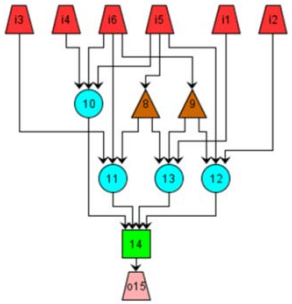
Functional Polymorphism for Intellectual Property Protection

J. Todd McDonald, Yong C. Kim, Todd R. Andel, James McVicar, Miles A. Forbes

Center for Forensics, Information Technology, Security (CFITS)
University of South Alabama



Polymorphic gates and circuits have been used in the past to design evolutionary components that can sense the environment, changing their function based on environmental properties such as temperature and power. We implement the concept of functional polymorphism at the design level using realized ***polygates*** and consider its application for IP protection in specific digital supply chain settings.

Key Contributions:

- Introduce new logic encryption algorithm for general circuits that utilize ***polygates***
- Profile 6 major generation options (full/random, key compression, polygate generation)
- Case study results of size/depth overhead on traditional combinational benchmarks
- Provide security characterization for foundry-attack model adversary

Future:

- Characterize logic encryption attack methods in Man-at-the-end (MATE) setting
- Address topological hiding / skeletal recovery
- Assess best mix of overhead / entropy for optimal security

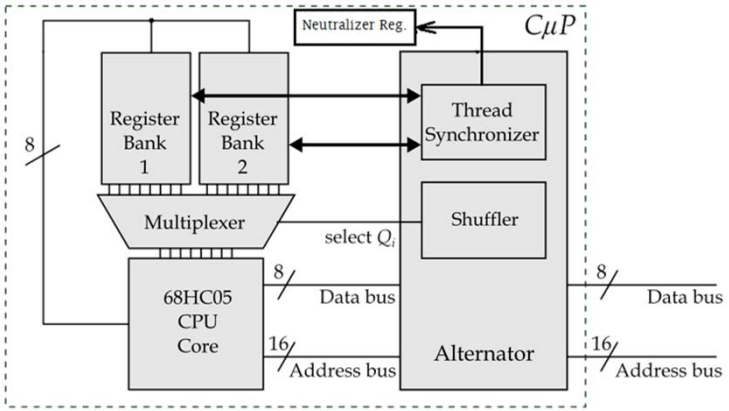
THE CONJOINED MICROPROCESSOR

- Ehsan Aerabi
- A. Elhadi Amirouche
- Houda Ferradi
- Rémi Géraud
- David Naccache
- Jean Vuillemin

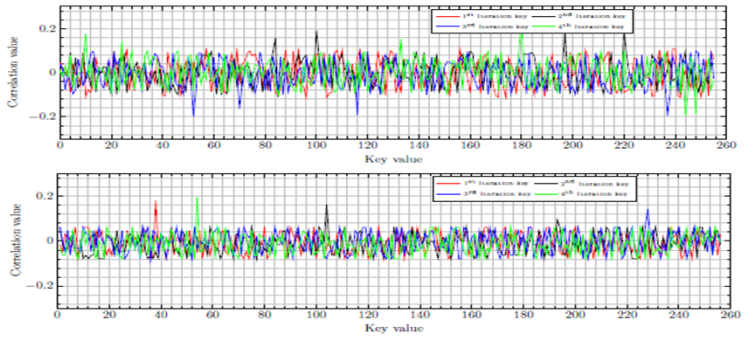
Algorithm 1: Generating queues from straight-line target code.

Data: Program $\mathcal{P}$
Result: Queues $\mathcal{Q}_0$ and $\mathcal{Q}_1$
// Initialization
for $k \in \{1, 2, ..., \textit{size of program } \mathcal{P}\}$ **do**
  $D[k] \leftarrow$ destinations of opcode$[k]$
  $S[k] \leftarrow$ sources of opcode$[k]$
  $n[k] \leftarrow \#S[k]$
  $\mathcal{Q}_i[k] \leftarrow -1$ *//assigned queue*
  $\mathcal{R}_i[k] \leftarrow -1$ *//recommendation queue*
end for
// Assigning nodes
while *there is an unassigned instruction in* $\mathcal{P}$ **do**
  find k s.t. $n[k] = 0$ and $\mathcal{Q}_i[k] = -1$
  if $\mathcal{R}[k] \neq -1$ **then**
    $\mathcal{Q}_i[k] \leftarrow \mathcal{R}[k]$
  else
    Assign opcode$[k]$ to the shortest queue
  end if
  if $\exists (R, J) \in S[k]$ *s.t.* $\mathcal{Q}_i[J] \neq \mathcal{R}[k]$ **then**
    Insert required xrr instructions before opcode$[k]$ in $\mathcal{R}[k]$
  end if
  Recommend $\mathcal{Q}_i[k]$ to appropriate nodes in $D[k]$
  for $(r, \ell) \in D[k]$ **do**
    $n[\ell] \leftarrow n[\ell] - 1$
  end for
end while

Instruction-Level Parallelization Algorithm



The Conjoined Architecture



Experimental & Analytical Results

Low Area Hardware Implementations of CLOC, SILC and AES-OTR

Subhadeep Banik[1], Andrey Bogdanov[1] and Kazuhiko Minematsu[2]

[1]DTU Compute, Technical University of Denmark, Lyngby, Denmark

[2]NEC Corporation, Kawasaki, Japan

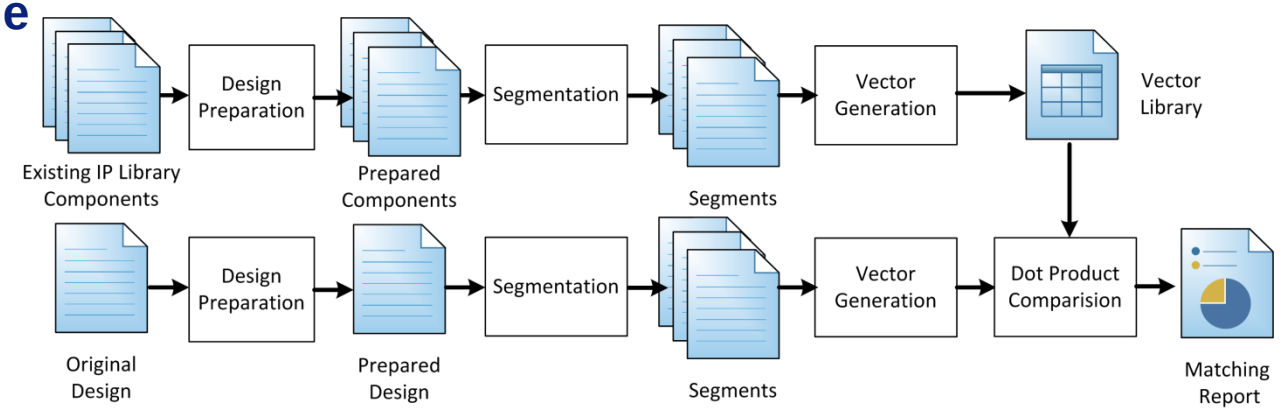
Salient Points

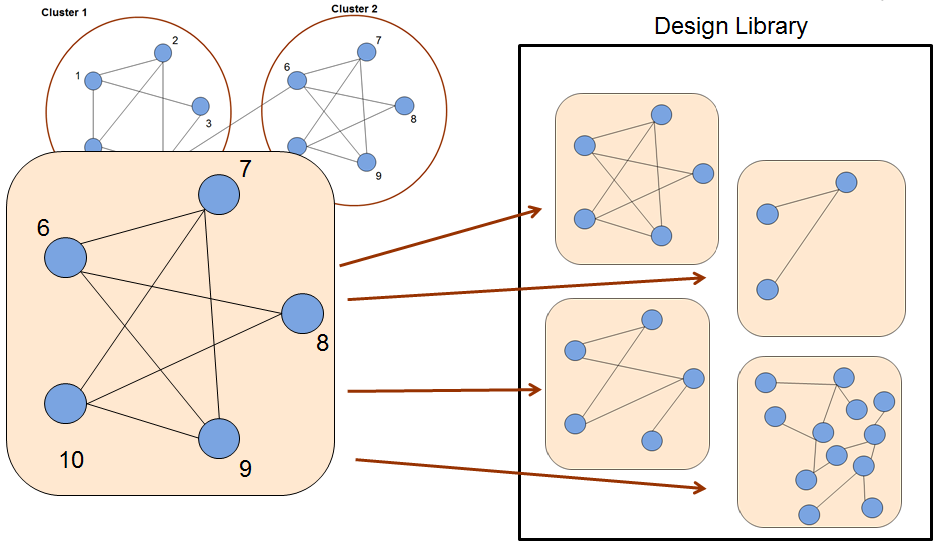
- CLOC, SILC and AES-OTR are 3 of the 29 authenticated encryption modes selected in round 2 of the Caesar competition.
- AES 128 is the underlying choice of block cipher in these modes.
- We use the 8-bit serial circuit of Moradi et al. to design circuits for the modes.
- We tweak the above design to include functionalities of the additional functions used in these modes.
- As a result our best implementation of CLOC, SILC and AES-OTR takes 3110, 3110 and 4720 GE respectively.

Functional Block Identification in Circuit Design Recovery

Jacob Couch, Elizabeth Reilly, Morgan Schuyler, Bradley Barrett

- **Mechanism to find known sub-circuits within a netlist through a computationally feasible segmentation and fuzzy matching algorithm.**
  - **Algorithm is based off the Ncut algorithm, dot product representation, and the Procrustean transform.**
  - **Applicable to both ASIC and FPGA designs.**





Blinded Random Corruption Attacks

Rodrigo Branco (Security Center of Excellence)
Shay Gueron (Core Architecture)

- Some memory protection technologies against active dynamic attacks exist (i.e.: limit physical ability to read/write memory and/or memory encryption)
- **Memory encryption using "transparent encryption" mode:**
  - Simpler, cheaper, faster than "encryption + authentication"; changes the assumptions on read/written memory capabilities of the attacker and therefore, seems to be effective for limiting active dynamic attacks
- Memory encryption effects :
  - Attacker has **limited control** on the result of active attacks
  - But the physical memory modification **capabilities remain available**
- Under memory encryption, the attacker has limited capabilities
  - **B**linded **R**andom **B**lock **C**orruption (**BRBC**) attack
    - (**Blinded**) The attacker does not know the plaintext memory values he can read from the (encrypted) memory.
    - (**Random** (**Block**) **Corruption**) The attacker cannot control nor predict the plaintext value that would infiltrate the system when a modified (encrypted) DRAM value is read in and decrypted
- The question: can memory encryption (that limits the active dynamic attacker capabilities to **BRBC** only) provide a "good enough" mitigation in practice?
- We show that:
  - Despite limited capabilities dynamic active attacks are still possible
  - Encryption-only does not offer a defense-in-depth mechanism against arbitrary memory overwrites without removing capabilities assumptions

Underlying attack assumption: attacker has physical means to modify DRAM

Trust Games: How Game Theory Can Guide the Development of Hardware Trojan Detection Methods

Jonathan Graf
Graf Research - jon@grafresearch.com
IEEE International Symposium on Hardware Oriented Security and Trust (HOST)
May 3-5, 2016

Main Contribution:

We present a game theoretic model that guides Trojan detection method development and selection. Taking into account method efficacy and security economic models of the "players," we solve to determine optimal strategies for both the adversary and the defender.

Graf Research
Unleashing Innovation

ACBuilder: A Tool for Hardware Architecture Security Evaluation

Henrique Kawakami, David Ott, Hao-Chi Wong, Ricardo Dahab, Roberto Gallo
University of Campinas (Brazil), Intel, Kryptus

- In this paper we present our research on software frameworks to aid security analysts in the development of assurance cases. Our objective is to help to discover vulnerabilities and flaws, before the costly process of design and manufacturing.

- We describe how our research prototype, ACBuilder, can be used to model hardware architectures, apply existing analysis patterns, develop analysis rules, and generate assurance cases.

LASCA LABORATÓRIO DE SEGURANÇA E CRIPTOGRAFIA

UNICAMP

On the Problems of Realizing Reliable and Efficient Ring Oscillator PUFs on FPGAs

Alexander Wild
Horst Görtz Institute for IT-Security
Ruhr-Universität Bochum, Germany

Georg T. Becker
Horst Görtz Institute for IT-Security
Ruhr-Universität Bochum, Germany

Tim Güneysu
Univeristy of Bremen & DFKI,
Germany

- Asynchronous Counters
  - Are they reliable?
  - Are they influenced by the environment or process variation?
- Structural Bias in ROs
  - What can be the reason for that?
  - Does normalization help to remove the bias?
- Evaluating RO-PUF on its own
  - What is the max. impact of surrounding logic?
  - Does it reduce the entropy of PUF?
- Area reduction of RO-PUF
  - Can components reused without entropy loss?
  - Is local routing ideal?

Model Checking to Find Vulnerabilities in an Instruction Set Architecture

Premise:

A correct and secure ISA is necessary, but not obvious

Hypothesis:

Model checking properties of the ISA is feasible

Case study:

SYSRET on Intel 64 and AMD64

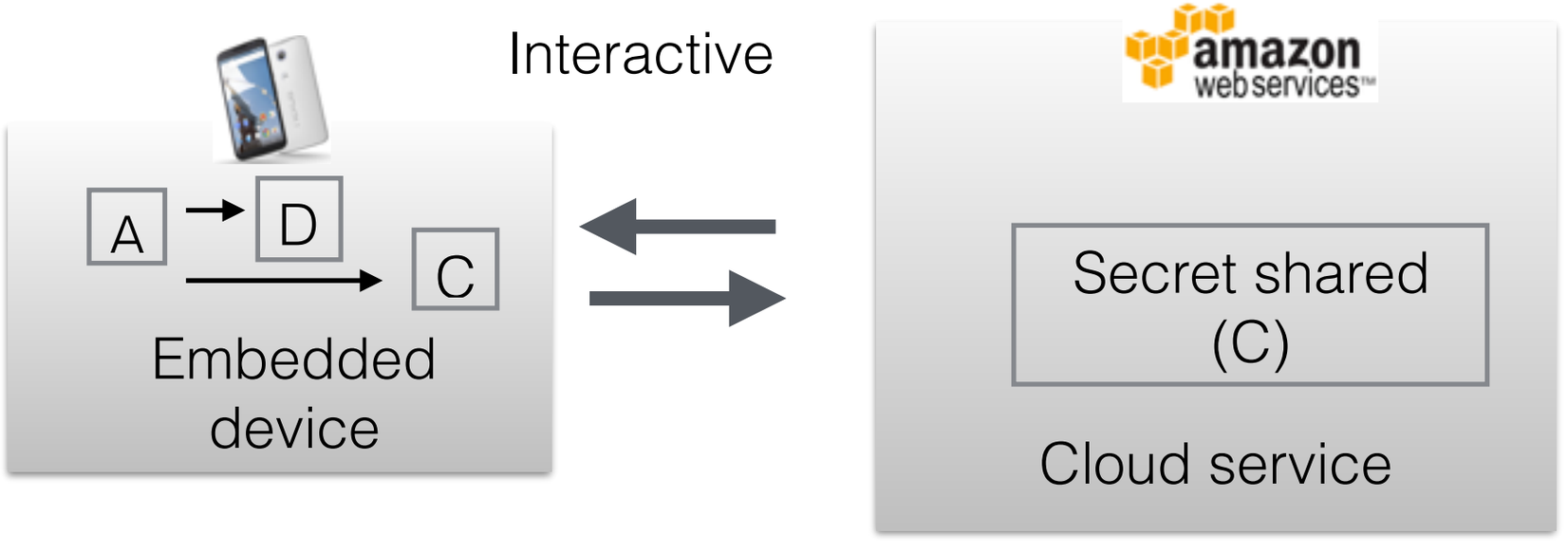
THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Chris Bradfield, Cynthia Sturton

CryptoML: Secure Outsourcing of Big Data Machine Learning Applications

Azalia Mirhoseini, Ahmad-Reza Sadeghi, and Farinaz Koushanfar
azalia@rice.edu, ahmad.sadeghi@trust.cased.de, and farinaz@ucsd.edu

- A framework for privacy-preserving delegation of a wide range of ML applications from computationally constrained clients to cloud servers
- A novel interactive data-aware delegation algorithm exploring trade-off between the efficiency and the accuracy of the ML task
- Proof of concept evaluations on datasets with billions of non-zero records



Fast and Scalable Security Support for Directory-Based Distributed Shared Memory

Ofir Shwartz, Yitzhak Birk

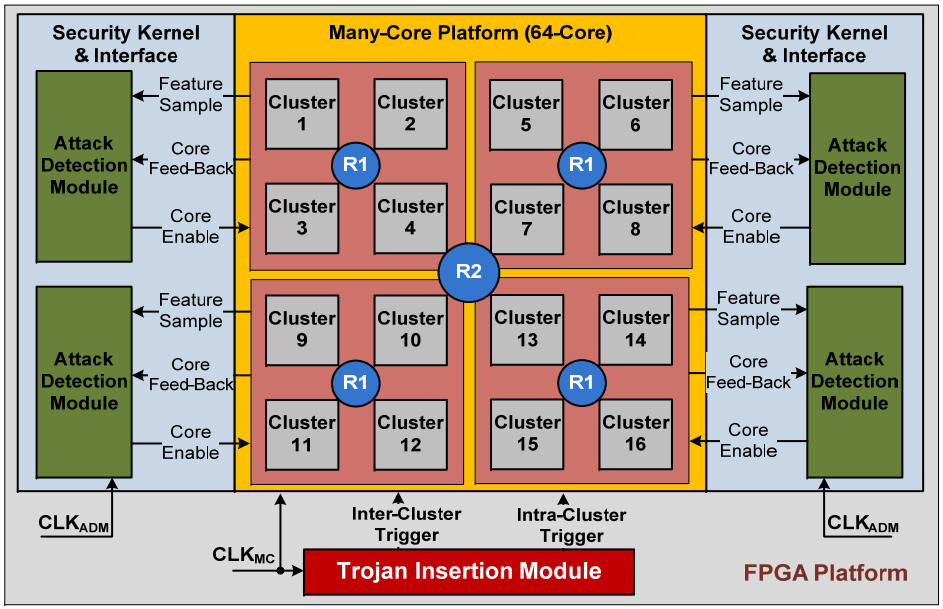
- Settings: distributed shared memory systems with memory coherence
- An efficient method for distributing encryption (one time) seeds
  - Exploiting inherent communication latencies
  - Scales to thousands of computers with constant per-core resources
  - Shows negligible (<1%) performance reduction
- A novel method for seed usage, avoiding initial / runtime encryption pad reuse
  - was not addressed before

TECHNION
Israel Institute of Technology

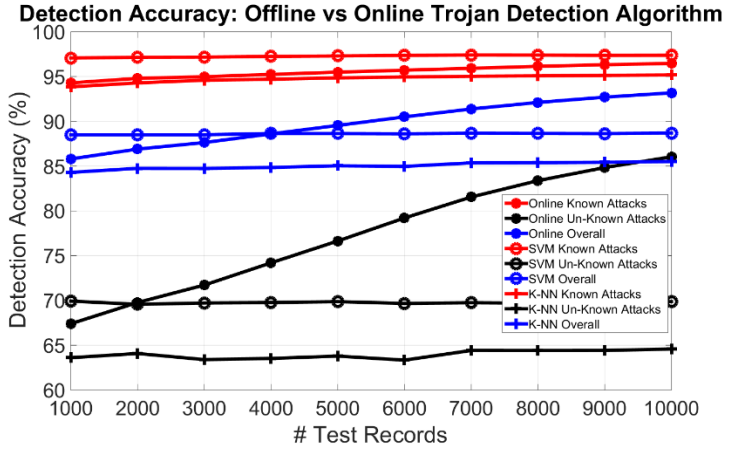
Adaptive Real-time Trojan Detection Framework through Machine Learning

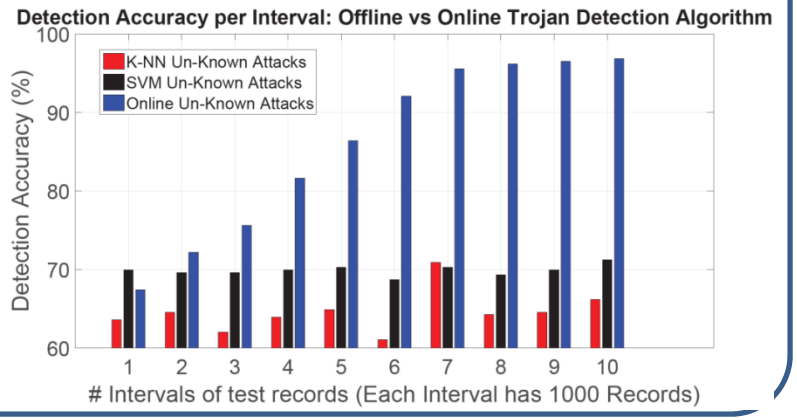
Amey Kulkarni, Youngok Pino, and Tinoosh Mohsenin

- Increase in attacker's resources and capabilities, we can anticipate unexpected new attacks from the attacker at run-time
- Real-time Learning of unexpected attacks is of utmost importance
- Assumptions: Processing cores and memories are safe , the Trojan is inserted at Design Phase triggers malicious activity on router internally at run-time
- Detects three different Denial-of-Service attacks
- Hardware area overhead of only 0.26% and requires 4 cycles for Trojan detection, performs 2.4x faster as compared to state-of-the-art implementation
- Achieves Average Trojan detection accuracy of 93%



Test Setup for PENC Many-Core Platform (64-Core), where Attack Detection Module implemented using Online Machine Learning technique to prevent unexpected attacks





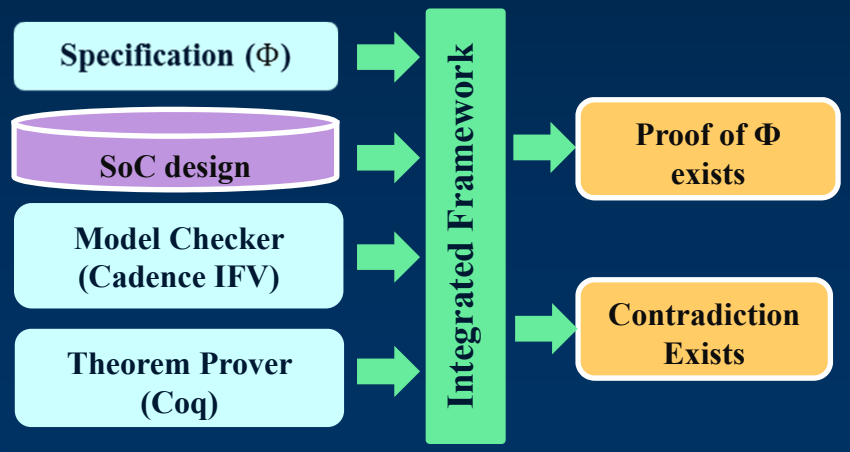
University of Central Florida

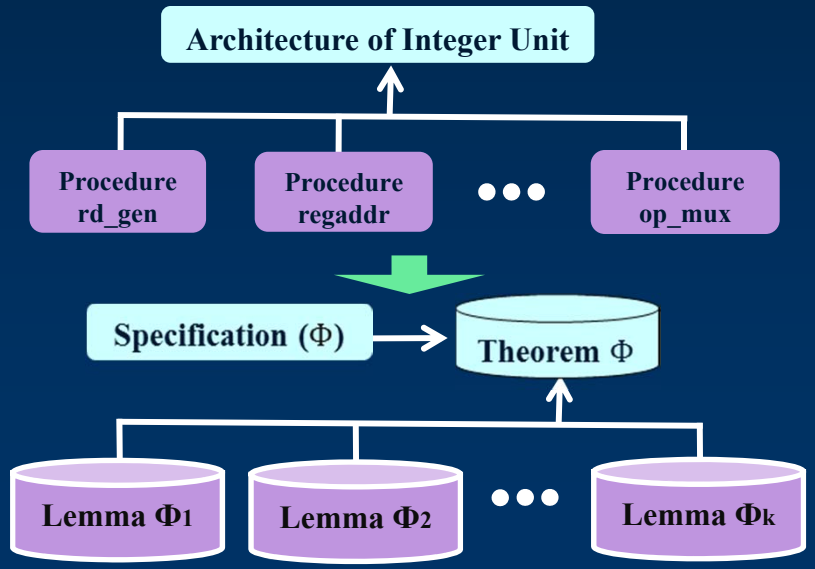
Scalable SoC Trust Verification using Integrated Theorem Proving and Model Checking

Authors: Xiaolong Guo, Raj Gautam Dutta, Prabhat Mishra, and Yier Jin

- **Formal Methods Integration**
  - **Theorem Prover (TP) - Coq**
  - **Model Checker (MC) – Cadence IFV**
  - **First attempt to verify security properties on large-scale hardware by integrating TP and MC**

- **Distributed Proof Construction**
  - **Decomposition of Hardware Design & Security Specification theorem**
  - **Sub-modules against lemmas of security properties**
  - **Prove Security Specification by combining results of lemmas of security properties**

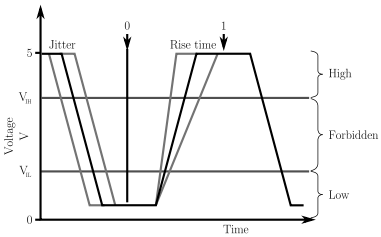




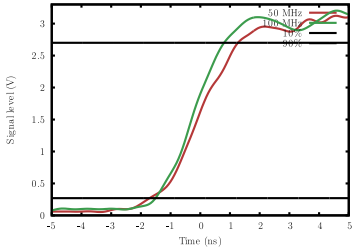
Security in Silicon Lab (SSL)

Information Leakage behind the Curtain: Abusing Anti-EMI Features for Covert Communication

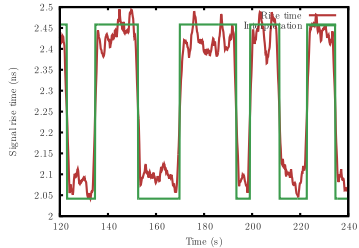
Johannes Bauer, Sebastian Schinzel, Felix Freiling, Andreas Dewald



Minimal signal changes (rise time or jitter) do not influence integrity a digital signal, but can be measured with analog equipment.



Modern microcontrollers bring facilities with them to influence certain analog aspects of signals. This image shows rise time of two differently configured GPIOs.

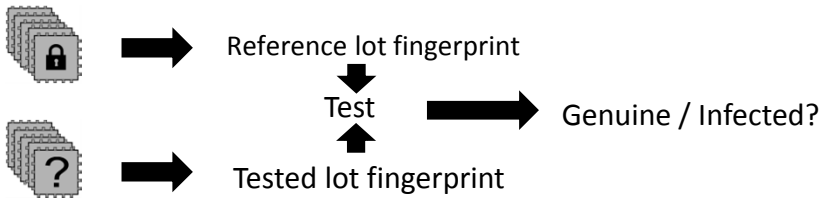


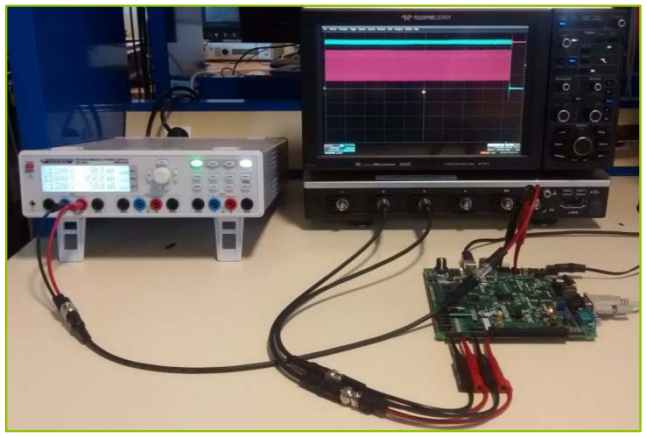
We abuse these facilities to modulate EMI and use this for communication.

GRANULARITY AND DETECTION CAPABILITY OF AN ADAPTIVE EMBEDDED HARDWARE TROJAN DETECTION SYSTEM

Maxime Lecomte, Jacques Fournier , Philippe Maurine

- **Embedded** Hardware Trojan detection method
- Novel **adaptive distinguisher** to detect small infections
- **Enhanced sensor** design with a higher spatial detection range
- Small **(0.45% of the area of the AES)** Hardware Trojan detected without activation

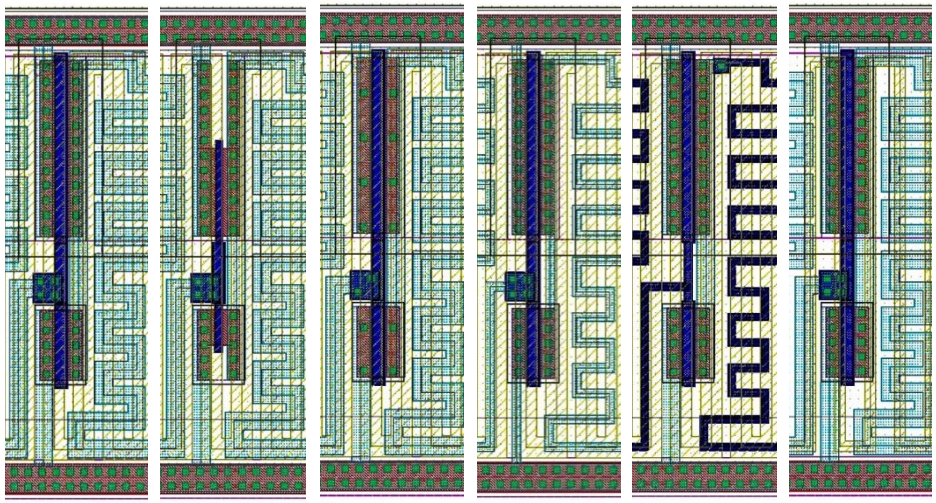




Electronic Forensic Techniques for Manufacturer Attribution

Ryan Helinski*, Edward Cole Jr.*, Gideon Robertson*, Jonathan Woodbridge, Lyndon Pierson
Sandia National Laboratories
Albuquerque, New Mexico 87123
E-mail: rhelins, coleei, garobe@sandia.gov

- Novel techniques presented
  - to measure multiple distinct manufacturing process variations
  - using self-contained, on-chip hardware (e.g., ring oscillators)



- Analysis of 159 silicon ICs
  - built as a proof of concept
  - 80 copies built at one fab
  - 80 more copies were built in two lots at a second fab
- Classification predictions
  - two fabs with up to 98.7% accuracy
  - two lots from the second fab with up to 98.8% accuracy

SAND2016-3875 C

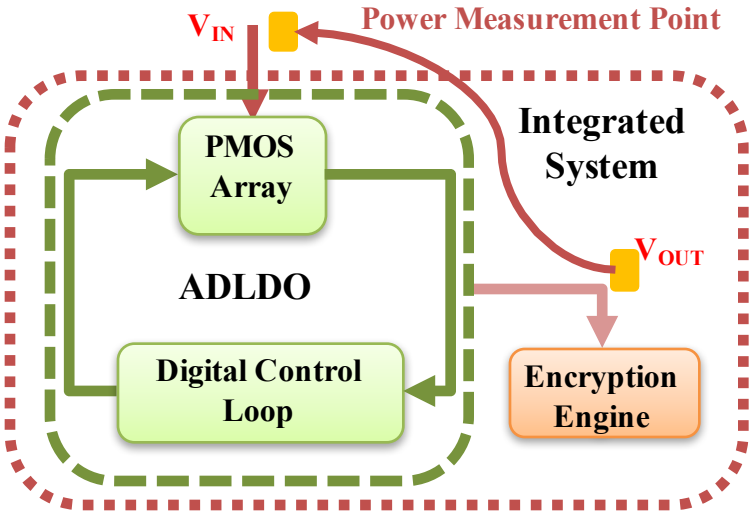
Sandia National Laboratories

Integrated All-Digital Low-dropout Regulator as a Countermeasure to Power Attack in Encryption Engines

A. Singh[1], M. Kar[1], A. Rajan[2], V. De[2], and S. Mukhopadhyay[1]
Georgia Institute of Technology[1], and Intel Labs[2]

GIGASCALE RELIABLE ENERGY EFFICIENT NANOSYSTEMS LAB

- Motivation: Introducing information loss on-chip to counter against side channel analysis attacks.
- On-chip digital LDO (ADLDO) can introduce information loss through
  1. Quantization error in ADC, 2. Limited sampling rate and 3. Integration effects



- Achievements
  - Modeling of on-chip LDO
  - Developed system level framework for AES encryption engine with LDO
  - Performed CPA on AES raw traces and transformed traces through ADLDO
  - Analysis of effect of ADLDO design parameters on CPA performance
  - Study of design tradeoffs
- Future work
  - Incorporating some circuit techniques in the LDO feedback loop to completely decorrelate measured power with respect to load pattern

- Acknowledgements: This work is in part supported by Intel Corp.