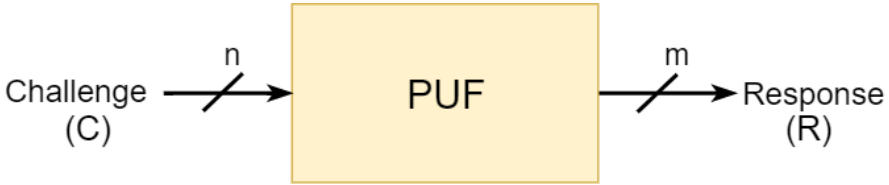
Formal Analysis of PUF Instances Leveraging Correlation Spectra in Boolean Functions

Durba Chatterjee, Aritra Hazra, Debdeep Mukhopadhyay
IIT Kharagpur, India

Presented By: Durba Chatterjee

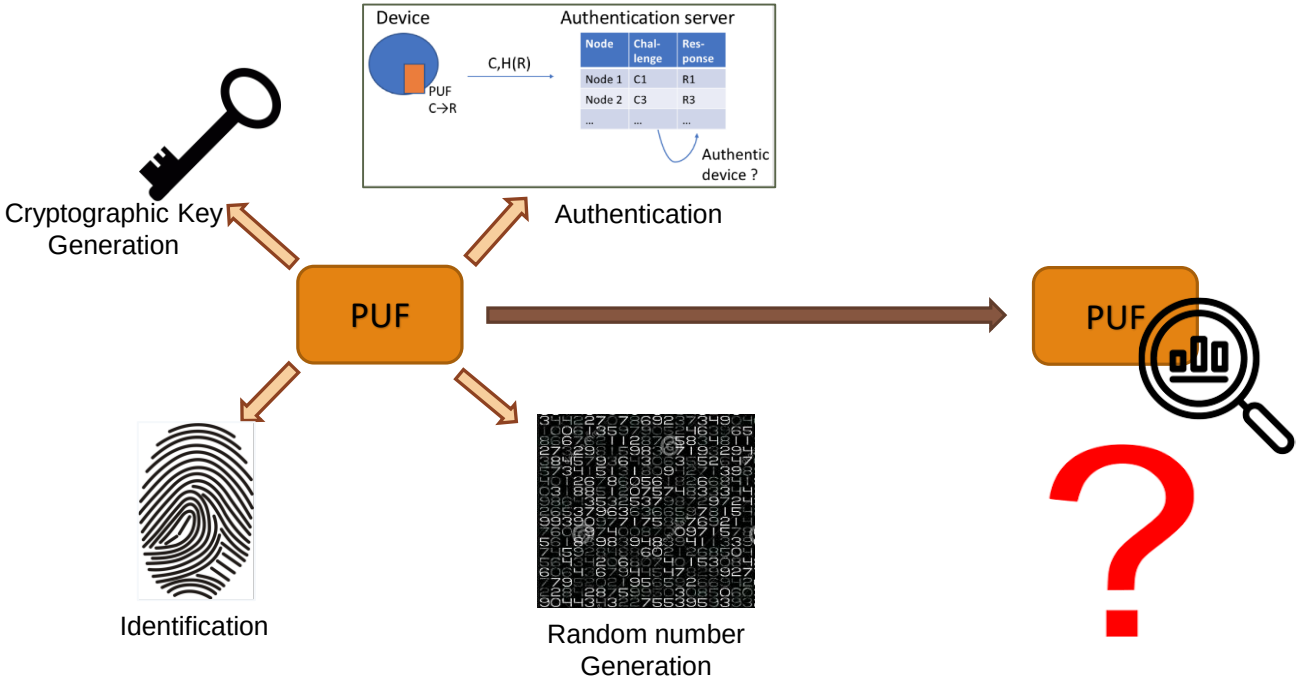
Introduction to Physically Unclonable Function (PUF)

- PUF: Physical mapping from set of challenges (**C**) to corresponding responses (**R**)
- Mapping represented by $\mathbf{f_{PUF}}$: **C**→**R**, where $\mathbf{f_{PUF}}$ (C)=R, C∈**C** and R∈**R**
  - depends on unpredictable instance specific and unclonable behavior
  - unique for every PUF instance and is independent of each other



- PUF can be considered as a black-box Boolean function $\mathbf{f_{PUF}}$:$\{0,1\}^n \rightarrow \{0,1\}^m$

PUFs in current scenario



Hurdles in Analysis of PUFs

- PUF does not have a fixed functionality – no ideal behavior or golden response
- Each instance is unique – Individual analysis not possible
- Difficult to identify any tampering with PUF without additional overhead
- Lack of a theoretical template to analyse PUFs

Formal Analysis Scheme from the perspective of Boolean Functions

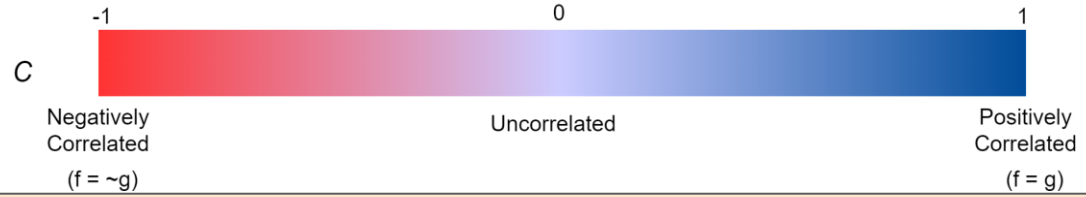
Boolean Functions and Correlation Properties

- Boolean function: A mapping of an assignment of m input variables to {0,1}

$$f: \{0,1\}^m \rightarrow \{0,1\}$$

  - Vector Representation $\boldsymbol{f} = < f_0, f_1, \ldots, f_{2^m-1} >$
- Cross correlation[1] is a measure of similarity between two functions $\boldsymbol{f}$ and $\boldsymbol{g}$ given by

$$C(\boldsymbol{f}, \boldsymbol{g}) = \frac{\sum_{x \in F_2{}^n} (-1)^{\boldsymbol{f}(x) \oplus \boldsymbol{g}(x)}}{2^m}$$



1. Sarkar, P., Maitra, S.:Cross-correlation analysis of cryptographically useful boolean functions and S-boxes. Theory Comput. Syst. 35(1), 39–57 (2002)

Correlation Properties

Given 2 functions $\boldsymbol{f}$ and $\boldsymbol{g}$,

$$C(\boldsymbol{f},\boldsymbol{g}) = \frac{\left(2^m - 2J(\boldsymbol{f},\boldsymbol{g})\right)}{2^m}$$

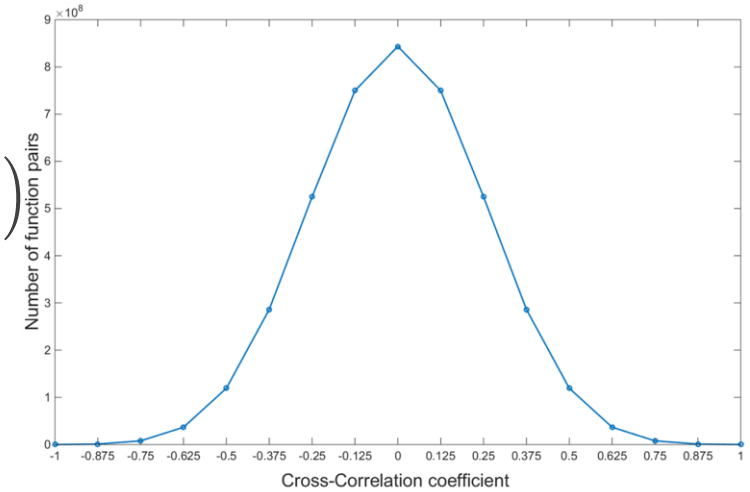
- Hamming distance

$$J(\boldsymbol{f},\boldsymbol{g}) = \frac{2^m(1 - C(\boldsymbol{f},\boldsymbol{g}))}{2}$$

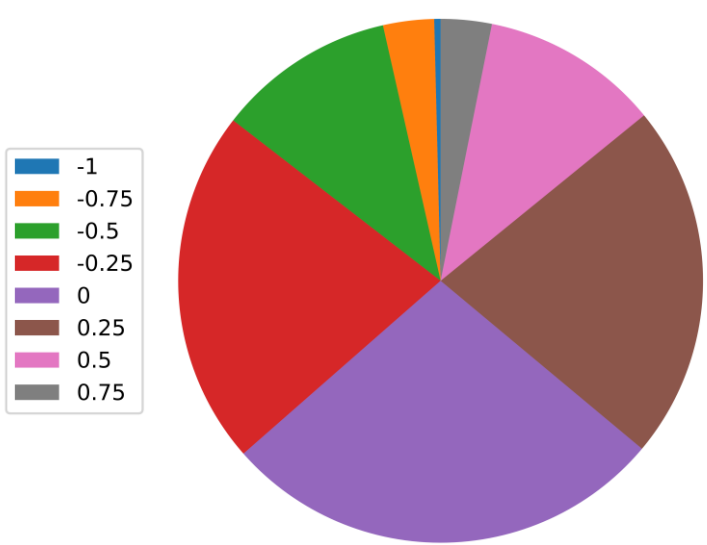
- Number of function pairs with correlation C_α

$$= 2^{2^m-1}\binom{2^m}{J_\alpha} = 2^{2^m-1}\binom{2^m}{2^{m-1}(1-C_\alpha)}$$

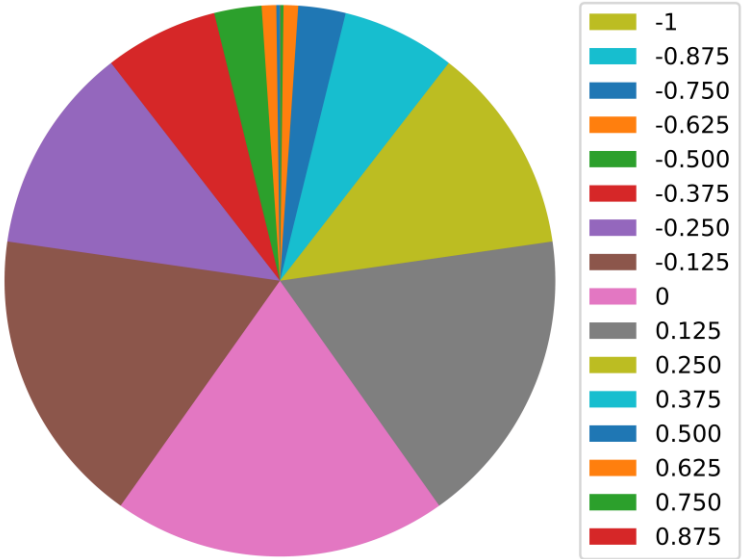
Gaussian distribution



Correlation Spectrum for Boolean Functions



For 3-input Boolean Function



For 4-input Boolean Function

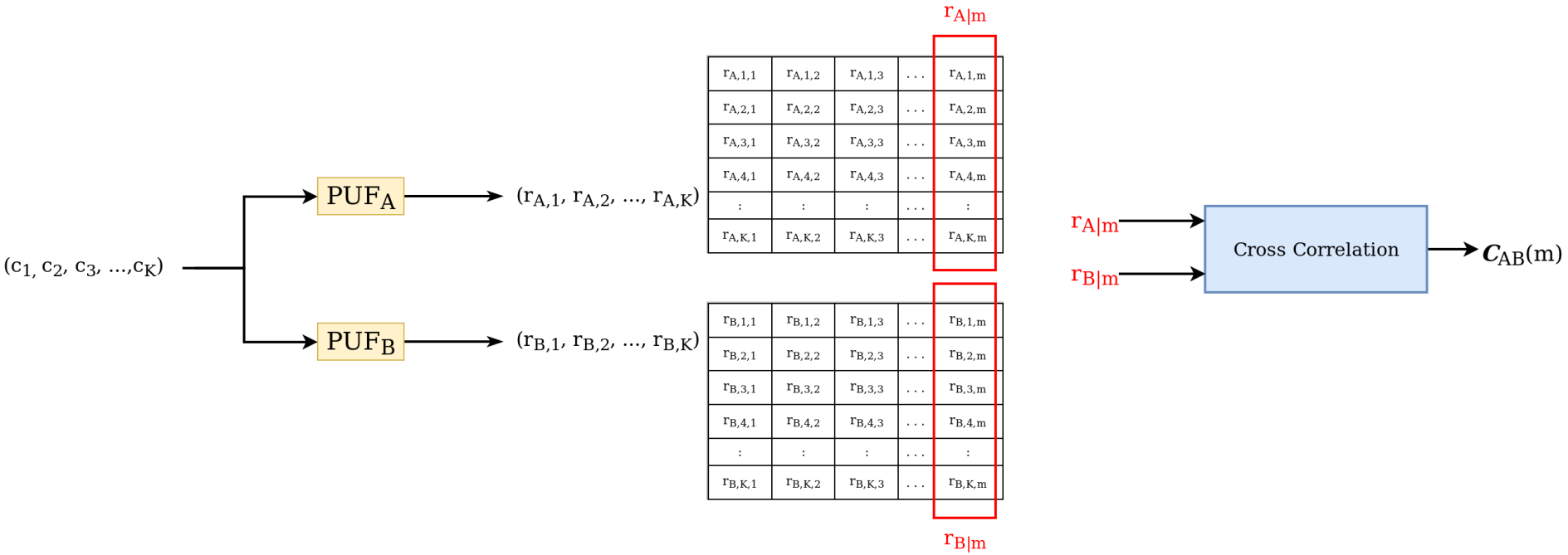
PUF as Boolean Function

- PUF : physical mapping given by

$$f_{PUF}: \{0,1\}^n \rightarrow \{0,1\}^m$$

- For response bit length (m) = 1, find correlation spectrum using response
- For m>1
  - Split response into m 1-bit outputs
  - Find correlation spectra for each bit individually
  - Separate analysis for each bit

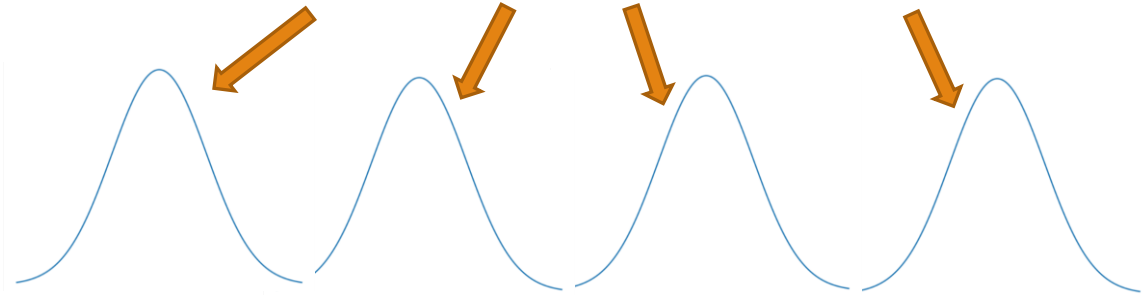
Computing PUF Correlation



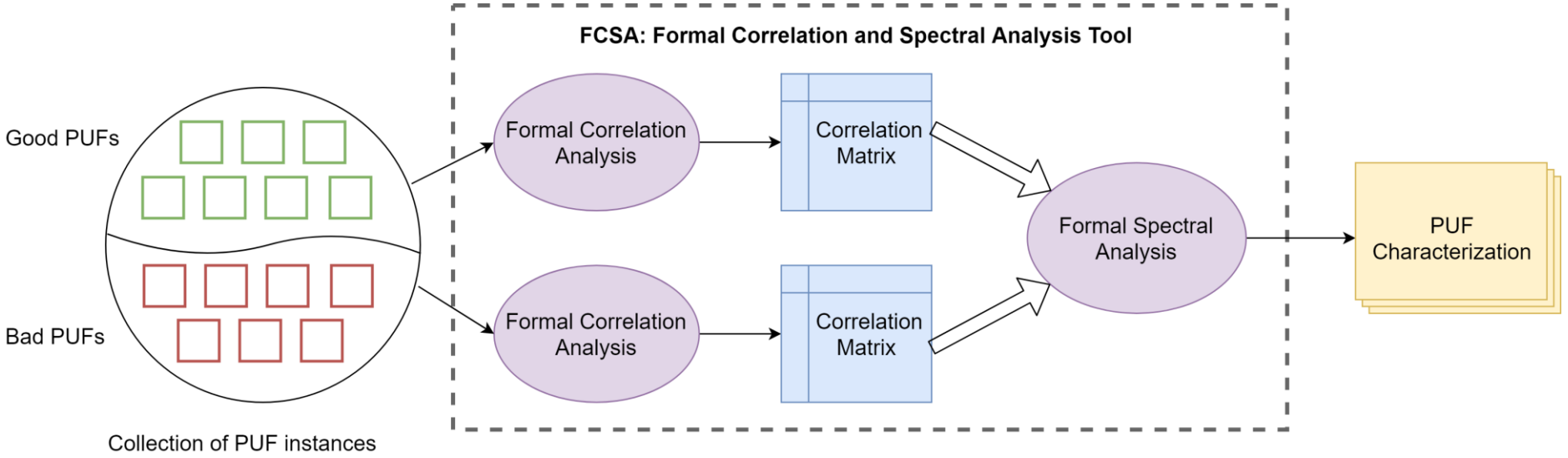
PUF Correlation Spectra

Correlation Matrix:

$C_{P_1}(1)$	$C_{P_1}(2)$	$C_{P_1}(3)$	. . .	$C_{P_1}(m)$
$C_{P_2}(1)$	$C_{P_2}(2)$	$C_{P_2}(3)$	. . .	$C_{P_2}(m)$
$C_{P_3}(1)$	$C_{P_3}(2)$	$C_{P_3}(3)$	. . .	$C_{P_3}(m)$
:	:	:	:	:
$C_{P_{N'}}(1)$	$C_{P_{N'}}(2)$	$C_{P_{N'}}(3)$	. . .	$C_{P_{N'}}(m)$



Formal Correlation and Spectral Analysis Tool (FCSA)

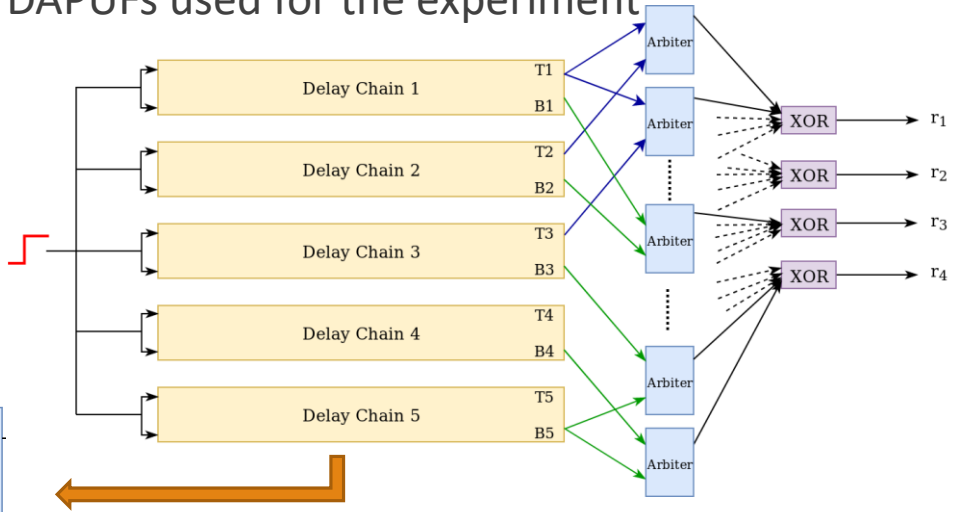


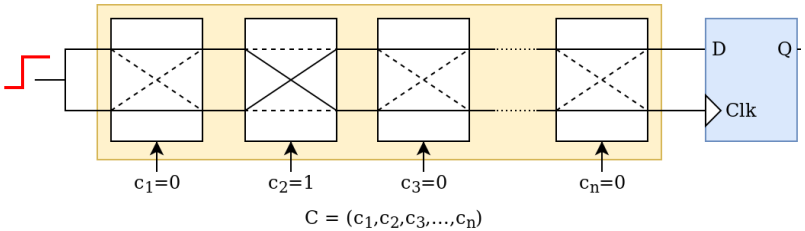
- Uses the correlation theory to distinguish between a collection of *good* and *bad* PUFs
- **Architecture independent scheme – can be used for any PUF class.**

Experimental Setup

- Hardware implementation of 5-4 DAPUFs used for the experiment
- Experiment Parameters:

Challenge Size	64 bits
Response Size	4 bits
Number of challenges	10000
Number of Instances	50





- Stuck at fault is induced at a switch in the delay chains of DAPUF to get a faulty instance.

Experiments performed

1. **Correlation Analysis:**
   - Discretization of correlation values
   - Generating cross-correlation spectra of *good* and *bad* PUF collections
   - Comparison of cross-correlation distribution

2. **Spectral Analysis:**
   - Apply statistical test on cross-correlation spectra

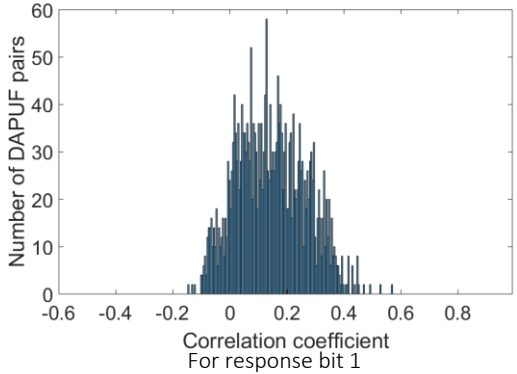
Quality metrics test

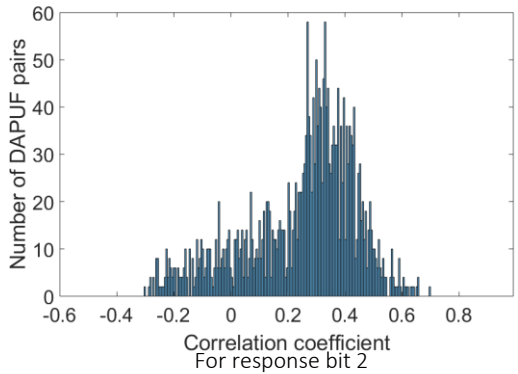
1. **Test using Uniformity:**
   - CRP generation for *good* and *bad* PUF instances
   - Comparison of uniformity metric

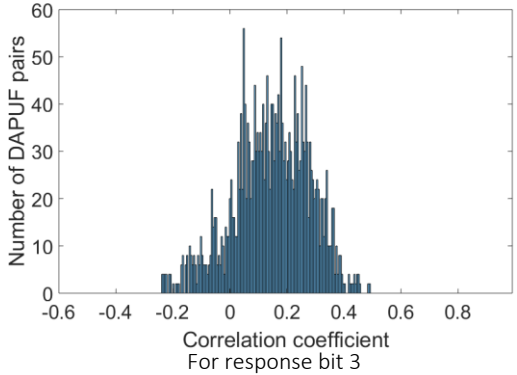
PUF Instance	Uniformity for correct PUF	Uniformity for faulty PUF
1	57.10	53.34
2	56.74	53.38
3	59.66	54.29
4	54.98	54.46
5	56.93	54.47

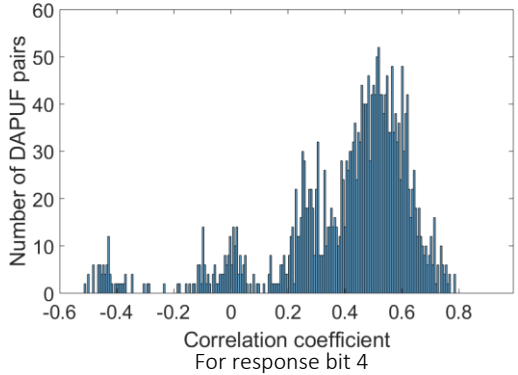
- No significant difference in uniformity

Correlation Spectra of *correct* PUF Instances

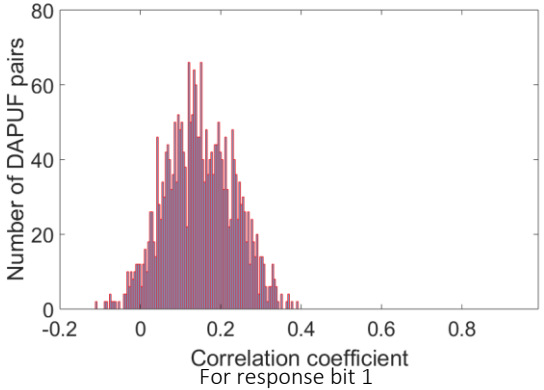


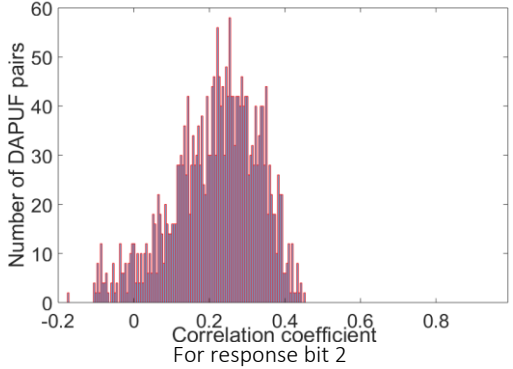


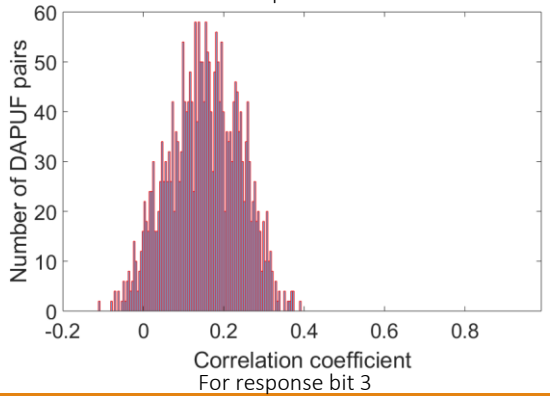


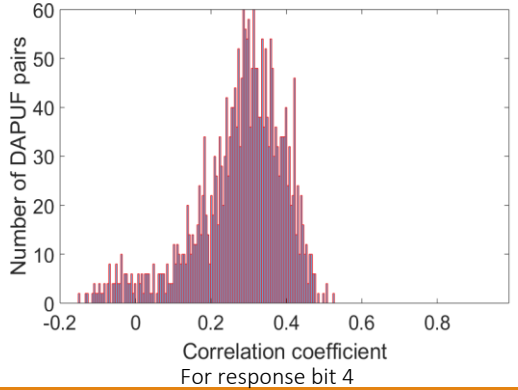


Correlation Spectra of *faulty* PUF Instances





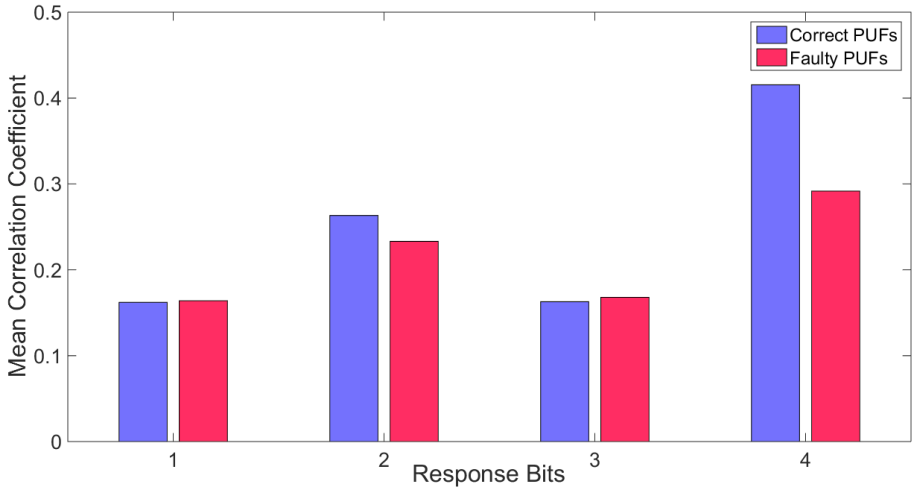


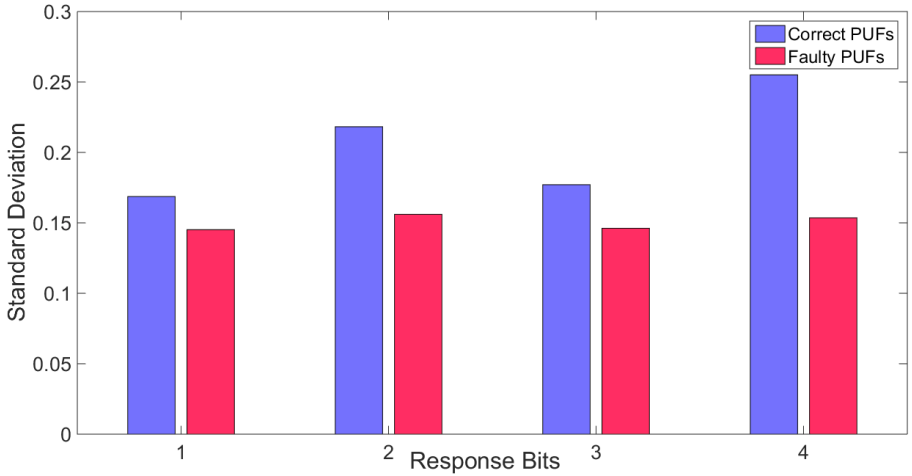


Note: For faulty DAPUF, stuck-at-1 fault is induced at one of the internal switches of delay chain.

Comparative Analysis

- Reduction in the standard deviation of the distribution





Spectral Analysis

- Statistical tests give quantitative value which helps to understand the difference better.
- Kullback-Leibler Divergence $D(Q|P) = \sum_i Q(i) ln\left(\frac{Q(i)}{P(i)}\right)$
  - Reference distribution: Spectra of non-faulty/correct PUFs
  - Distribution under test: Spectra of faulty PUFs
- Larger Divergence value indicates that the distributions are more distant.

KL Divergence	Bit 1	Bit 2	Bit 3	Bit 4
Between faulty and correct distributions	21.97	27.10	22.18	32.50
Between correct and correct distributions	19.75	22.83	22.06	22.77

Conclusion

- Cross-correlation of a sample of PUFs follows Gaussian distribution, similar to a sample of randomly selected Boolean functions.
- Forms a concrete base for analysis of PUF instances.
- A combination of correlation analysis and statistical test can be used during a new PUF characterization.

Thank you