Foundations for Future On-chip Fingerprints

PIs: P. Schaumont, L. Nazhandali, I. Kim

Electrical and Computer Engineering & Statistics, Virginia Tech

What is a Physical Unclonable Function, and why do we need it?

PUF

- A PUF is a one-way function with a mapping determined by uncontrolled, but static, variations of a physical object

Applications

- Cryptographic Key Generation
- Authentication

Requirements

- Stable
- Unique
- Unclonable
- Unpredictable
- One-way

A Silicon PUF is a fingerprint, a biometric unique a single chip

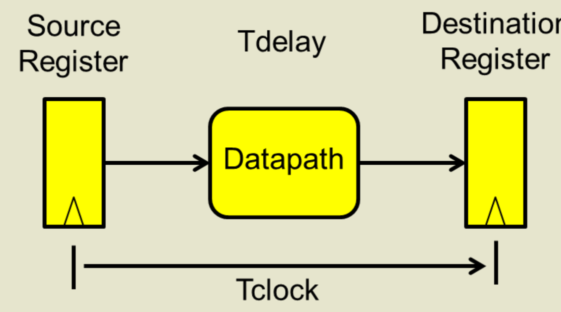
This project explores novel PUF artifacts, data, and analysis methods

Artifact

[FPL 2012]

Microprocessor-based Physical Unclonable Function

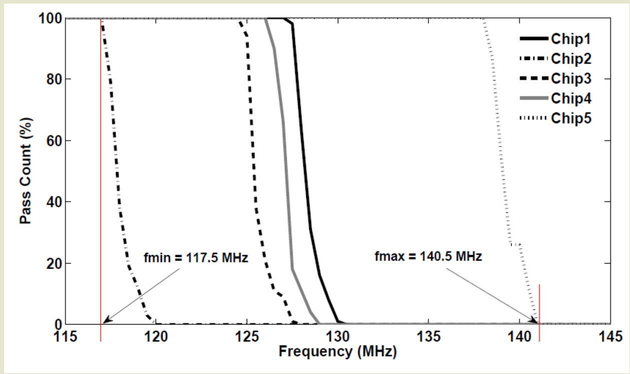
Measureme CPU Delay with Clock Sweeping



SW-driven Measurement

```
<set clock>
mov r1, #0x7FFFFFFF
mov r2, #0x1
add r1, r2, r3
cmp r3, 0x80000000
```

CPU Characterization



Analysis

[FPL 2011]

Aging of PUF

Are old PUF stable? Are they unique?

Stability Degrades (5-10%)

Uniqueness Almost Constant (0.5%)

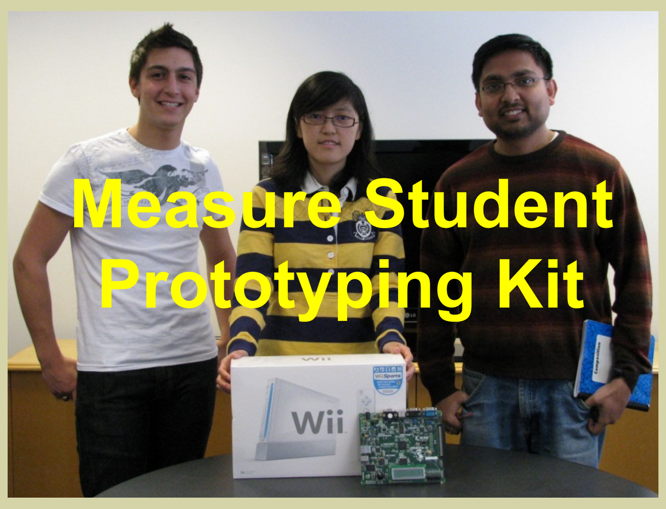
Aging tolerable w error correction

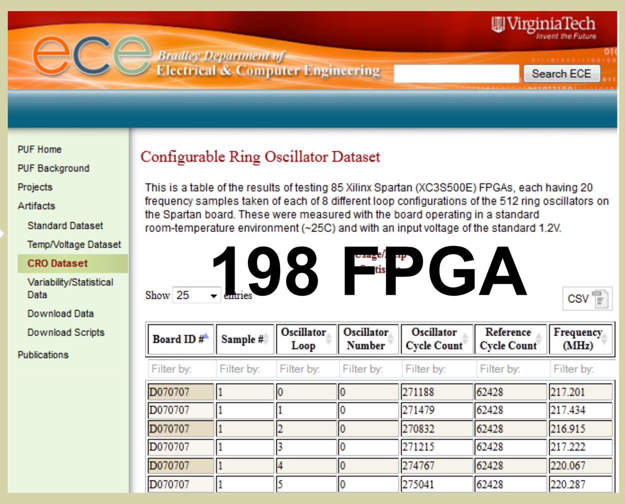
Data

[HOST 2010]

FPGA Measurements of RO PUF

How to quickly measures lots of chips?





http://rijndael.ece.vt.edu/puf

Selected Publications

- Kim, A. Maiti, L. Nazhandali, P. Schaumont, V. Vivekraja, H. Zhang, "*From Statistics to Circuits: Foundations for Future Physical Unclonable Functions*," chapter in "Towards Hardware Intrinsic Security," eds. A. Sadeghi, Springer Information Security and Cryptography Series, Part 1, 55-78, 2010, Springer, DOI: http://dx.doi.org/10.1007/978-3-642-14452-3_3
- A. Maiti, J. Casarona, L. McHale, P. Schaumont "*A Large Scale Characterization of RO-PUF*," IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2010), Anaheim, June 2010, DOI: http://dx.doi.org/10.1109/HST.2010.5513108
- D. Ganta, V. Vivekraja, K. Priya, L. Nazhandali, "*A Highly Stable Leakage-Based Silicon Physical Unclonable Function*", 24th International Conference on VLSI Design (VLSI Design), Chennai, India, Jan 2011, DOI: http://dx.doi.org/10.1109/VLSID.2011.72
- A. Maiti, L. McDougall and P. Schaumont, "*The Impact of Aging on An FPGA-Based Physical Unclonable Function*," 21st International Conference on Field Programmable Logic and Applications (FPL 2011), September 2011, DOI: http://dx.doi.org/10.1109/FPL.2011.35
- A. Maiti, I. Kim and P. Schaumont, "*A Robust Physical Unclonable Function with Enhanced Challenge-Response Set*," IEEE Transactions on Information Forensics and Security, 7(1): 333-345, February 2012
- A. Maiti, P. Schaumont, "*A novel microprocessor-intrinsic Physical Unclonable Function*," Field Programmable Logic and Applications (FPL), 2012 22nd International Conference on , vol., no., pp.380-387, 29-31 Aug. 2012 doi: 10.1109/FPL.2012.6339208
- Y. Xu, I. Kim, P. Schaumont, "*A Spatial Test Statistic to Compare Identity Distributions*," Technical Report, Virginia Tech, June 2012 (currently under review).

Interested in meeting the PIs? Attach post-it note below!