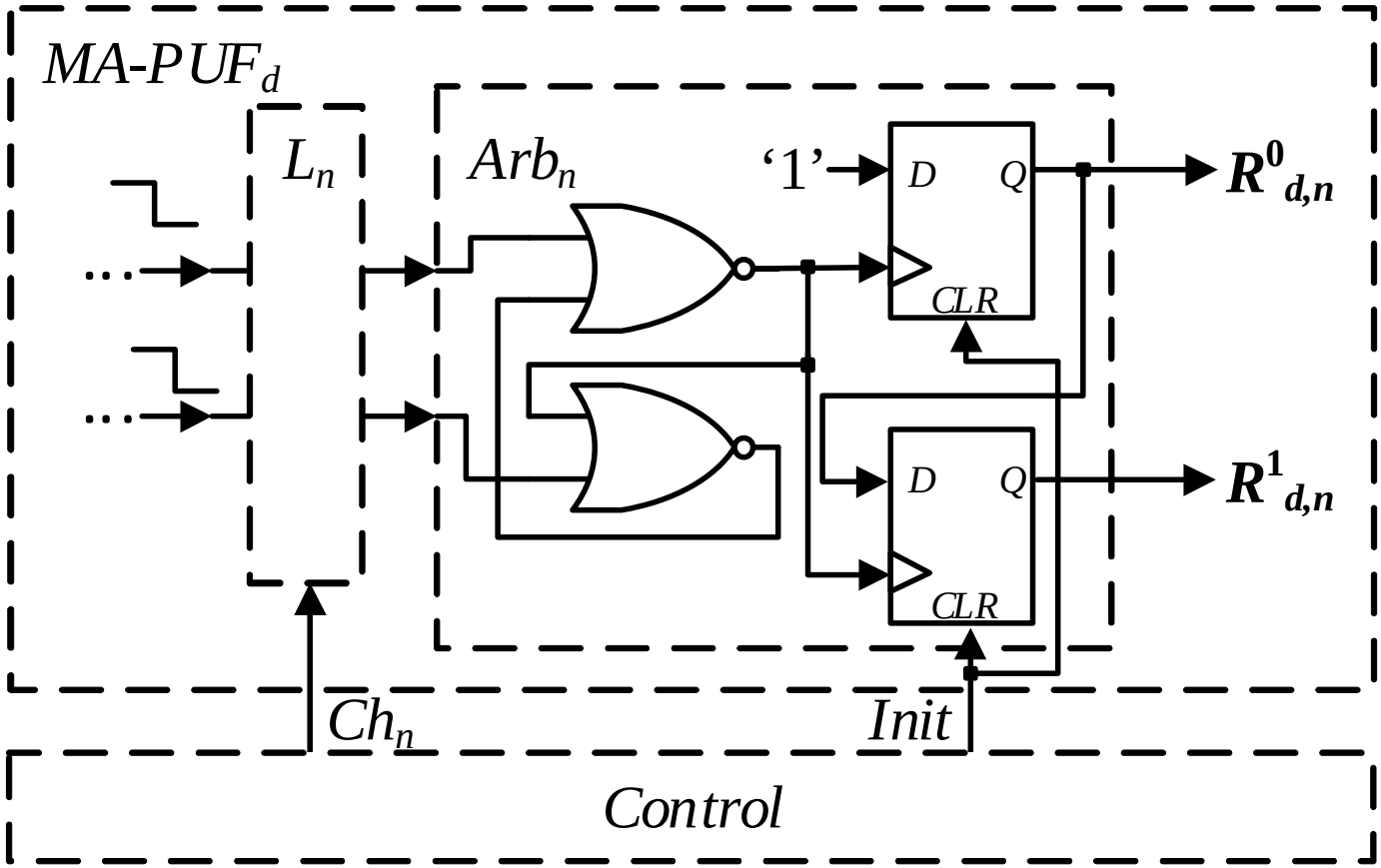
Stable one



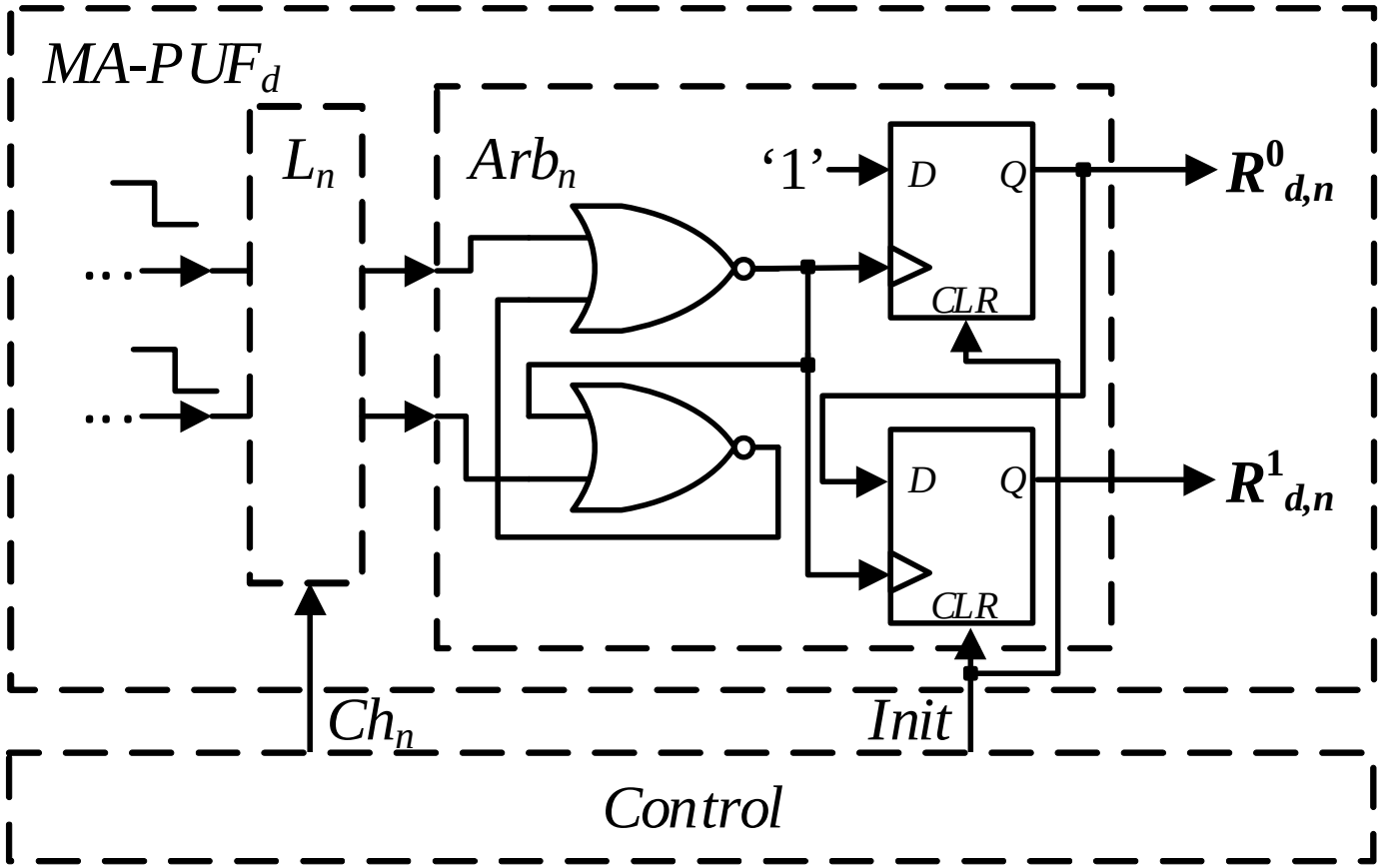
4-DFF outputs distribution



SR latch based arbiter

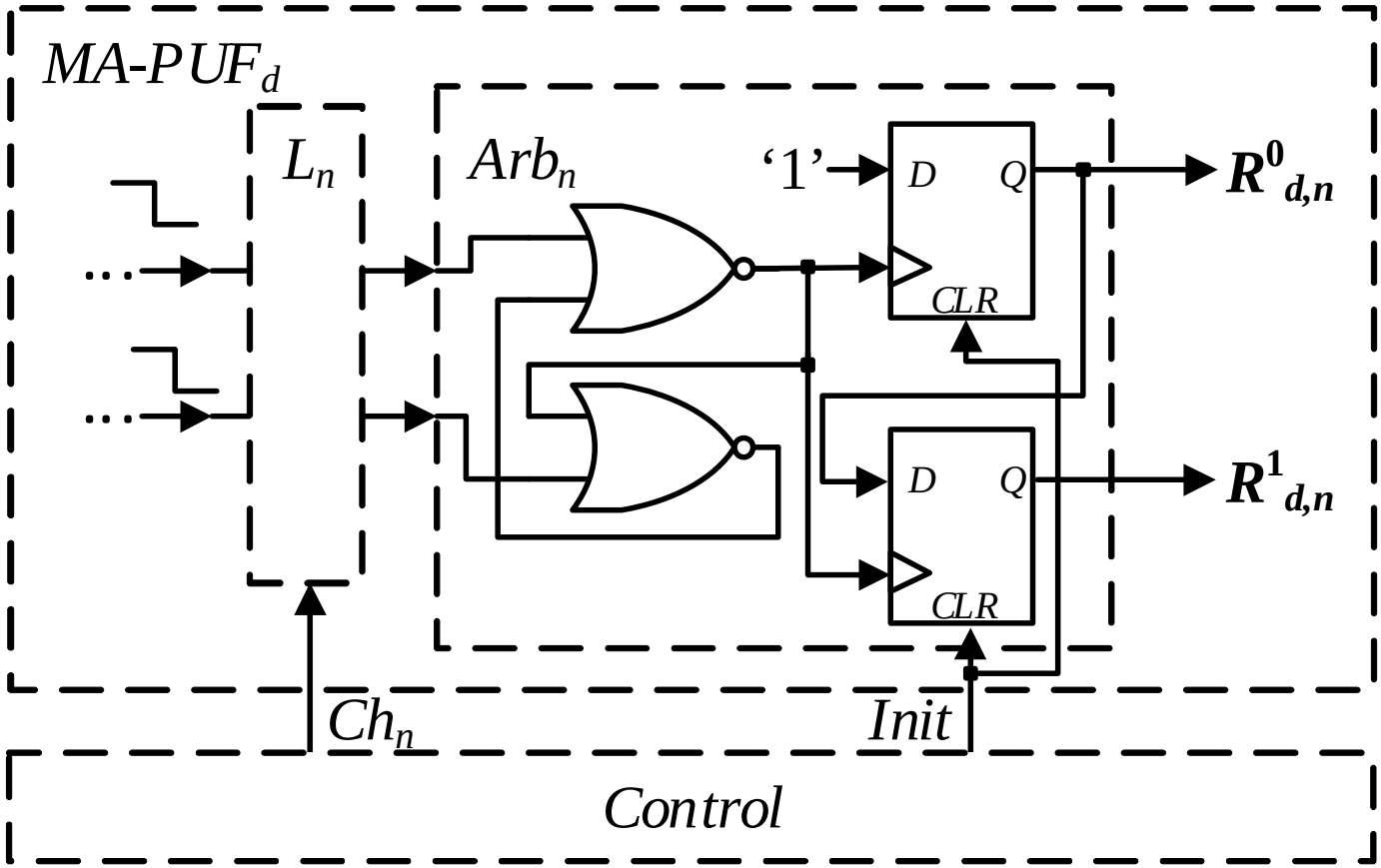


SR latch based arbiter



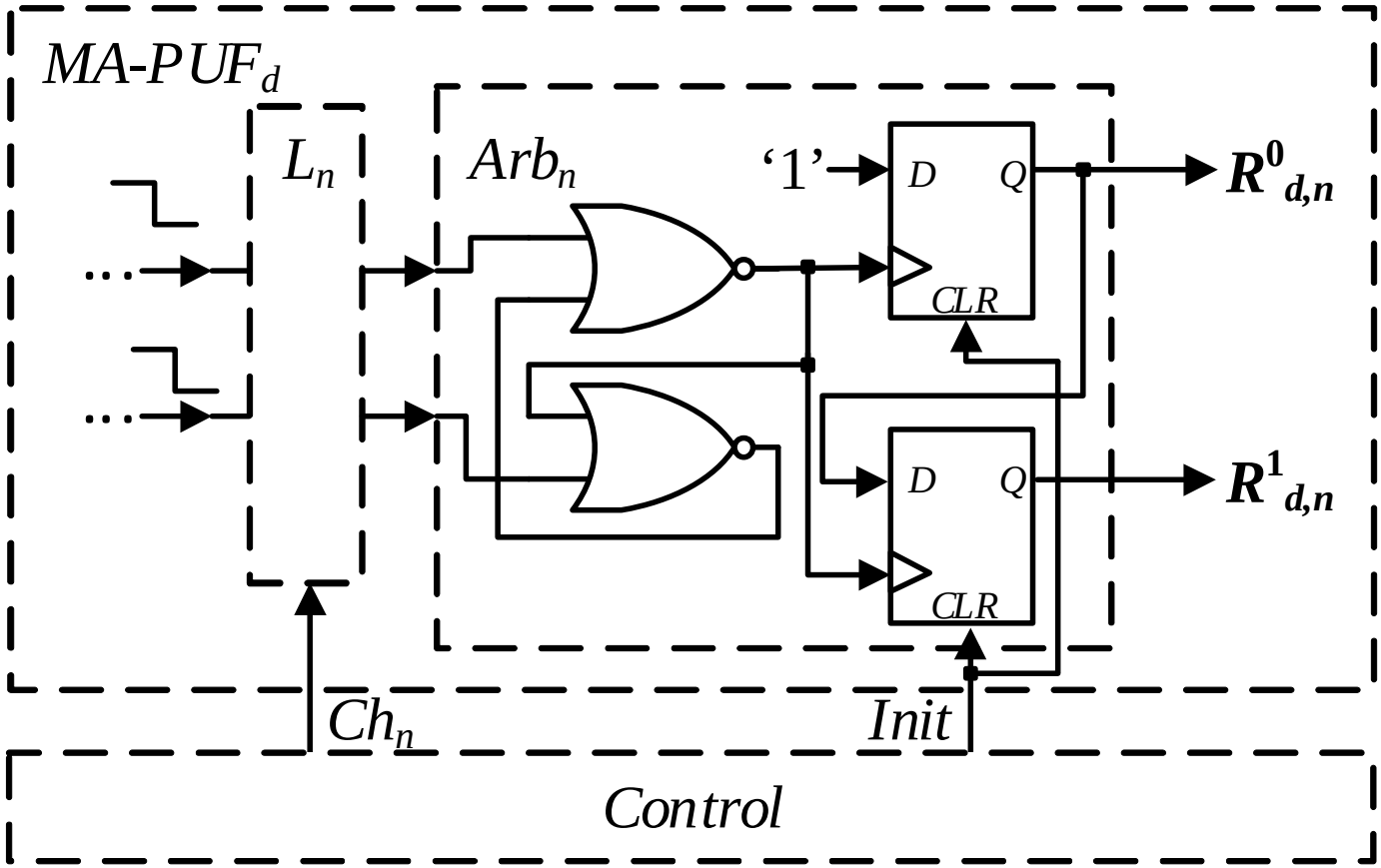
- $R^0_{d,n} = 0, R^1_{d,n} = 0$ – stable one

SR latch based arbiter



- $R^0_{d,n} = 0, R^1_{d,n} = 0$ – stable one
- $R^0_{d,n} = 1, R^1_{d,n} = 0$ – stable zero

SR latch based arbiter



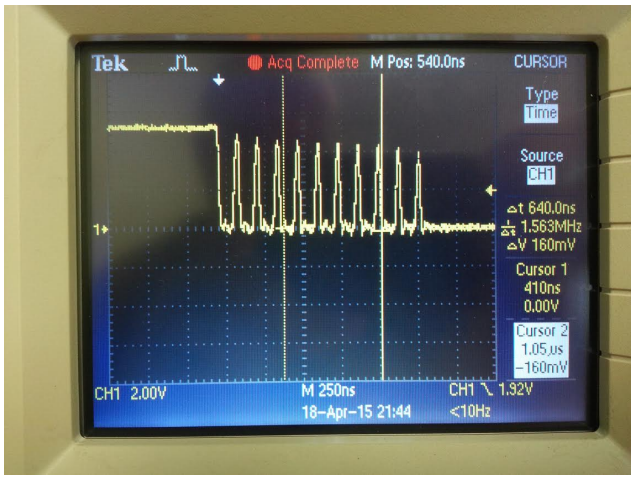
- $R^0_{d,n} = 0, R^1_{d,n} = 0$ – stable one
- $R^0_{d,n} = 1, R^1_{d,n} = 0$ – stable zero
- $R^0_{d,n} = 1, R^1_{d,n} = 1$ – high frequency oscillation (HFO)

Damping oscillation detection

Each metastable output is unique and repeatable for particular challenge:

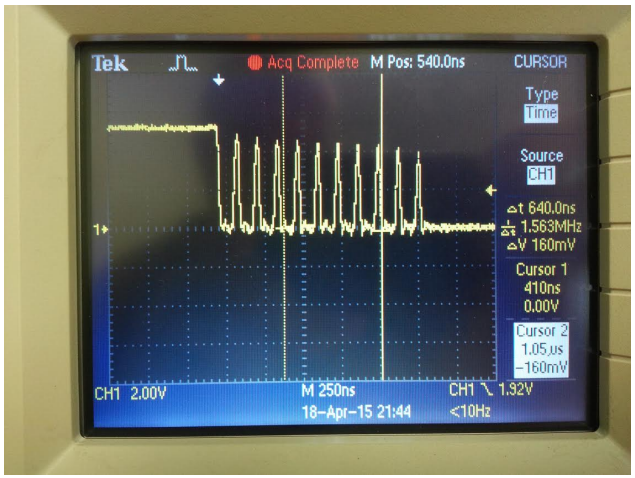
Damping oscillation detection

Each metastable output is unique and repeatable for particular challenge:



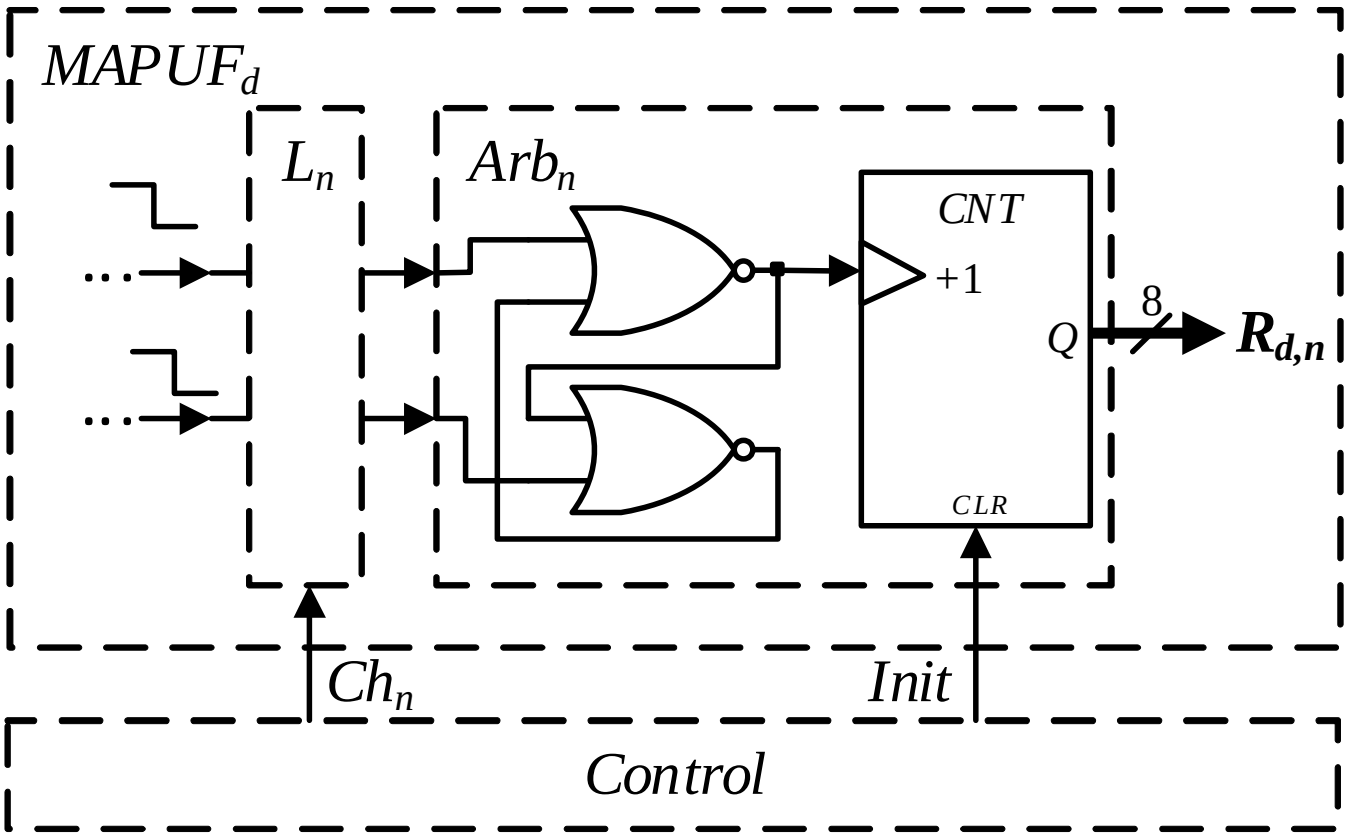
Damping oscillation detection

Each metastable output is unique and repeatable for particular challenge:



The frequency can be roughly measured by a counter.

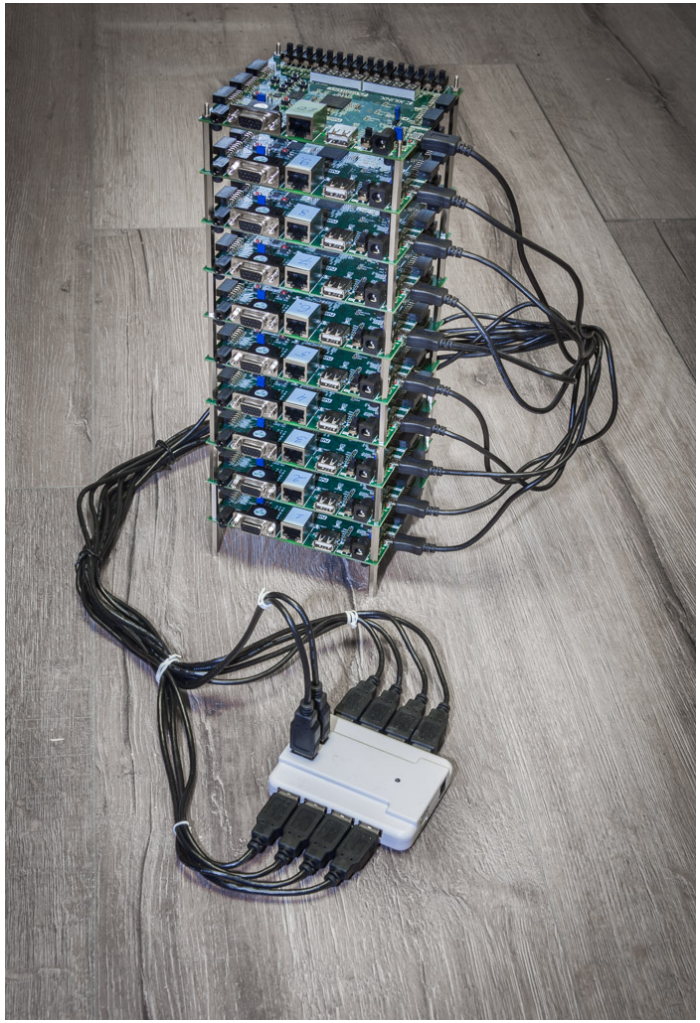
SR latch based arbiter with a counter



* T. Kacprzak "Analysis of Oscillatory Metastable of an RS Flip-Flop", IEEE SSC (Journal), February 1988

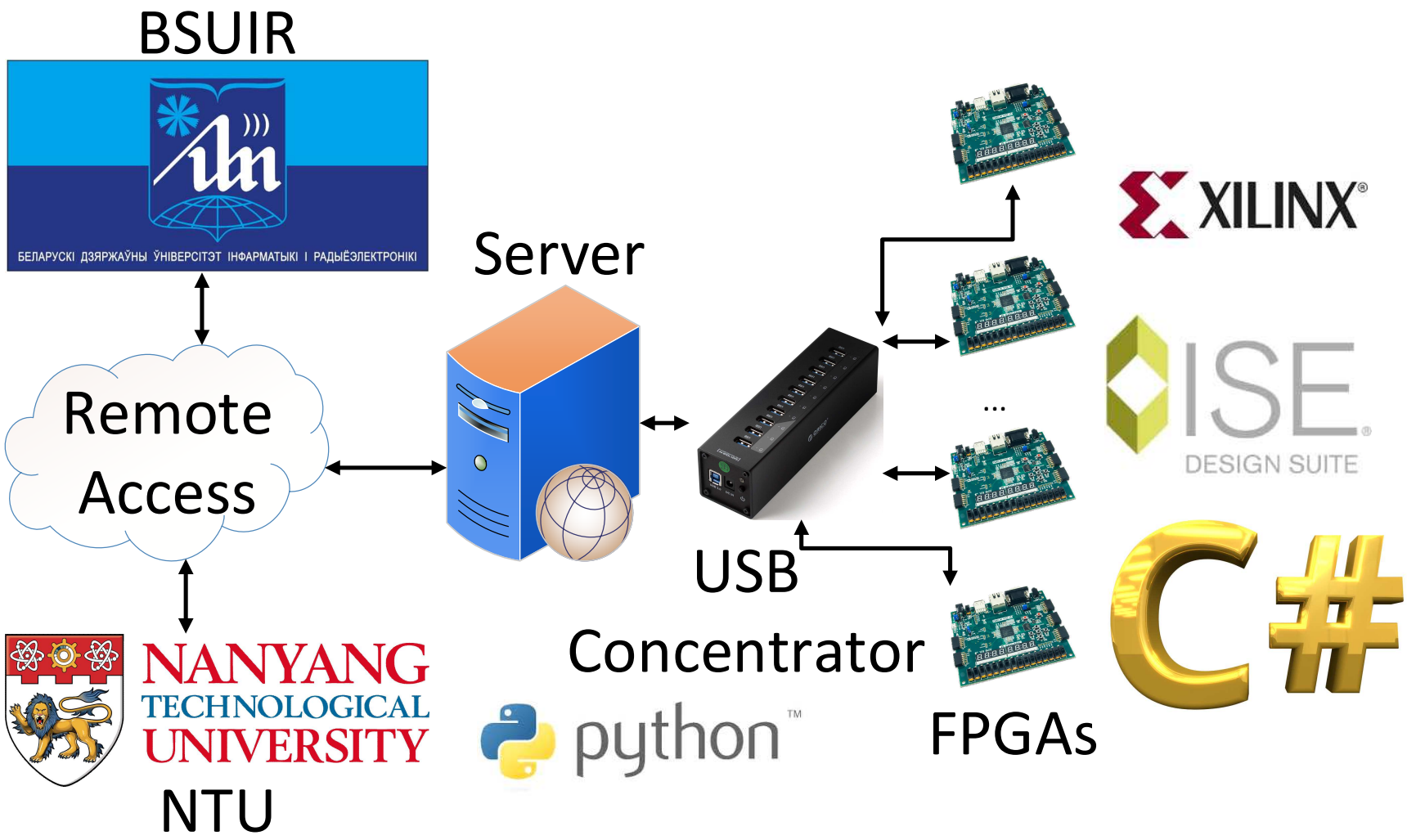
Experimental Results

Experimental equipment



- 10 Digilent Nexys-4 Artix-7 FPGA boards.
- Data transferred via UART interface.
- CAD Xilinx ISE 14.7.
- Scripts in C# and Python.
- 30 experiments with 10,000 challenges applied.

Experiment Structure



Figures of merit for PUF designs

- Uniqueness.
- Reliability.
- Randomness.

Figures of merit for PUF designs

- Uniqueness.
- Reliability.
- Randomness.
- Sokal-Michener Distance (similar to Uniqueness).

Experimental results. Uniqueness

- Let R_u and R_v – two n-bit responses generated by *different* PUF instances for the same challenge.
- Uniqueness for the m PUF instances can be computed by:

$$U = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{n}$$

- The ideal value is 0.5.

Type of arbiter	DFF (Classical)	**4 DFF**	**SR latch**
Uniqueness	0.4898	0.4972	0.4982

Distance metrics modification with respect to metastability

Values	**0**	**1**	***X***
0	0	1	0.5
1	1	0	0.5
X	0.5	0.5	0

Variable	$v_1(i)v_2(i)$
a	11
b	01
c	10
d	00
e	XX
f	$0X$
g	$X0$
h	$1X$
i	$X1$

Distance metrics modification with respect to metastability

Values	**0**	**1**	***X***
0	0	1	0.5
1	1	0	0.5
X	0.5	0.5	0

Variable	$v_1(i)v_2(i)$
a	11
b	01
c	10
d	00
e	XX
f	$0X$
g	$X0$
h	$1X$
i	$X1$

Experimental results. Sokal-Michener distance

- This is also a metric to estimate uniqueness.
- Let v_1 and v_2 are two ternary vectors.
- The Sokal-Michener distance can be computed as follows:

$$D_{Sokal-Michener} = \frac{b+c}{m} + \frac{0.5 \cdot (f+g+h+i)}{m} = \frac{2 \cdot (b+c)+f+g+h+i}{2 \cdot m}$$

- The ideal value is 0.5

Type of arbiter	DFF (Classical)	**4 DFF**	**SR latch**
Average	0.4898	0.4971	0.4954
Minimum	0.4854	0.4868	0.4867

Experimental results. Reliability

- Reliability measures the temporal reproducibility of the responses.
- Let R_i is a reference response of size n.
- $E = 30$ tests were done.
- Each element can be computed as follows:

$$R_i = \frac{max(n_0, n_1, n_X)}{n_0 + n_1 + n_X}$$

- Let $R_{i,e}$ is the response at different time e.
- The reliability S can be computed by:

$$S = 1 - BER = 1 - \frac{1}{E} \sum_{e=1}^{E} \frac{HD(R_i, R_{i,e})}{n}$$

Type of arbiter	DFF (Classical)	**4 DFF**	**SR latch**
Average	0.5769	0.9986	0.9985
Minimum	0.5648	0.9979	0.9978

The NIST test results

Test Description	Passed/Total		P-value	
	4-DFF	SR	4-DFF	SR
Frequency (Monobit) Test	100/100	100/100	0.74	0.53
Frequency Test within a Block	100/100	100/100	0.12	0.53
Runs Test	100/100	100/100	0.74	0.12
Test for the Longest Run of Ones in a Block	100/100	100/100	0.53	0.99
Binary Matrix Rank Test	100/100	100/100	0.35	0.91
Discrete Fourier Transform (Spectral) Test	100/100	100/100	0.53	0.21
Non-overlapping Template Matching Test	97/100	98/100	0.73	0.76
Overlapping Template Matching Test	100/100	100/100	0.74	0.91
Maurer's "Universal Statistical" Test	100/100	100/100	0.07	0.02
Serial Test	100/100	100/100	0.21	0.74
Cumulative Sums (Cusum) Test	100/100	100/100	0.12	0.07
Random Excursions Test	10/10	10/10	—	—
Random Excursions Variant Test	10/10	10/10	—	—

Hardware overhead analysis

Component	# slice LUTs	# slice registers
A-PUF	256 / 63400	1 / 126800
MA-PUF	298 / 63400	128 / 126800
4 DFF	302 / 63400	512 / 126800
SR latch	506 / 63400	256 / 126800
Entire system	2494 / 63400	1263 / 126800

Hardware overhead analysis

Component	# slice LUTs	# slice registers
A-PUF	256 / 63400	1 / 126800
MA-PUF	298 / 63400	128 / 126800
4 DFF	302 / 63400	512 / 126800
SR latch	506 / 63400	256 / 126800
Entire system	2494 / 63400	1263 / 126800

- Less than 0.4% of logic slices and 0.4% of registers.

Hardware overhead analysis

Component	# slice LUTs	# slice registers
A-PUF	256 / 63400	1 / 126800
MA-PUF	298 / 63400	128 / 126800
4 DFF	302 / 63400	512 / 126800
SR latch	506 / 63400	256 / 126800
Entire system	2494 / 63400	1263 / 126800

- Less than 0.4% of logic slices and 0.4% of registers.
- Flexibility to choose different arbiter outputs.

Correlations analysis

Arb_i	121	122	123	124	125	126	127	128
121		-0.08	0.23	0.00	-0.10	0.12	-0.09	0.13
122	-0.08		-0.01	-0.01	0.02	-0.00	-0.02	-0.03
123	0.23	-0.01		0.00	-0.06	0.08	0.08	0.09
124	0.00	-0.01	0.00		0.01	-0.04	-0.01	-0.03
125	-0.10	0.02	-0.06	0.01		-0.01	-0.00	0.00
126	0.12	-0.00	0.08	-0.04	-0.01		0.01	0.01
127	0.09	-0.02	0.08	-0.01	-0.00	0.01		0.00
128	0.13	-0.03	0.09	-0.03	0.00	0.01	0.00	

Correlations analysis

Arb_i	121	122	123	124	125	126	127	128
121		-0.08	0.23	0.00	-0.10	0.12	-0.09	0.13
122	-0.08		-0.01	-0.01	0.02	-0.00	-0.02	-0.03
123	0.23	-0.01		0.00	-0.06	0.08	0.08	0.09
124	0.00	-0.01	0.00		0.01	-0.04	-0.01	-0.03
125	-0.10	0.02	-0.06	0.01		-0.01	-0.00	0.00
126	0.12	-0.00	0.08	-0.04	-0.01		0.01	0.01
127	0.09	-0.02	0.08	-0.01	-0.00	0.01		0.00
128	0.13	-0.03	0.09	-0.03	0.00	0.01	0.00	

- The average correlation per Arbiter is 29 out of 128.

Correlations analysis

Arb_i	121	122	123	124	125	126	127	128
121		-0.08	0.23	0.00	-0.10	0.12	-0.09	0.13
122	-0.08		-0.01	-0.01	0.02	-0.00	-0.02	-0.03
123	0.23	-0.01		0.00	-0.06	0.08	0.08	0.09
124	0.00	-0.01	0.00		0.01	-0.04	-0.01	-0.03
125	-0.10	0.02	-0.06	0.01		-0.01	-0.00	0.00
126	0.12	-0.00	0.08	-0.04	-0.01		0.01	0.01
127	0.09	-0.02	0.08	-0.01	-0.00	0.01		0.00
128	0.13	-0.03	0.09	-0.03	0.00	0.01	0.00	

- The average correlation per Arbiter is 29 out of 128.
- The minimum – 3 out of 128.

Correlations analysis

Arb_i	121	122	123	124	125	126	127	128
121		-0.08	0.23	0.00	-0.10	0.12	-0.09	0.13
122	-0.08		-0.01	-0.01	0.02	-0.00	-0.02	-0.03
123	0.23	-0.01		0.00	-0.06	0.08	0.08	0.09
124	0.00	-0.01	0.00		0.01	-0.04	-0.01	-0.03
125	-0.10	0.02	-0.06	0.01		-0.01	-0.00	0.00
126	0.12	-0.00	0.08	-0.04	-0.01		0.01	0.01
127	0.09	-0.02	0.08	-0.01	-0.00	0.01		0.00
128	0.13	-0.03	0.09	-0.03	0.00	0.01	0.00	

- The average correlation per Arbiter is 29 out of 128.
- The minimum – 3 out of 128.
- The maximum – 78 out of 128.

Conclusion and future works

Contributions

- Reconfigurable multi-response A-PUF design with enhanced response alphabet.
- Two metastability detection techniques.
- Adopted PUF figures of merit.

Future works

- Simulate proposed design on ASIC platform.
- Test the PUF under varying operational conditions.
- Check the vulnerability to modeling attacks (machine learning attacks).
- Arbiter choosing algorithm considering correlation.
- Develop the high level concept of metastability detection.

Thanks and Q & A