# Reliability and Uniqueness Analysis of Stochastic Physical Unclonable Functions

Carl Anderson and Keshab K. Parhi
Department of Electrical and Computer Engineering
University of Minnesota
Driven to Discover℠

## Introduction

***Motivation:***

- With the advent of mobile computing, devices are becoming widely used for secure transactions
- Smartphones and credit cards are entrusted with important financial and private information
- The security of the information these devices hold is ensured solely by the security of the devices themselves

***Conventional Hardware Security:***

- Requires costly on-chip storage for hidden keys and cryptographic processing hardware
- Is only secure as long as physical access to the device is prevented

***Physical Unclonable Functions (PUFs):***

- Use randomness in manufacturing processes to generate cryptographically secure keys [1]
- Require significantly less power and space than traditional methods
- Require many challenges to generate cryptographically secure signature

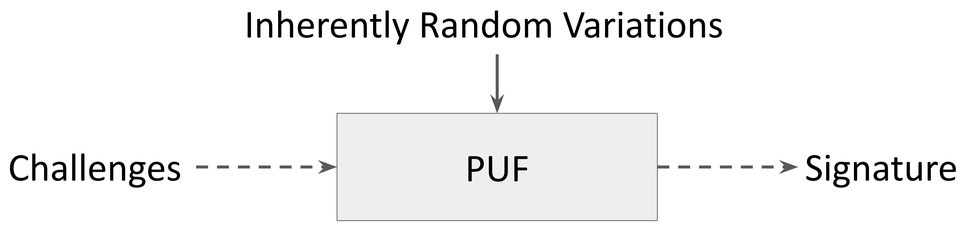


Fig. 1: Physical Unclonable Function

## Background

***Multiplexer (MUX) Based Arbiter PUFs:***

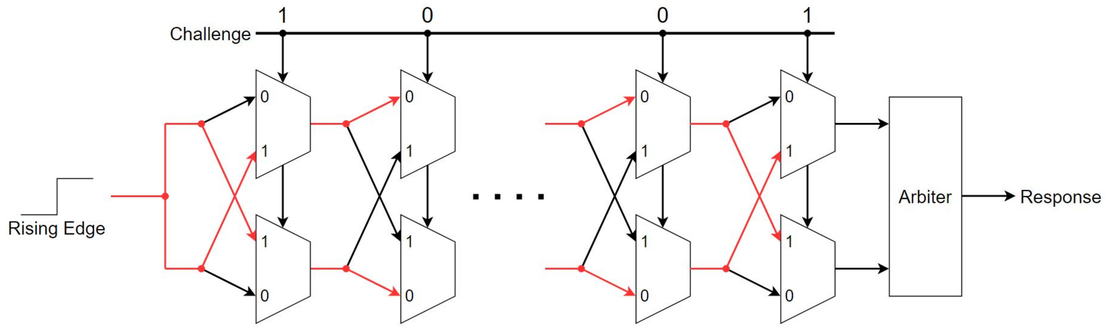


Fig. 2: MUX-based arbiter PUF structure

- The response is determined by which rising edge reaches the arbiter first

***Stochastic Computing:***

- Stochastic logic encodes real valued numbers in unary bitstreams based on the percentage of 1's found in the bitstream over a period of time [2]

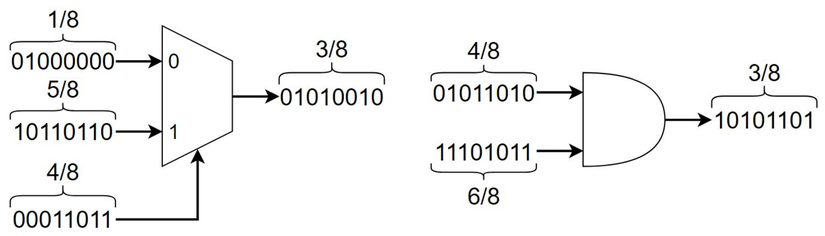


Fig. 3: Stochastic computations
(a) Scaled addition (b) Unsigned multiplication

***Stochastic (Soft) PUF:***

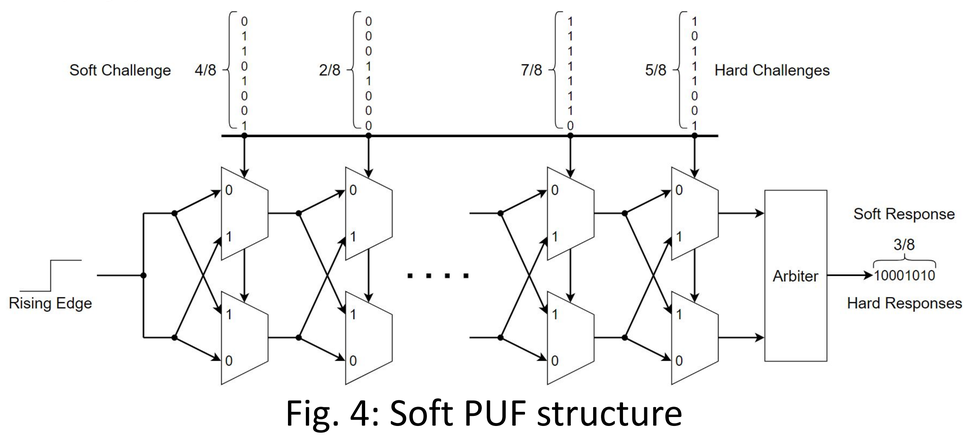


Fig. 4: Soft PUF structure

- Soft challenges are applied by querying many sets of hard challenges conforming to the soft challenge stochastic value
- The soft response is calculated by dividing the number of 1's in the response vector by the total number of responses
- The soft response is the real stochastic value of the hard responses [3]

## Reliability Analysis

***Definition:***

- A measure of how responses to the same challenge vary under noise

$$P_{intra} = \frac{1}{K(K-1)} \sum_{i=1}^{K-1} \sum_{j=i+1}^{K} |R'_i - R'_j|$$

R' is a collection of K noisy response vectors

$$Reliability = (1 - P_{intra}) \times 100\%$$

***Results:***

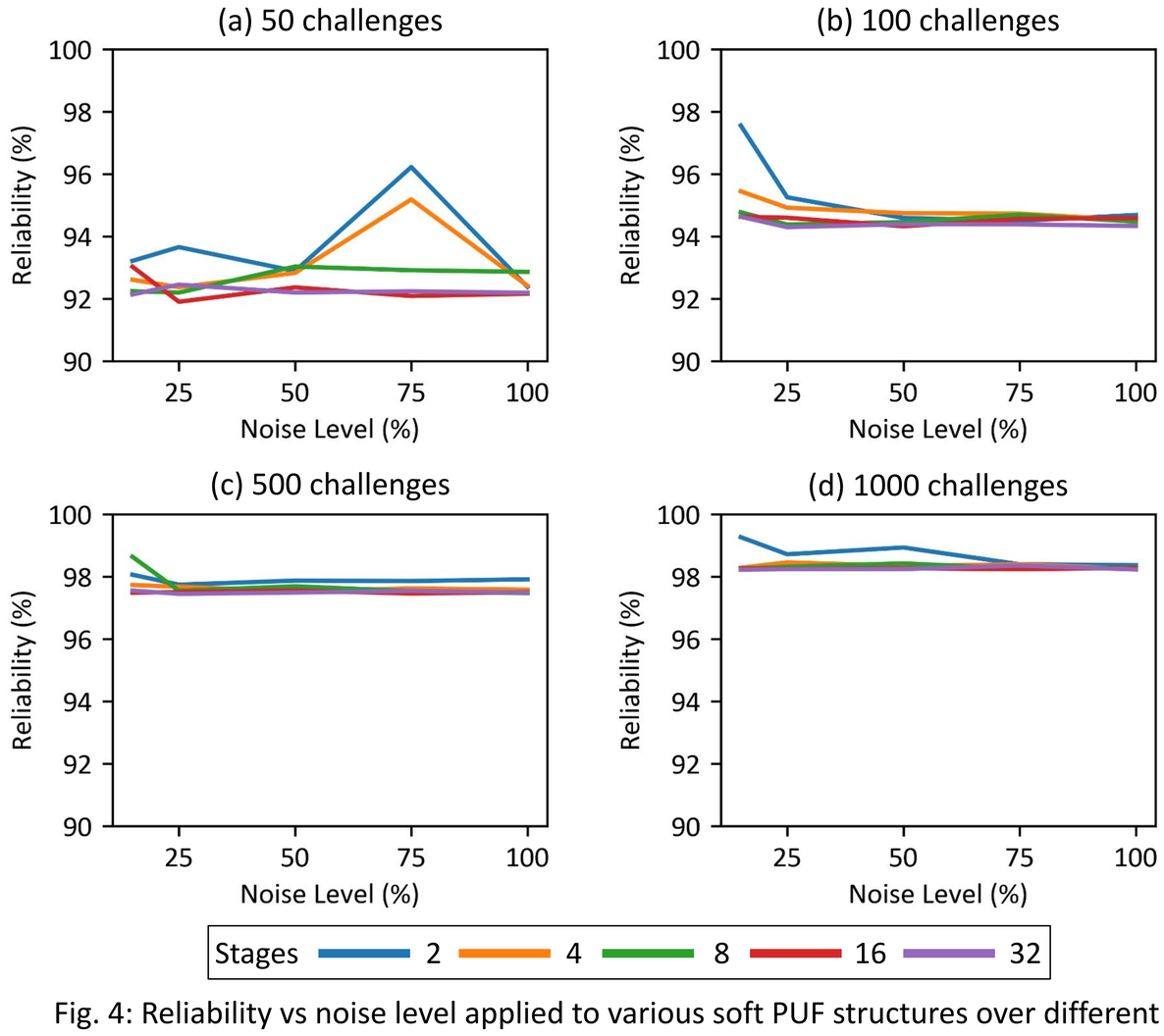


Fig. 4: Reliability vs noise level applied to various soft PUF structures over different amounts of challenges applied

- Simulation results showed that the soft PUF was incredibly robust under even extremely noisy conditions compared to traditional MUX-based arbiter PUFs which breakdown past 15% noise
- Reliability of the PUF had little to do with the structure of the PUF itself, within each plot the different structures are closely packed
- The number of challenges applied did heavily influence the reliability, as more challenges are applied the average reliability increases

## Uniqueness Analysis

***Definition:***

- A measure of the distance between different PUFs responses to the same challenge

$$P_{inter} = \frac{1}{K(K-1)} \sum_{i=1}^{K-1} \sum_{j=i+1}^{K} |R(i) - R(j)|$$

R is a collection of responses from K PUFs

$$Uniqueness = (1 - |2P_{inter} - 1|) \times 100\%$$

***Results:***

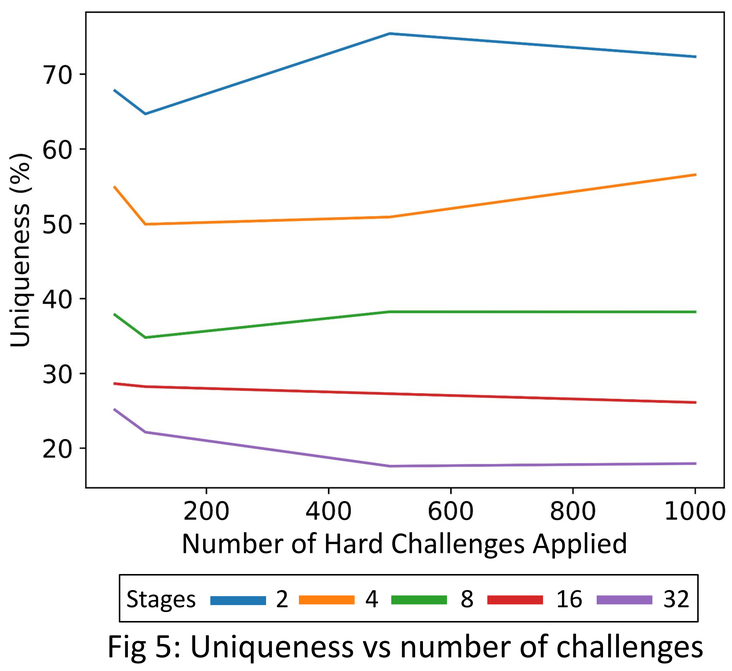


Fig 5: Uniqueness vs number of challenges applied for various soft PUF structures

- Simulation results showed that the uniqueness of the soft PUF is primarily dependent on the structure of the PUF
- The uniqueness of the soft PUF is still lagging that of standard MUX-based arbiter PUFs which boast minimum values of 60%
- The fewer stages in the PUF, the better the uniqueness
- The number of challenges applied has little to no impact on the uniqueness

## References

[1] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in Proc. of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 148–160.

[2] Brian R Gaines. 1967. Stochastic computing. In Proceedings of the AFIPS Spring Joint Computer Conference. ACM, 149–156.

[3] C. Zhou, S. Satapathy, Y. Lao, K. K. Parhi and C. H. Kim, "Soft response generation and thresholding strategies for linear and feed-forward MUX PUFs", Proc. Int. Symp. Low Power Electron. Design (ISLPED), pp. 124-129, Aug. 2016.