Enhanced Arbiter PUF Construction Model to Strengthening PUF-based Authentication

Rizka Reza Pahlevi[1], Hirokazu Hasegawa[2], Yukiko Yamaguchi[3], Hajime Shimada[3]

[1]Graduate School of Informatics, Nagoya University
[2]Center for Strategic Cyber Resilience Research and Development, National Institute of Informatics
[3]Information Technology Center, Nagoya University
email : pahlevirr@net.itc.nagoya-u.ac.jp

Presenter Profile

Rizka Reza Pahlevi received the bachelor's and master's degree in Informatics from Telkom University, Indonesia in 2018 and 2019. He is currently a doctoral student majoring in Computer Security at the Graduate School of Informatics, Nagoya University, Japan.

His research interest lies in internet of things, hardware-based security, and embedded systems.

Introduction

Background and Motivation

- **Evolving Security Challenges in Authentication**
  - Rapid technological advancements have led to more sophisticated malicious methods.
  - Traditional authentication mechanisms are increasingly inadequate.
- **Physically Unclonable Functions (PUFs) as a Promising Solution**
  - Exploit inherent randomness from manufacturing processes.
  - Provide unique and unpredictable responses—difficult to replicate or predict.
  - Ideal for generating secure authentication tokens.

Introduction

Our Enhanced Arbiter PUF Construction

- **Limitations of Traditional Arbiter PUFs**
    - Vulnerable to statistical model attacks due to Challenge-Response Pair (CRP) correlations.
    - Previous enhancements (e.g., XOR arbiter PUF) improved uniqueness but still faced security gaps.

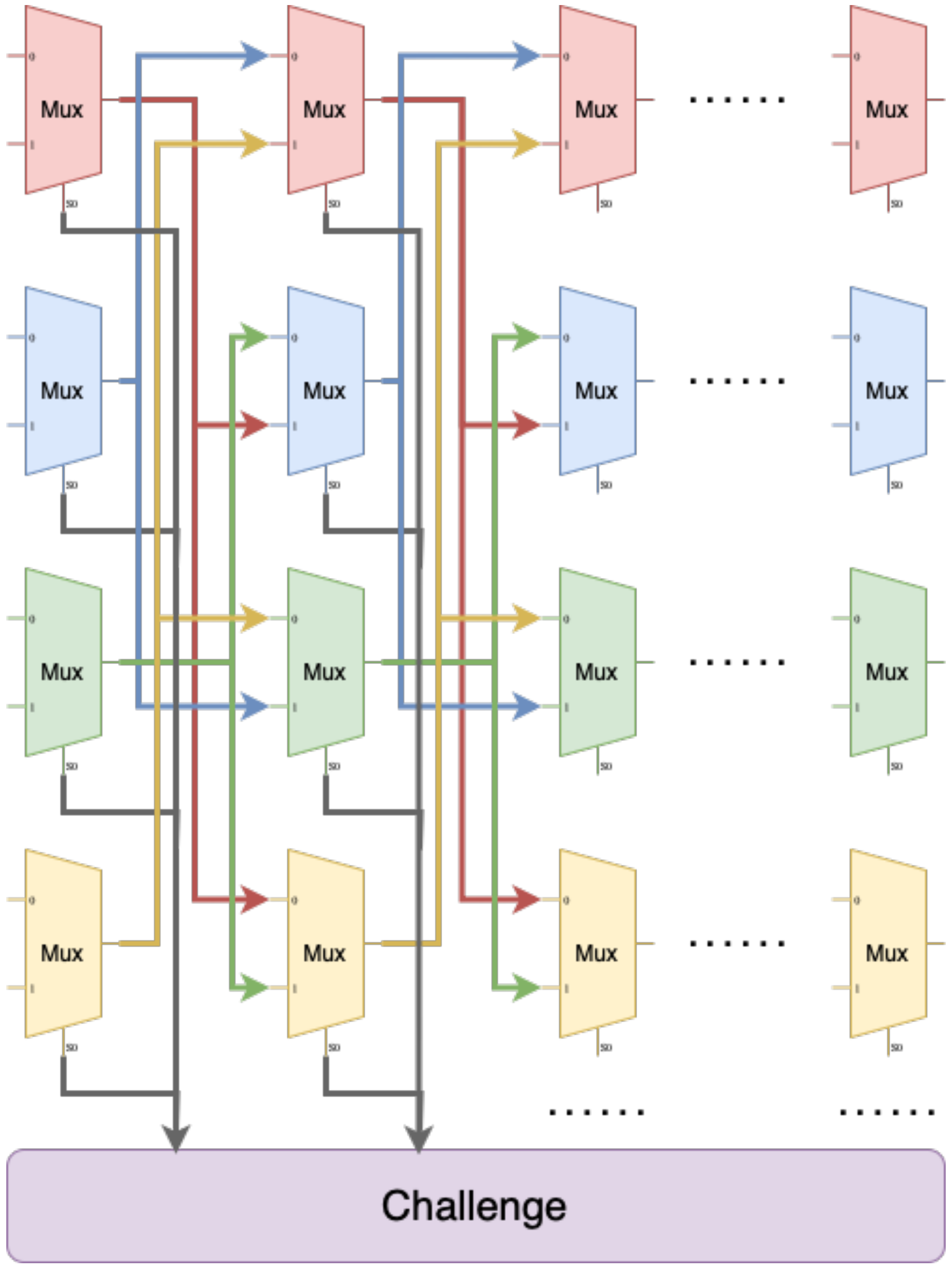
Our Propose

- **Our Proposed Solution**
  - Introduces a novel arbiter PUF design that enhances and maintains nearly ideal security attributes.
  - Outperforms existing models like XOR, flip-flop, and traditional arbiter PUFs in security metrics.
- **Comprehensive Security Evaluation**
  - Assessed using metrics: FAR, FRR, uniqueness, reliability, uniformity, and bit aliasing.
  - Implemented on six different FPGA boards to validate effectiveness and reliability across varied hardware environments.

Method

Proposed PUF Construction

- **Signature Generator**:
  - Produces the signal for the PUF.
  - Comprises four lines, each containing a series of **MUX gates.**
  - **Unique Design Features**:
    - **Four Sets of Lines**: Unlike previous models (e.g., double arbiter PUF by Machida et al.), it uses four lines instead of two.
    - **Cyclic Model** with **Crossing Patterns**: Ensures fair and balanced circuit delays by evenly distributing signals across all paths.
    - **Maintained Circuit Delay**: Reduces bias from minimal delay paths, enhancing PUF quality.



Method

Proposed PUF Construction

- Arbiter Component:
  - Utilizes elements from the conventional arbiter PUF.
  - Final MUX gates produce a spike signal.
  - Spike signal is distributed to multiple D Flip-Flops.

Method

Evaluation Metric - Classical Evaluation Metric

- Uniqueness
  - Measures the average Hamming distance between responses from different chips to the same challenge.

$$Uniqueness = \frac{2}{n(n-1)} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \frac{HD(R_i, R_j)}{m}$$

- Uniformity
  - Assesses whether each bit in the PUF response has an equal probability of being ‘0’ or ‘1’.

$$Uniformity = \frac{1}{n} \sum_{l=1}^{n} R_{i,l}$$

- Steadiness
  - Measures the consistency of PUF responses to the same challenge.

$$HD_{intra} = \sum_{i=1}^{k} |x_i - x_i'| \quad \text{where} \quad D = \begin{cases} 0 & \text{if \$x = x'\$} \\ 1 & \text{if \$x not x'\$} \end{cases}$$

Method

Evaluation Metric - PUF authentication-specific evaluations

- Bit Aliasing
  - Measures the bias of each bit position across multiple responses.

$$BA(n) = \frac{1}{N}\sum_{i=0}^{R-1} r_{i,n}$$

- FAR and FRR
  - FAR : Probability of incorrectly accepting an unauthorized response.
  - FRR : Probability of incorrectly rejecting an authorized response.

$$FAR = \frac{1}{\sigma_{\text{inter}}\sqrt{2\pi}}\int_{-\infty}^{HD_{\text{max}}} \exp\left(-\frac{1}{2}\left(\frac{x-\mu_{\text{inter}}}{\sigma_{\text{inter}}}\right)^2\right)dx$$

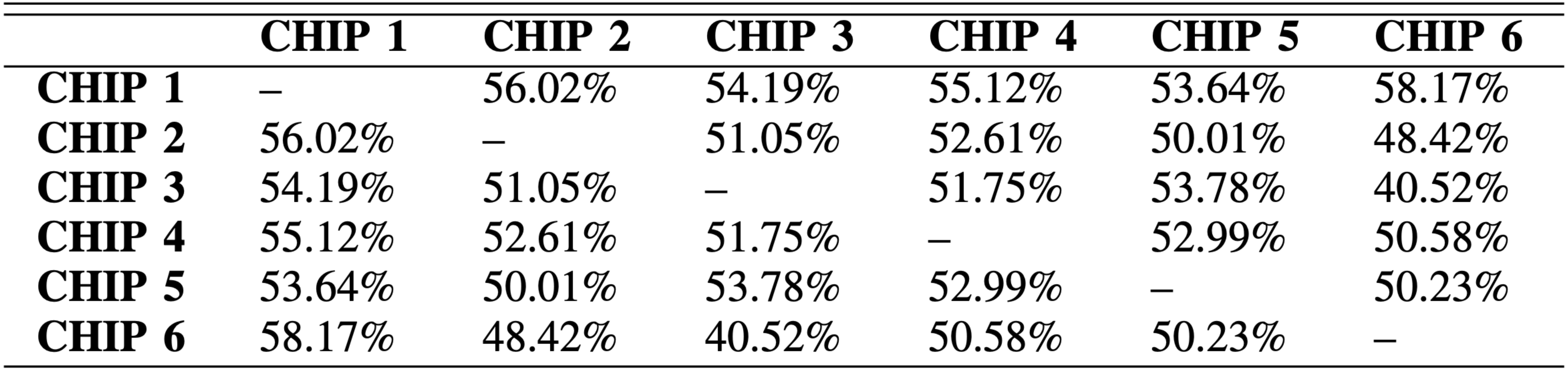
$$FRR = \frac{1}{\sigma_{\text{intra}}\sqrt{2\pi}}\int_{HD_{\text{max}}}^{\infty} \exp\left(-\frac{1}{2}\left(\frac{x-\mu_{\text{intra}}}{\sigma_{\text{intra}}}\right)^2\right)dx$$

Dataset

- Implementation on six different FPGA Boards
- Data Collection Process:
  - Challenges Sent per Board: **10,052** different challenges
  - Responses Collected per Challenge: **1,000** samples
  - Total Responses per Chip: **10,052,000** samples
  - Grand Total Dataset Entries: **60,312,000** responses across all six chips

Result

Uniqueness

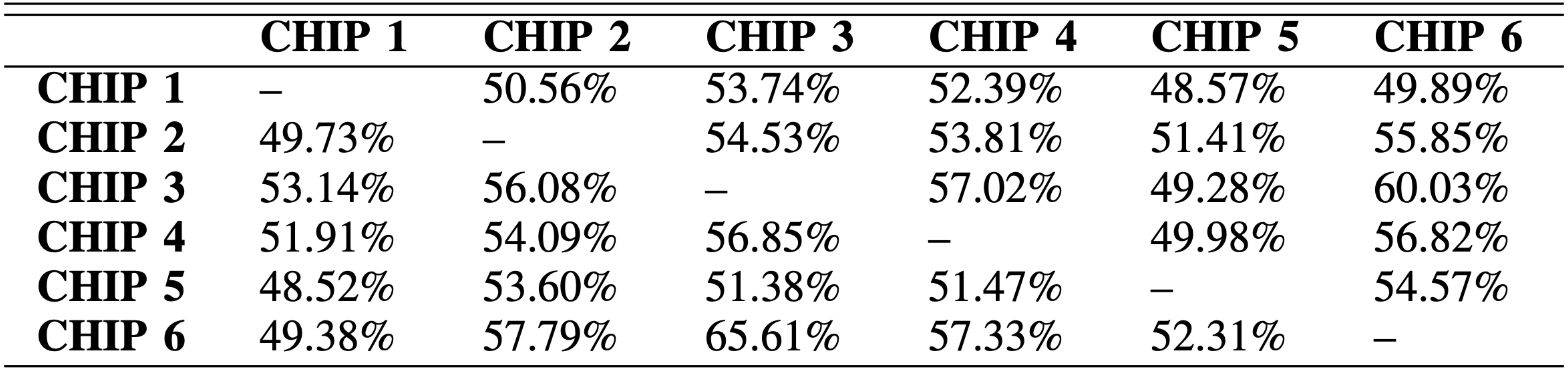


	CHIP 1	CHIP 2	CHIP 3	CHIP 4	CHIP 5	CHIP 6
CHIP 1	–	56.02%	54.19%	55.12%	53.64%	58.17%
CHIP 2	56.02%	–	51.05%	52.61%	50.01%	48.42%
CHIP 3	54.19%	51.05%	–	51.75%	53.78%	40.52%
CHIP 4	55.12%	52.61%	51.75%	–	52.99%	50.58%
CHIP 5	53.64%	50.01%	53.78%	52.99%	–	50.23%
CHIP 6	58.17%	48.42%	40.52%	50.58%	50.23%	–

- The average Hamming distances between chips are mostly above 50%.
- Indicates high uniqueness and distinctiveness in PUF responses across different chips.

Result

Bit-Aliasing

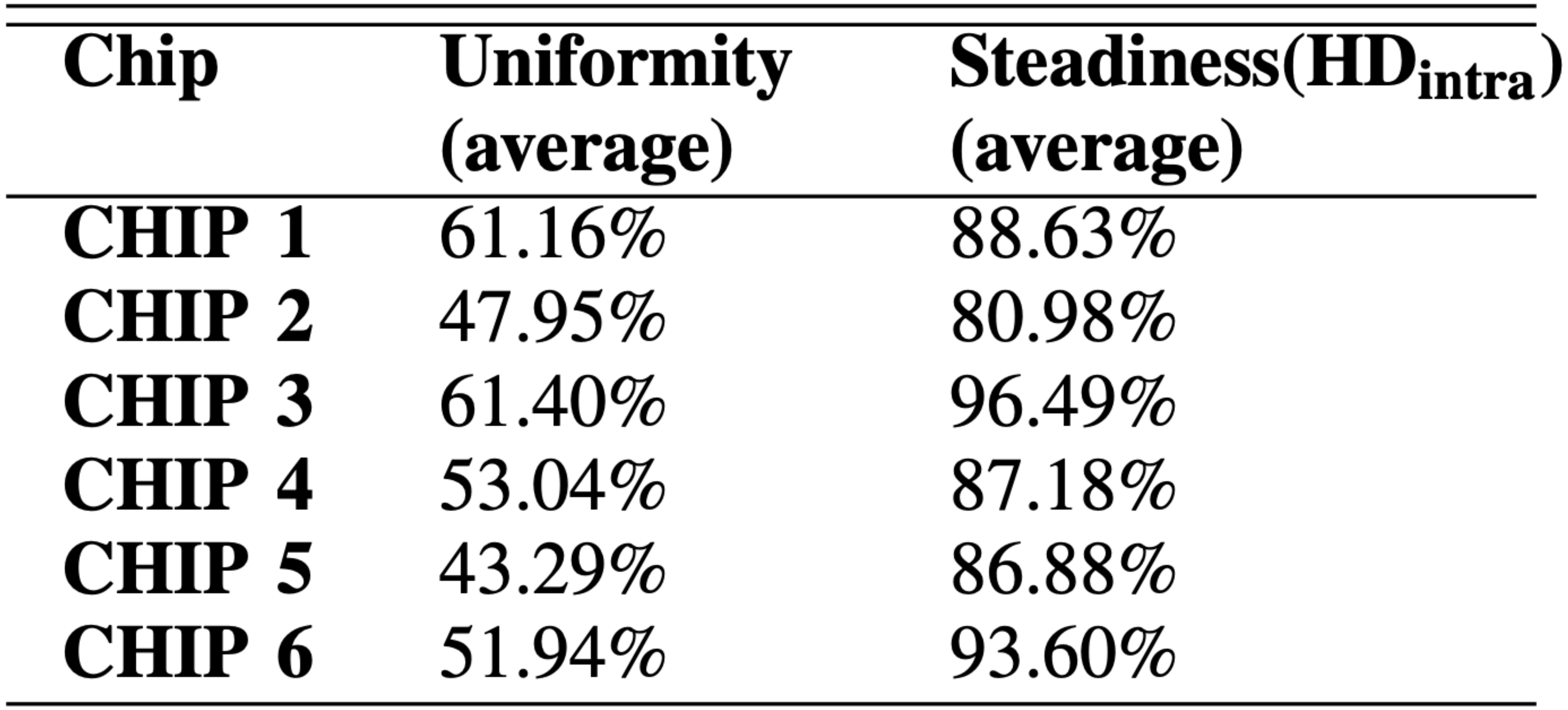


	CHIP 1	CHIP 2	CHIP 3	CHIP 4	CHIP 5	CHIP 6
CHIP 1	–	50.56%	53.74%	52.39%	48.57%	49.89%
CHIP 2	49.73%	–	54.53%	53.81%	51.41%	55.85%
CHIP 3	53.14%	56.08%	–	57.02%	49.28%	60.03%
CHIP 4	51.91%	54.09%	56.85%	–	49.98%	56.82%
CHIP 5	48.52%	53.60%	51.38%	51.47%	–	54.57%
CHIP 6	49.38%	57.79%	65.61%	57.33%	52.31%	–

- Bit aliasing values are generally close to the ideal 50%.
- Values range from 48.52% to 65.61%, with most clustering around 50%.

Result

Uniformity

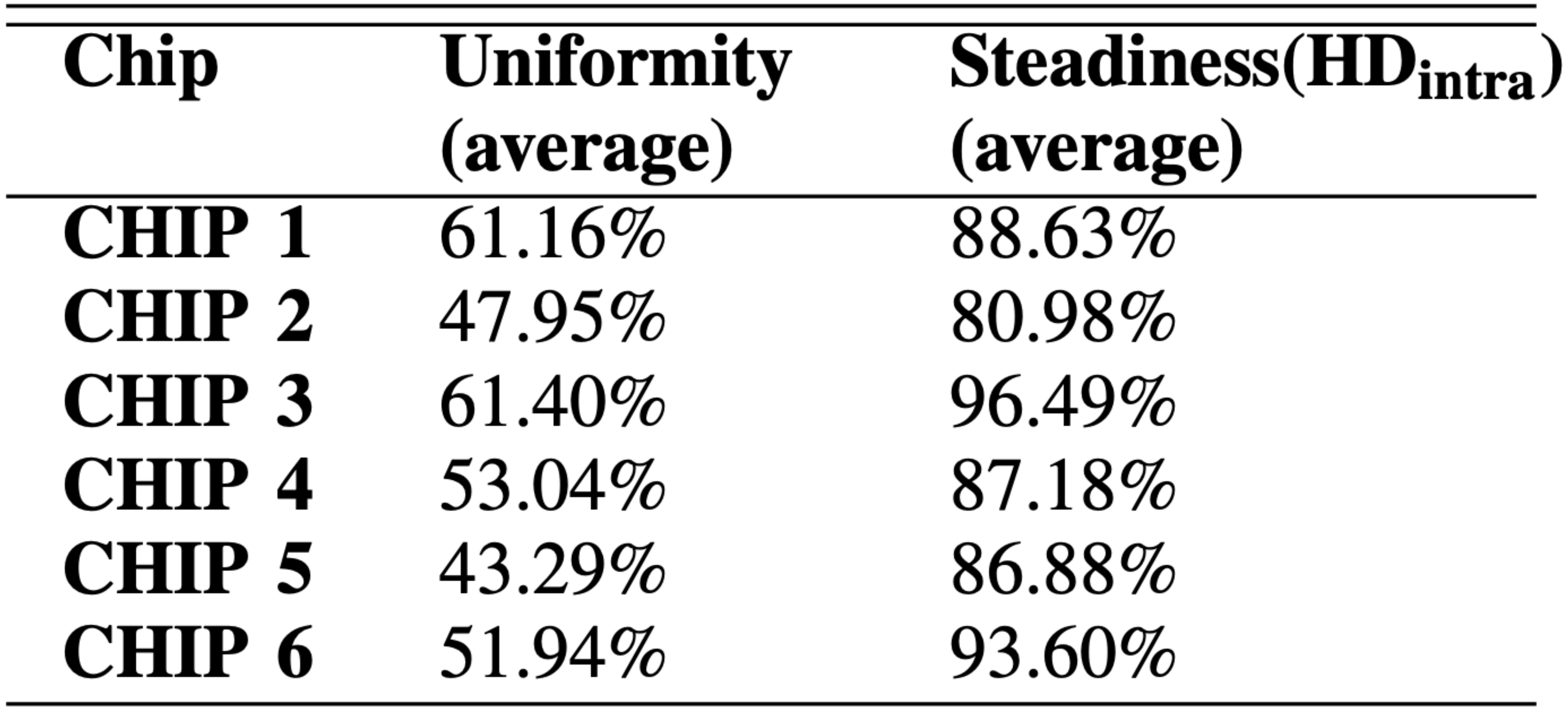


Chip	Uniformity (average)	Steadiness($\mathrm{HD}_{\mathrm{intra}}$) (average)
CHIP 1	61.16%	88.63%
CHIP 2	47.95%	80.98%
CHIP 3	61.40%	96.49%
CHIP 4	53.04%	87.18%
CHIP 5	43.29%	86.88%
CHIP 6	51.94%	93.60%

- Uniformity values are generally close to the ideal 50%.
- CHIP 2 has the closest average to the ideal at 47.95%.
- CHIP 3 has the highest average at 61.40%, slightly further from the ideal but still acceptable.

Result

Steadiness

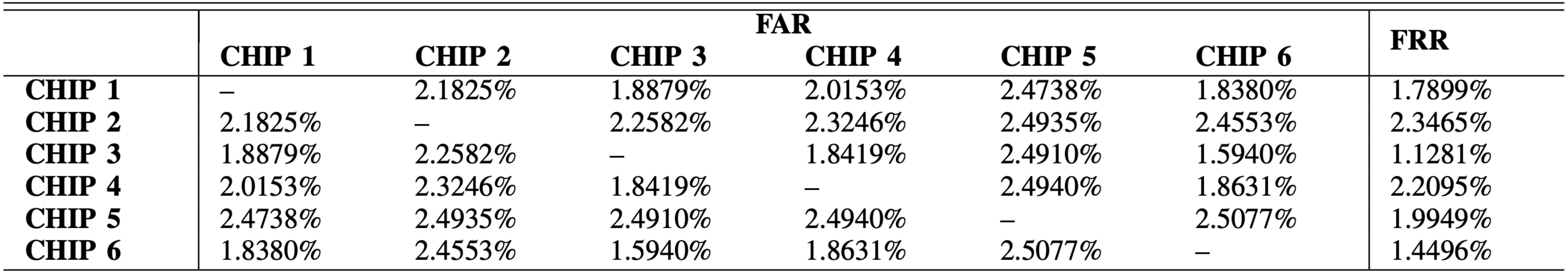


Chip	**Uniformity (average)**	**Steadiness(HD_{intra}) (average)**
CHIP 1	61.16%	88.63%
CHIP 2	47.95%	80.98%
CHIP 3	61.40%	96.49%
CHIP 4	53.04%	87.18%
CHIP 5	43.29%	86.88%
CHIP 6	51.94%	93.60%

- Steadiness values range from 80.98% to 96.49%.
- CHIP 3 shows the highest steadiness at 96.49%.
- CHIP 2 shows the lowest steadiness at 80.98%.

Result

FAR and FRR

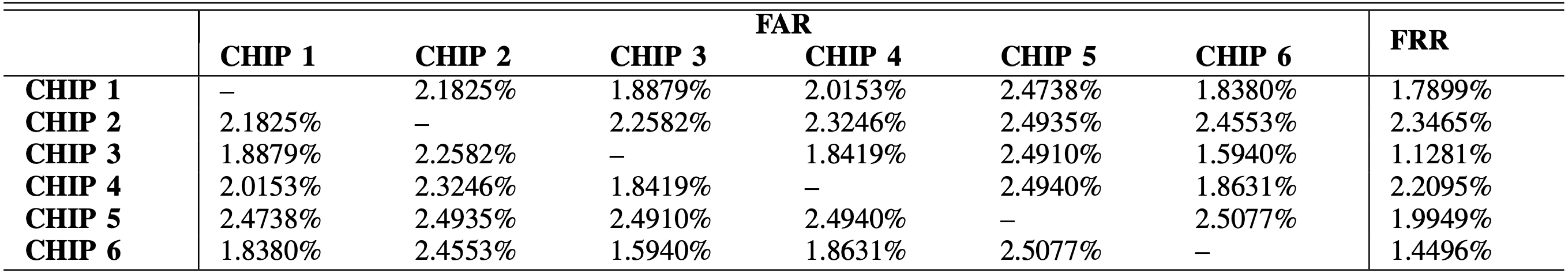


	FAR						FRR
	CHIP 1	**CHIP 2**	**CHIP 3**	**CHIP 4**	**CHIP 5**	**CHIP 6**	
CHIP 1	–	2.1825%	1.8879%	2.0153%	2.4738%	1.8380%	1.7899%
CHIP 2	2.1825%	–	2.2582%	2.3246%	2.4935%	2.4553%	2.3465%
CHIP 3	1.8879%	2.2582%	–	1.8419%	2.4910%	1.5940%	1.1281%
CHIP 4	2.0153%	2.3246%	1.8419%	–	2.4940%	1.8631%	2.2095%
CHIP 5	2.4738%	2.4935%	2.4910%	2.4940%	–	2.5077%	1.9949%
CHIP 6	1.8380%	2.4553%	1.5940%	1.8631%	2.5077%	–	1.4496%

- FAR values are mostly under 2.5%, indicating a low rate of false acceptances.
- Values range from 1.5940% to 2.5077%.

Result

FAR and FRR

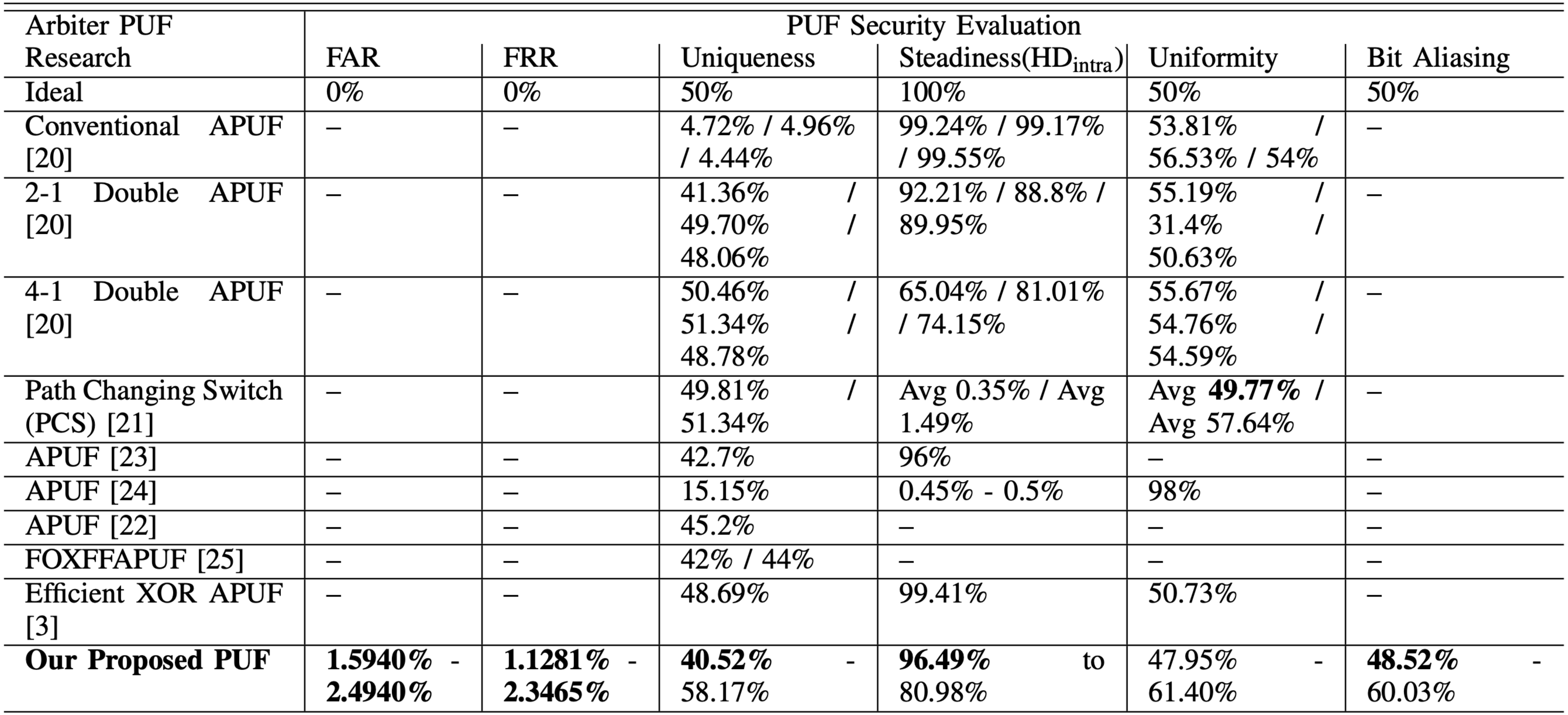


	FAR						FRR
	CHIP 1	CHIP 2	CHIP 3	CHIP 4	CHIP 5	CHIP 6	
CHIP 1	–	2.1825%	1.8879%	2.0153%	2.4738%	1.8380%	1.7899%
CHIP 2	2.1825%	–	2.2582%	2.3246%	2.4935%	2.4553%	2.3465%
CHIP 3	1.8879%	2.2582%	–	1.8419%	2.4910%	1.5940%	1.1281%
CHIP 4	2.0153%	2.3246%	1.8419%	–	2.4940%	1.8631%	2.2095%
CHIP 5	2.4738%	2.4935%	2.4910%	2.4940%	–	2.5077%	1.9949%
CHIP 6	1.8380%	2.4553%	1.5940%	1.8631%	2.5077%	–	1.4496%

- FRR values are under 2.5%, indicating a low rate of false rejections.
- Values range from 1.1281% to 2.3465%.

Result

Comparison



Arbiter PUF	PUF Security Evaluation					
Research	FAR	FRR	Uniqueness	Steadiness(HD$_{\text{intra}}$)	Uniformity	Bit Aliasing
Ideal	0%	0%	50%	100%	50%	50%
Conventional APUF [20]	–	–	4.72% / 4.96% / 4.44%	99.24% / 99.17% / 99.55%	53.81% / 56.53% / 54%	–
2-1 Double APUF [20]	–	–	41.36% / 49.70% / 48.06%	92.21% / 88.8% / 89.95%	55.19% / 31.4% / 50.63%	–
4-1 Double APUF [20]	–	–	50.46% / 51.34% / 48.78%	65.04% / 81.01% / 74.15%	55.67% / 54.76% / 54.59%	–
Path Changing Switch (PCS) [21]	–	–	49.81% / 51.34%	Avg 0.35% / Avg 1.49%	Avg **49.77%** / Avg 57.64%	–
APUF [23]	–	–	42.7%	96%	–	–
APUF [24]	–	–	15.15%	0.45% - 0.5%	98%	–
APUF [22]	–	–	45.2%	–	–	–
FOXFFAPUF [25]	–	–	42% / 44%	–	–	–
Efficient XOR APUF [3]	–	–	48.69%	99.41%	50.73%	–
Our Proposed PUF	**1.5940% - 2.4940%**	**1.1281% - 2.3465%**	**40.52%** - 58.17%	**96.49%** to 80.98%	47.95% - 61.40%	**48.52%** - 60.03%

Conclusion and Future Work

- Significant Advancements in PUF-Based Authentication
- Validated Effectiveness Through Comprehensive Testing
- Robustness Confirmed by FAR and FRR Measurements
- Contributions to Digital Security
    - Offers a promising solution for enhancing authentication mechanisms.
    - Paves the way for widespread adoption in security-critical applications.

Conclusion and Future Work

- Optimization for Lower FAR and FRR
- Enhancing Reliability
- Broader Hardware Implementation
- Exploration of Practical Applications

Thank You