Research Spotlight Forum

8.6.19 Cybersecurity

Hardware-Oriented Security and Trust

PRESENTED BY:

Jim Plusquellic, ECE at UNM, jimp@ece.unm.edu

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

SAND2019-9382 PE

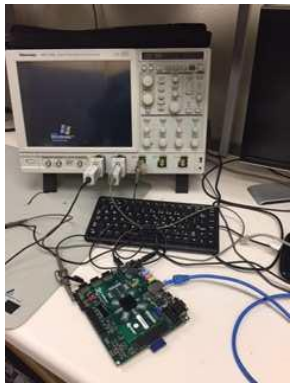
Professor Jim Plusquellic, ECE, UNM

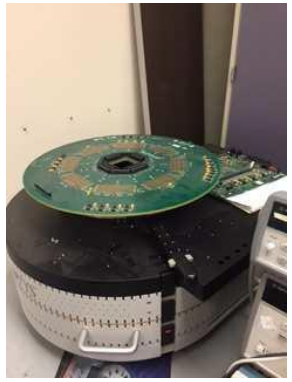
Research Areas:

- Physical Unclonable Functions (PUFs)
- Trusted and Secure Boot of FPGAs
- Hardware Trojan Detection Methods
- Differential Power Analysis Resistance

Co-founder of Hardware-Oriented Security and Trust (HOST) Symposium

Integrated Circuit Hardware Analysis Laboratory (IC-HAL)





Physical Unclonable Functions (PUFs)

Secret keys serve as the root-of-trust in most systems

Threat: Adversaries steal keys from chips using probing attacks

PUFs give chips unique identities

Chips, like snow flakes, are never identical

Manufacturing variations give chips a 'DNA' like fingerprint

PUFs are designed to derive bitstrings by measuring small 'analog' differences that exist among otherwise identical chips

The bitstrings can be used as keys for encryption, authentication, and tamper detection

Physical Unclonable Functions (PUFs)

Benefits:

- PUF keys are generated on-the-fly and cannot be accessed when the chip is powered off
- PUFs provide an alternative to storing secrets in non-volatile memories (NVM)
- PUFs are changed or destroyed by invasive probing attacks
- PUFs create keys from ***unclonable*** physical and electrical variations introduced naturally by manufacturing process variations

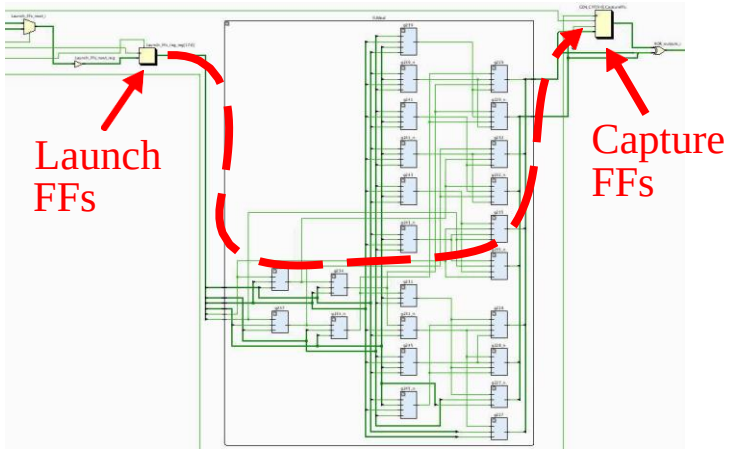
PUFs eliminate the need for NVM, saving on chip cost and eliminating vulnerabilities associated with NVM

Research: We developed a strong PUF called HELP

HELP measures path delays in combination logic circuits as a source of Entropy

Logic transitions are 'launched' into the logic circuit and delays measured at the Capture FFs

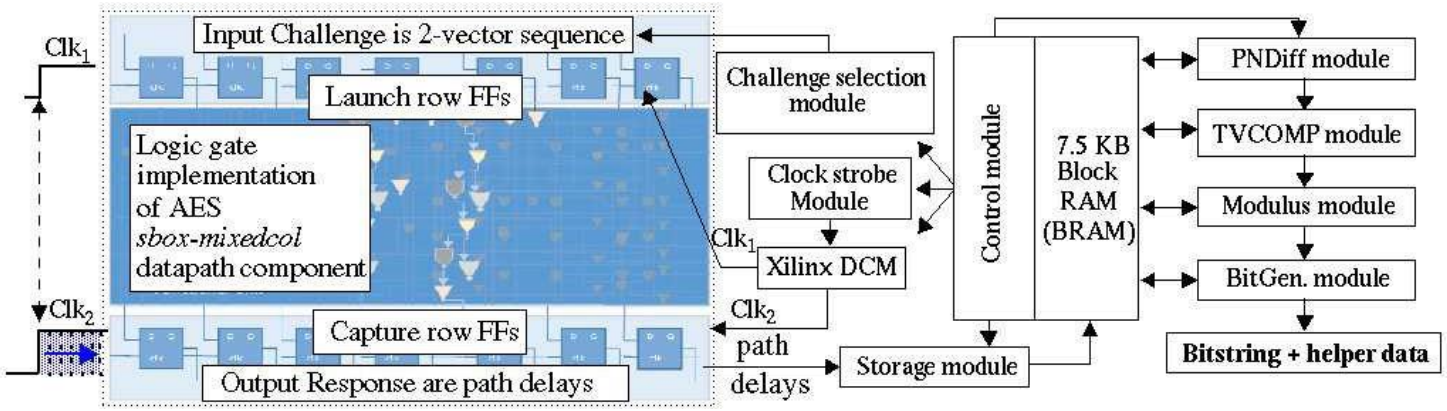
The path delays are distinct from one copy of the chip to another



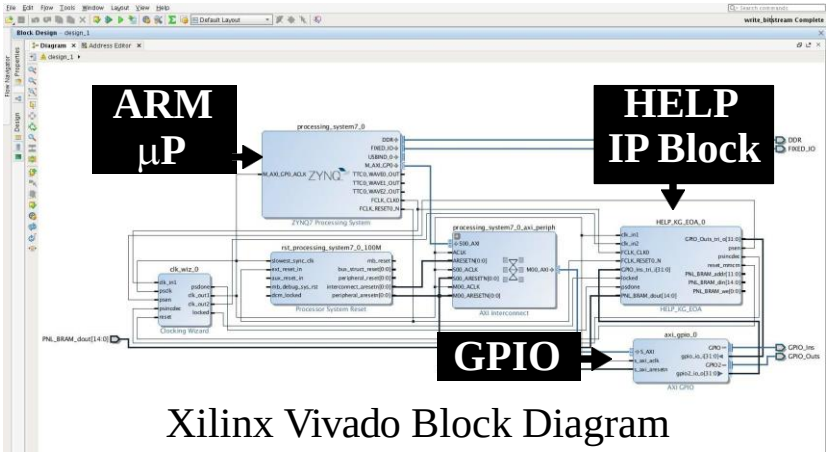
Professor Jim Plusquellic, jimp@ece.unm.edu, ece-research.unm.edu/jimp

Tech-Transfer and Commercialization by Enthentica Inc.

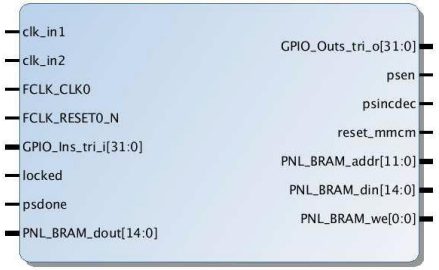
Block Diagram of HELP



Intellectual Property (IP) Block for HELP



Xilinx Vivado Block Diagram



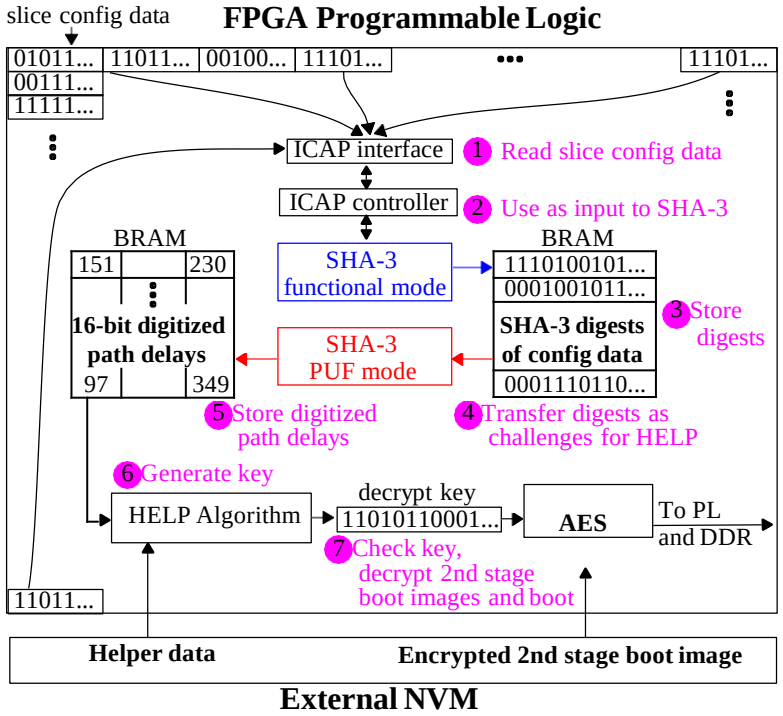
Drag and drop IP into design

Professor Jim Plusquellic, jimp@ece.unm.edu, ece-research.unm.edu/jimp

Trusted and Secure Boot of FPGAs

Threat: Adversaries reverse engineer, manipulate and replace source code in fielded systems with back-doors, information leakage channels and 'kill-switches'

Research: A novel, autonomous, self-authenticating and self-contained FPGA secure boot process is proposed that leverages the HELP PUF called BulletProoF.



Professor Jim Plusquellic, jimp@ece.unm.edu, ece-research.unm.edu/jimp

Trusted and Secure Boot of FPGAs

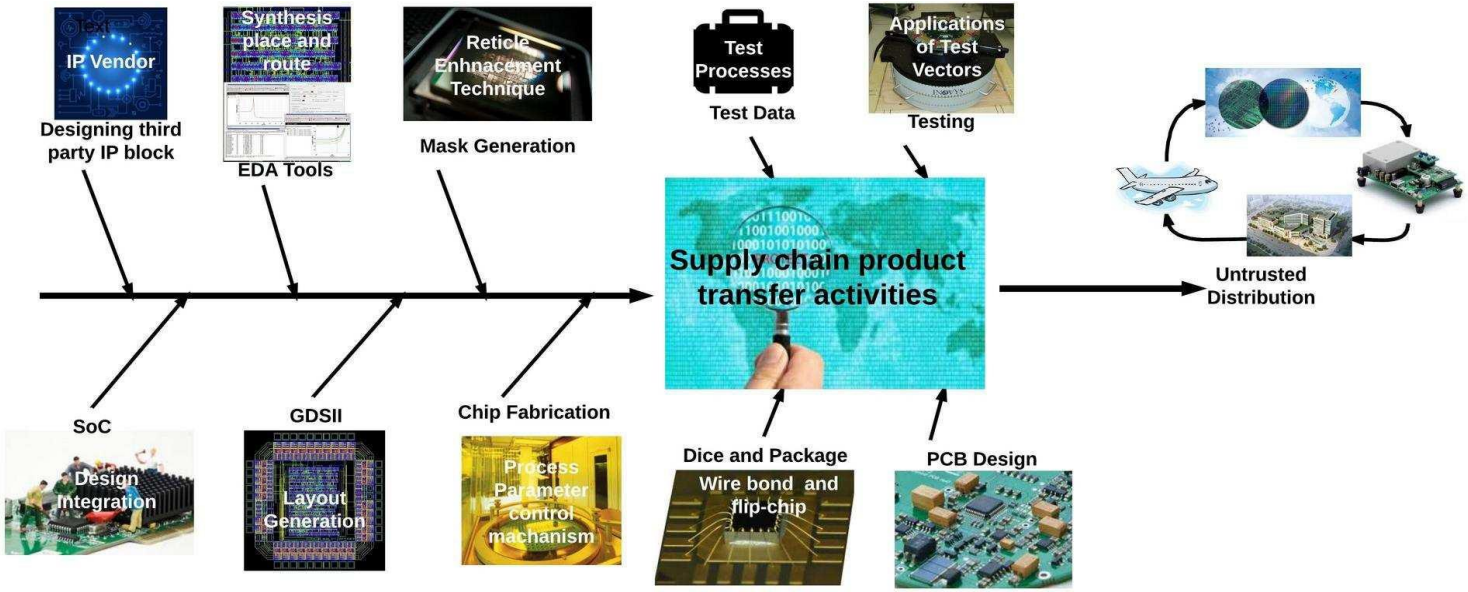
Benefits:

- The secure boot process uses a PUF-generated encryption/decryption key, and therefore avoids vulnerabilities with Battery-backed RAM, eFuses and NVM
- The key is never revealed, even during the provisioning stage which occurs in a secure environment
- BulletProoF is entirely self-contained, and therefore does not use any embedded/hard- wired clock generation or security blocks on the FPGA
- BulletProoF is autonomous and therefore cannot be stopped once it is started, mitigating fault injection, differential power analysis and many other semi-invasive attacks

Professor Jim Plusquellic, jimp@ece.unm.edu, ece-research.unm.edu/jimp

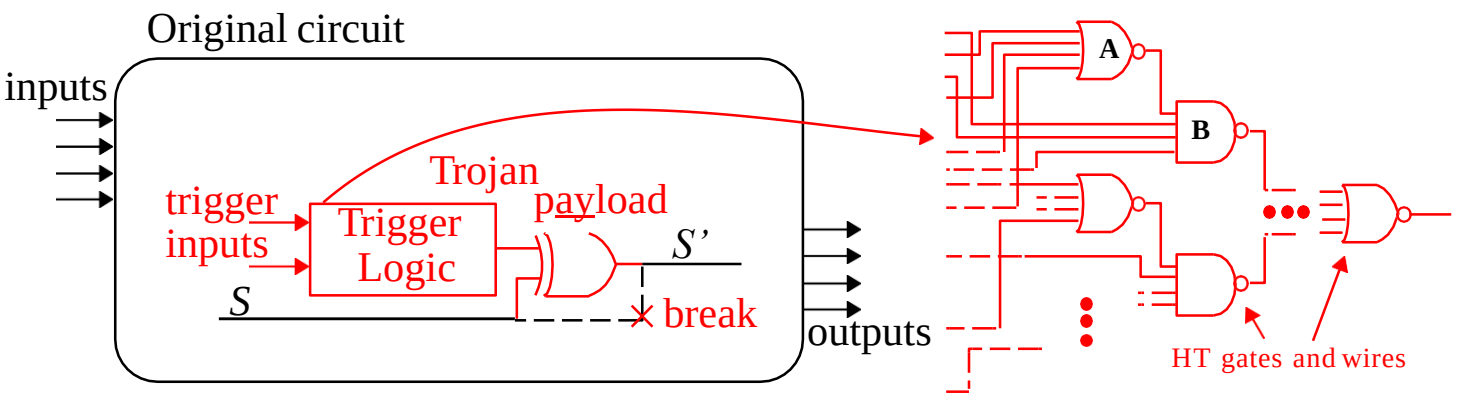
Hardware Trojan Detection Methods

Threat: Supply Chain Vulnerabilities



Threat: Adversaries add functionality to the chip design or field programmable gate array (FPGA) that introduce an information leakage channel or ‘kill-switch’

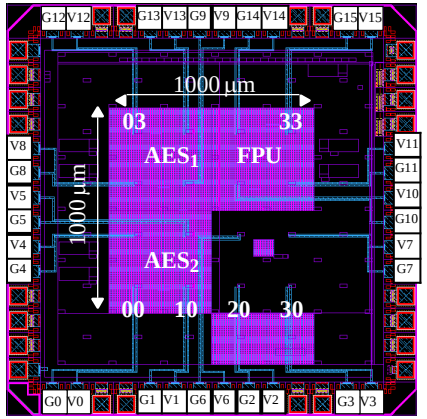
Hardware Trojan Detection Methods



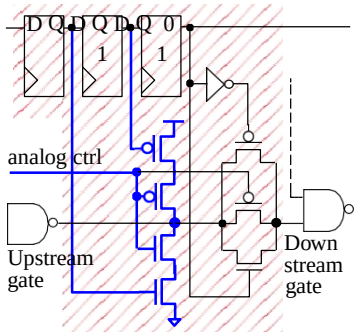
Research: VLSI test methods that are able to detect additional circuitry

Power Supply Methods

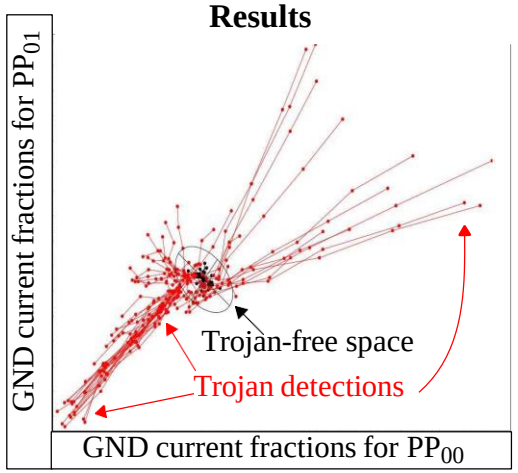
Custom chip



Trojan circuit



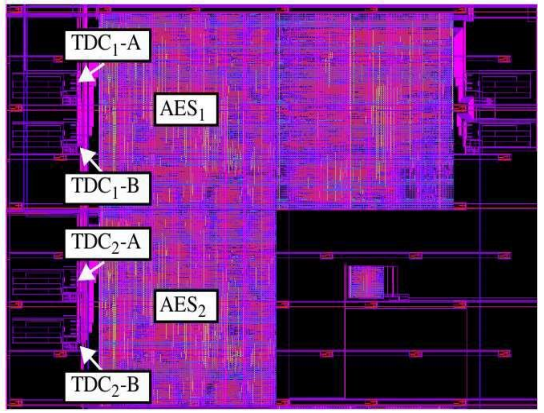
Results



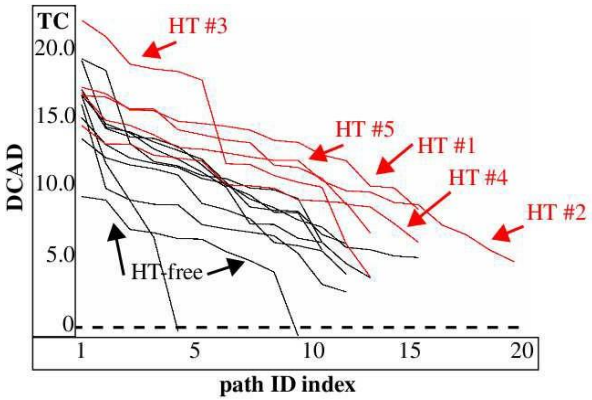
Professor Jim Plusquellic, jimp@ece.unm.edu, ece-research.unm.edu/jimp

Hardware Trojan Detection Methods Path Delay Testing Methods

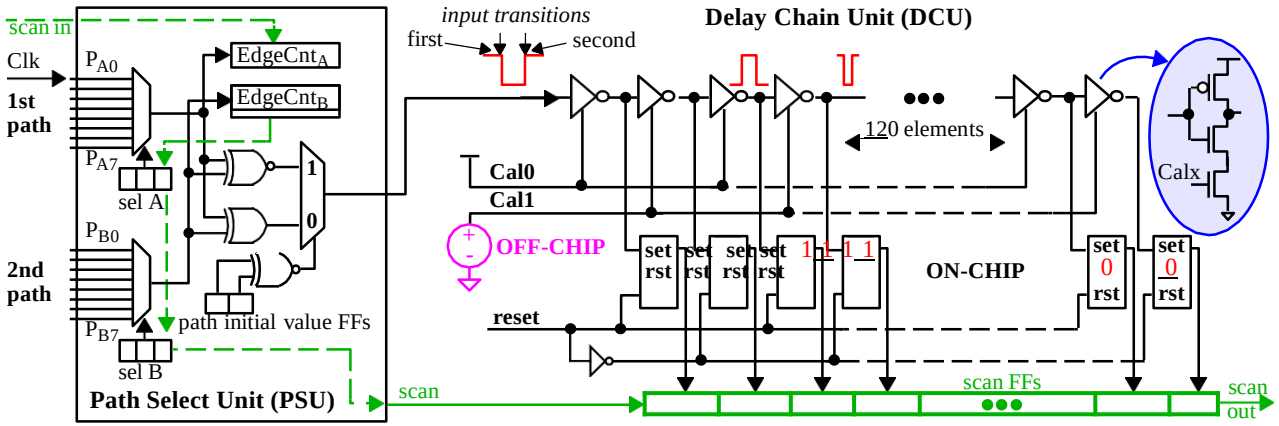
Custom Chip with NIST Encryption Engine



Results



Time-to-digital converter (TDC): On-Chip High Resolution Delay Measurement Circuit



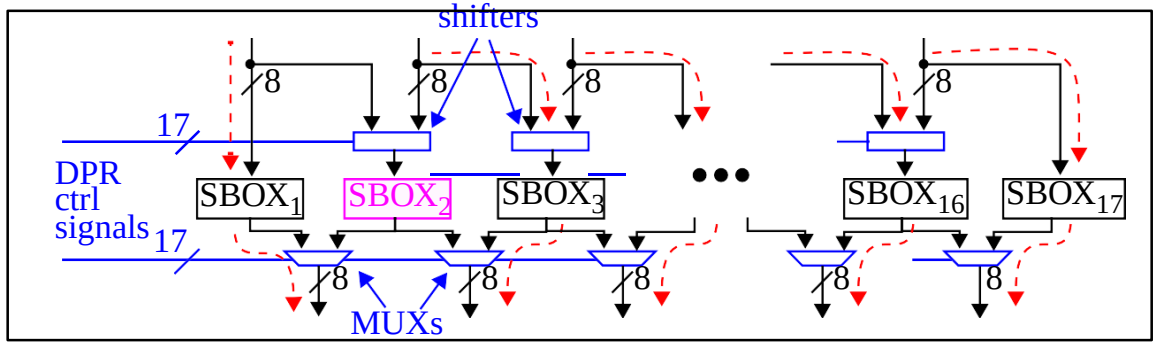
Professor Jim Plusquellic, jimp@ece.unm.edu, ece-research.unm.edu/jimp

Differential Power Analysis Resistance

Threat: Adversaries use oscilloscopes to probe chips and steal internal secrets: keys

Research: We use **implementation diversity** and **dynamic partial reconfiguration** (DPR) in FPGAs as a means of making this difficult/impossible for the adversary

Advanced Encryption Standard (AES) block diagram



We call our technique "Side-channel Power Resistance for Encryption Algorithms using Dynamic partial reconfiguration" or **SPREAD**

SPREAD rapidly changes the implementation characteristics of components of encryption algorithm (while preserving the functionality) using DPR

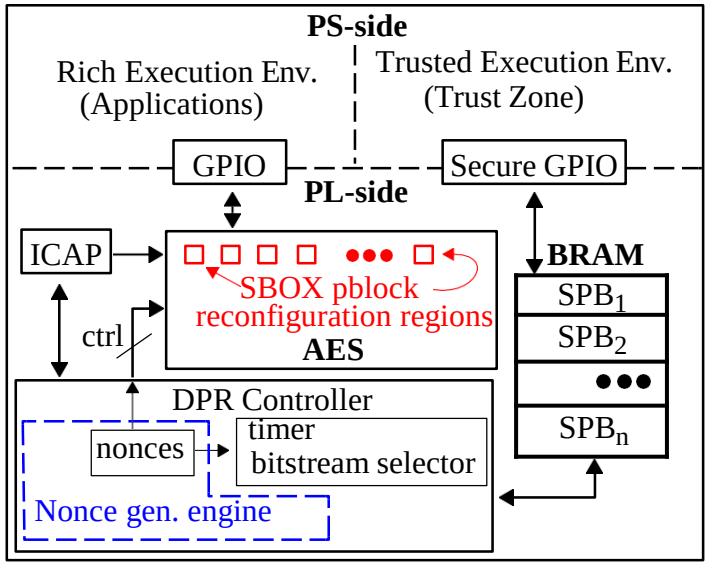
CAD synthesis tools are used to create different implementations of the SBOX

Differential Power Analysis Resistance

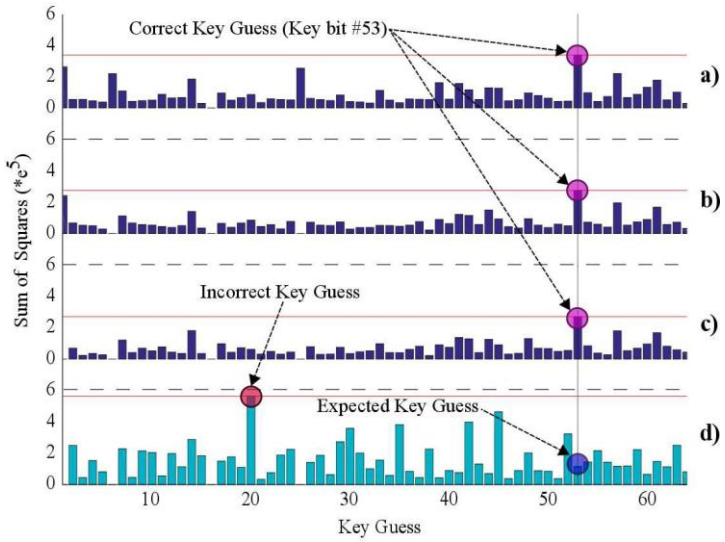
Benefits:

- SPREAD implements a countermeasure defeating the fundamental assumption on which DPA depends, that the underlying circuit implementation remains **invariant**
- SPREAD is autonomous and implemented entirely within the programmable logic of the FPGA, mitigating attacks that attempt to disable it
- SPREAD uses a PUF for key generation, mitigating vulnerabilities associated with NVM and other types of on-chip key storage mechanisms

FPGA



Preliminary Results



Professor Jim Plusquellic, jimp@ece.unm.edu, ece-research.unm.edu/jimp