POLYMORPHIC PUF

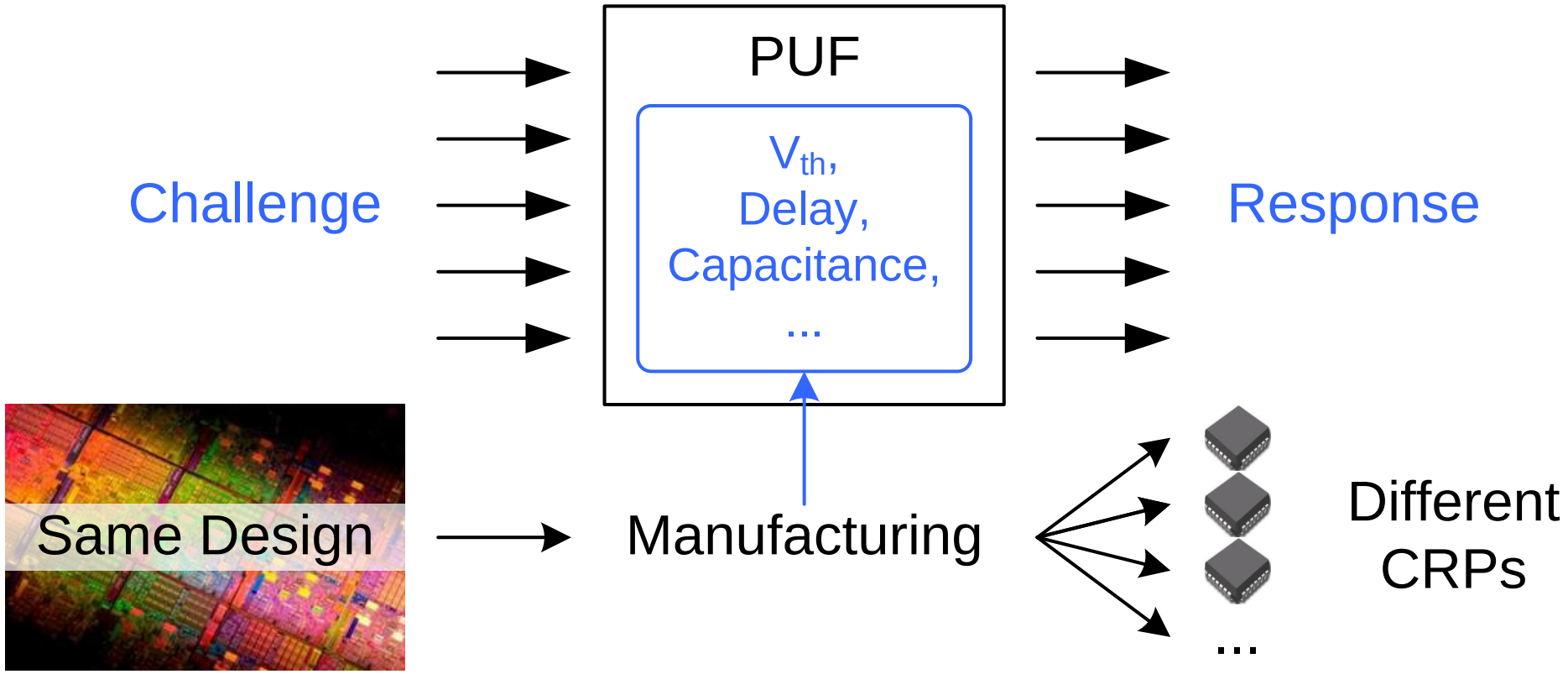
Exploiting Reconfigurability of CPU+FPGA SoC to Resist Modeling Attack

Jing Ye, Yue Gong, Yu Hu, Xiaowei Li

State Key Laboratory of Computer Architecture
Institute of Computing Technology
Chinese Academy of Sciences

Physical Unclonable Function

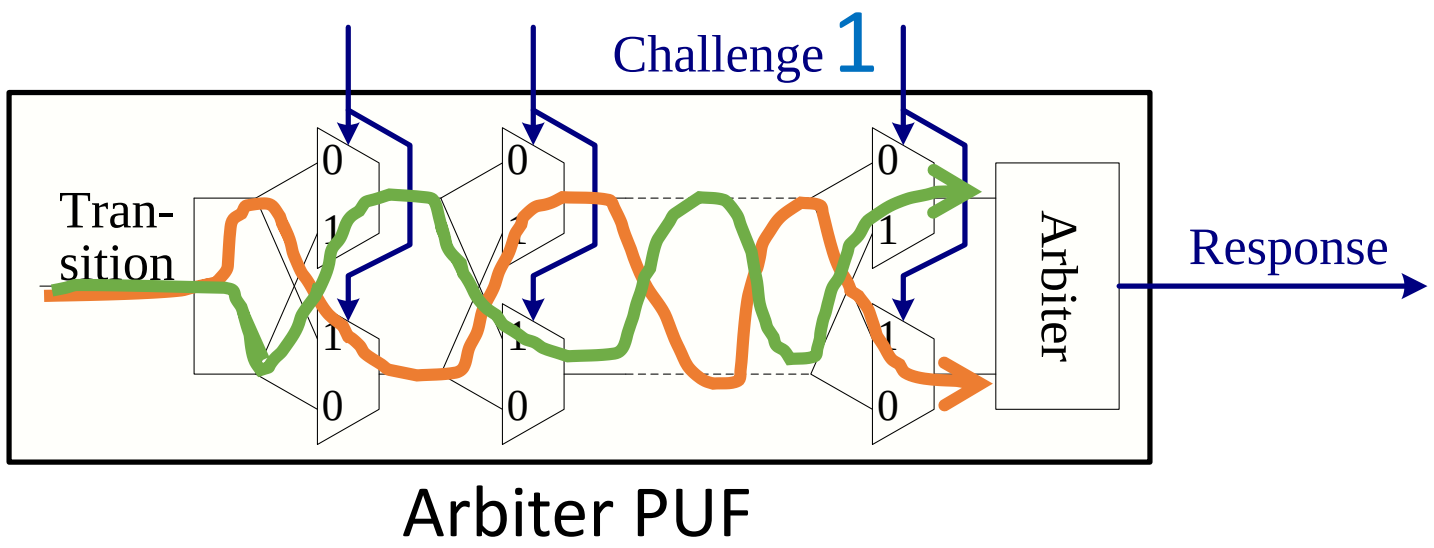
PUF is a hardware security primitive, which exploits the random process variations to produce particular **Challenge-Response Pairs (CRPs)**



Strong PUF

Strong PUF has **numerous CRPs**

n-bit challenge: 2^n CRPs

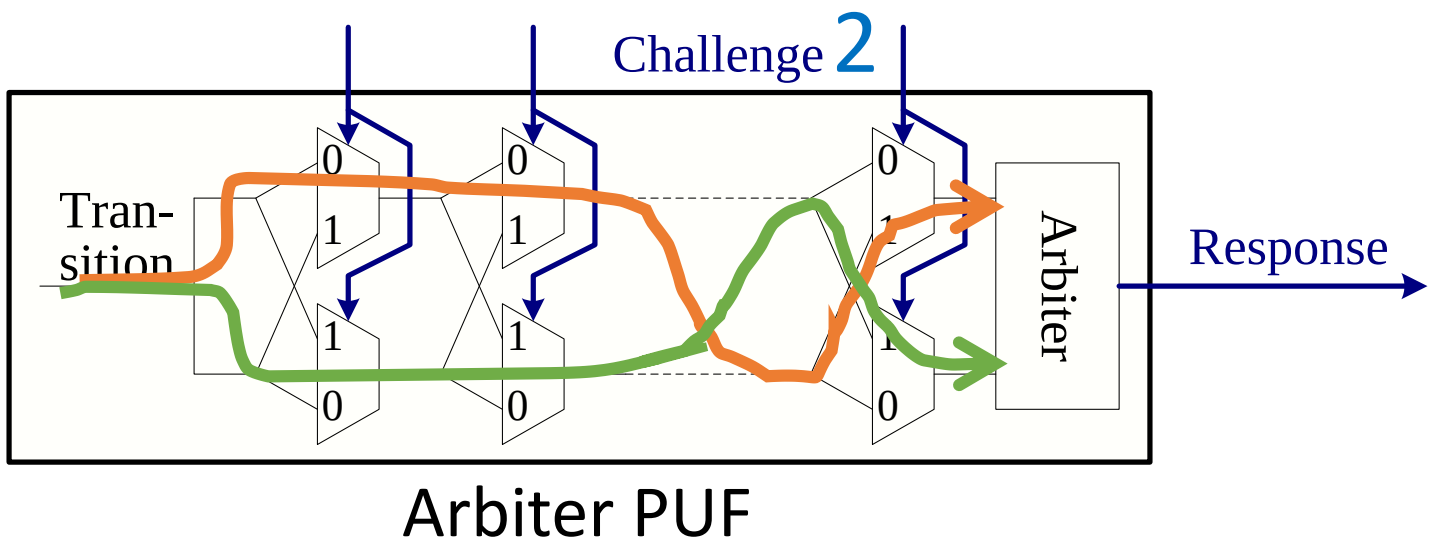


Arbiter PUF

Strong PUF

Strong PUF has **numerous CRPs**

n-bit challenge: 2^n CRPs



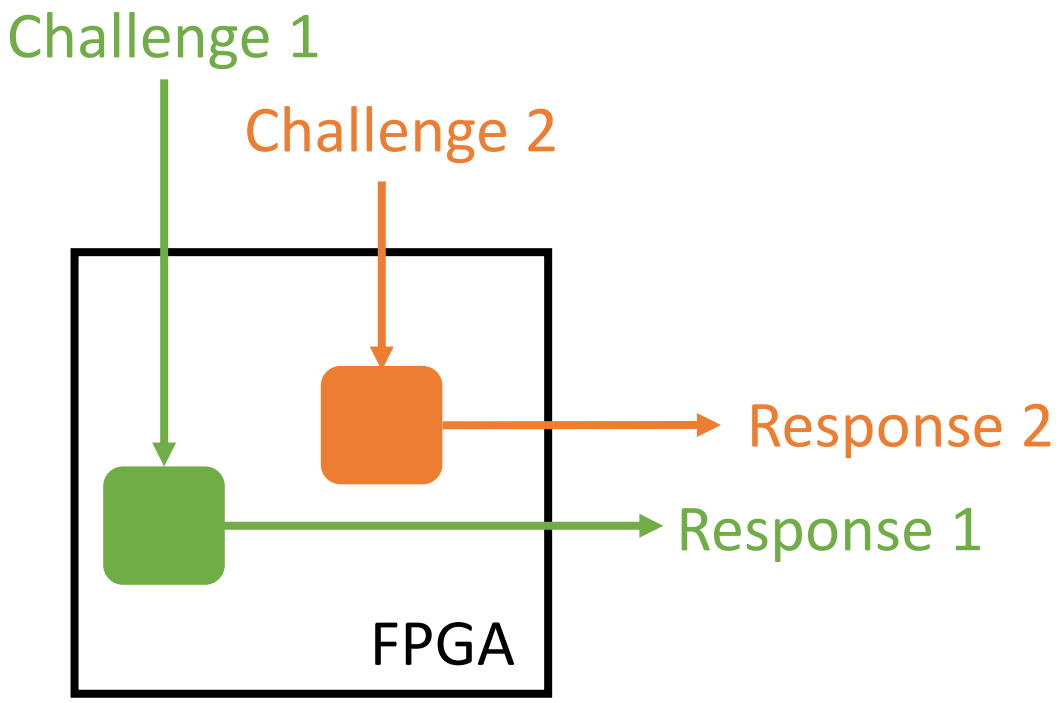
Arbiter PUF

Numerous CRPs **share** a small number of path segments

Surrender to
machine learning based modeling attacks

Strong PUF based on FPGA Reconfigurability

For **different challenges**, **different circuits** are implemented in the FPGA to produce the responses [1-4].



Advantage:

Reducing the correlation among CRPs to **resist modeling attack**

~~**Contribution:**~~

~~Constraints of LUTs and routing~~ for generating CRPs to better resist modeling attack.

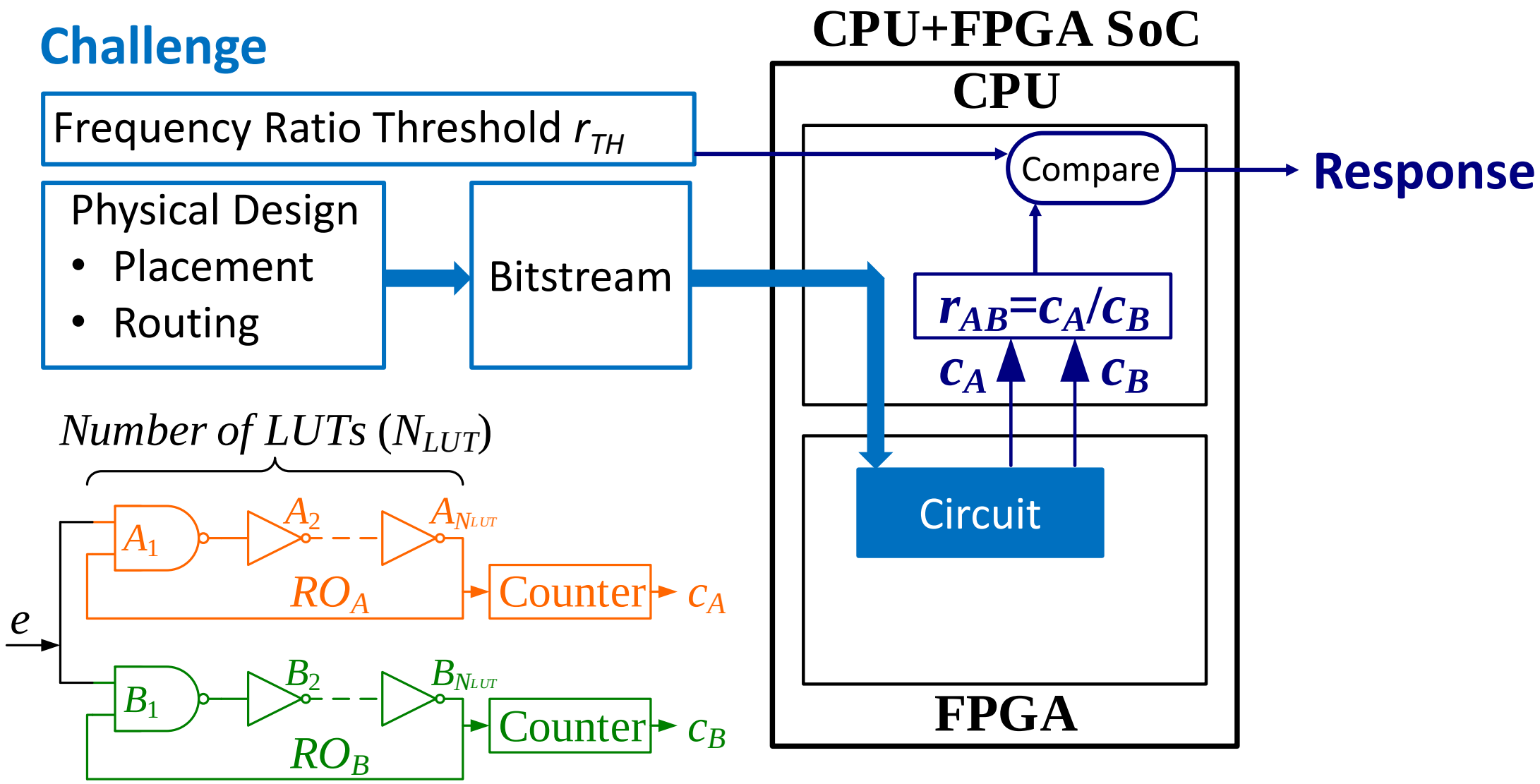
Cost: Increasing the CRP data

[1] G. E. Suh, S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," DAC, 2007.
[2] S. Gehrer, G. Sigl, "Using the Reconfigurability of Modern FPGAs for Highly Efficient PUF-Based Key Generation," ReCoSoC, 2015.
[3] J. Ye, Y. Hu, X. Li, "DCPUF: Placement and Routing Constraint based Dynamically Configured Physical Unclonable Function on FPGA," FPGA, 2016.
[4] A. Spenke, R. Breithaupt, R. Plaga, "An arbiter PUF secured by remote random reconfigurations of an FPGA," Trust and Trustworthy Computing, 2016.

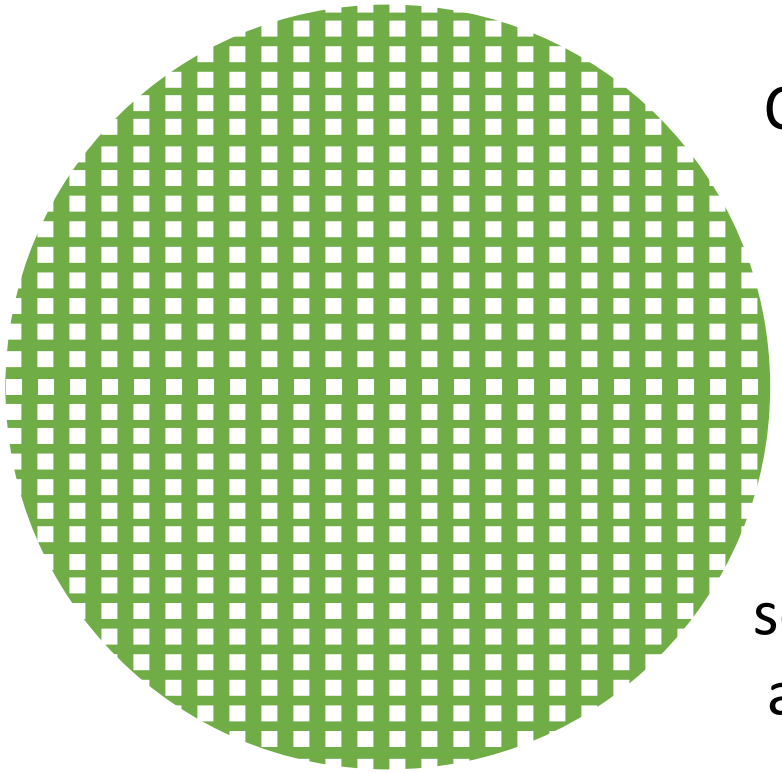
Outline

- ✓ Background and Motivation
- ☐ **Polymorphic PUF**
- ☐ Experimental Results

Polymorphic PUF



Frequency Ratio Threshold



Challenges (Physical Design)

Randomly select some as samples

Frequency Ratios

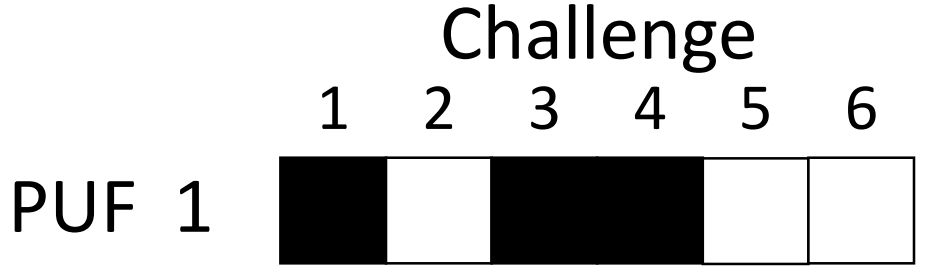
Achieve good uniformity & uniqueness

Frequency Ratio Thresholds

Frequency Ratio Threshold

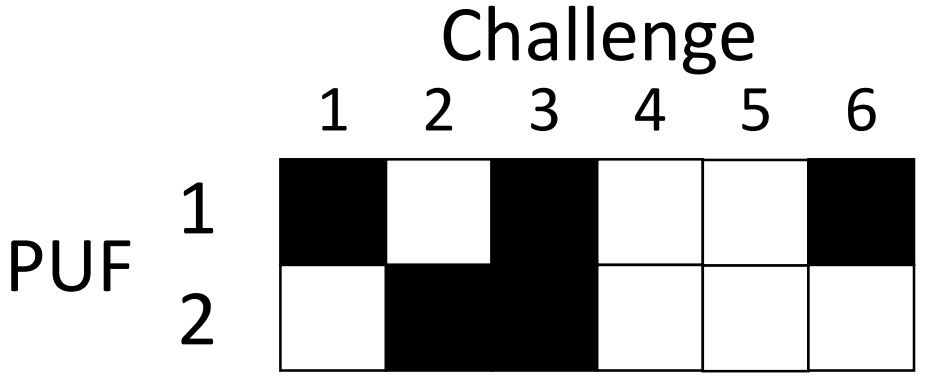
Response=0 Response=1

Uniformity



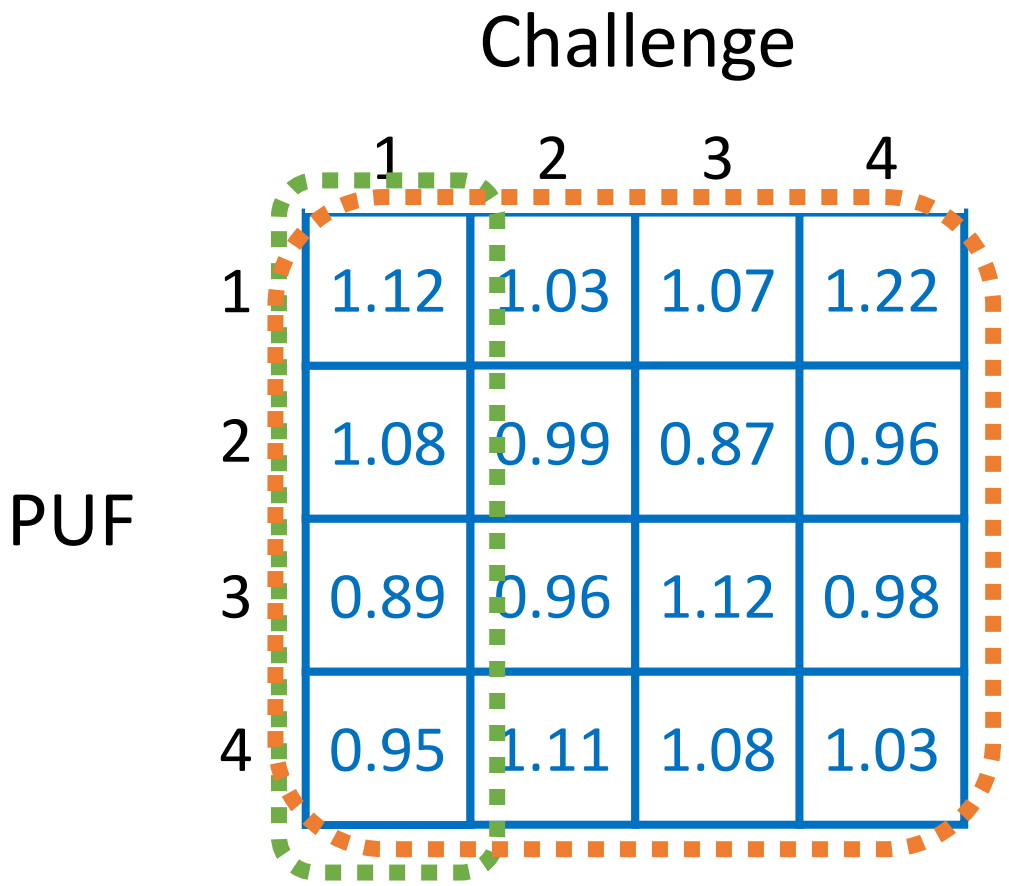
Ideal:
1s%=50%

Uniqueness



Ideal:
Different%=50%

Frequency Ratio Threshold



Frequency Ratio r_{AB}

Dependently calculate all challenge's

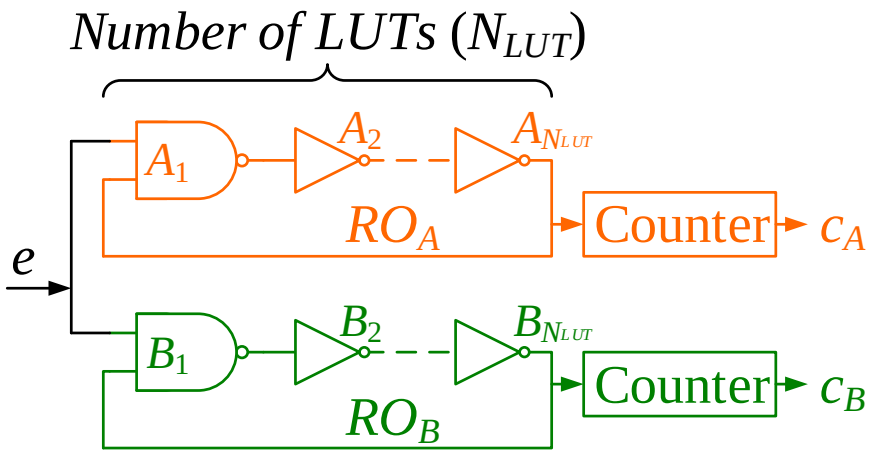
Thresholds : Heuristically Adjusted

Simulated annealing algorithm for achieving uniformity and uniqueness as good as possible

Independently calculate each challenge's

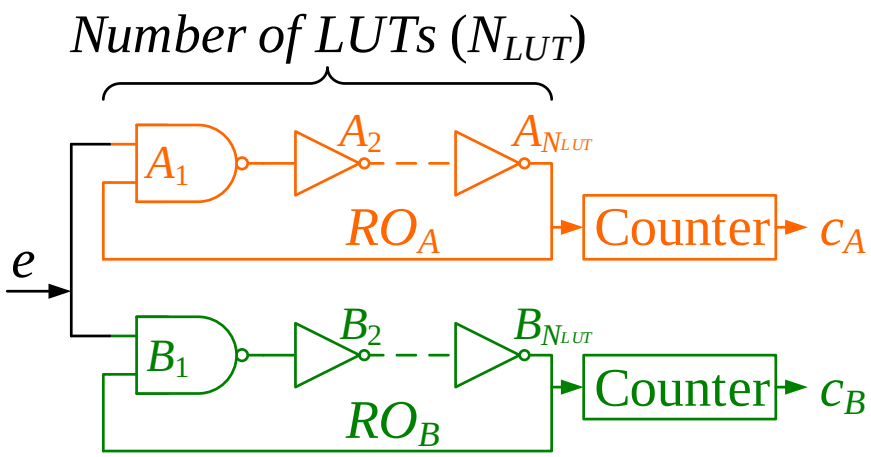
Threshold : Average Value

Challenge Space

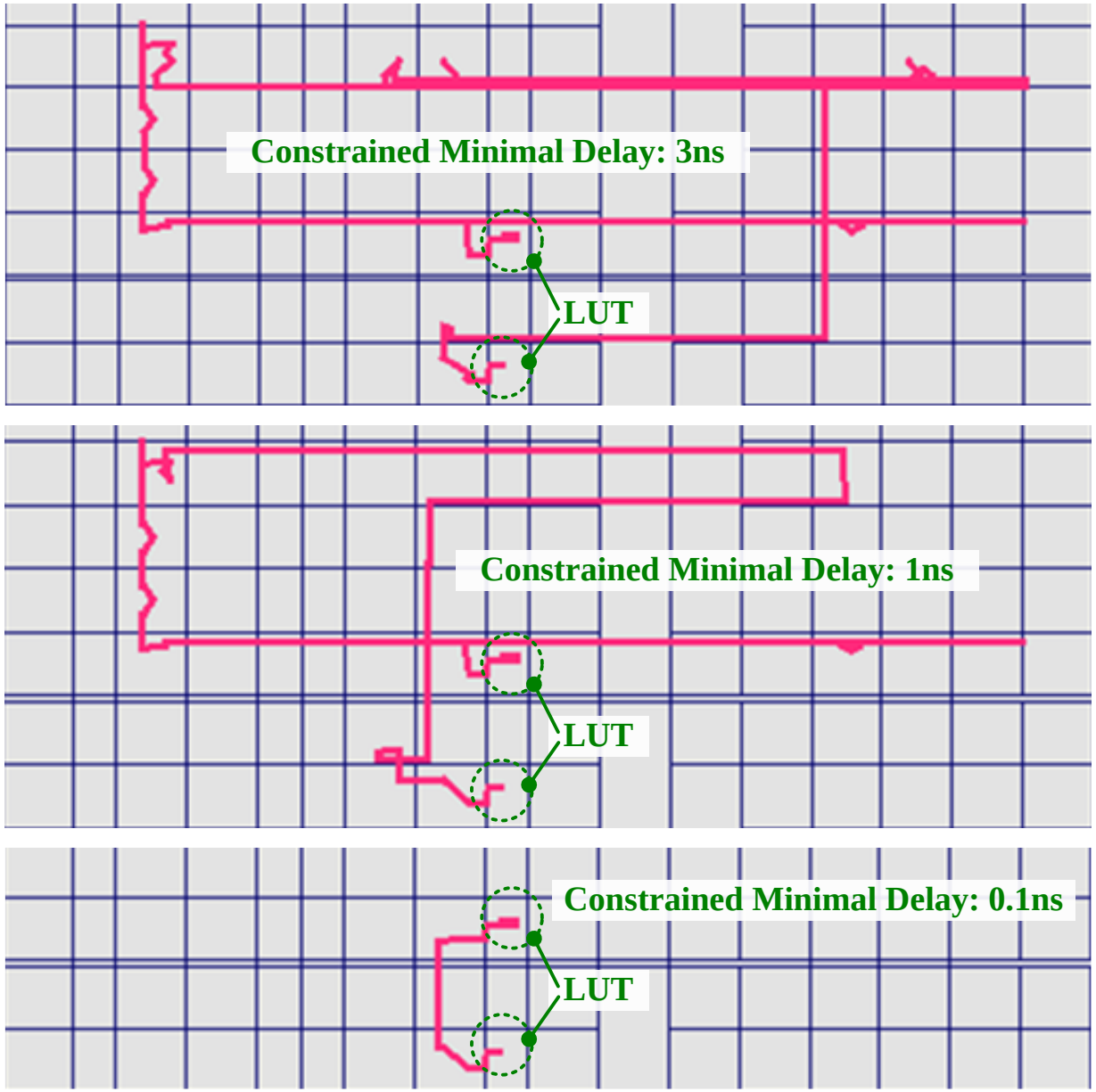


- N_{LUT}
- Placement
- Routing
  - Delays of wires are normally larger than those of LUTs in FPGA

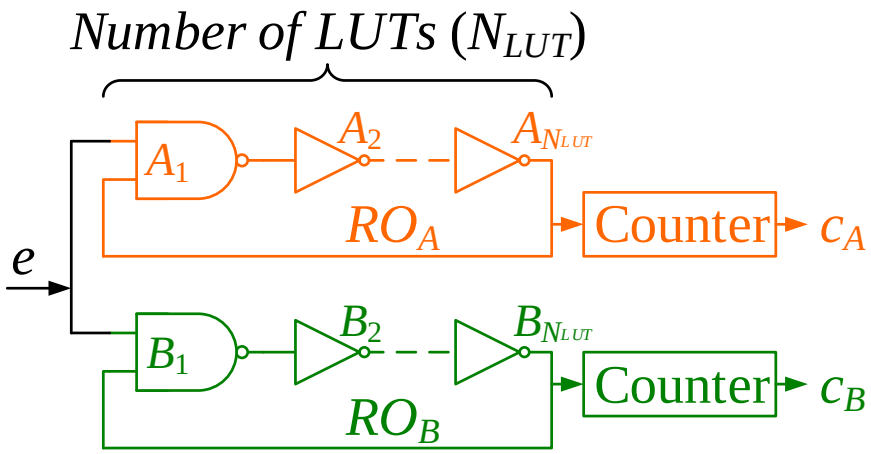
Challenge Space



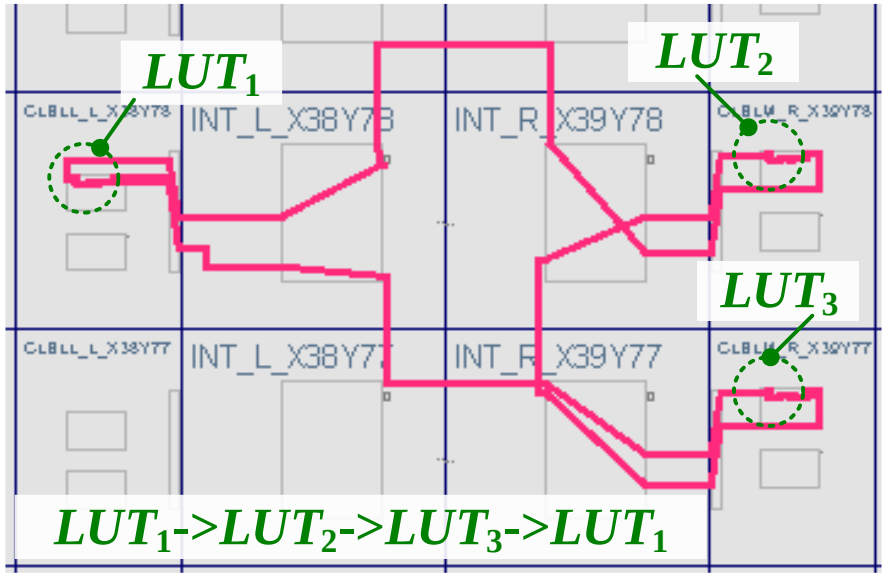
- N_{LUT}
- Placement
- Routing
  - Delays of wires are normally larger than those of LUTs in FPGA
  - There are many different routing ways to connect the same two LUTs

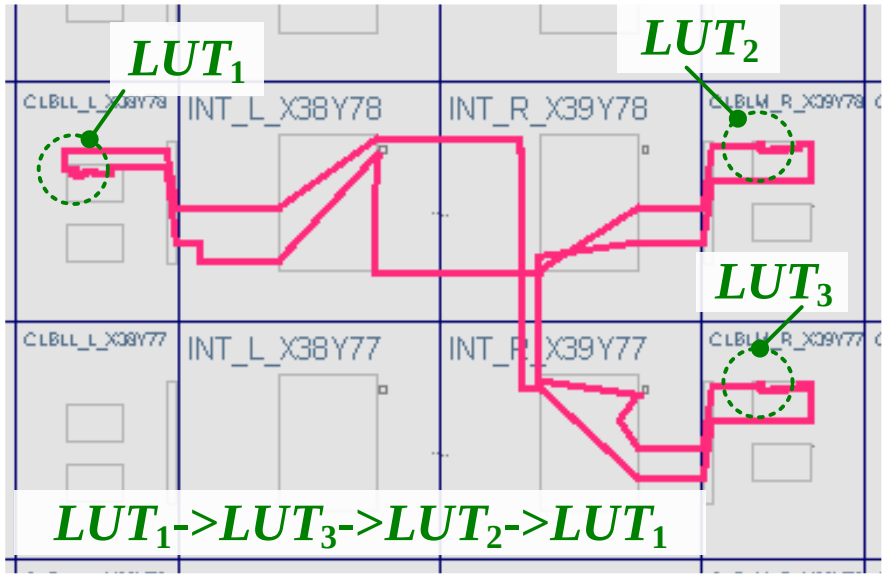


Challenge Space



- N_{LUT}
- Placement
- Routing
  - Delays of wires are normally larger than those of LUTs in FPGA
  - There are many different routing ways to connect the same two LUTs.
  - LUTs with different connection order have different routings.





Outline

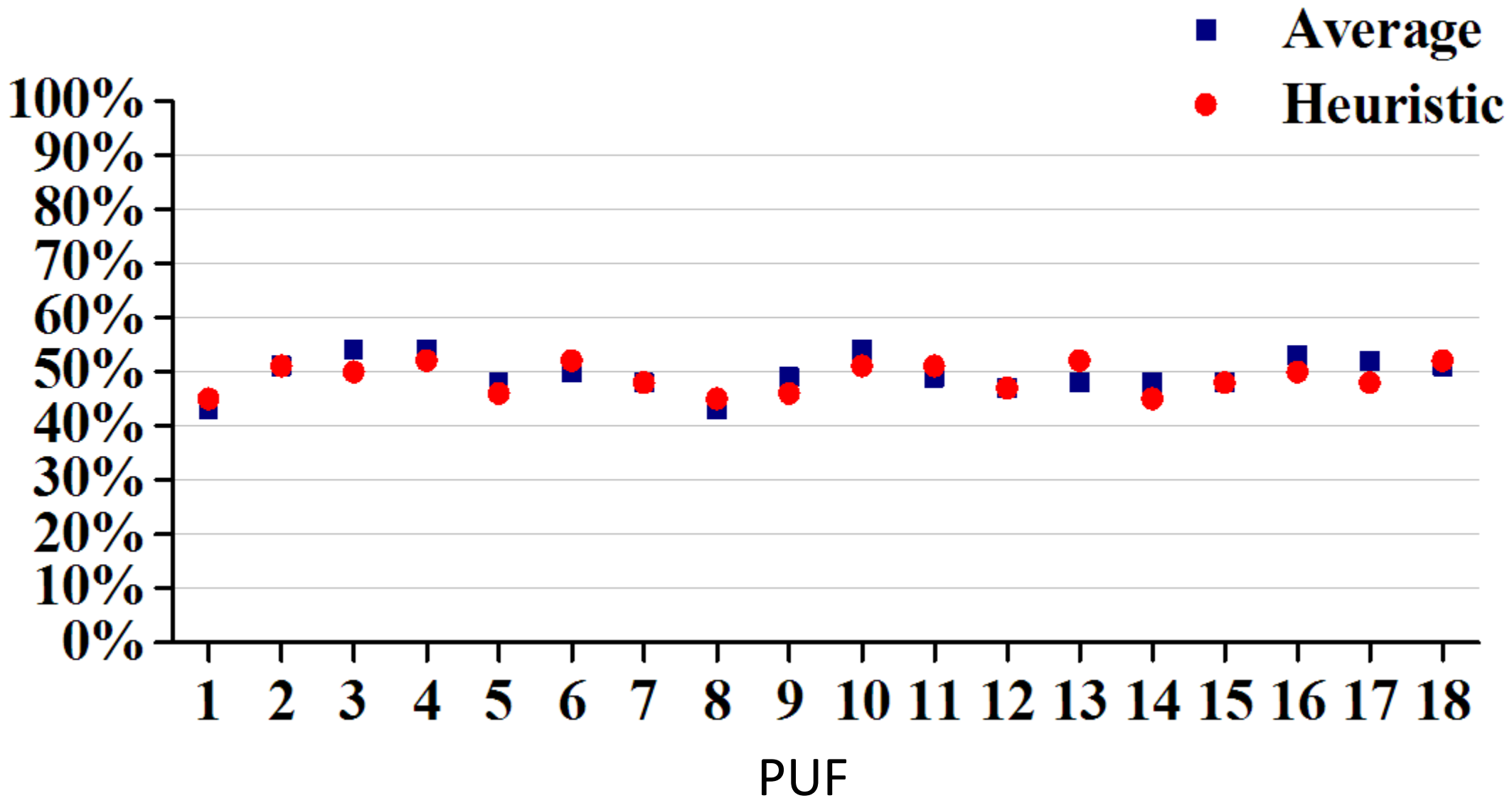
- ✓ Background and Motivation
- ✓ Polymorphic PUF
- ☐ **Experimental Results**

Experimental Results

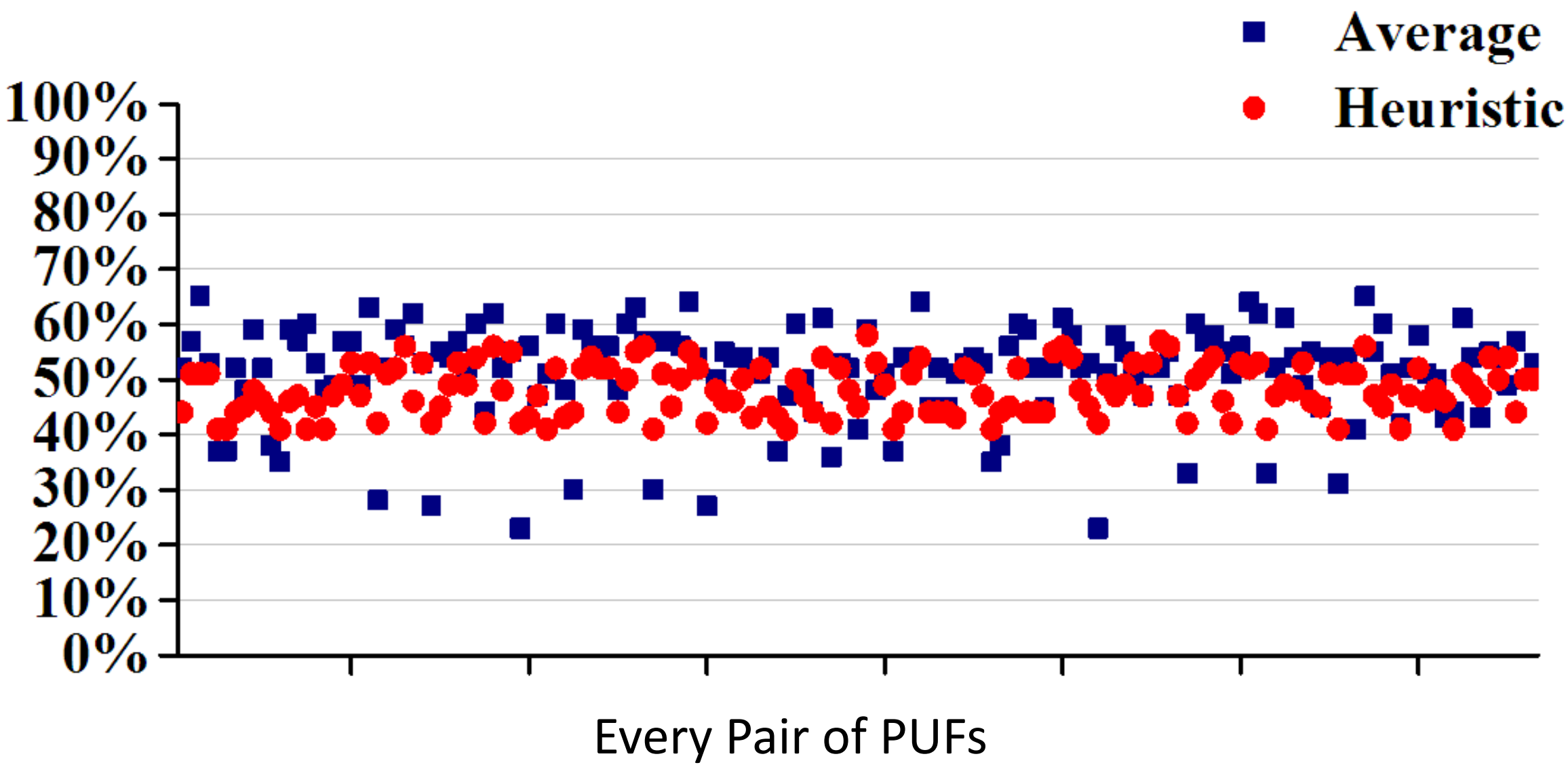
Experimental Setup

- Xilinx Zynq7000 Z-7020 SoC
- N_{LUT}=3
- 128000 RO Pairs
- 18 Polymorphic PUFs

Uniformity

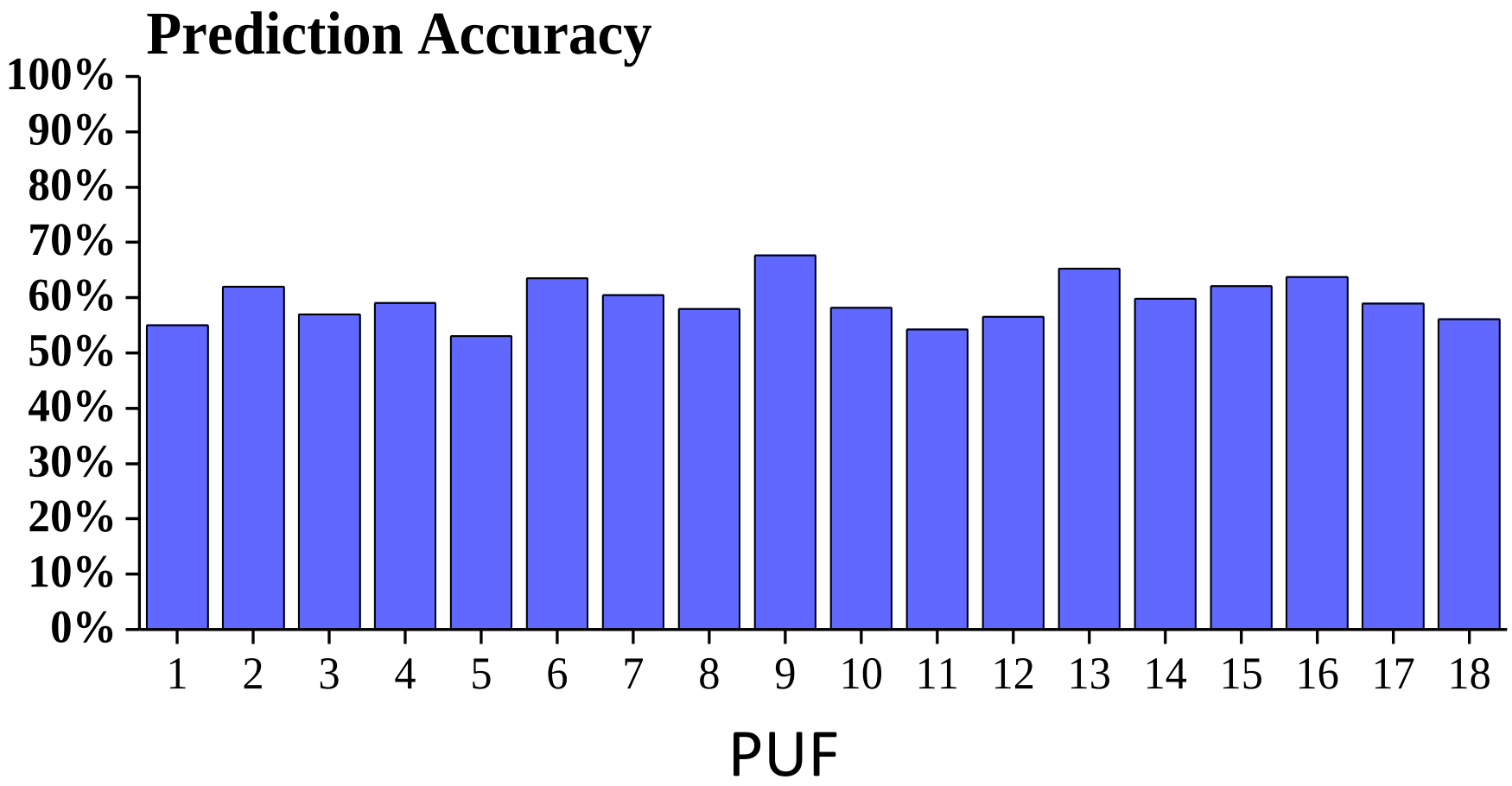

Average
Heuristic
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
PUF

Uniqueness


Average
Heuristic
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Every Pair of PUFs

Modeling Attack Resistance

$$r_{AB} = \frac{\sum Delay\ of\ \ LUT\ in\ RO_A + \sum Delay\ of\ Wire\ in\ RO_A}{\sum Delay\ of\ \ LUT\ in\ RO_B + \sum Delay\ of\ Wire\ in\ RO_B}$$



Conclusion

- An asymmetric RO pair circuit is proposed to produce the response bit.
- No placement and routing constraints exist.
- Good uniformity, uniqueness, and modeling attack resistance are achieved.

Thank You
Q&A