Research Spotlight Forum

8.6.19 Cybersecurity

Model-building Resistance and Entropy Investigation of Physically Unclonable Functions for Device Authentication

PRESENTED BY:

Wenjie Che

Klipsch School of Electrical and Computer Engineering

New Mexico State University

Contact information: wche@nmsu.edu

Sandia National Laboratories | Georgia Institute of Technology | The University of New Mexico | Illinois | NM State University | Purdue University | New Mexico Tech | The University of Texas at Austin

SAND2019-9382 PE

ABOUT MYSELF

Brief biography

- I joined NMSU August 2018 as a tenure track assistant professor
- I worked as a research engineer in Enthentica Inc., 2017-2018
- Ph.D. University Of New Mexico, December 2016

- **Research areas**
  - Hardware Security and Trust, Hardware-Software Codesign
  - Physically Unclonable Functions, Entropy Enhancement, PUF Model-building resistance
- **Research group interests, size and demographics**
  - I am now advising one undergraduate student.
  - Looking for more graduate students.

Keywords:

Hardware Security, Physically Unclonable Functions, Entropy Enhancement, Model-building resistance, Compressive Sensing

PREVIOUS AND ON-GOING WORK IN CYBERSECURITY

- **Novel Offset Techniques to Improve Uniqueness and Reliability of a Hardware-Embedded Delay PUF (HELP PUF)**
  - A population-based offset technique that significantly improves the uniqueness of the HELP PUF bitstring
  - Proposed a chip-specific offset technique that improves the reliability and increases the bitstring length of the HELP PUF

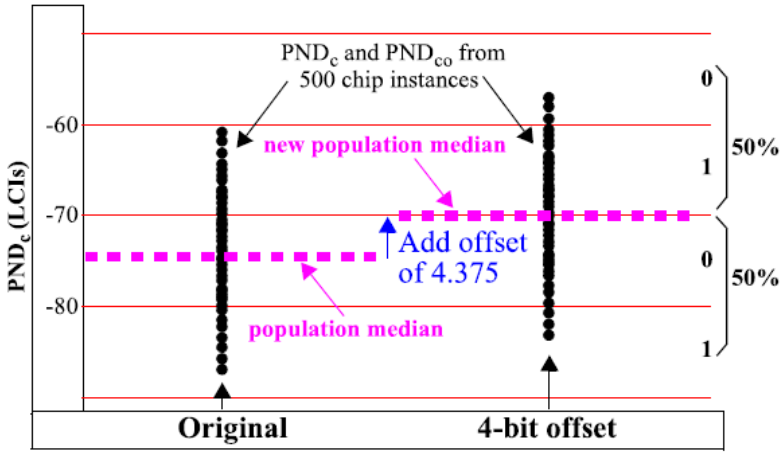


Fig. 1. Illustration of an offset calculation using one set of PNDc from 500 chip instances and a 4-bit offset.

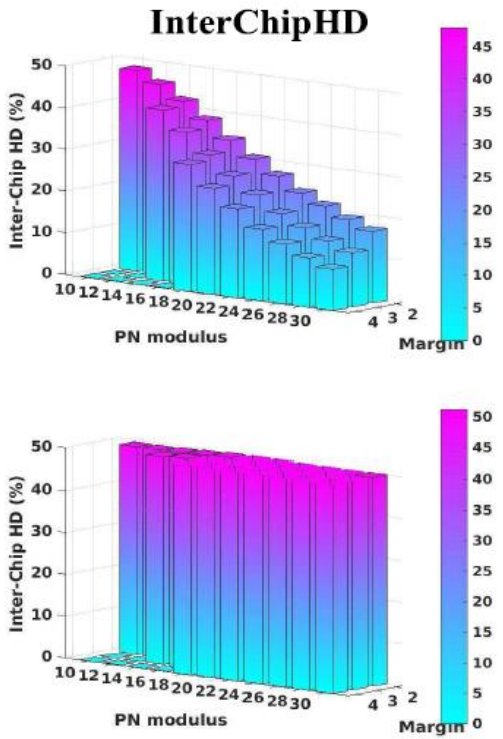
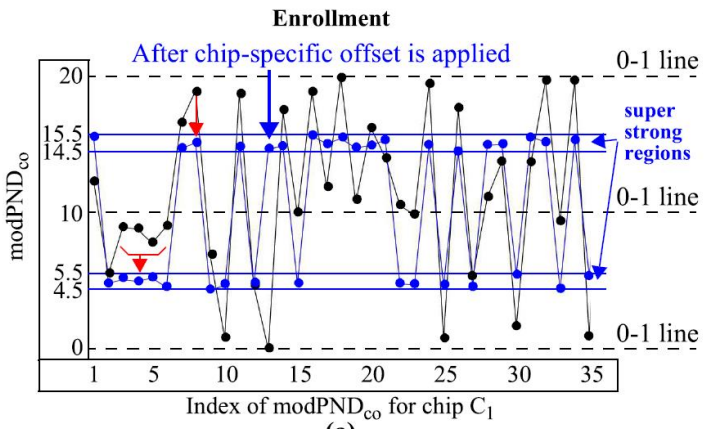
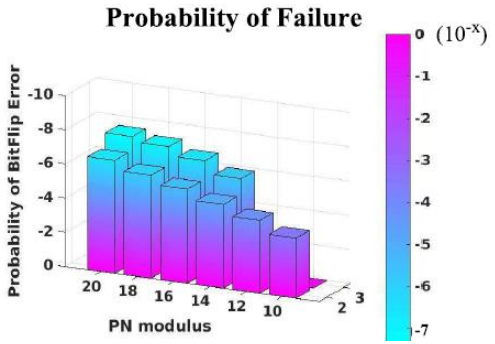


Fig. 2 Inter-chip Hamming Distance before and after the offset technique



(a)



(b)

Fig. 3. (a) Illustration of modifications made to modPNDco before and after the chip-specific offset is applied (b) Enhanced reliability

PREVIOUS AND ON-GOING WORK IN CYBERSECURITY

- **Entropy Analysis of a Hardware-Embedded Delay PUF**
  - A complete Entropy analysis at each response bit position for 500 PUF instances including Entropy, min-Entropy and Uniqueness
  - Correlation Analysis that measures if knowing one response bit allows a second response bit to be predicted with probability more than 50%.
  - Two types of the correlations are investigated: (1) Path segment reuse where only a small portion of the path components of the two paths are different; (2) Full path delay reuse where one path delay is used more than once to be paired with other path delays

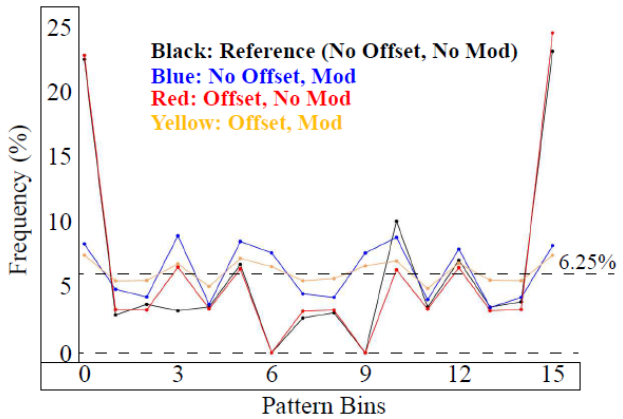


Fig. 4. Frequency of 4-bit patterns for bin 0 with pattern "0000" through bin 15 with pattern "1111" under 2-PN reuse case

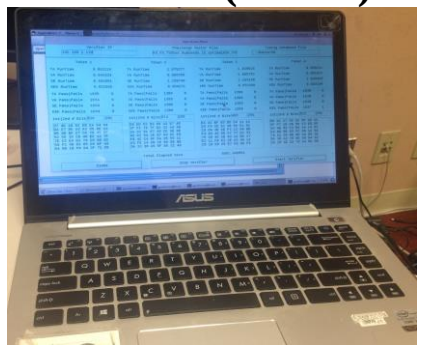
Table 2: minEntropy for PND_c and x-PN experiments.

	2-PN	Normal	3-PN	Normal	4-PN	Normal
No Offset, No Mod	2.11 of 4	3.05 of 4	3.17 of 9	6.15 of 9	4.3 of 16	7.0 of 16
No Offset, Mod	3.92 of 4	3.81 of 4	6.10 of 9	7.89 of 9	8.3 of 16	10.2 of 16
Offset, No Mod	2.02 of 4	2.82 of 4	3.05 of 9	5.34 of 9	4.1 of 16	8.5 of 16
Offset, Mod	**3.73 of 4**	**3.92 of 4**	**6.95 of 9**	**8.40 of 9**	**9.2 of 16**	**11.1 of 16**

PREVIOUS AND ON-GOING WORK IN CYBERSECURITY - Continued

- **A Mutual and Privacy-preserving Authentication Protocol Based on a Hardware-Embedded Delay PUF**
  - 1. Mutual and privacy-preserving
  - 2. No crypto primitives needed on the token (resource-constrained)
  - 3. Server-side storage efficient (store timing instead of response bitstrings)
  - 4. Resistant to model-building attacks (HOST paper 2018)

Verifier (Server)



Mutual
privacy-preserving

Resource-constrained

Prover (HW Tokens)

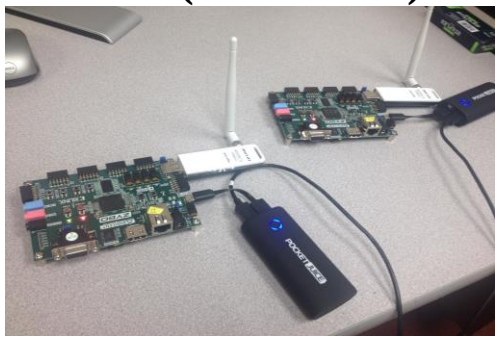


Fig. 5 Implementation of the protocol using a laptop and multiple Xilinx Zybo FPGAs

PREVIOUS AND ON-GOING WORK IN CYBERSECURITY - Continued

- **Machine Learning Attacks and Delay Model Investigation of the HELP PUF**
  - Proposed a delay model that represents the path sensitization conditions using Boolean expressions. The delay model helps to analyze the complexity of the path sensitization phase of the HELP PUF
  - Investigated the model-building attack resistance of the HELP PUF using multiple state-of-art machine learning algorithms (LR, SVM and AdaBoost)

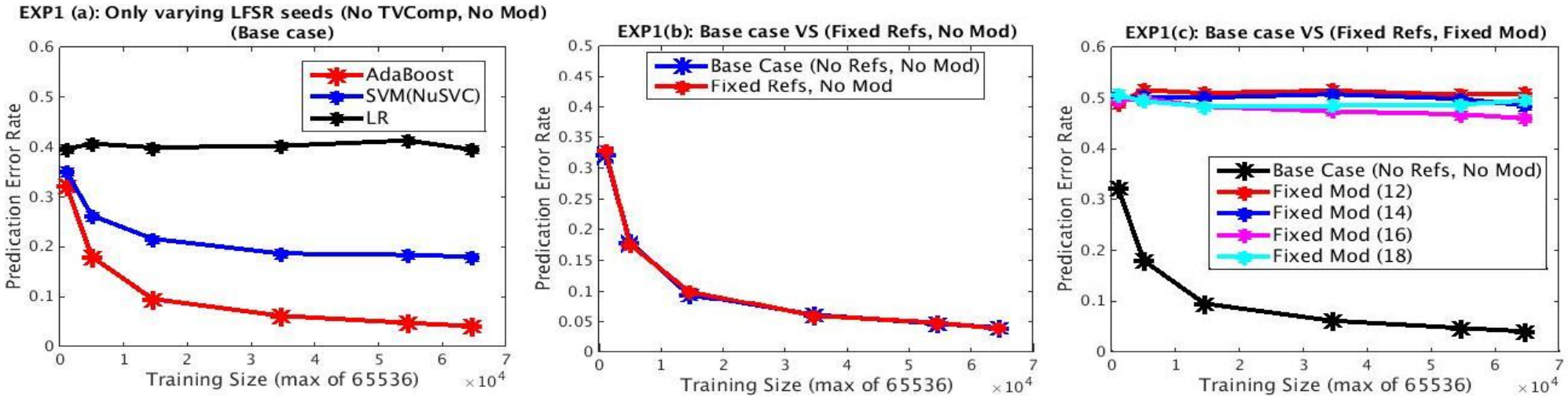


Fig. 2 ML prediction error (using Logistic Regression, SVM and AdaBoost) when fixed parameter values are used

CURRENT WORK IN CYBERSECURITY

- I have been recently working on how to extend the techniques that enhanced the entropy and model-building resistance of the Hardware-Embedded Delay PUF (HELP PUF) to other general delay based PUFs, such as RO-PUFs and Arbiter-PUFs.

- I have been recently looking into security issues (authentication and encryption) in compressed sensing, specifically on how to apply hardware security and physical layer security to security problems in the area of compressed sensing.

FUNDING SOURCES

Project title: CREST: Interdisciplinary Center for Research Excellence in Design of Intelligent Technologies for Smartgrids Phase II

Funding agency: NSF

Role: Senior personnel

RESEARCH NEEDS

- **Directions/Areas that would benefit from collaboration:**
  - Compressed Sensing, security issues of compressed sensing
  - Embedded systems

Thank you!

Questions?