SAND2020-7290D

The Center for Cyber Defenders

Expanding computer security knowledge

Computational Diversity for CS

Characterizing PUFs though Statistical and Physical Tests

Philip Dawson, Santa Clara University
Derek Dervishian, Purdue University

Project Mentor: Ryan Helinski, Org. 5627

Problem Statement

Physical Unclonable Functions (PUFs) are functions that take in an m-bit challenge C and produces an n-bit response R, similar to hash functions. Most PUFs derive their randomness from variations during the IC fabrication process. They are commonly used for generating encryption keys or for generating a unique response for authentication.

The characteristics of an ideal PUF are:

- Random – like a dice roll
- Unique – like fingerprints
- Reliable – good plumbing

We want to investigate the physical source of entropy, PUF performance and the effect that environmental conditions have on a new kind of PUF, such as noise, temperature, aging, etc.

Property	Characteristic	Identifier	Ideal Value
Mean value	Bias, randomness	μ or $P(b)$	$0.5, \quad \sigma = \frac{\sqrt{n}}{2}$
Error rate or fraction of noisy bits	Reliability	HD_{noise} (or HD_{intra} if $m = 0$)	$\mu = 0$
Autocorrelation between response bits	Randomness	R_{xx}	$\mu = 0, \quad \sigma = \frac{1}{2\sqrt{n}}$
Hamming distance between responses to different challenges	Randomness	HD_{intra} (if $m > 0$)	$\mu = 0.5, \quad \sigma = \frac{\sqrt{n}}{2}$
Hamming distance of responses between devices	Uniqueness	HD_{inter}	$\mu = 0.5, \quad \sigma = \frac{\sqrt{n}}{2}$
Statistical test value	Randomness	v or P-value	$\mu = 1 - \alpha$

Objectives and Approach

We are using the NIST 800-90B standard, along with other conventions, to assess the entropy and randomness of the bits generated from the PUFs.

Our main objective is to create our own Python library implementation of these standards that are:

- Easy to understand
- Implement the standards correctly
- Run in a reasonable amount of time

There are 2 sections of tests: IID and non-IID. The IID tests provides assurance that the bits are independent and identically distributed, and the non-IID tests provide an estimate of entropy of the bits without the IID assumption.

Results

By implementing these standards in our Python library, not only do we get clean and understandable code, but we are also better able to understand what these statistical tests are actually computing and how they work.

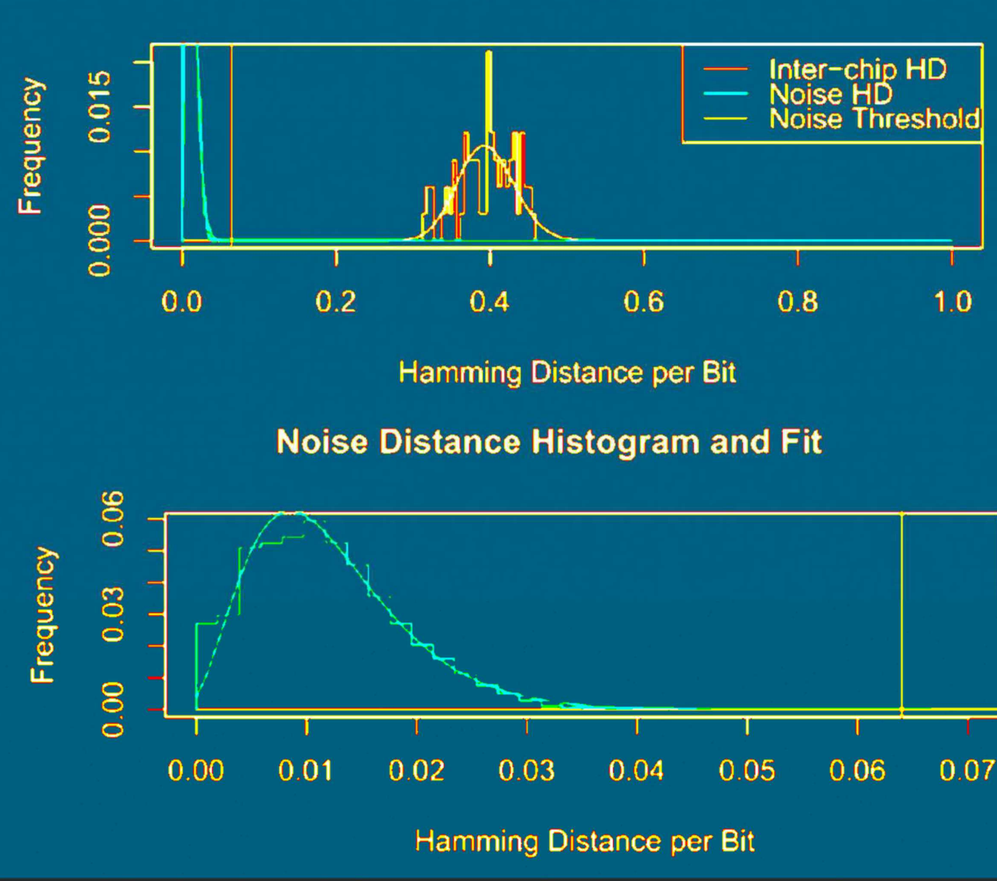
The Python library is modular with a robust self-test suite that validates that the software is outputting correct results. Being modular, an engineer can refactor the implementation of the tests and not have to worry about breaking the rest of the code.

If an engineer modifies the code, the test suite can be used to ensure that the function still performs correctly, and can give developers helpful feedback if a test fails.

Impact and Benefits

We can now determine whether or not the bit strings generated by these PUFs are non-deterministic and have the characteristics of an ideal PUF. This is very important because we do not want adversaries to use unintended patterns within the bits to compromise the security of a cryptographic system that uses PUFs.

This library gives Sandia National Labs an essential tool in making their independent valuation on these kinds of PUFs, and allows them to make new contributions to this exciting and expanding field.



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2020-XXXX X.