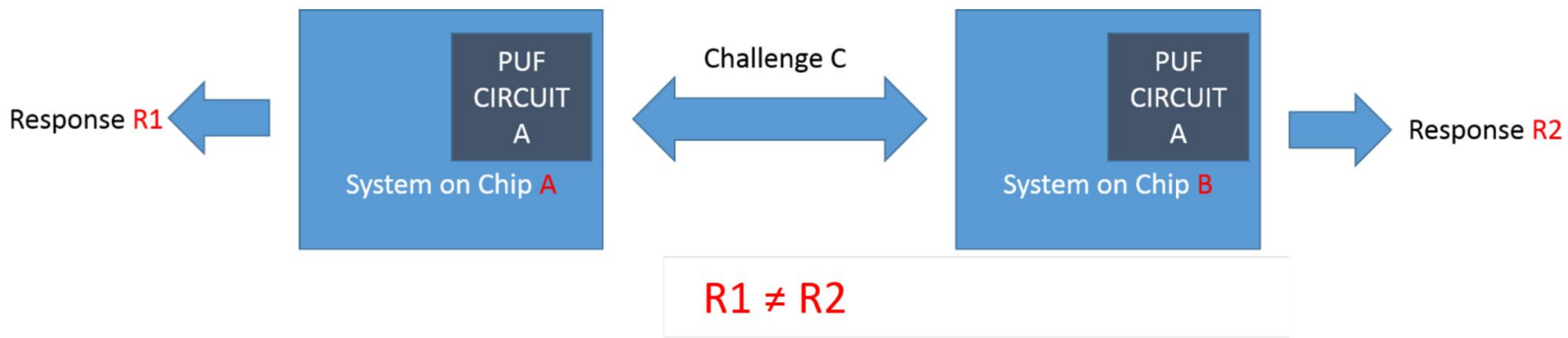
Design and Analysis of Physically Unclonable Functions on Artix-7 FPGA

Suvrat Pal and Urbi Chatterjee

IIT Kanpur, India

Goal: Assessment of Arbiter-PUF implemented on FPGA



What are PUFs

- Physically Unclonable Functions (PUFs) are electronic devices or components that exploit inherent physical variations within their manufacturing process to generate unique and unpredictable responses.
- PUFs serve as a means of establishing hardware-based security and can be utilized in various applications, including authentication, key generation, and secure storage.
- The operation of a PUF typically involves challenging the device with a specific input or stimulus and obtaining a corresponding output or response. The response is derived from the unique physical characteristics of the device, making it difficult to replicate or clone.

Evaluation Metrics for PUFs

Uniqueness (U): It is the measurement of the ability of PUF to uniquely distinguish two identical devices. The same challenge is applied to two similar PUF instances, and their hamming distance is calculated as uniqueness. For I PUF instances, uniqueness can be calculated as follows:

$$u = \frac{2}{I(I-1)} \sum_{i=1}^{I-1} \sum_{j=i+1}^{I} AHD(P_i, P_j) \quad X\ 100\%$$

Where AHD(Pi,Pj) denotes the average Hamming distance between the response of the PUF instance Pi and Pj . Ideally, the value of the uniqueness (u) should be 50%.

Reliability (R): It denotes the stability of the PUF response across repeated measurement in uncontrolled environmental condition. Reliability is measured as:

$$R = (1 - \frac{1}{N} \sum_{i=1}^{N} AHD({}^{r}P_j, {}^{i}P_j))\ X\ 100\%$$

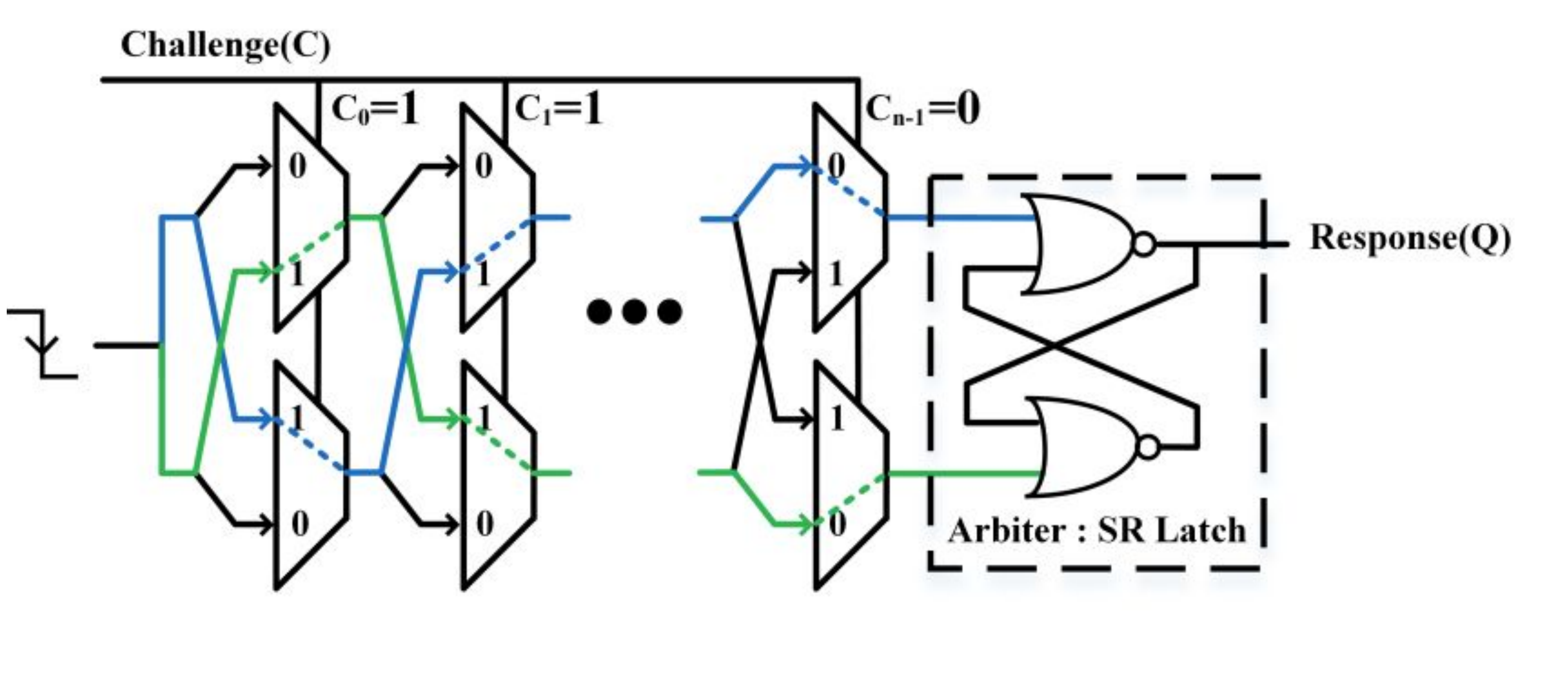
where rPj denotes the response of PUF instance Pj measured in reference environmental condition r and iPj denotes the response during ith measurement using same challenge. N is the number of different measurement. Ideally, reliability (R) should be 100%

Uniformity (Un): It indicates the probability of 0 and 1 in the PUF response. For better security of PUF 0 and 1 should be equiprobable. For a particular PUF instance uniformity can be calculated as:

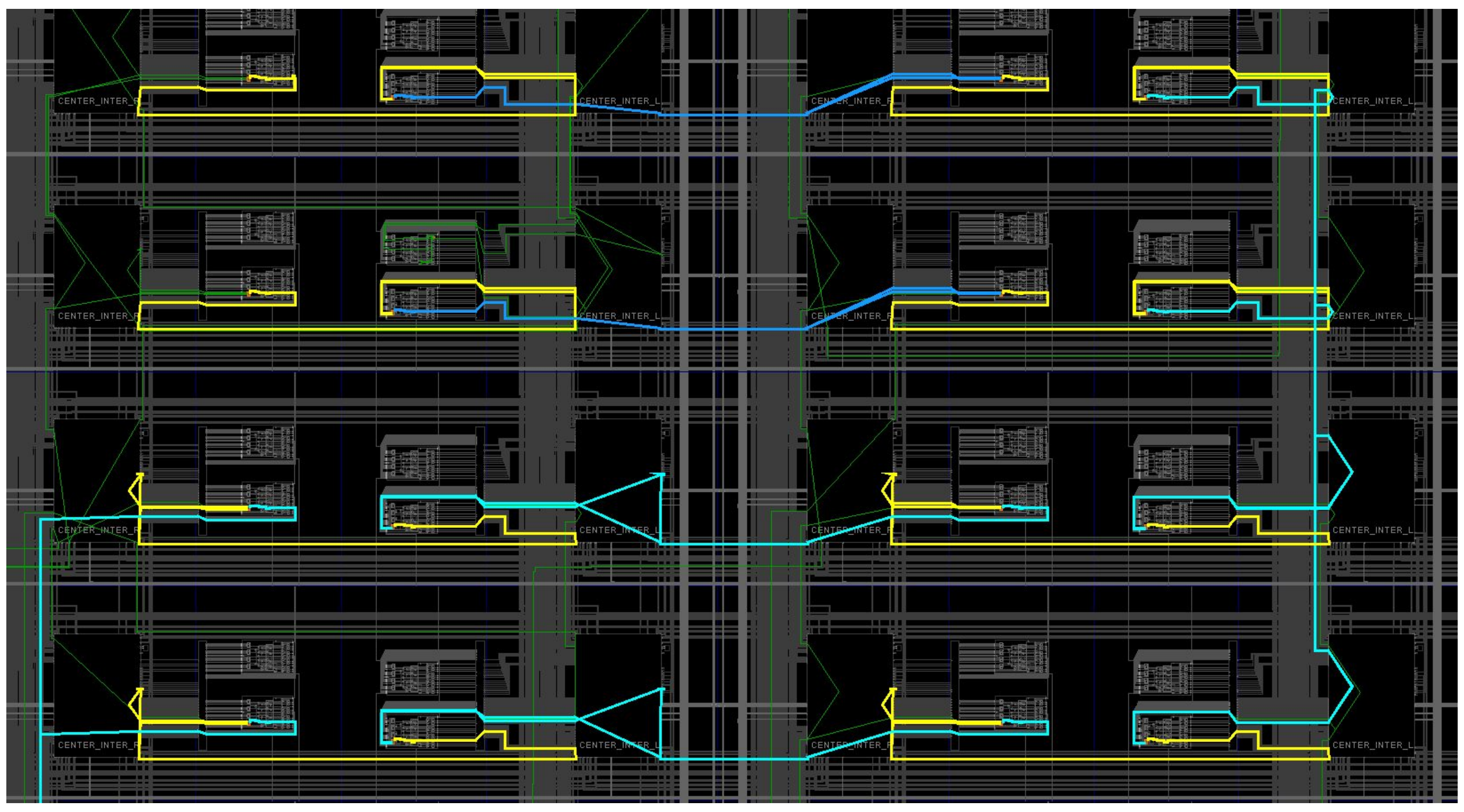
$$U_n = \frac{1}{n} \sum_{i=1}^{n} (r_i\ X\ 100\%)$$

where ri is the ith response bit (i.e. 0 or 1) and n is the number of response bit. Ideally uniformity should be 50%.

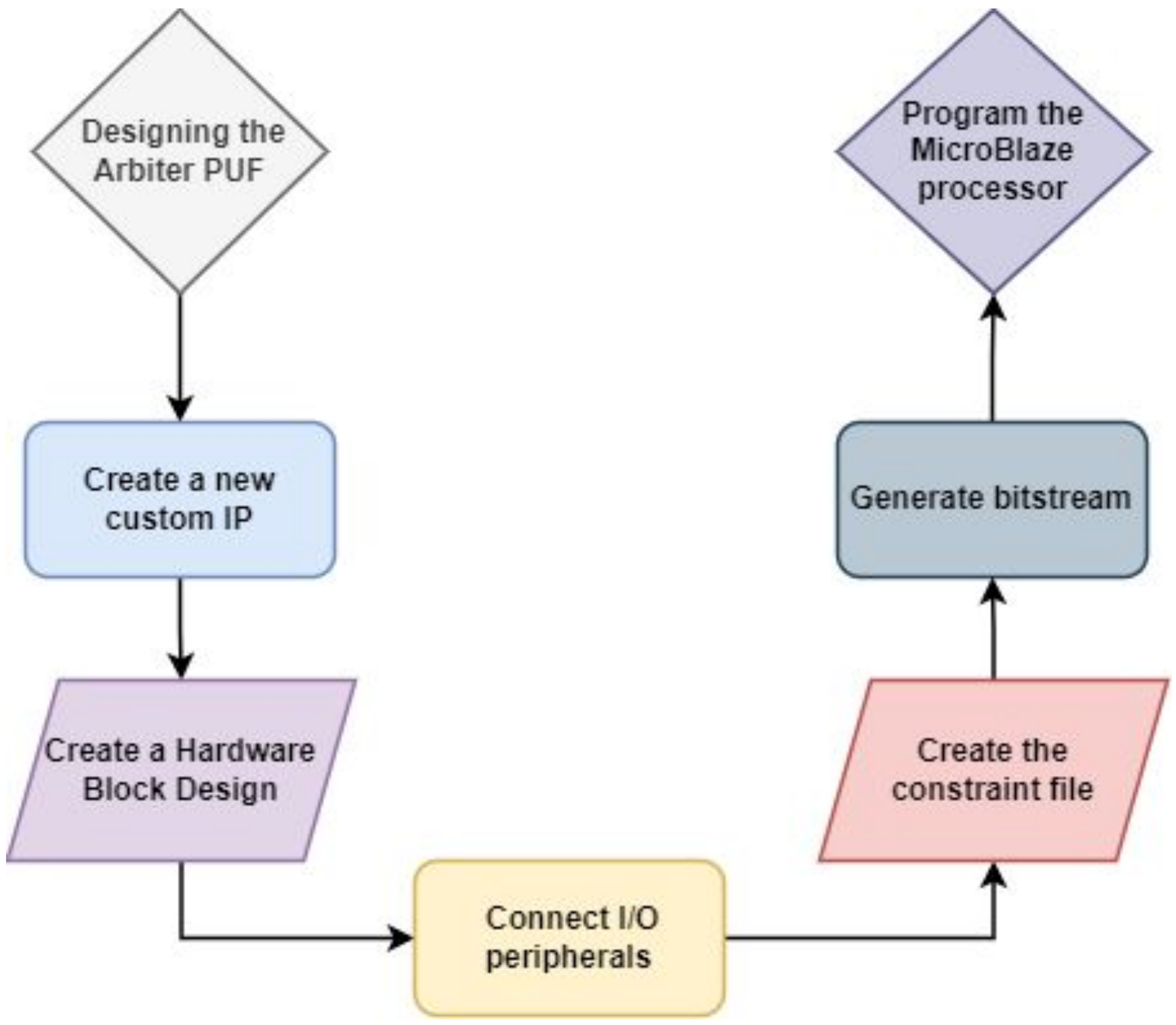
Block Diagram



Schematic Diagram

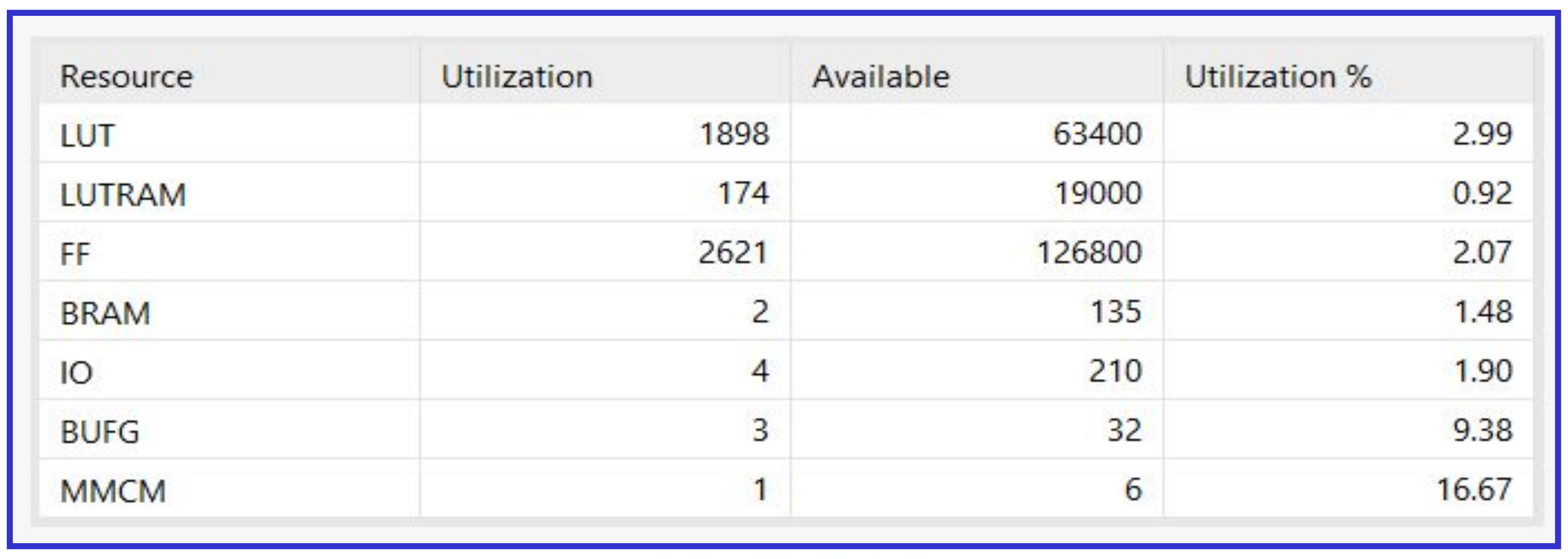


Methodology

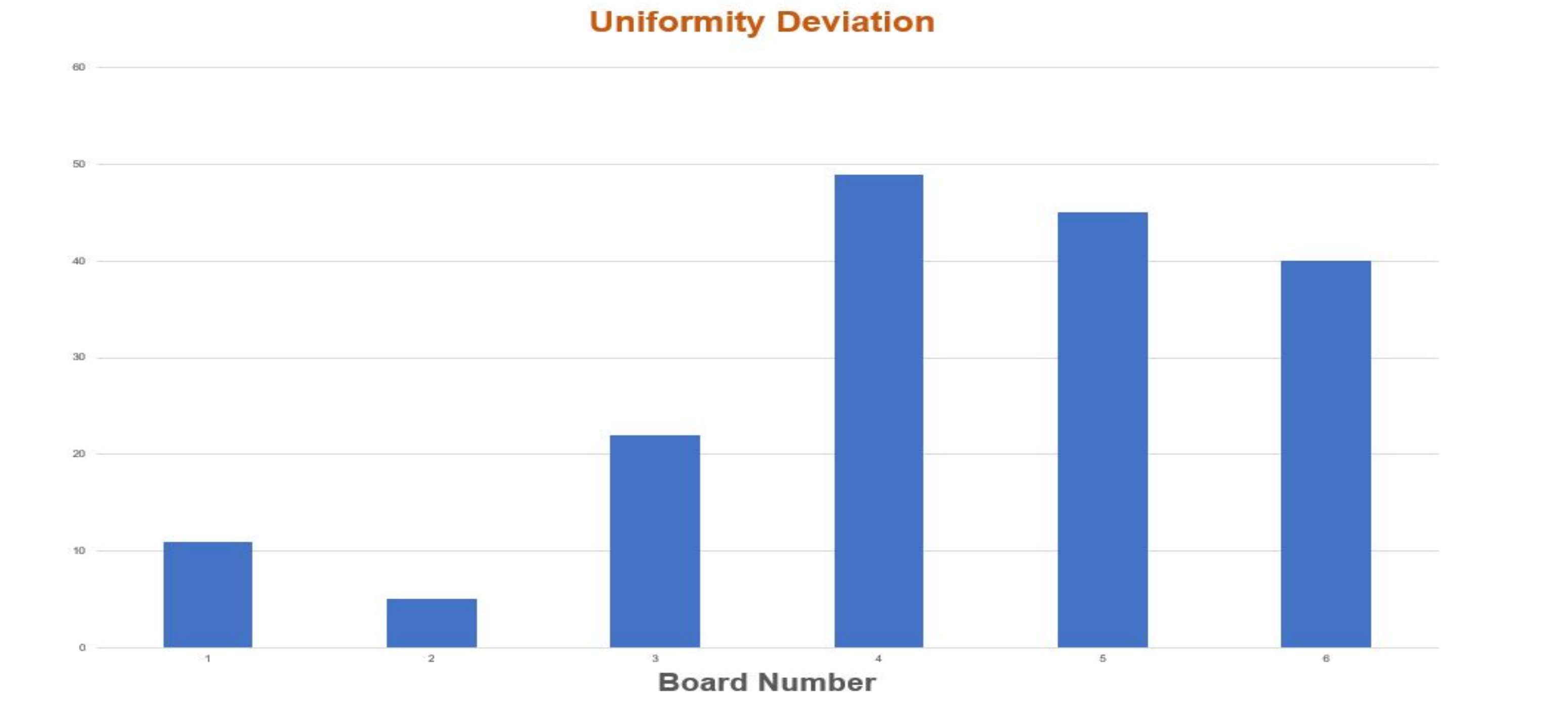

Designing the Arbiter PUF
Create a new custom IP
Create a Hardware Block Design
Connect I/O peripherals
Create the constraint file
Generate bitstream
Program the MicroBlaze processor

Experimental Results

FPGA	Uniqueness (%)	Uniformity (%)	Reliability (%)	Challenge Length
ARTY A7100T-CSG324	51.34	57.64	97.57	64



Resource	Utilization	Available	Utilization %
LUT	1898	63400	2.99
LUTRAM	174	19000	0.92
FF	2621	126800	2.07
BRAM	2	135	1.48
IO	4	210	1.90
BUFG	3	32	9.38
MMCM	1	6	16.67



Application No. - 2330283

Mentor: Dr. Urbi Chatterjee (Dept. of CSE)