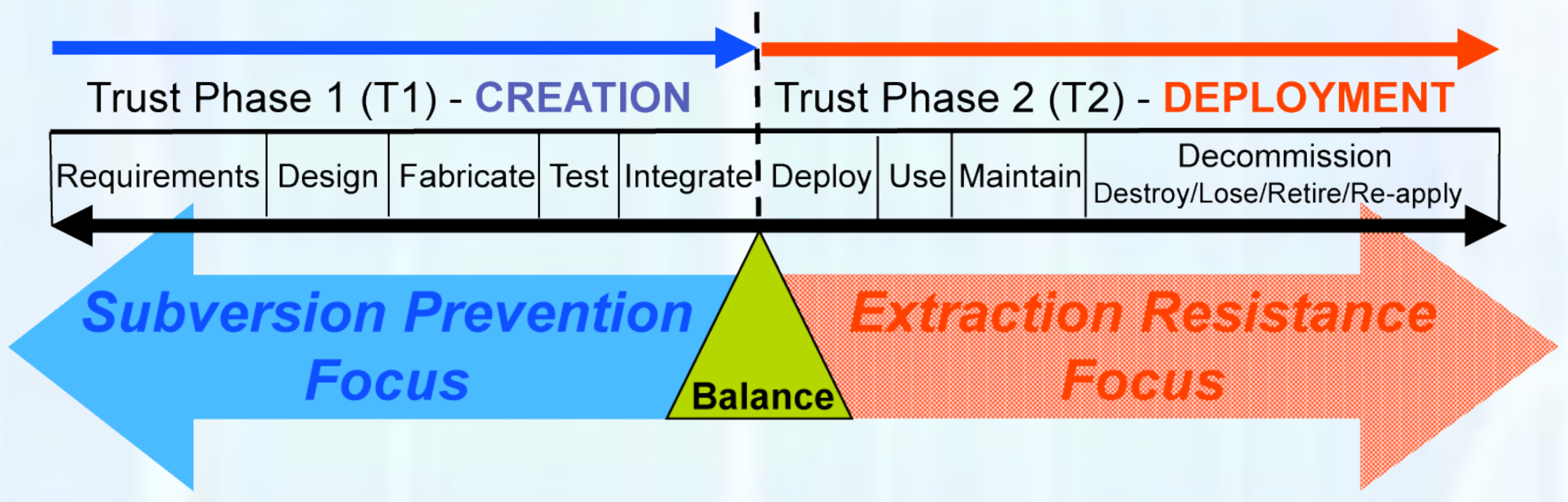
Infrastructure for Nondestructive Real-time Fingerprinting of Integrated Circuits

Sandia National Laboratories
Todd Bauer, Lyndon Pierson, Jason Hamlet

Problem

- The nation state adversary is uniquely capable of subversion of microelectronics in the creation portion of the life cycle and extraction in the deployment portion of the life cycle.
- "Trusted Foundry" processing of microelectronics protects against subversion during the fabrication phase of a product life cycle. However, during the deployment phase of a product life cycle, component authenticity can be difficult to determine.


Trust Phase 1 (T1) - CREATION
Trust Phase 2 (T2) - DEPLOYMENT
Requirements
Design
Fabricate
Test
Integrate
Deploy
Use
Maintain
Decommission
Destroy/Lose/Retire/Re-apply
Subversion Prevention Focus
Balance
Extraction Resistance Focus

Simplified Threat Model

- Some deployed systems rely on physical protections to maintain trustworthiness. An alternative to physical protections is to employ robustly authenticated hardware. Physical Unclonable Functions (PUFs) can be leveraged for robust authentication to harden systems against substitution of counterfeit components. PUFs are derived from random physical characteristics of the system from which they are sourced, which makes a PUF output difficult to predict. The random PUF output can subsequently be used to establish a unique "fingerprint" for authentication.
- We note that component substitution can be motivated by the desire to subvert the intended function of the targeted component (the goal of a nation-state adversary), or by financial gain (the goal of a commercial counterfeiter). Robust authentication protects against both.
- This project seeks to augment the trustworthiness of deployed information processing systems by advancing the state of the art for authentication of microelectronics components to protect against substitution of counterfeit components.

Approach

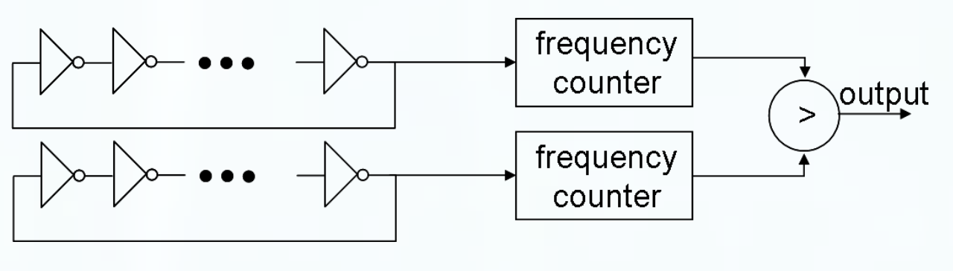
- Our goal is to characterize the infrastructure required to fully leverage PUFs technology. An attractive test bed for PUFs implementation is commercially available FPGAs. FPGAs allow insertion of user-defined logic into a system without requiring custom, long lead time application specific integrated circuits (ASICs). For these reasons, FPGAs are widely deployed in commercial and military systems. Because FPGAs are widely deployed, improving their trustworthiness against counterfeit insertion has the potential to benefit a broad spectrum of end users.
- We have endeavored to
  1. consider open literature PUFs and their inputs and outputs, and discover PUF data handling conventions if any exist,
  2. formulate strategies for a) implementing PUFs into FPGAs and other integrated circuits, and b) handling PUF-based data,
  3. implement the proposal on an FPGA-based system for proof-of-principle.
- Although our demonstration vehicle is the FPGA, we assert that the result of our effort will prove useful to authenticating ASICs.

Results

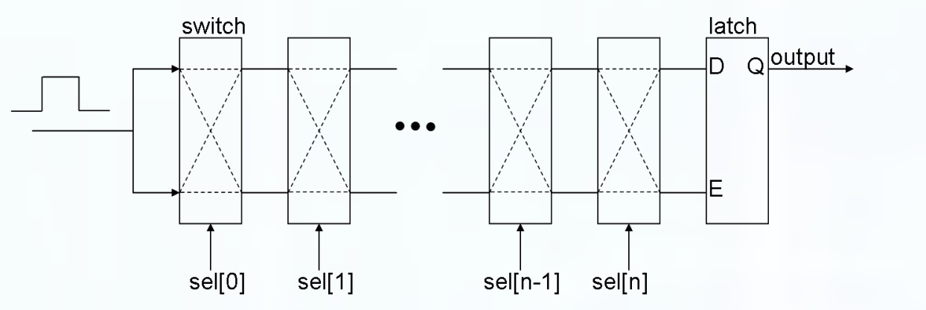
Physical Unclonable Functions (PUFs)

- The ideal PUF provides large inter-device variation so different devices produce different outputs, while intra-device variation should be nil so that a given device provides the same response to a given challenge. A good PUF should be robust to changes in environmental conditions. The open literature provides examples of circuit-based PUFs. Two examples are shown below.

Ring oscillator PUFs exploit variations in the resonant frequencies of a pair of ring oscillators (Suh, 2007). The resonant frequencies are measured and compared, and the output bit is determined by which oscillator resonates at the highest frequency. A k bit sequence is produced comparing k resonator pairs.



Arbiter PUFs use multiplexed switch circuits (Suh, 2007). A pulse is presented to the inputs. The signal races along the two user-selectable paths through n switches. After the last switch an arbiter determines the output of the circuit; if the D input arrives first the output is '0'; if the E input arrives first the output is '1'. A k bit sequence is produced by evaluating k chains.



G. E. Suh and S. Devadas, *Physical unclonable functions for device authentication and secret key generation*. In *Proceedings of the 44th Annual Conference on Design Automation,* DAC 2007, pp. 9-14.

Results (cont.)

Fuzzy Extractors with Error Correcting Code (ECC)

- PUF-based authentication relies on generation of a secret, reproducible, random bit stream. Fuzzy extractor algorithms can be used to extract such a bit stream from a PUF output in a manner that accommodates irreproducible noise in the PUF output. In mathematical terms, fuzzy extraction with error correction is described as follows, where key generation connotes an initialization of the PUF output after a first measurement and key reconstruction connotes an authentication after subsequent measurements.

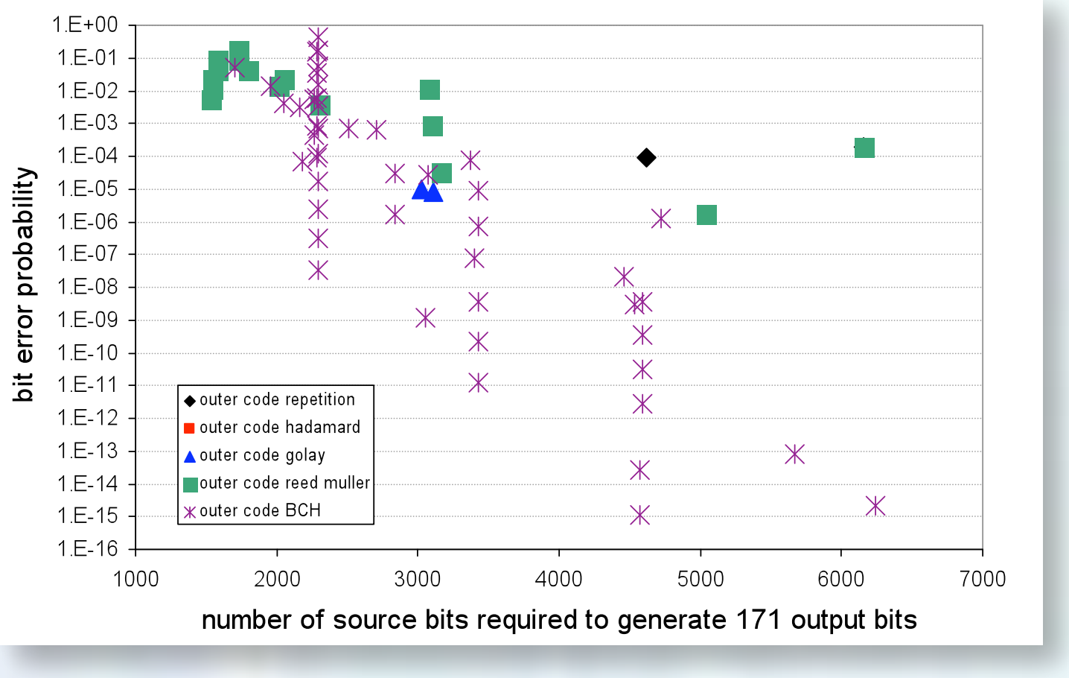
Key Generation/Enrollment

- Input: PUF output R
- Output: Key K, helper data (W_1,W_2)
- Choose codeword C_s at random from error-correcting code C
  Set $W_1 \leftarrow C_s \oplus R$
- Choose hash function h_i, set
  $K \leftarrow h_i(R)$
  $W_2 \leftarrow i$
- Output $(K, W) = (K, (W_1, W_2))$

Key Reconstruction/Authentication

- Input: PUF output R', $W=(W_1,W_2)$
- Output: Key K
- Calculate $W_1 \oplus R' = C_s \oplus R \oplus R' = C_s \oplus e$
- Use ECC decoding algorithm to recover C_s from $C_s \oplus e$
- Recover R:
  $W_1 \oplus C_s = (C_s \oplus R) \oplus C_s = 0 \oplus R = R$
- Reconstruct K
  $K \leftarrow h_i(R)$

- Implementation of fuzzy extractors with ECC shows that the selection of ECC is critical. The goal for ECCs is to force intra-device variation to 0% (low bit error probability within a device), while maintaining good inter-device variation (to establish unique identification among devices).
- The plot below shows intra-device bit error probability as a function of the number of source bits needed to generate 171 output bits for assorted ECC concatenation schemes.
  - Compared to single pass ECC, ECC concatenation improves output bit error probability at a given number of source bits by many orders of magnitude.



- The analysis assumes a large amount of intra-device variation between initial and subsequent measurements.
  - Using a PUF that is robust over time and to changes in environmental conditions (low intra-device variation) can dramatically reduce the overhead associated with bit generation, fuzzy extraction, and error correction.

List infrastructure

- For authentication, PUFs implementation results in a unique PUF output that is tied to a specific IC. An IC manufacturer will maintain this association in a list. The integrity of this IC-PUF association will determine the robustness of the authentication, so the integrity of the list infrastructure becomes critically important.
- To evolve list infrastructure, we have developed and analyzed efficient protection mechanisms to detect and prevent:
  - Insertion of bogus authentication information into the list generated and maintained by a trusted party.
  - Playback/masquerade of a prerecorded or maliciously fabricated response intended to spoof the proper authentication of an IC.
  - We have analyzed myriad list infrastructure implementations and documented potential vulnerabilities associated with each implementation.
- We have prototyped FPGA-based PUFs, fuzzy extractors with error correction, and public key infrastructure to accomplish the protection measures for robust IC authentication.
- We are beginning to analyze the required intra-device stability, inter-device randomness, and protections against bogus list insertion and playback to achieve robust IC authentication.

Significance

- Of the three categories of computer attacks identified by Meyers, 1980:
  1. Inadvertent Disclosure.
  2. Penetrations.
  3. Subversions.
     - Subversion is the most dangerous and difficult to deal with (because hard to detect if done well…)*.
     - Subversion separates Nation State Adversaries from lesser adversaries**.
- A "Trusted Foundry" may produce highly trustworthy components, but these can still be substituted with subverted components later in the life cycle, unless some method of positively recognizing the trustworthy components is employed.
- The methods under development in this LDRD will provide a foundation for implementing new protection measures for hardware (and for software running on such hardware) that enables detection (and deterrence) against IC component substitution, which improves the trustworthiness of even widely deployed hardware.

*Meyers, Philip A., Subversion: the Neglected Aspect of Computer Security, June 1980 Masters Thesis, http://csrc.nist.gov/publications/history/myer80.pdf

** J. Gosler, "Vaults, Mirrors, Masks, page 182"

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department
of Energy's National Nuclear Security Administration under contract
DE-AC04-94AL85000. SAND2009-5101P