Security and Trust in the Analog/Mixed-Signal/RF Domain: A Survey and a Perspective

Yiorgos Makris

Trusted & **REL**iable **A**rchitectures Laboratory

Department of Electrical and Computer Engineering
The University of Texas at Dallas

A Word About Myself

Education:

- Diploma of Computer Engineering, University of Patras, Greece, 1995
- MS & Ph.D. in Computer Engineering, UC San Diego, 1997 & 2001

Professional Trajectory:

- Faculty of Electrical Engineering and Computer Science, Yale Univ., 2001-2011
- Faculty of Electrical and Computer Engineering, UT Dallas, 2011-present
- Various industrial internships and consulting stints

Research Interests:

- Applications of machine learning in the design of trusted and reliable integrated circuits and systems, with emphasis in the analog/RF domain
- On-die learning, neuromorphic systems with emerging technologies
- Hardware-enabled forensics and malware detection in microprocessors
- Analog/RF IC testing and reliability
- Novel computation modalities with emerging technologies

Contributions to Hardware Security

A track-record of innovation:

- First delay-based statistical side-channel fingerprinting method for hardware Trojan detection (HOST’08)
- First Trojan detection method for analog/RF circuits (D&T’10)
- First silicon demonstration of hardware Trojans and statistical side channel fingerprinting in wireless crypto ICs (ICCAD’13, TVLSI’17)
- First in-field/real-time Trojan detection (DATE’13, ITC’15)
- First golden chip-free Trojan detection method (DAC’14)
- First statistical counterfeit IC detection (DFTS’12, TCAD’15)
- First proof carrying hardware IP method (HOST’11, TIFS’12, HOST’16)
- First statistical fab-of-origin attestation method (ICCAD’16)
- First IFT method for analog/mixed-signal/RF ICs (DATE’17)
- First hardware Trojan in an 802.11a/g network (HOST’17)

Counterfeit chips in military

Source: wired.com, 2010

Syrian radar case

"Israeli jets bombed a suspected nuclear installation in northeastern Syria. Among the many mysteries still surrounding that strike was the failure of a Syrian radar—supposedly state-of-the-art—to warn the Syrian military of the incoming assault. It wasn't long before military and technology bloggers concluded that this was an incident of electronic warfare—and not just any kind."

Source: IEEE Spectrum, 2008

Dell warns of hardware Trojans

Homeland Security News Wire

BIOMETRICS BORDER/IMMIG. BUSINESS CYBERSECURITY
PUBLIC SAFETY PUBLIC HEALTH REGIONAL SCI-TECH

Cybersecurity

Dell warns of hardware trojan

Published 21 July 2010

Share

Computer maker Dell is warning that some of its server motherboards have been delivered to customers carrying an unwanted extra: computer malware; it could be confirmation that the "hardware trojans" long posited by some security experts are indeed a real threat; the Pentagon is spending millions on research designed to ensure it can trust the microchips in critical systems, especially those made outside the United States

Source: homelandsecuritynewswire.com, 2010

Compromised chip in a BOEING

Source: dailymail.co.uk, 2012

Security and Trust in the Digital Domain

Extensive research over the last decade:

[1] M. Tehranipoor and F. Koushanfar, “A Survey of Hardware Trojan Taxonomy and Detection,” IEEE Design Test of Computers, vol. 27, no. 1, pp. 10–25, 2010.

[2] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, “Hardware Trojans: Lessons Learned After One Decade of Research,” ACM Transactions on Design Automation of Electronic Systems, vol. 22, no. 1, pp. 6:1–6:23, 2016.

[3] M. Rostami, F. Koushanfar, and R. Karri, “A Primer on Hardware Security: Models, Methods, and Metrics,” Proceedings of the IEEE, vol. 102, no. 8, pp. 1283–1295, 2014.

[4] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, “Hardware Trojan Attacks: Threat Analysis and Countermeasures,” Proceedings of the IEEE, vol. 102, no. 8, pp. 1229–1247, 2014.

[5] D. Forte, S. Bhunia, and M. Tehranipoor, “Hardware Protection through Obfuscation,” 2017.

[6] P. Mishra, S. Bhunia, and M. Tehranipoor, “Hardware IP Security and Trust,” 2017.

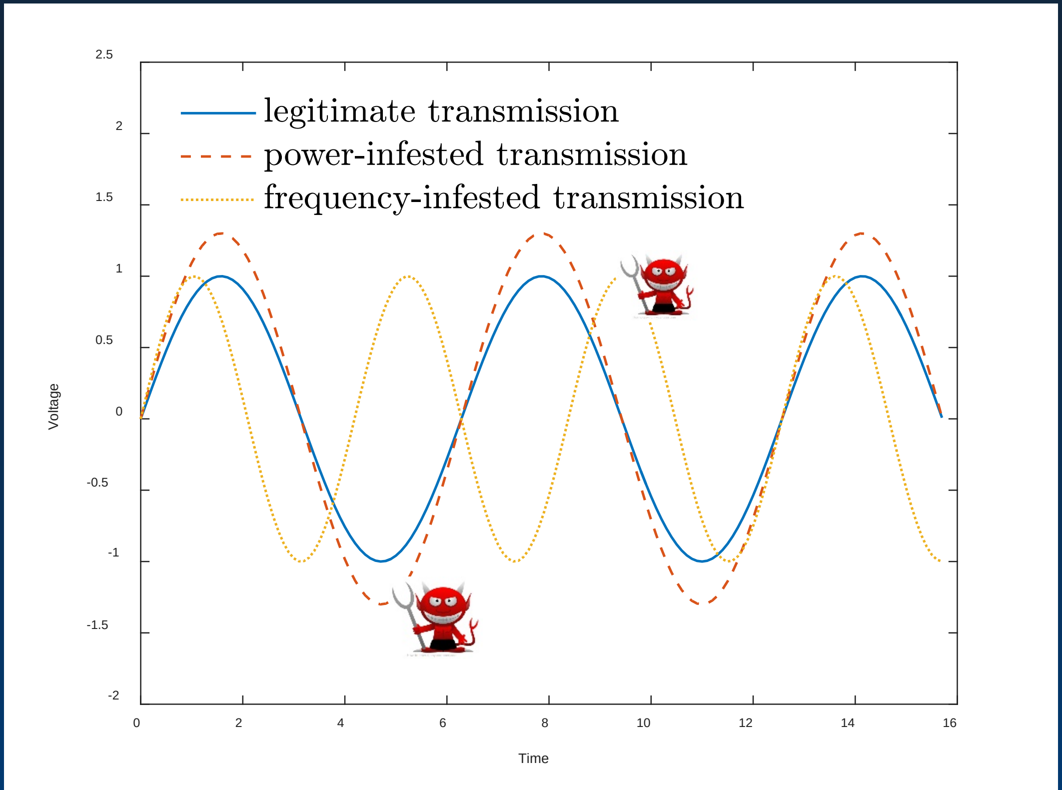
[7] M. Tehranipoor, U. Guin, and S. Bhunia, "Invasion of the Hardware Snatchers: Fake Hardware Could Open the Door to Malicious Malware and Critical Failure," IEEE Spectrum, 2017

Extensive funding by plethora of agencies

(DARPA, DHS, IARPA, DoD, AFRL, ONR, ARO, NSF, SRC, etc…)

Security and Trust in the Analog Domain

- Continuous domain – increased opportunity
- Real threat – practical examples of attack targets
- Limited work reported in the literature
- Can be as simple as this:



Presentation Overview

- Security and Trust in the Analog/Mixed-Signal/RF Domain: A Survey and a Perspective
  - Hardware Trojans and Trojan states in analog/mixed-signal/RF ICs
    - HTs in wireless crypto ICs
    - Spread spectrum techniques
    - Multiple equilibrium states
    - Analog triggers
    - Detection/Prevention methods
  - Piracy, reverse engineering and theft of analog/mixed-signal/RF IPs
    - Obfuscation
    - Logic encryption
    - Watermarking
    - Split manufacturing
  - Counterfeiting of analog/mixed-signal/RF ICs
    - Electrical inspection
    - Aging-based fingerprinting
    - Statistical methods
    - On-chip sensors
    - PUFs
  - Limitations and actions needed
    - Experimental verification
    - Payload
    - Ad-hoc detection methods
    - Problem formalization

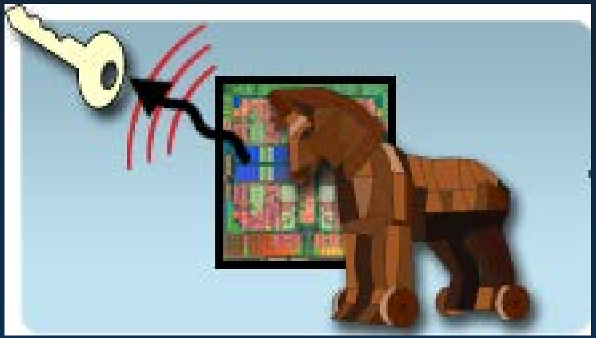
PART I.a:
Hardware Trojans in RF ICs

Do you Trust your Silicon?

Problem motivation:

- Globalization of IC design/manufacturing raises trust concerns:

  "Does my chip do what it is supposed to, nothing less / nothing more?"
- Cost of an entirely "trusted" supply chain too high
- Impact of malicious hardware in "sensitive" applications can be devastating



Hardware Trojans

- Hidden, malicious circuitry causing errors, leaking sensitive data, and/or incapacitating a chip
- Compromising a circuit is possible at every level from 3rd party IP down to the mask level

Hardware Trojan Basics

- Hardware Trojan: A malicious modification to an integrated circuit allowing a perpetrator to interfere with its operation, steal information, or destroy it.
- Trigger: The activation mechanism of the Trojan (e.g. always on, input condition, etc.)
- Payload: The harmful effect of Trojan activation (e.g. alter functionality, deny service, destroy)
- Implanting Stage: Anywhere in the fabrication chain. Most current research assumes culprit in fabrication foundry. 3rd party Hardware IP also a plausible target
- Limitations of Test Methods: Small input subspace applied targeting manufacturing defects. Cannot exercise entire functionality. Reverse engineering expensive/destructive

Hardware Trojan Literature

Hardware Trojan overview articles

- Bhunia et al., “Hardware Trojan Attacks: Threat Analysis and Countermeasures,” IEEE Proceedings, 2014
- Xiao et al., “Hardware Trojans: Lessons Learned After One Decade of Research,” ACM TODAES, 2016

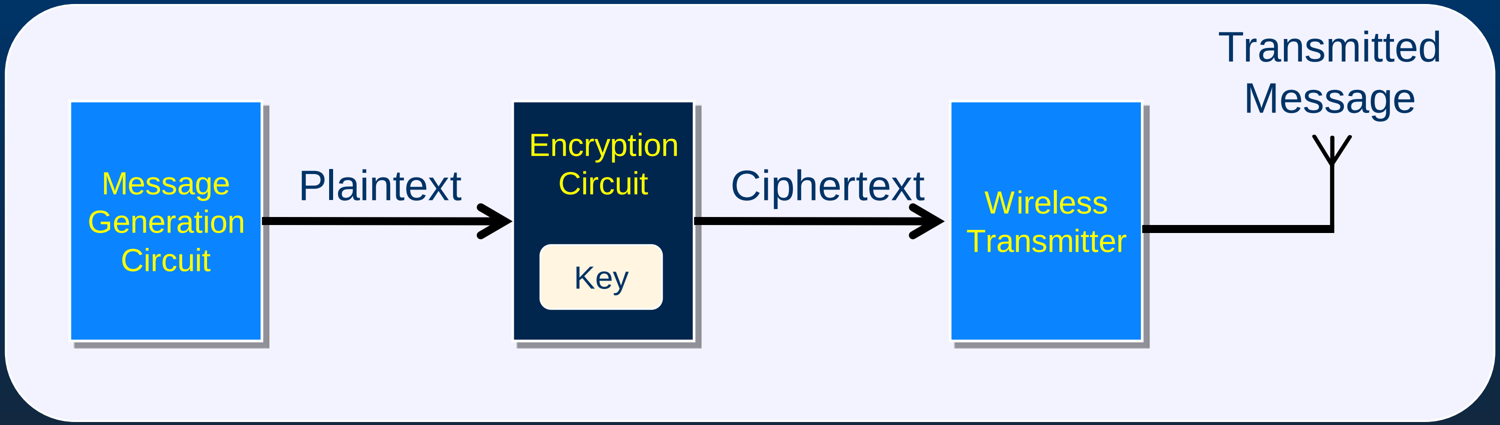
Hardware Trojan examples

- Trust-hub Benchmarks (https://www.trust-hub.org/taxonomy)
- Jin et al., “Experiences in Hardware Trojan Design & Implementation,” HOST 2009

Hardware Trojan detection methods

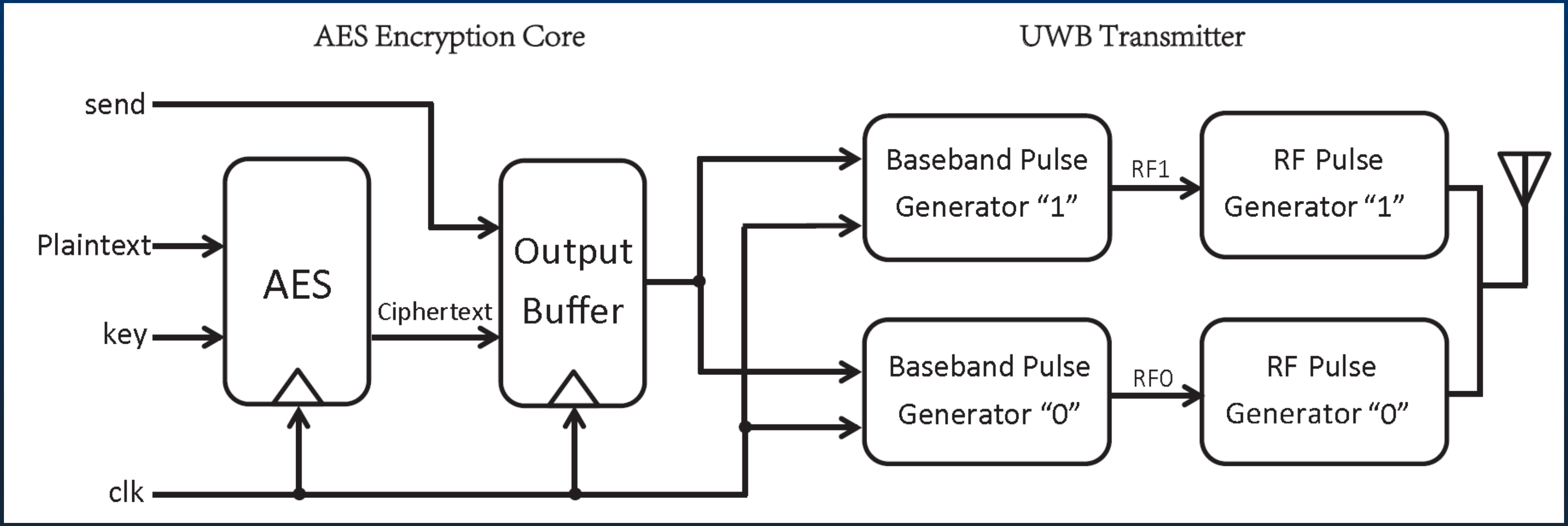
- Chip Imaging (Song 2011, Gopalakrishnan 2014)
- Enhanced Functional Testing (Wolf 2008, Salmani 2009)
- Statistical Side-Channel Fingerprinting (Agrawal 2007, Jin 2008)

Hardware Trojans in Wireless Crypto ICs



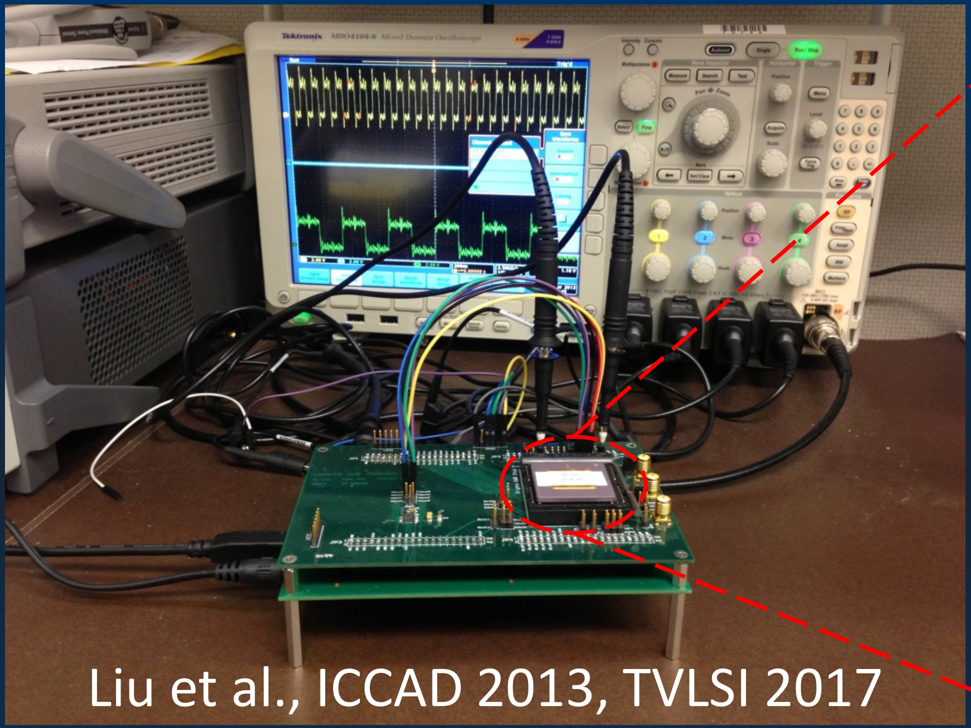
- Tangible Objective
  - Steal information (i.e. key, plaintext, etc.)
- General Method
  - Hide leaked data as added "structure" on the parameters of the wireless transmission signal (which the attacker has access to)
- Realistic Assumptions
  - No violation of digital, analog/RF, or system-level specifications
  - Structure of leaked data known only to attacker – many options
  - Added structure hidden within margins of process variations

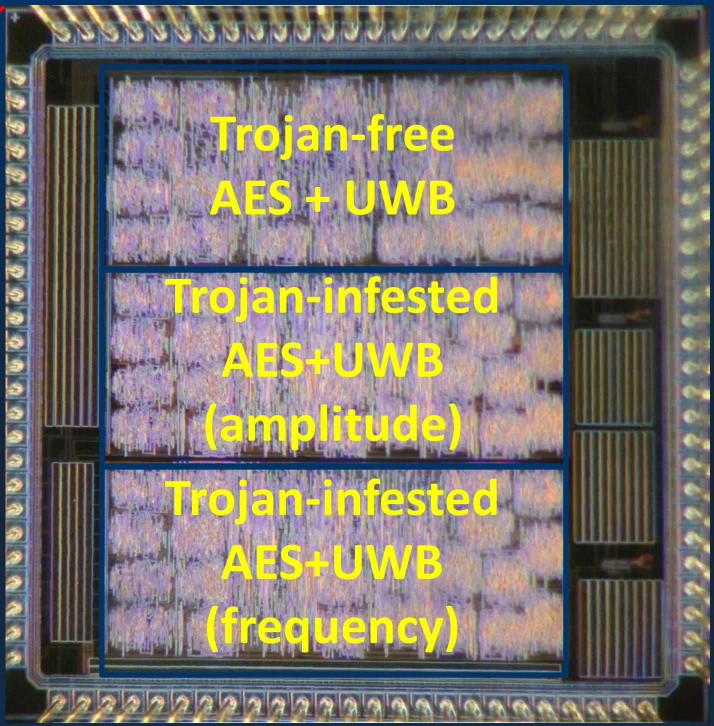
Example Wireless Cryptographic IC



- Digital Part
  - Pipelined Advanced Encryption Standard (AES) Core
  - First-in First-Out (FIFO) queue holding 128-bit blocks for transmission
  - Output Buffer (Serializer)
- Analog Part
  - Ultra Wide Band (UWB) transmitter

Experimentation Platform

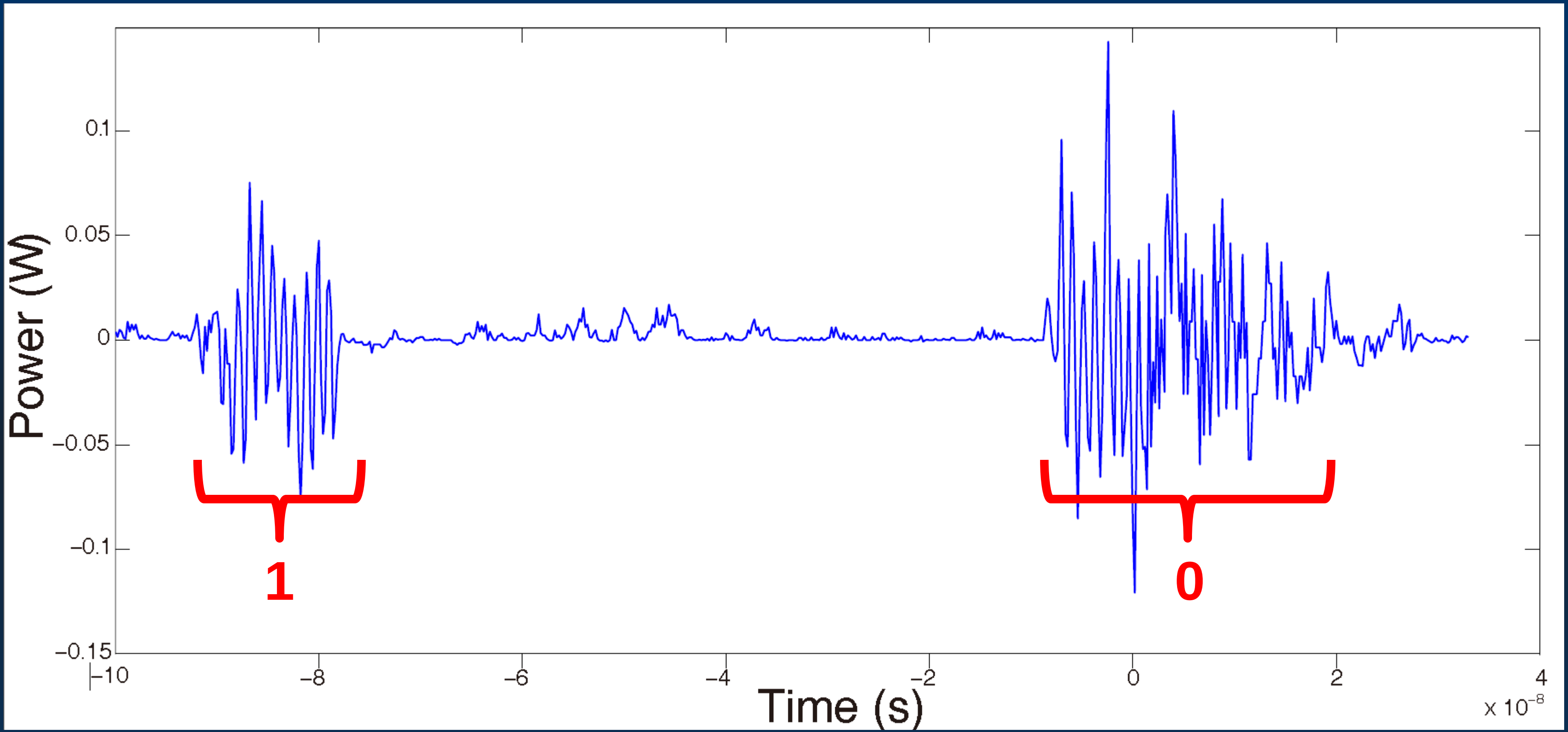




Technology	Chip Size	Modulation Scheme	Data Rate	Pulse Width	Frequency of '0'	Frequency of '1'
TSMC 0.35 µm	3mm x 3mm	FSK-OOK	Up to 96MHz	7ns - 48ns	900 MHz	1.6 GHz

- 40 functional chips fabricated via MOSIS

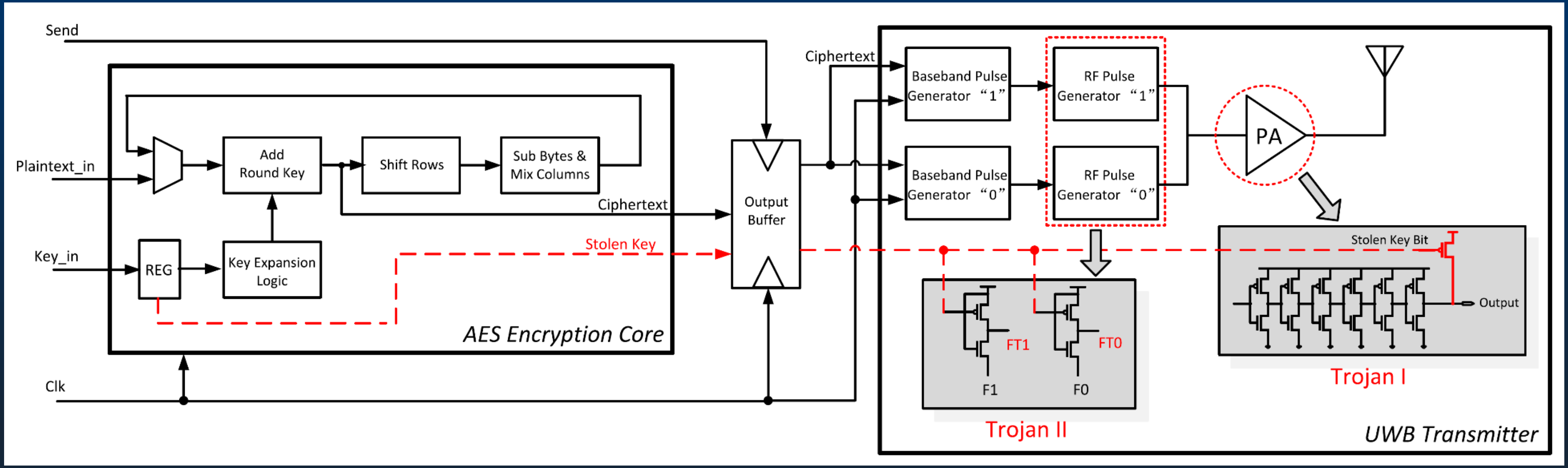
Trojan-free Transmission



Trojan-free transmission waveform of ‘1’ and ‘0’

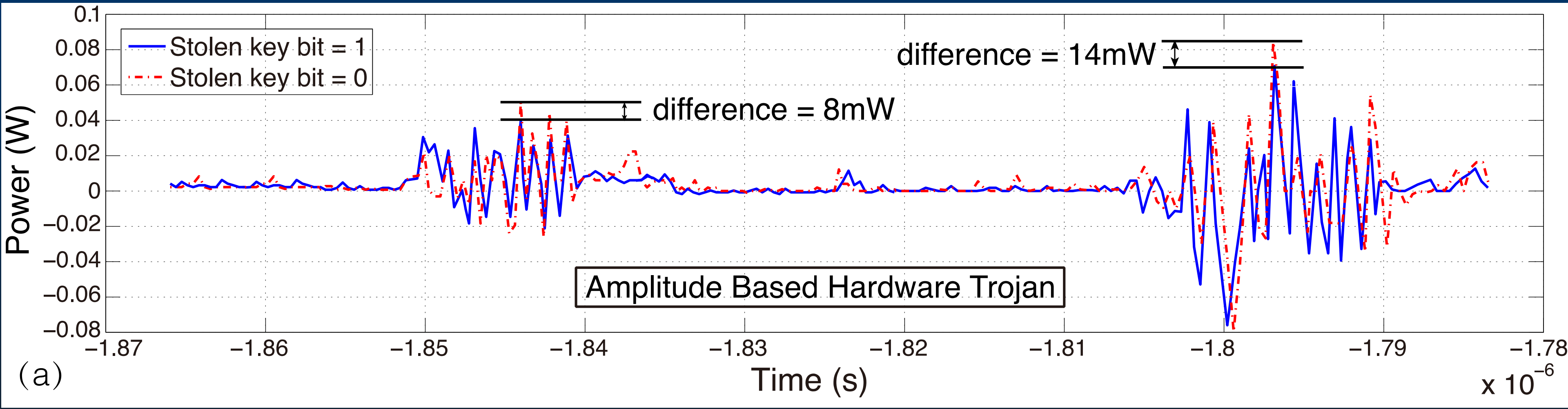
(this is the only information the attacker has access to)

Trojan-infested Wireless Cryptographic IC

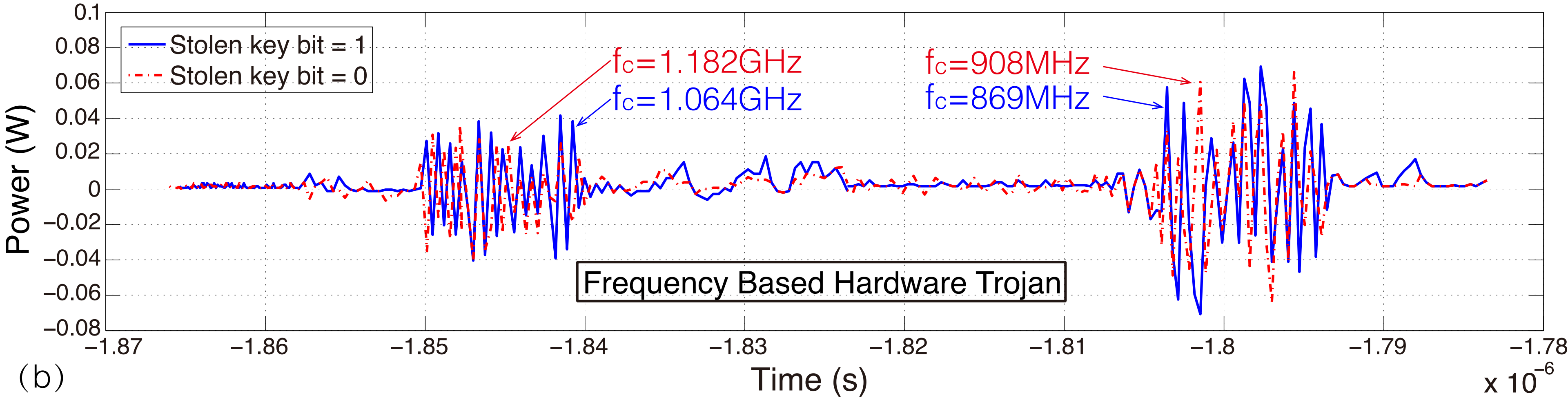


- Modification to digital part
  - Tap into register holding the encryption key, read and pass one bite at a time to the UWB transmitter. No impact on functionality, minimal logic.
- Modification to analog part
  - Trojan-I: A simple PMOS is inserted to output stage of power amplifier. When stolen key is ‘0’, PMOS turns on and more current is drawn to output. When stolen key is ‘1’, PMOS is off, no impact on functionality.
  - Trojan-II: Similar philosophy but modulating transmission frequency.

Trojan-infested Transmissions

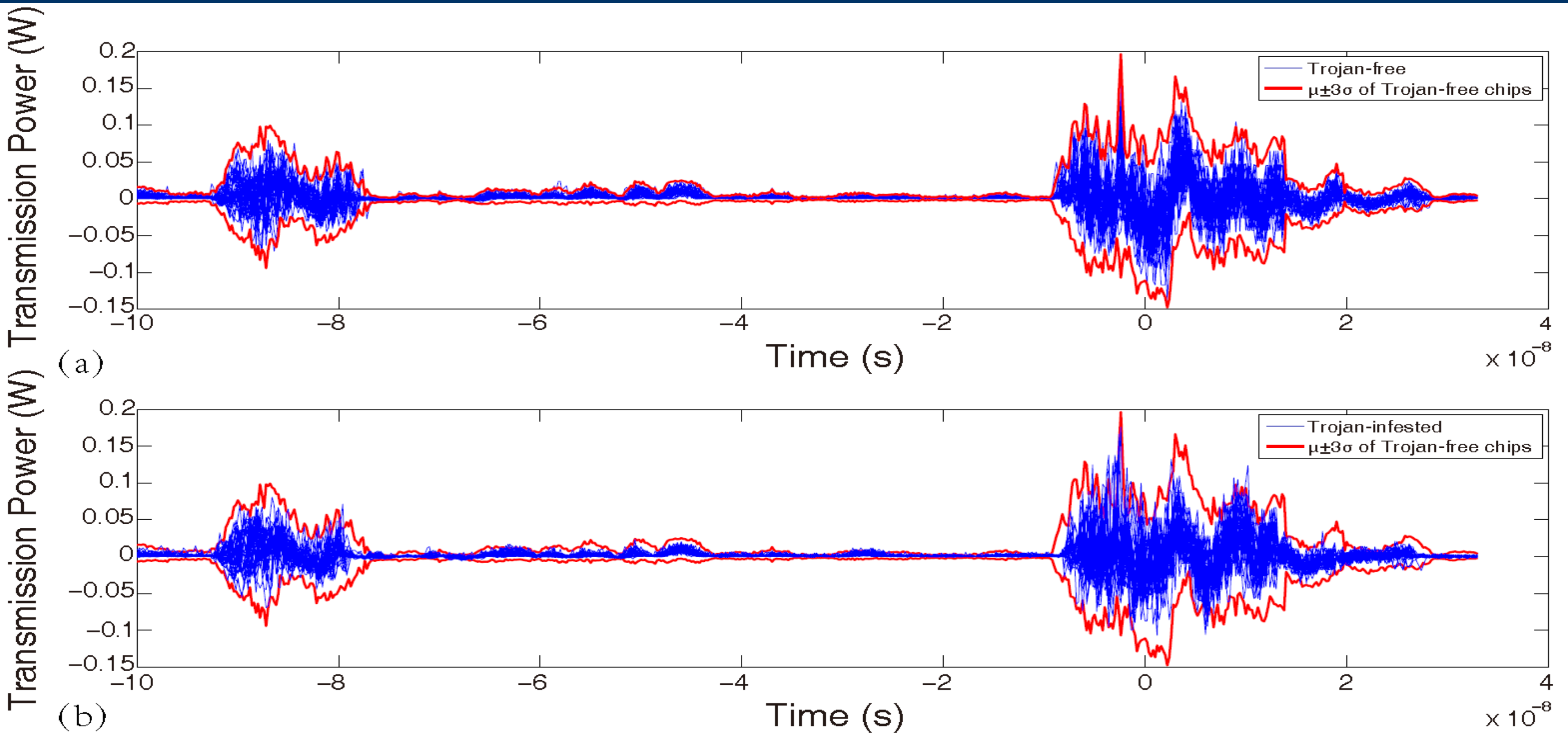


Transmission power waveforms from Trojan-I infested chip



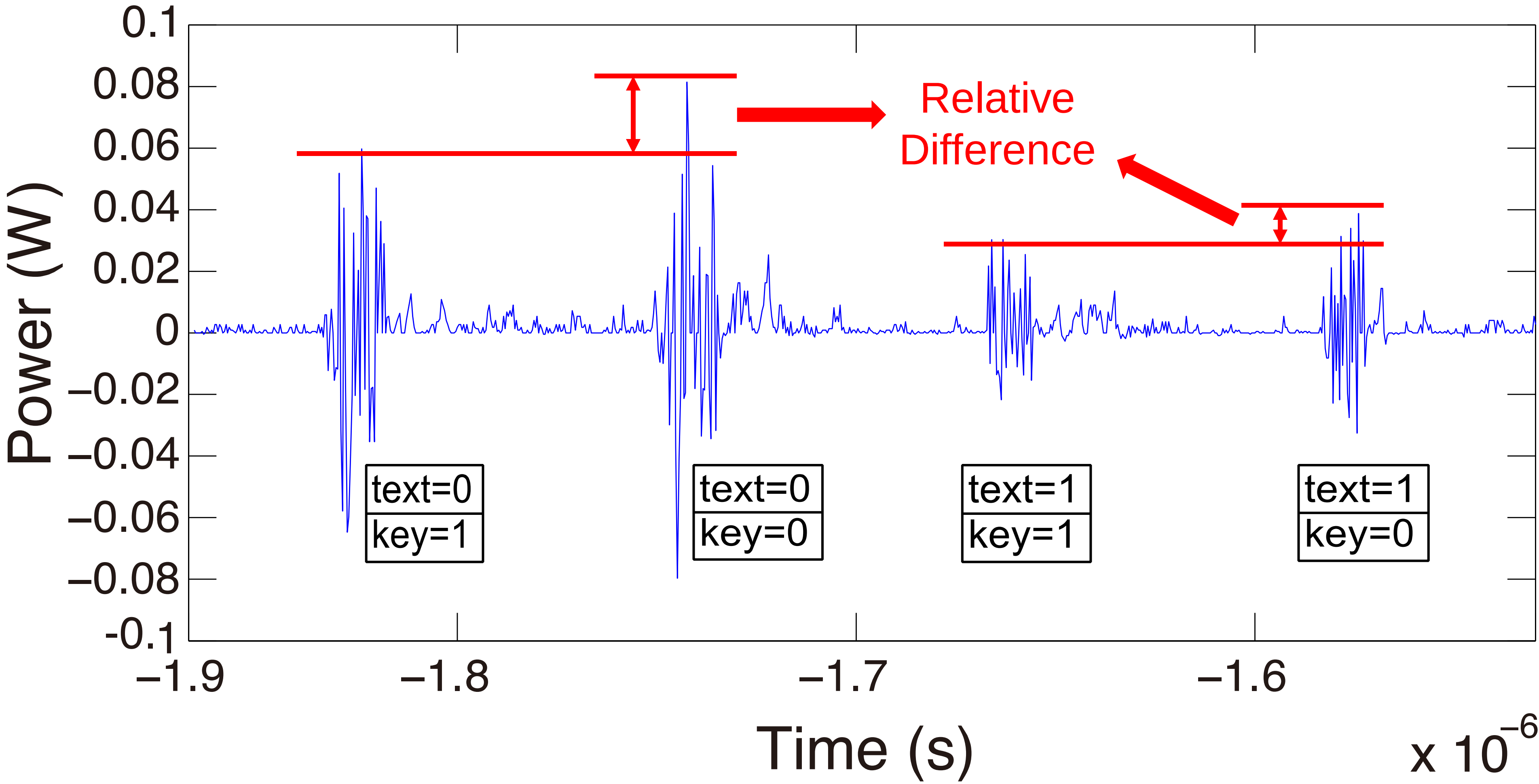
Transmission power waveforms from Trojan-II infested chip

Trojan-free vs. Trojan-infested Chips



- Transmission power of (a) the 40 Trojan-free chips, and, (b) the 80 Trojan-infested chips, enclosed in the $\mu \pm 3\sigma$ envelop of the Trojan-free chips. Given the transmission power waveform of a chip, it is impossible to tell which distribution it came from.

Leaking the Key



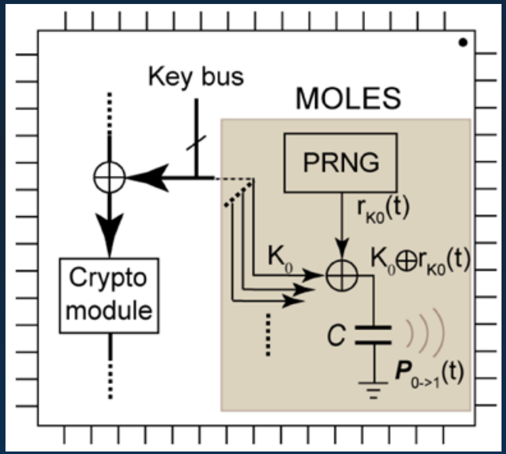
- Decoding leaked key bit values relies on relative difference in amplitude

MOLES

- Malicious off-chip leakage enabled by side-channels (ICCAD’09)
- Communicate below the noise floor of the compromised IC
- Power side-channel
- Exploiting unused space on-chip
- Requires:
  - Low SNR to evade detection

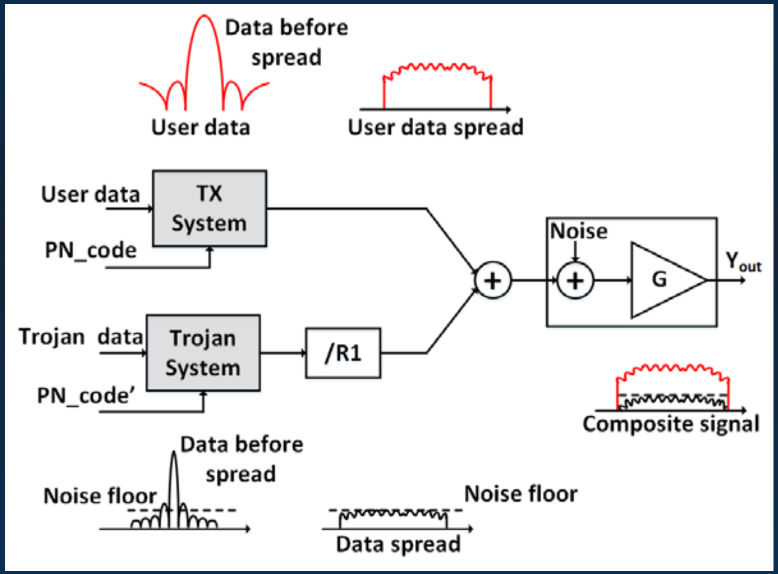
MOLES

- Spread spectrum to distribute the power of side-channel leakage to multiple cycles
- SNR of each block low enough to evade detection
- Attacker averages power over a large number of clock cycles
- Exploiting unused space on-chip
- Capacitor leaks small amount of power when a ‘1’→’0’ logic transmission occurs



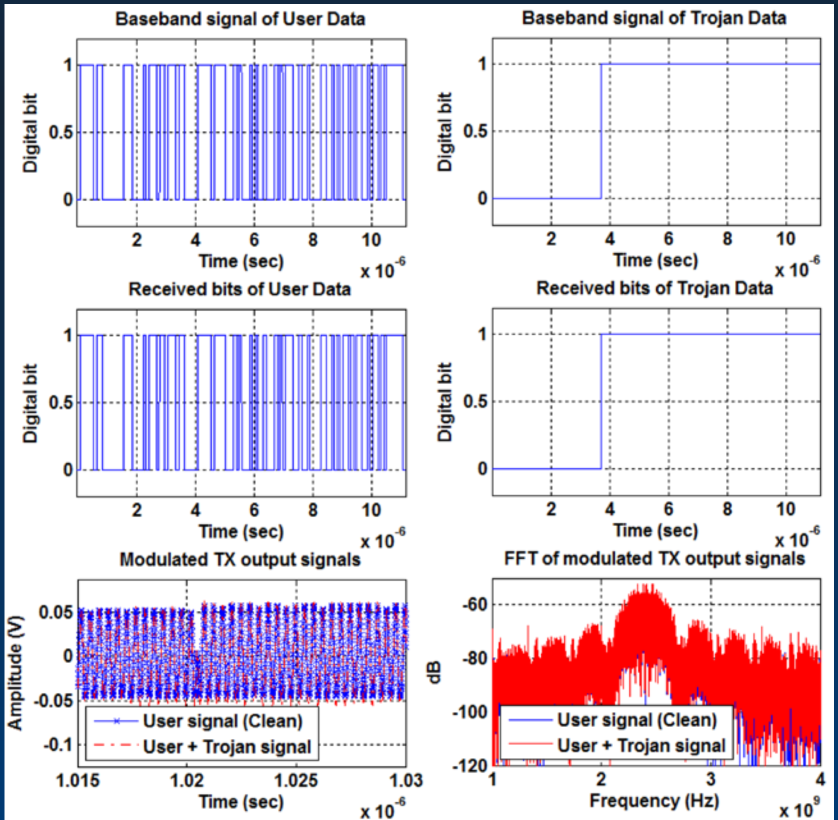
RF Transmission Below Noise Floor

- Unauthorized transmission signal within the ambient noise floor (VTS'15)
- Spread spectrum technique
- Low-rate data multiplied with higher rate spread spectrum code
- Legitimate and rogue data added in the analog domain
- Original information de-spreaded in the receiver
- Legitimate transmission evades any performance testing



RF Transmission Below Noise Floor (2)

- Trojan transmits small number of bits per transmit burst
- Trojan exploits channel equalization techniques to enable coherent demodulation.



PART I.b:
Hardware Trojans in Analog ICs

Trojan States in Analog ICs

- No extra hardware needed
- No signature left during normal operation
- Exploit Trojan states in circuits with positive feedback loops
  - Used to desensitize the output from supply variations
- Transistor networks can have more than one DC operating points [Proc. IEEE,1980]
  - Verification problem
  - Startup circuit problem
- Never studied in the context of hardware security until recently

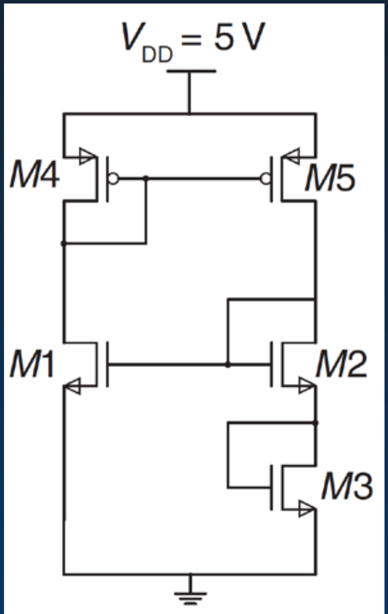
Trojan States in Analog ICs

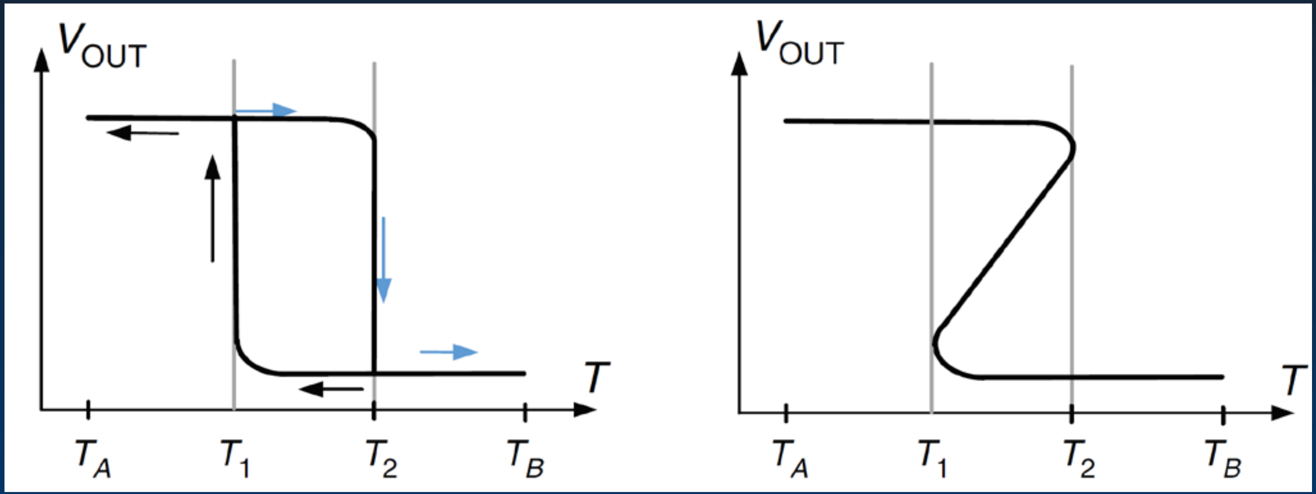
- Hardware security implications
- Undesired circuit behavior
  - Inconsistent output results
  - May affect preceding blocks
- Demonstration in several analog ICs

Circuit Topology	Simulation Level
Inverse Widlar current mirror [Electronics Letters'15]	Cadence Spectre
Filter (ISCAS'99, NAECON'15)	HSPICE
Bandgap reference (ISCAS'14)	Cadence Spectre
OP-AMP (ISCAS'15)	Cadence Spectre
Wien-bridge oscillator (NAECON'15)	Cadence Spectre

Trojan States in Analog ICs

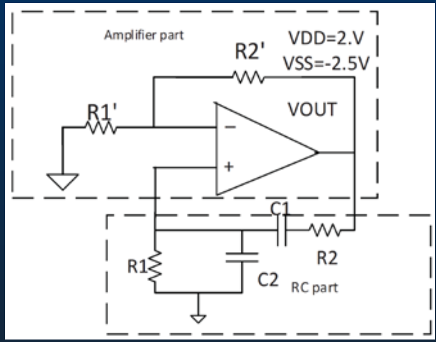
- Inverse Widlar current mirror [Electronics Letters'15]
  - Multiple DC operating points with temperature sweep



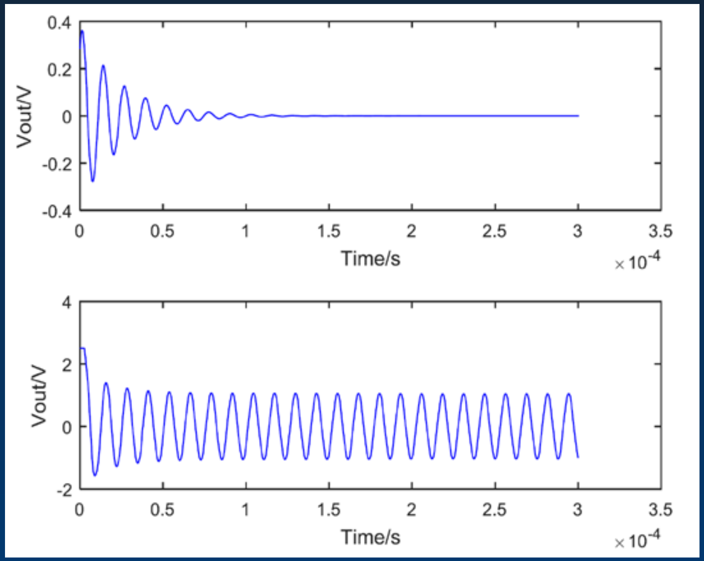


Trojan States in Analog ICs

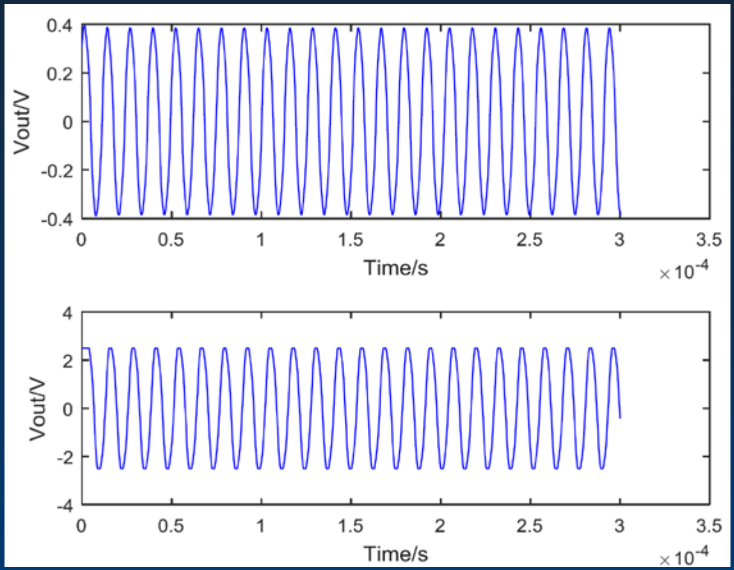
- Wien-bridge oscillator (NAECON'15)
- Initial conditions on C1, C2 affect operation
- Static - incapacitating chip
- Dynamic – leaking information



Stable static mode



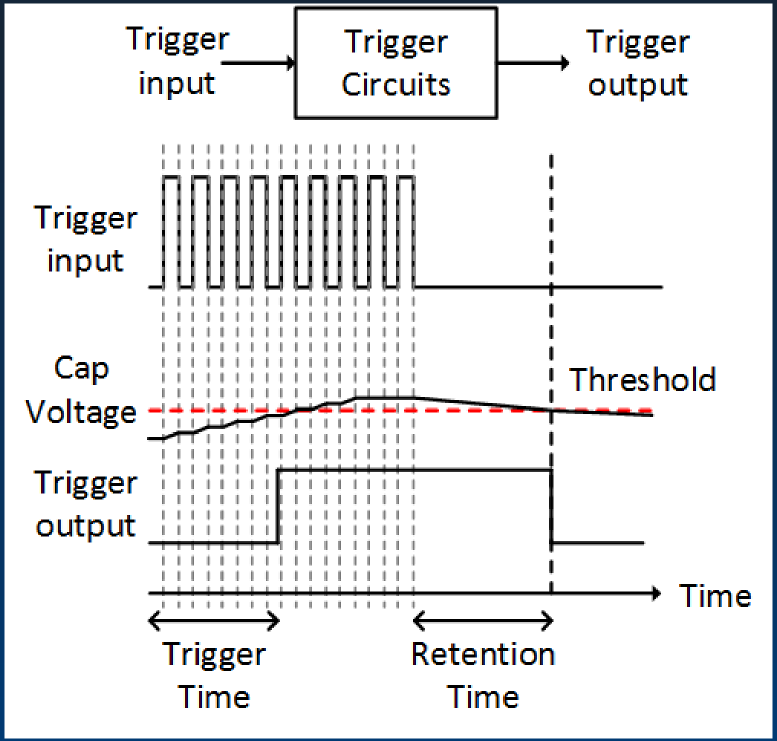
Dynamic mode



PART I.c:
Analog Triggers

Analog Triggers

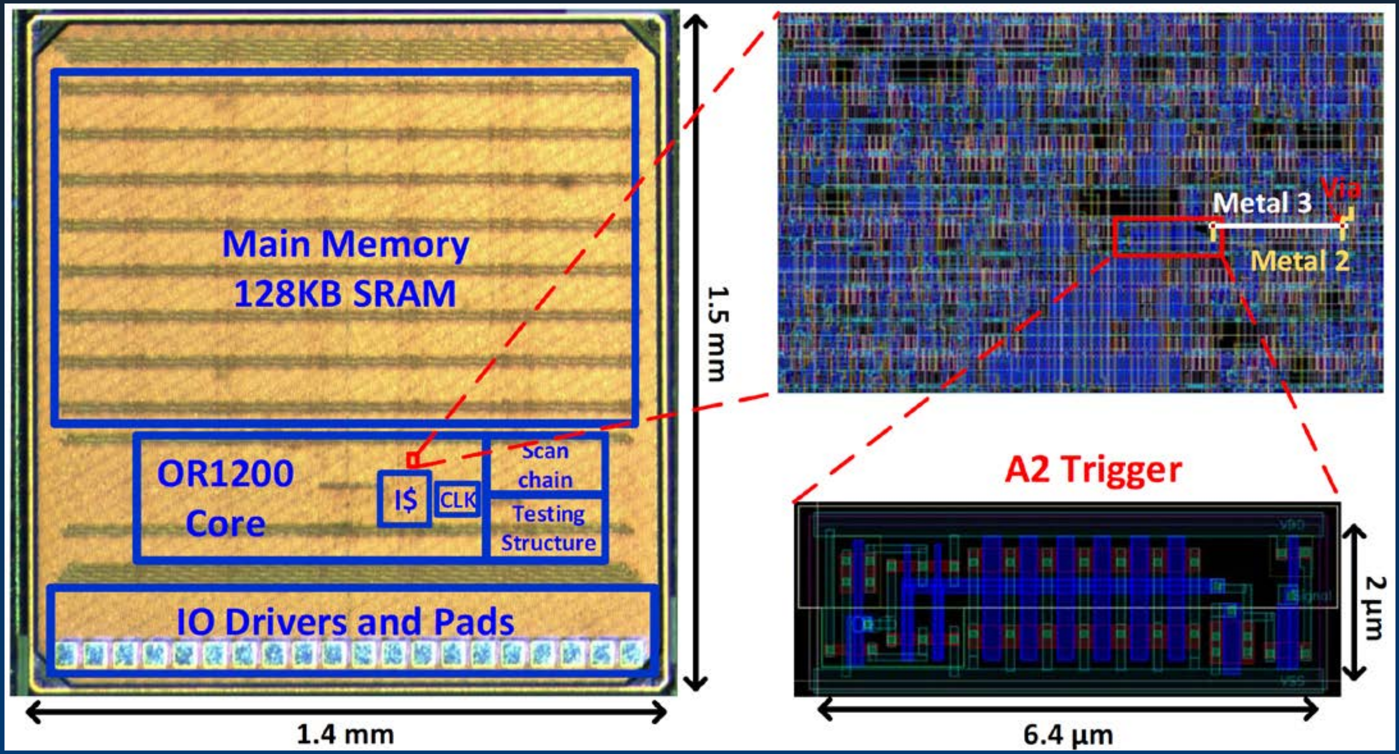
- Capacitor used to leak information (S&P'16)
- Siphons charge from nearby wires as their value transitions
- When fully charged trigger is activated
- Resets through charge leakage
- Demonstration on a microprocessor



Analog Triggers (2)

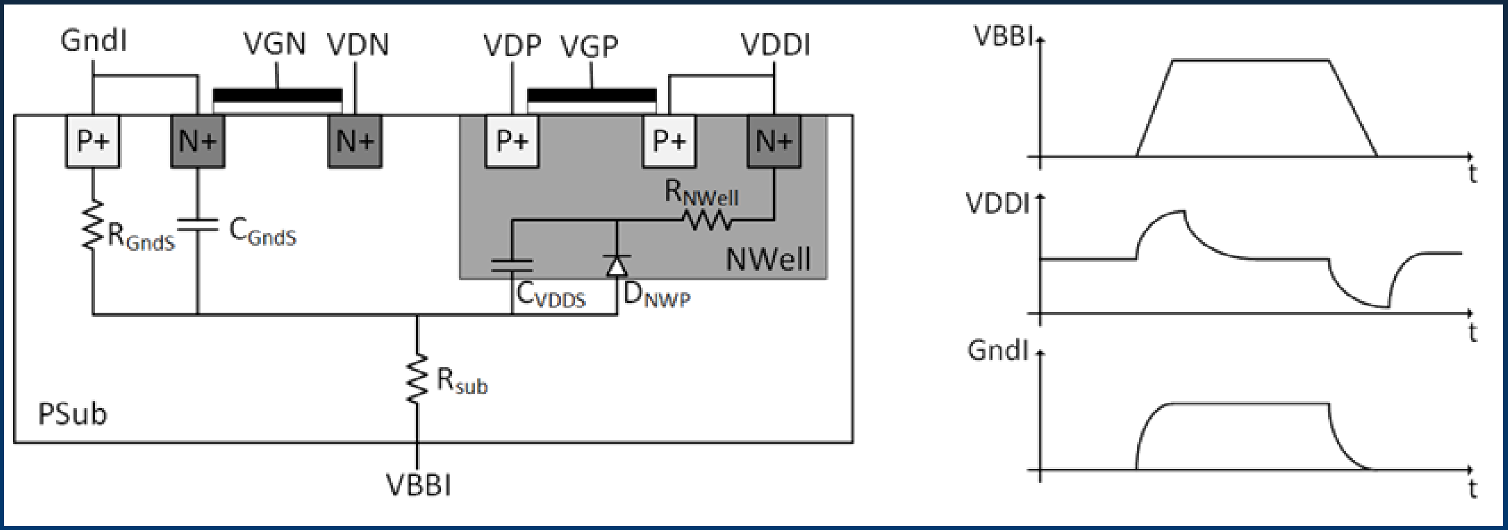
- Effectively flips register values upon trigger activation
- Robust over temperature variations
- 0.08% area overhead

[S&P'16]



Analog Triggers (3)

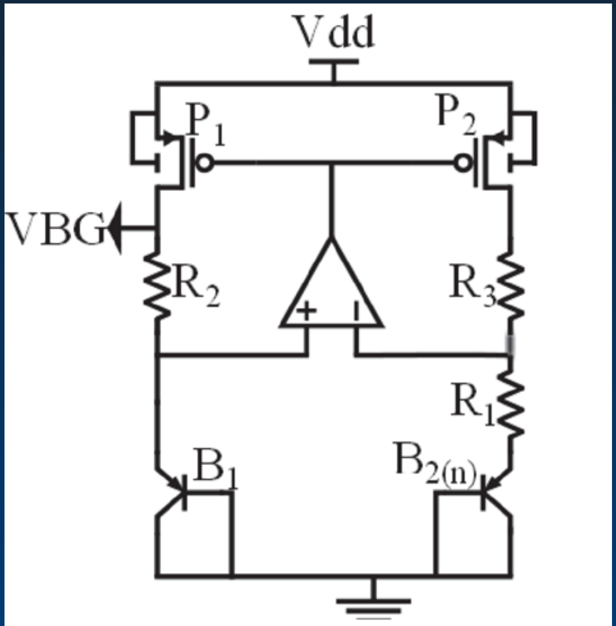
- Voltage glitches (Workshop on Crypt. & Sec. in Comp. Systems'16)
- Significant effect in frequency synthesis
- Body biasing attack
  - High voltage pulses on the circuit substrate
  - Modifies coupling between substrate and power supply/ground
  - Demonstration on PLL (frequency shift)



Analog Triggers (4)

- Voltage glitches in bandgap references
- Theoretically small variation of output voltage
- Practically transistors may be driven to their linear region – bandgap functioning not guaranteed

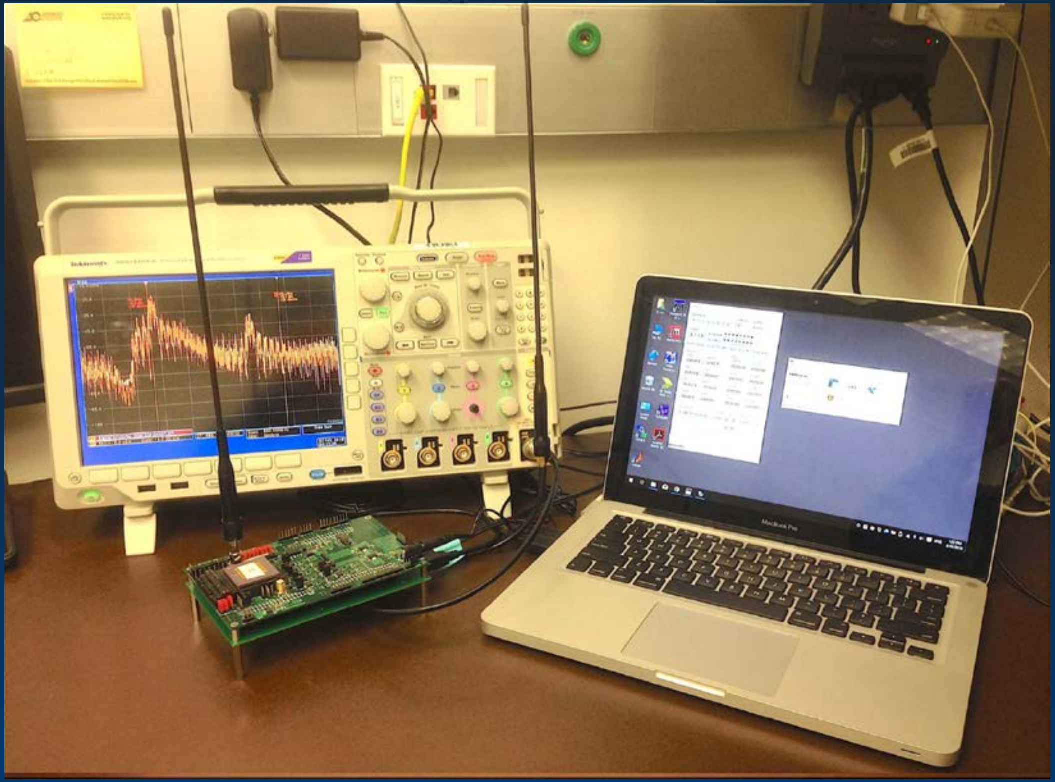
[Euromicro Conference on Digital System Design’14]

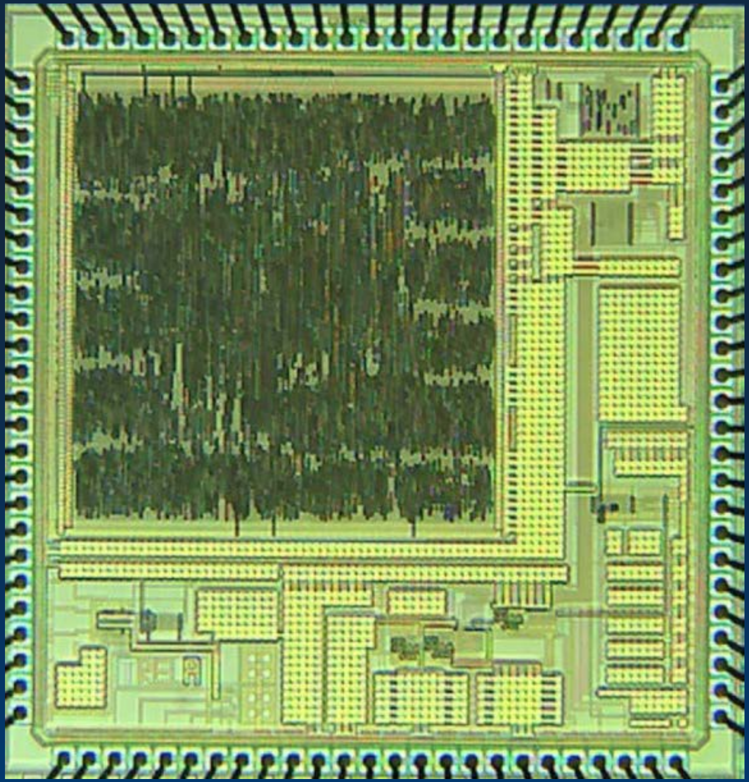


PART I.d:
AMS/RF Trojan Detection

Statistical Side-Channel Fingerprinting

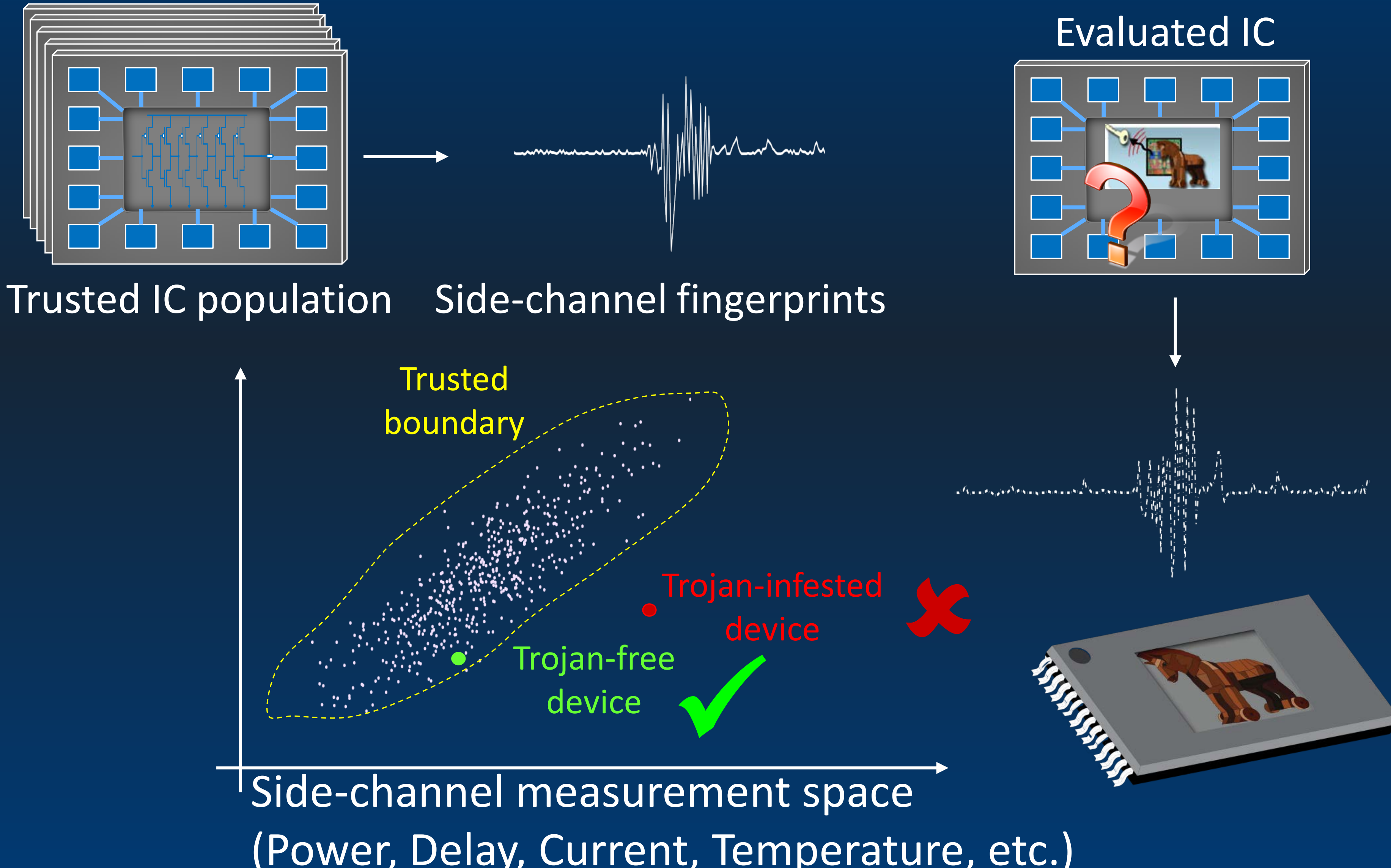
- Applied on the wireless cryptographic IC [TVLSI'16]





Statistical Side-Channel Fingerprinting

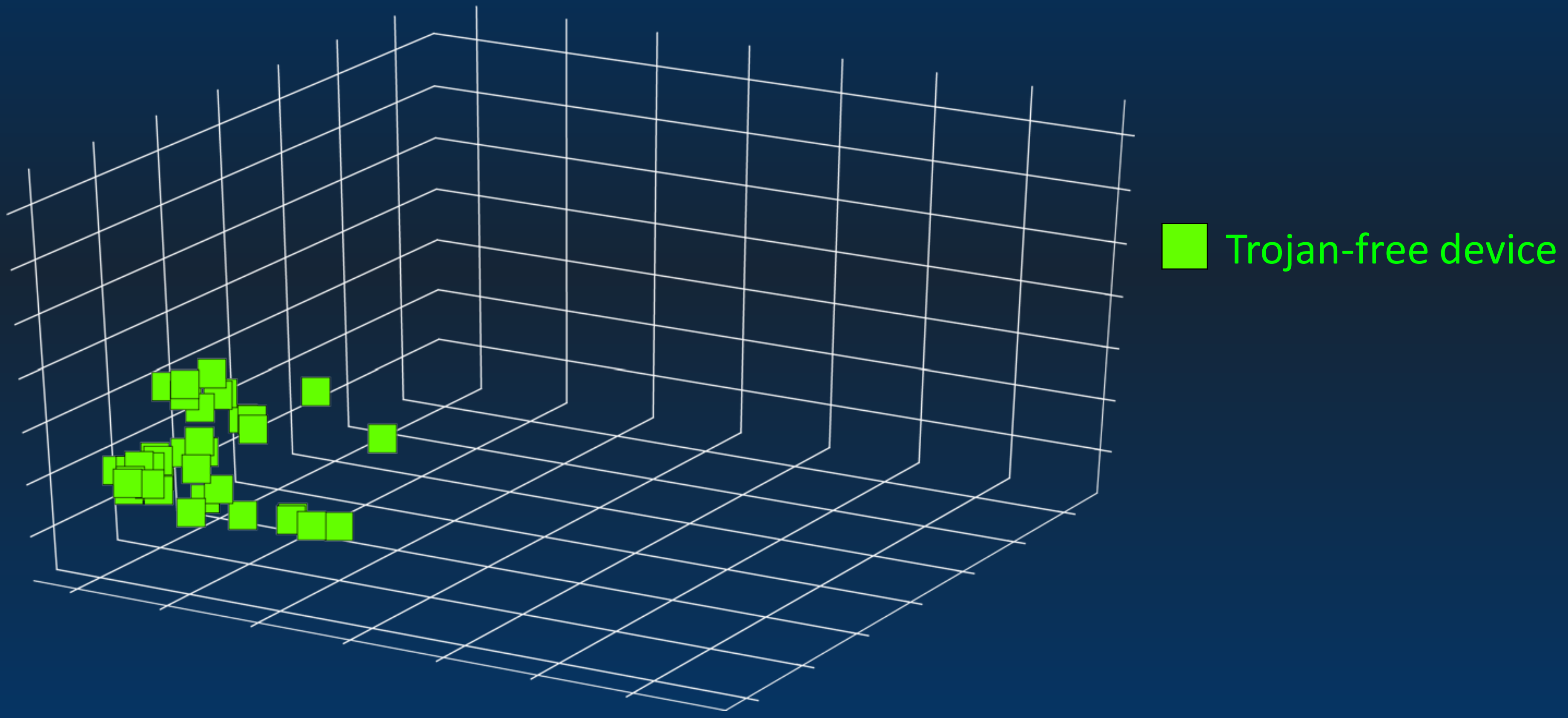
Parametric signatures generated from “golden” chips



Trojan Detection Results

Projection of 40 Trojan-free devices onto fingerprint space*

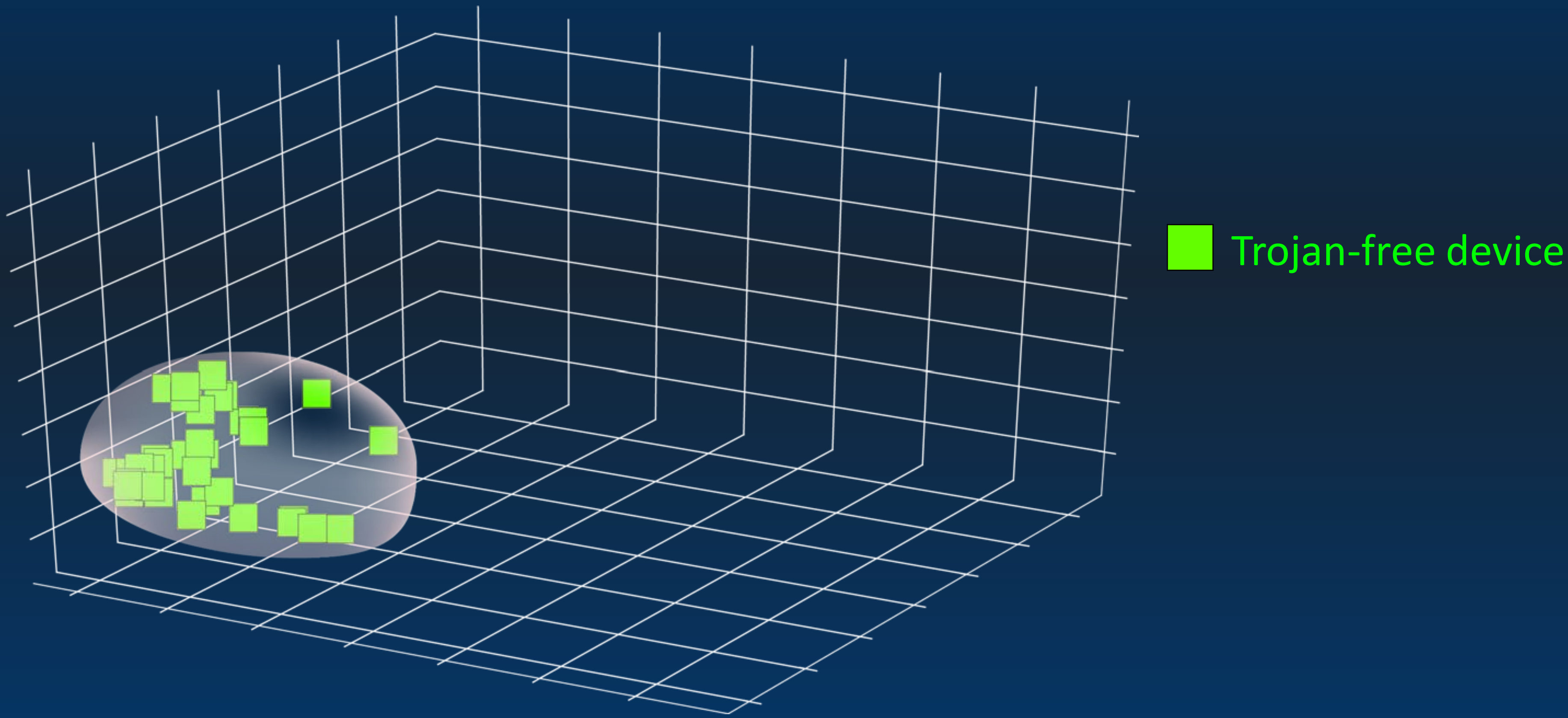
(i.e. transmission power measurements for several blocks)



Trojan Detection Results

Establishment of trusted region in fingerprint space*

(i.e. One-class Support Vector Machine (SVM))

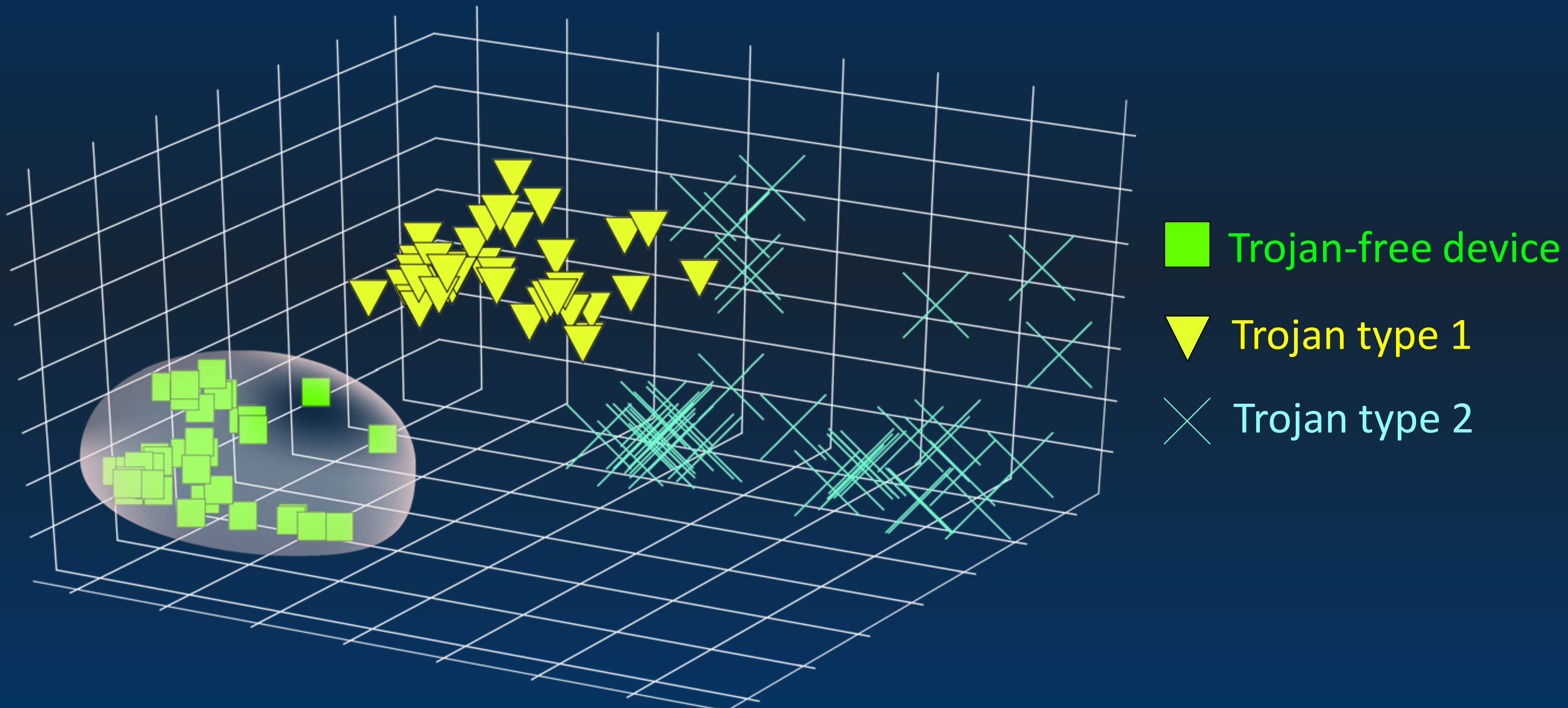


ICCAD'13

Trojan Detection Results

Evaluation of boundary effectiveness on Trojan-infested ICs*

(i.e. Type 1: contaminated amplitude and Type 2: contaminated frequency)



All Trojan-free & Trojan-infested devices correctly classified

ICCAD'13

Trojan Detection Results

Evaluation of boundary effectiveness on Trojan-infested ICs*

(i.e. Type 1: contaminated amplitude and Type 2: contaminated frequency)

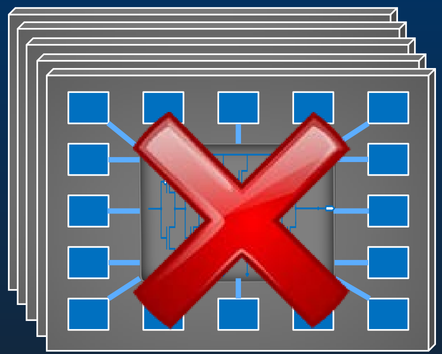
- What if golden chips are not available?
- What if Trojan keeps dormant in training stage, and turn active in operation stage?

All Trojan-free & Trojan-infested devices correctly classified

ICCAD’13

Shortcoming of Fingerprinting Methods

What if golden ICs are not available?

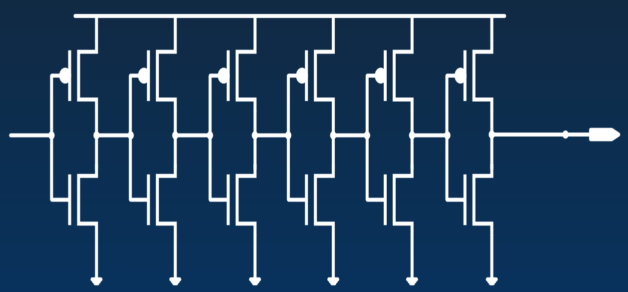


Measurements

Trusted IC population

Side-channel fingerprints

Use golden simulation model: how well would it work?



Monte Carlo

Simulations

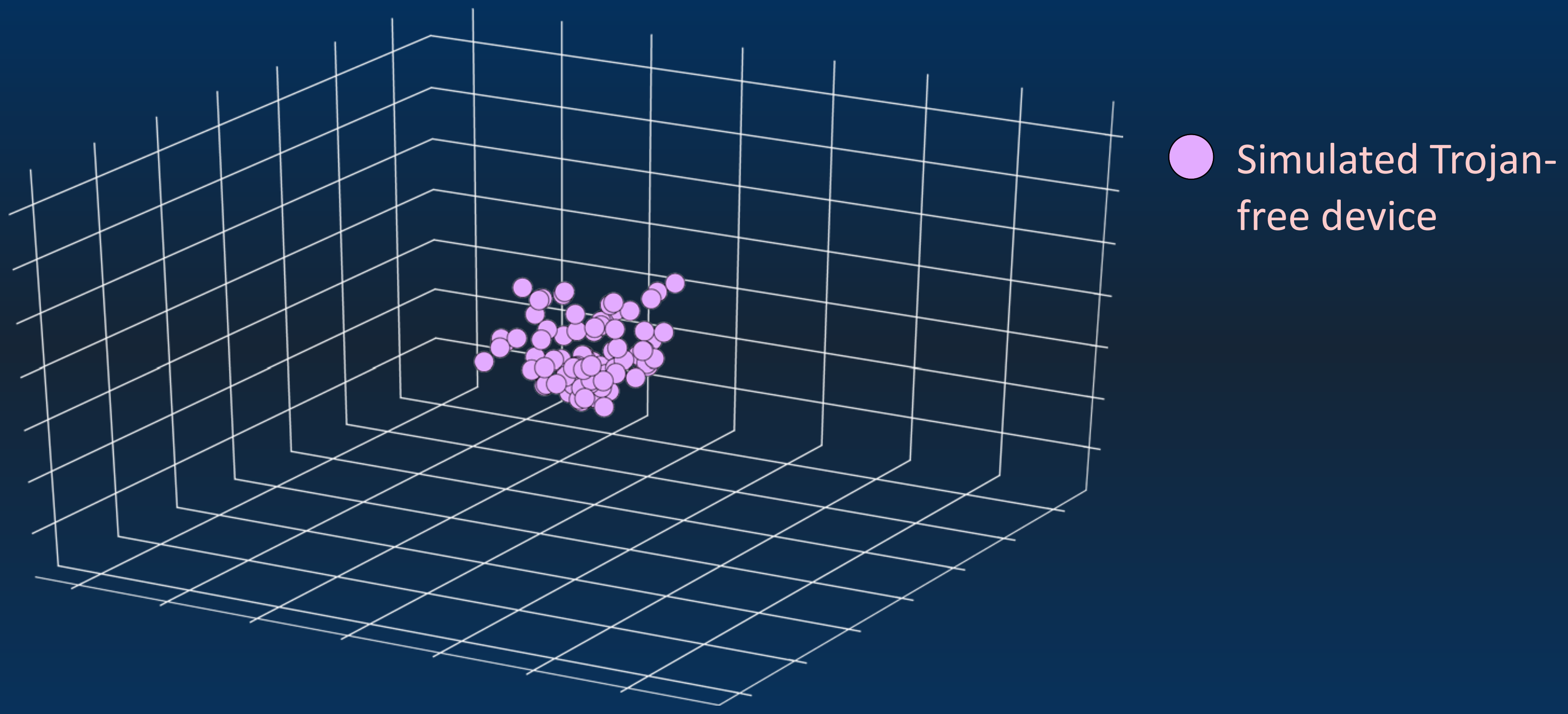
Golden Spice-level simulation model

Synthetic side-channel fingerprints

Learning Trusted Boundary from Simulation

Projection of 100 Trojan-free devices onto fingerprint space

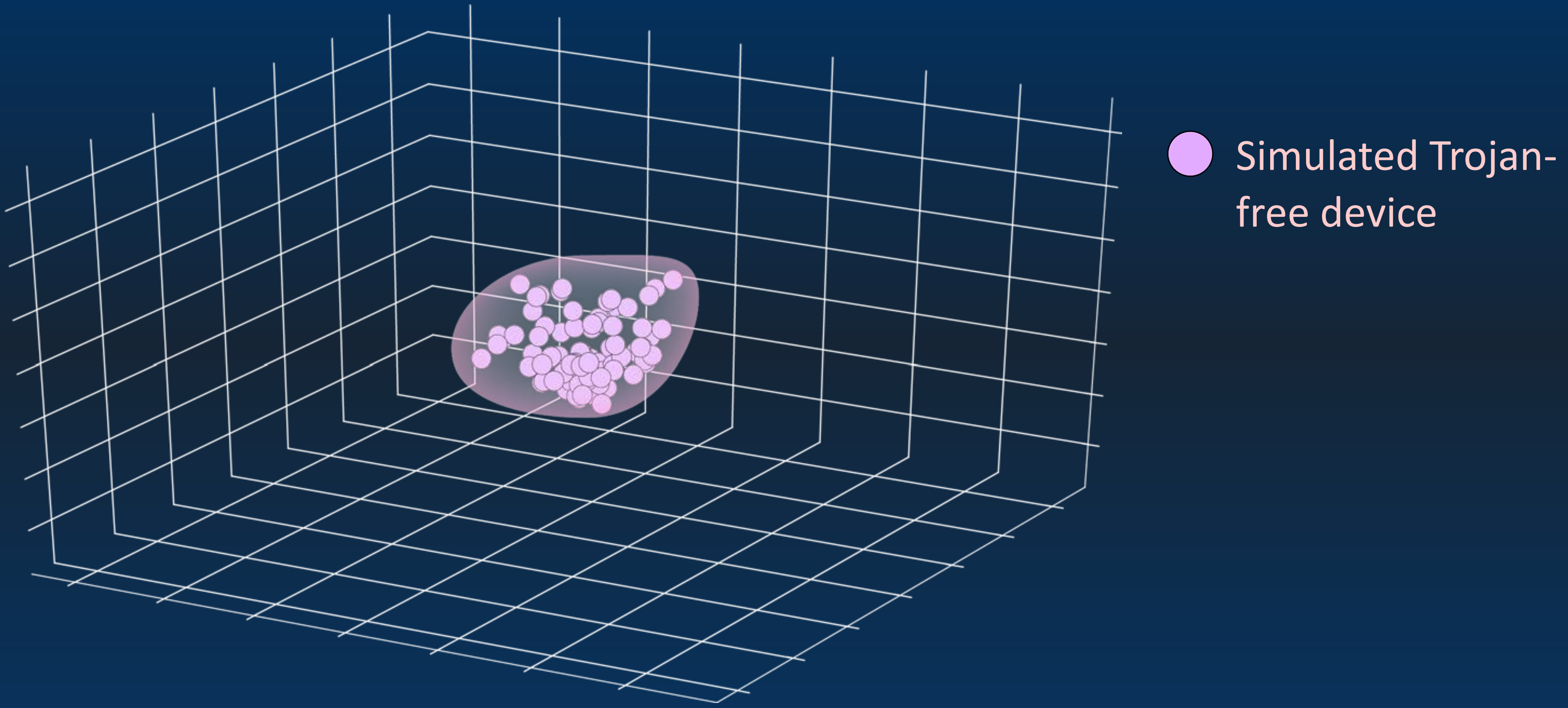
(i.e. Monte Carlo transmission power simulations)



Learning Trusted Boundary from Simulation

Establishment of trusted region in simulated fingerprint space

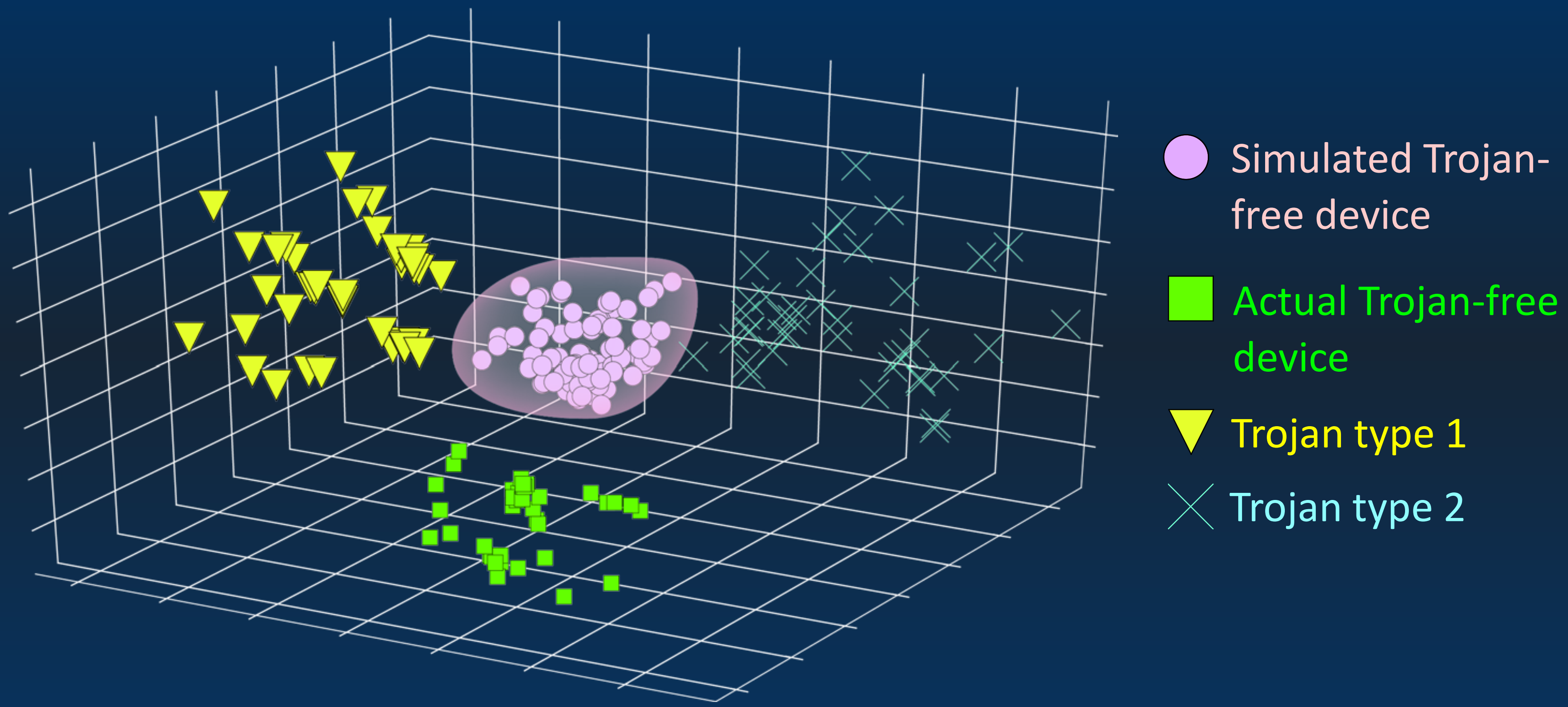
(i.e. One-class Support Vector Machine (SVM))



Learning Trusted Boundary from Simulation

Evaluation of boundary effectiveness on actual ICs

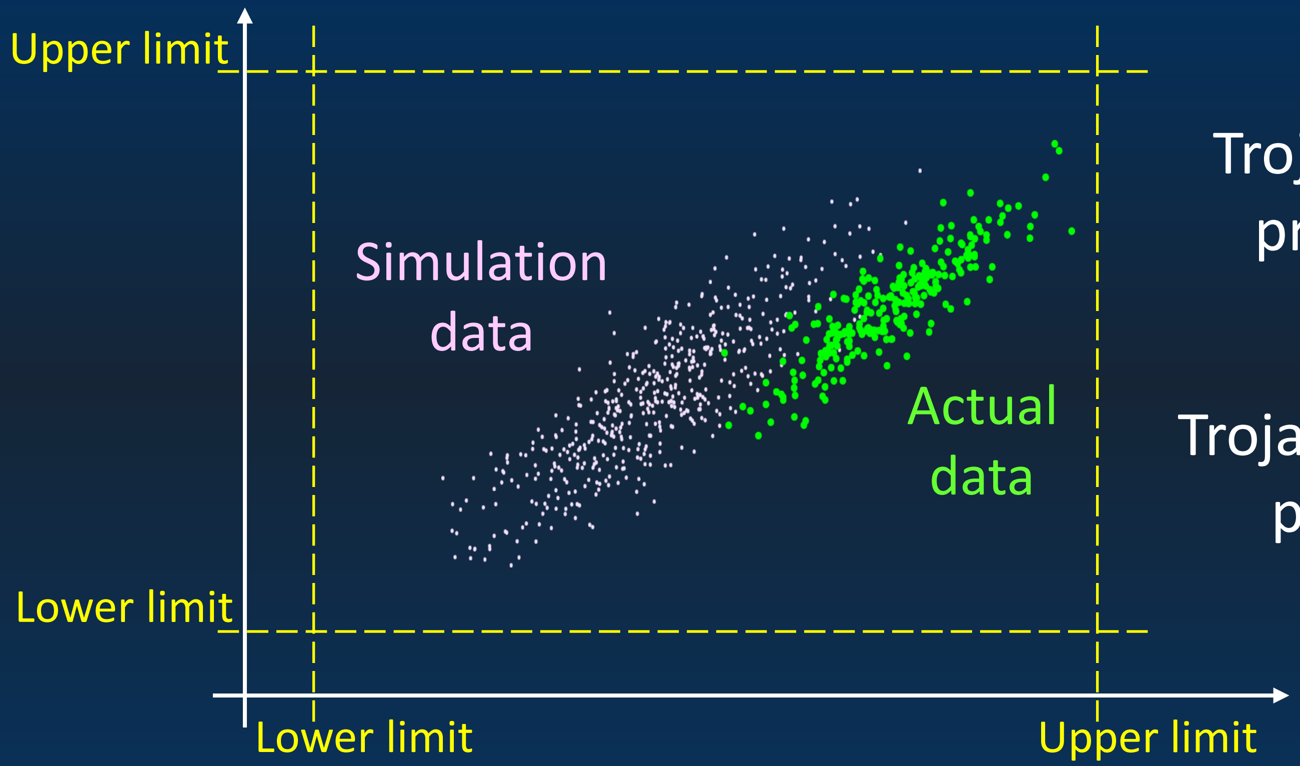
(i.e. Trojan-free, type 1 Trojan-infested and type 2 Trojan-infested)



Incorrectly classified Trojan-infested ICs	Incorrectly classified Trojan-free ICs
0/80	40/40

Inaccuracy of Simulation-Based Boundary

Limitation #1: Discrepancy between Spice model & silicon



Side-channel measurement space

Trojan-free chips from process corner #1?

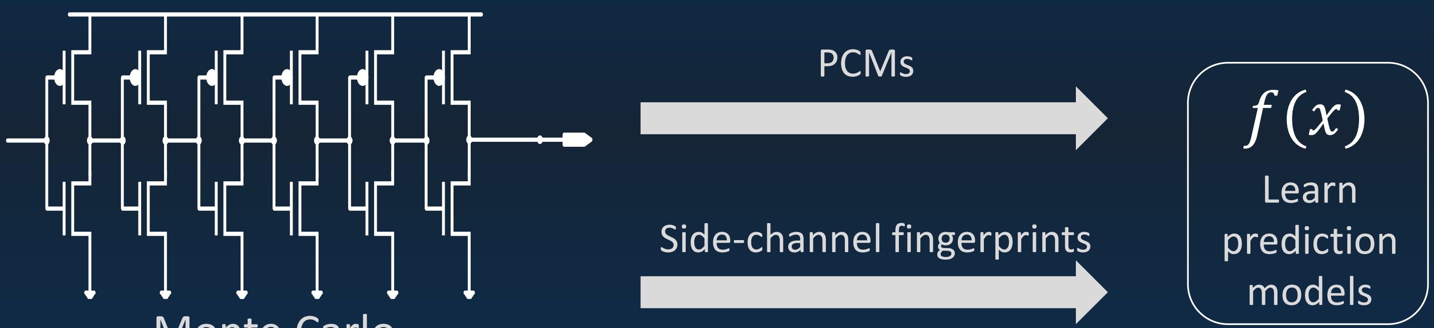
OR

Trojan-infested chips from process corner #2?

Trusted Silicon Anchor Point

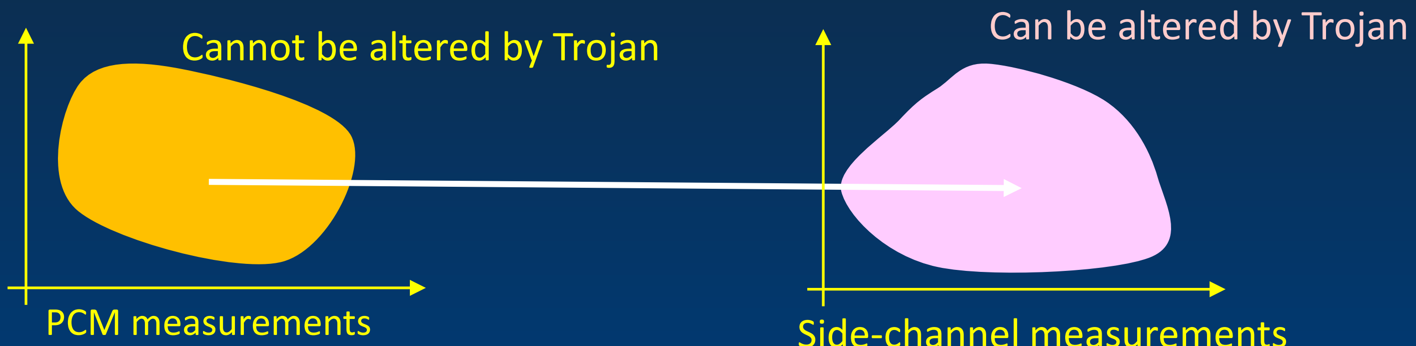
On-die Process Control Monitors (PCMs)

- Indicate process operation point
- Use as proxy for side-channel fingerprints
- Simple circuitry, hard to contaminate



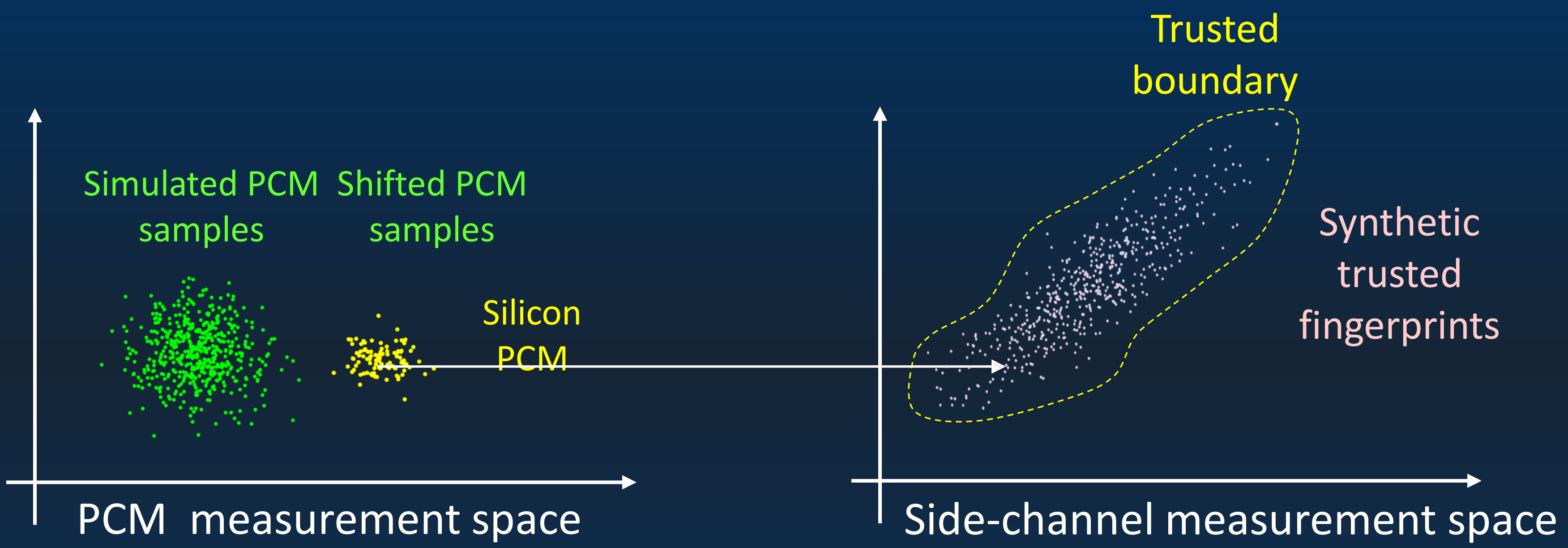
Monte Carlo

Simulation model



Synthetic Data Calibration to Process Corner

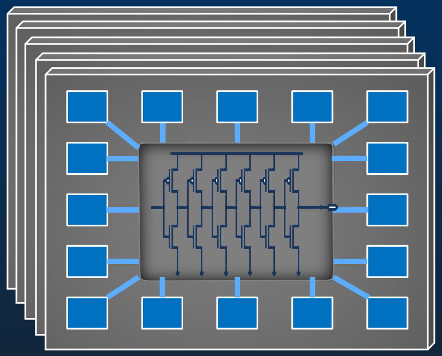
Kernel Mean Matching (KMM)



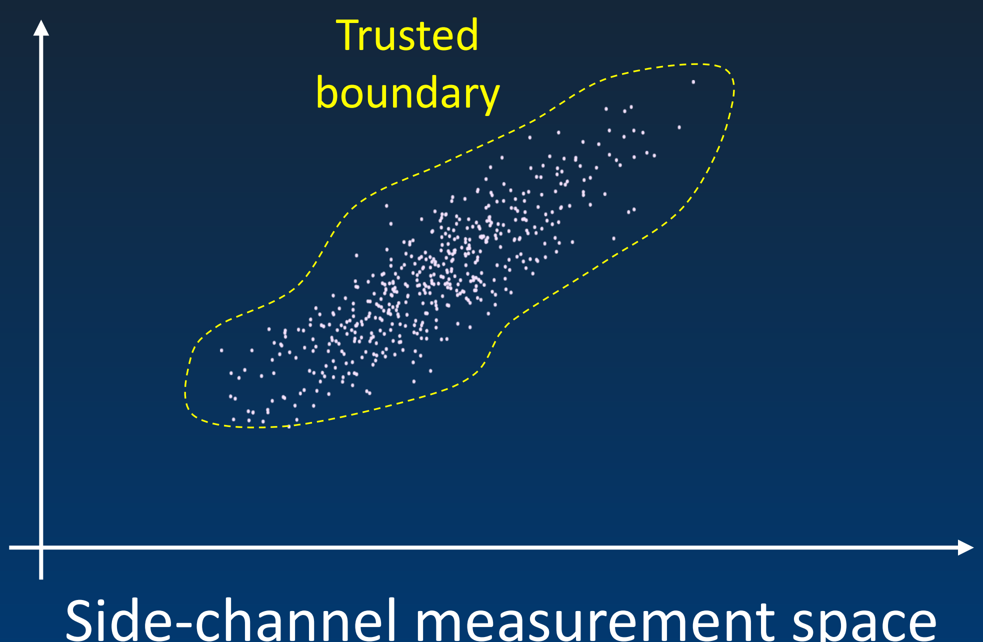
Kernel Mean Matching (KMM) is used to calibrate simulated PCM samples to the process corner producing the evaluated ICs

Inaccuracy of Simulation-Based Boundary

Limitation #2: Sample size

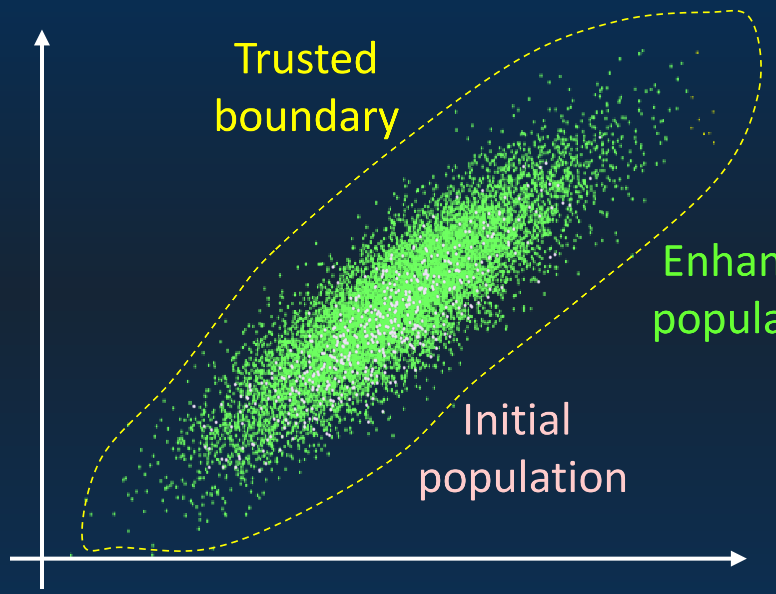


Tail of the distribution inadequately reflected by limited sample size

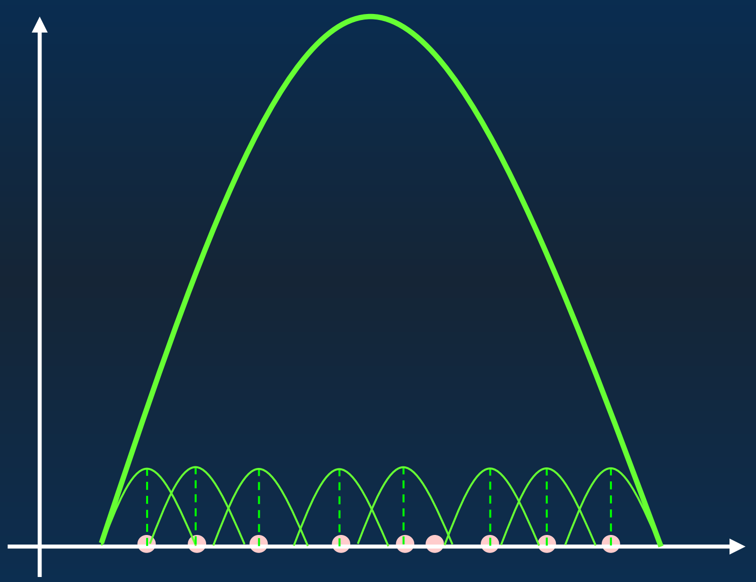


Tail Modeling Solution

1. Non-parametric Kernel Density Estimation (KDE)*



Side-channel measurement space

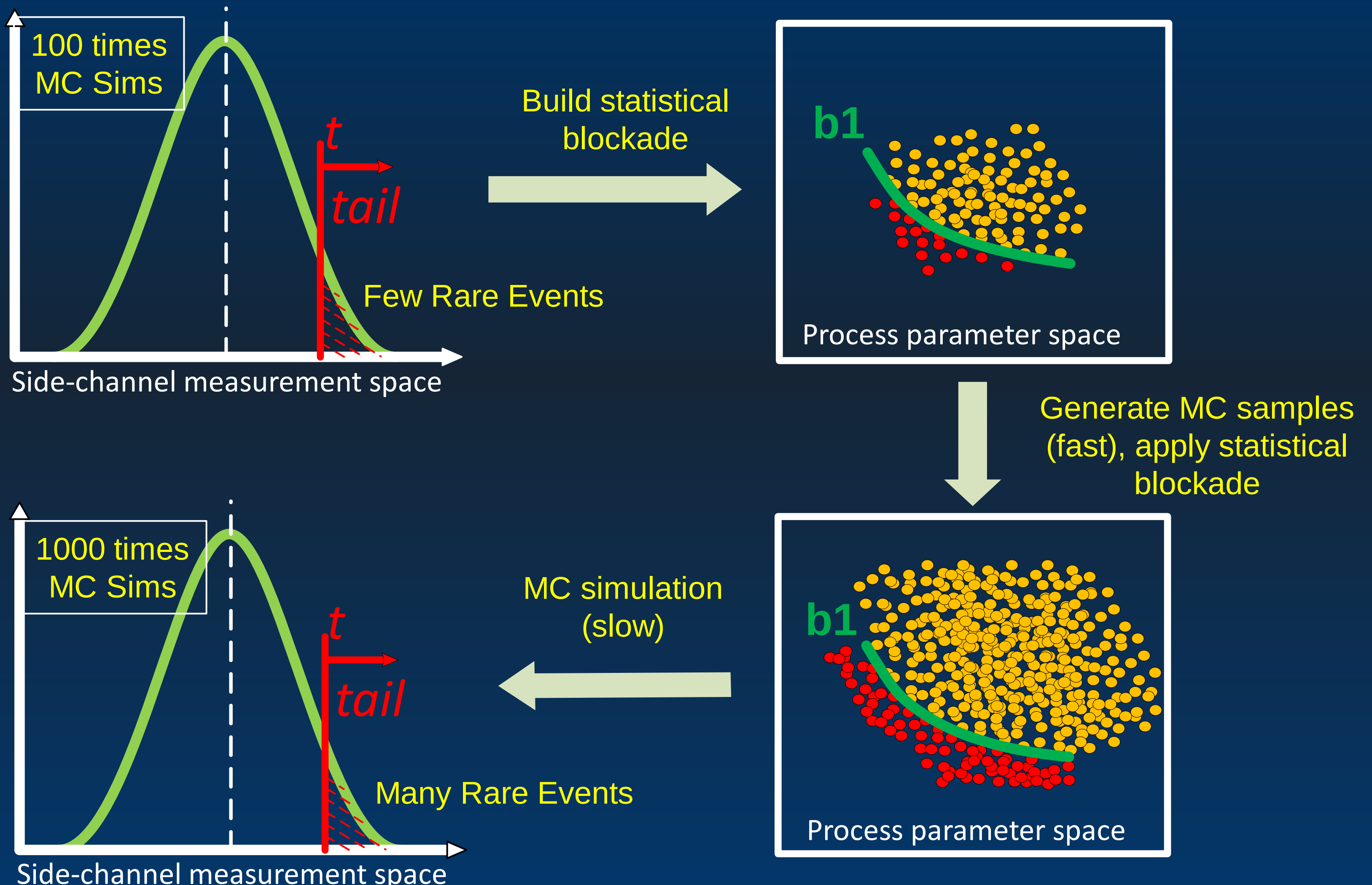


Probability Density Estimation

TCAD'09

Tail Modeling Solution

2. Statistical Blockade*

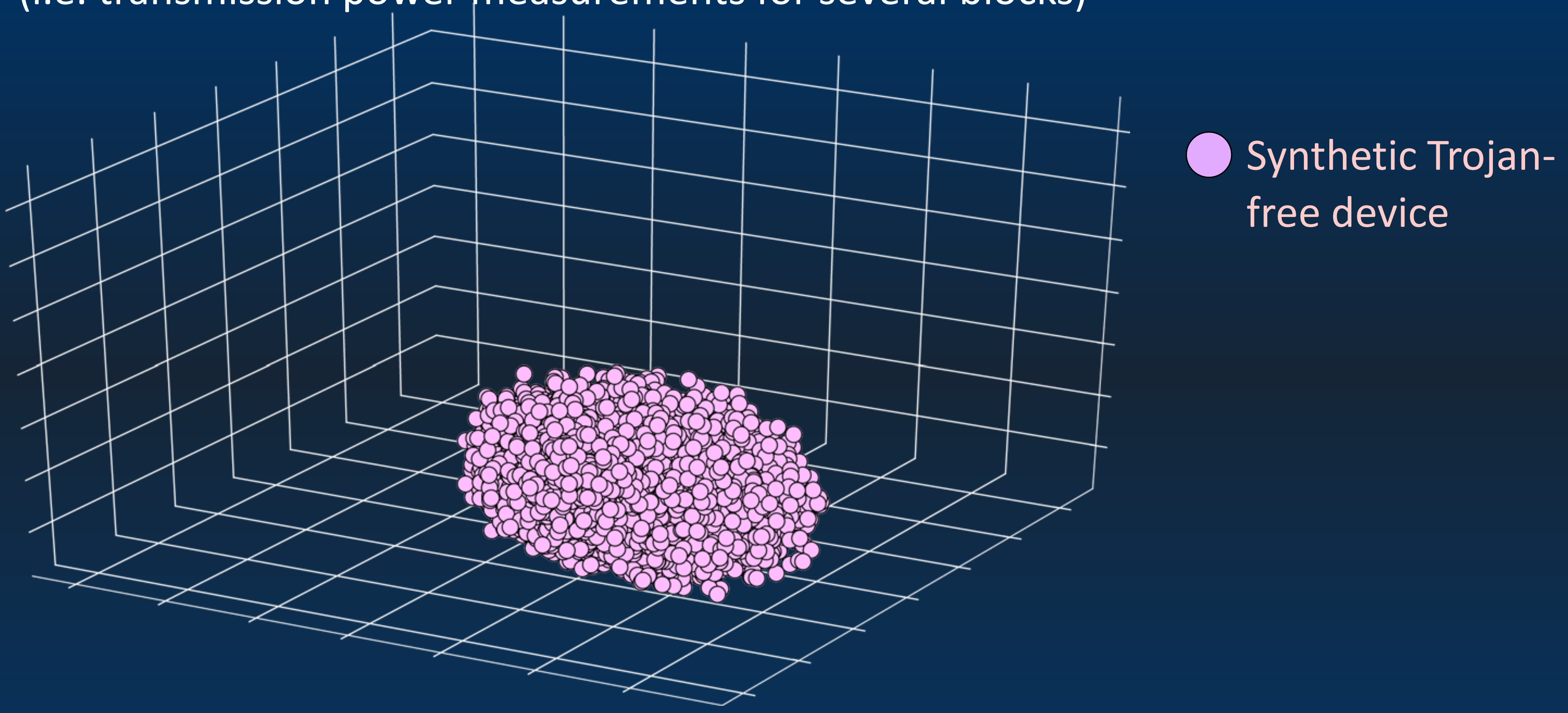


DATE'07

Golden-Chip Free Trojan Detection Results

Projection of calibrated and enhanced population

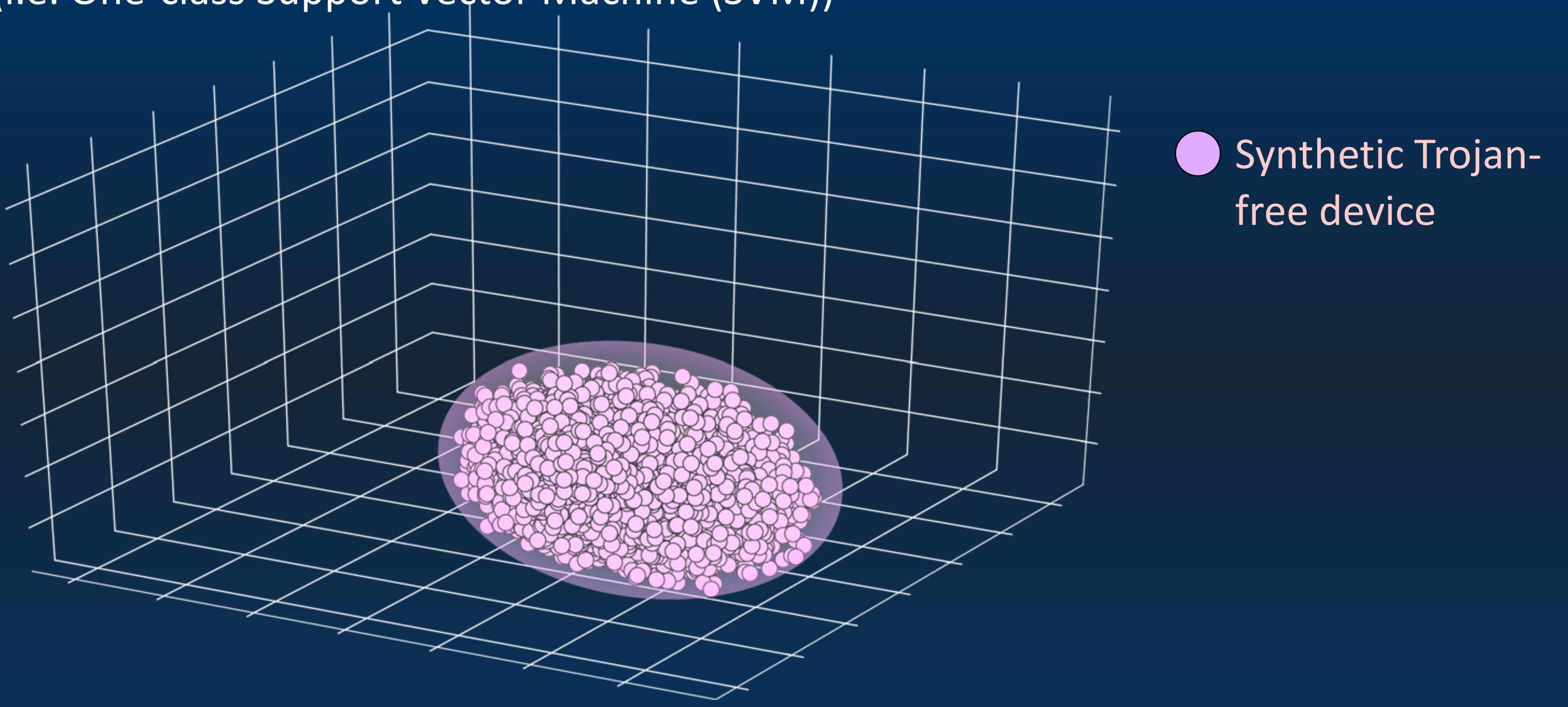
(i.e. transmission power measurements for several blocks)



Golden-Chip Free Trojan Detection Results

Establishment of trusted region in simulated fingerprint space

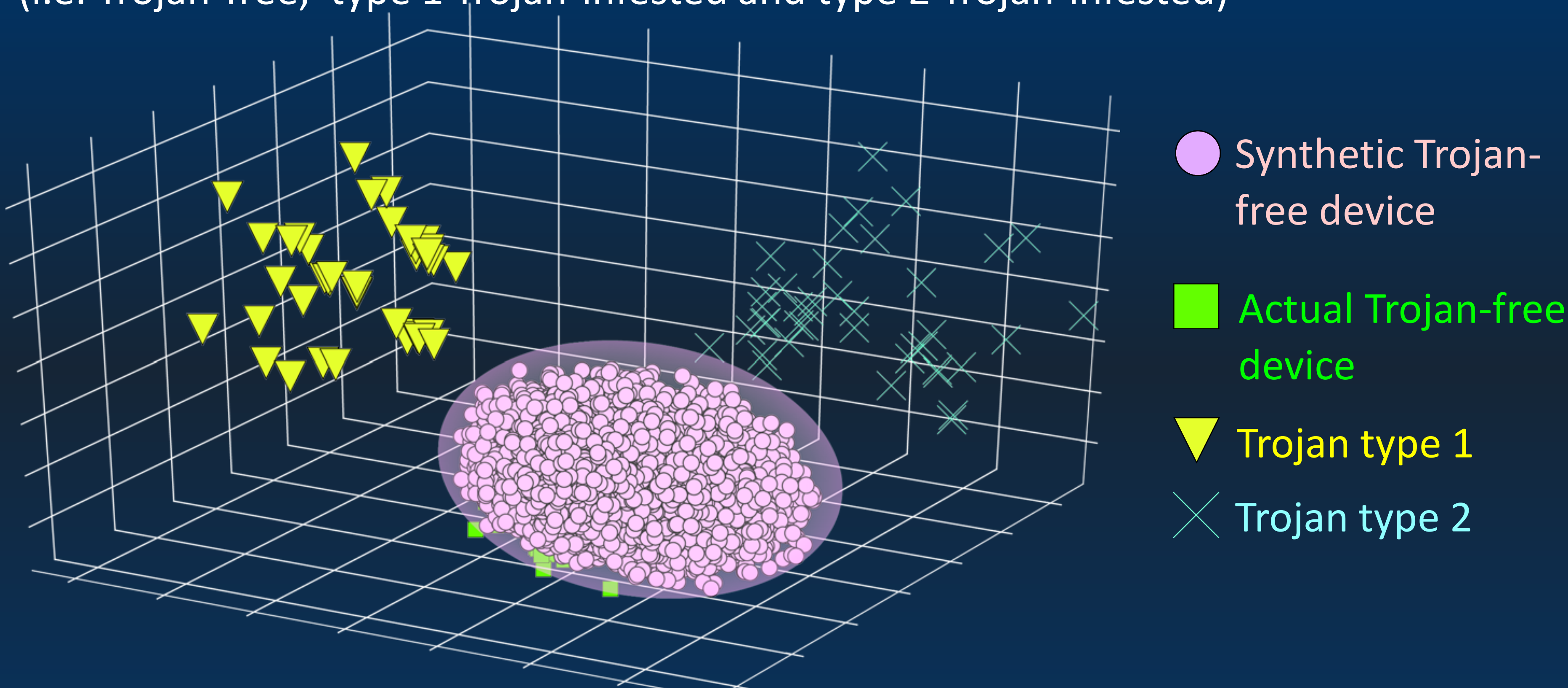
(i.e. One-class Support Vector Machine (SVM))



Golden-Chip Free Trojan Detection Results

Evaluation of boundary effectiveness on actual ICs

(i.e. Trojan-free, type 1 Trojan-infested and type 2 Trojan-infested)



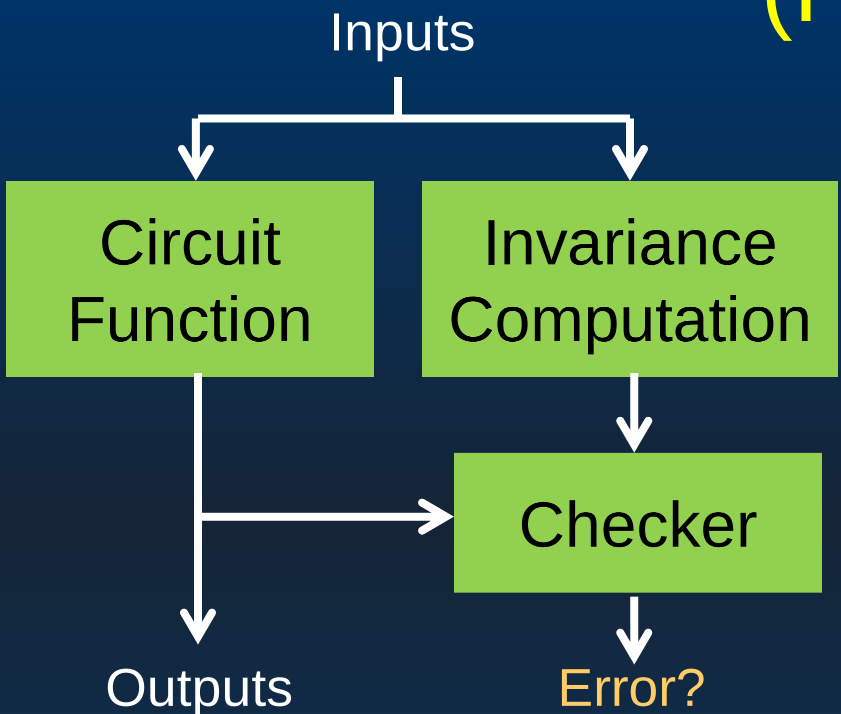
	Incorrectly classified Trojan-infested ICs	Incorrectly classified Trojan-free ICs
KDE	0/80	3/40
Blockade	0/80	0/40

DAC'14

Limitation: Dormant Trojans

- Trojans can be dormant (inactive) during testing
- Input trigger or lapsed-time counter can activate during normal functionality
- Statistical side-channel fingerprinting ineffective in this case

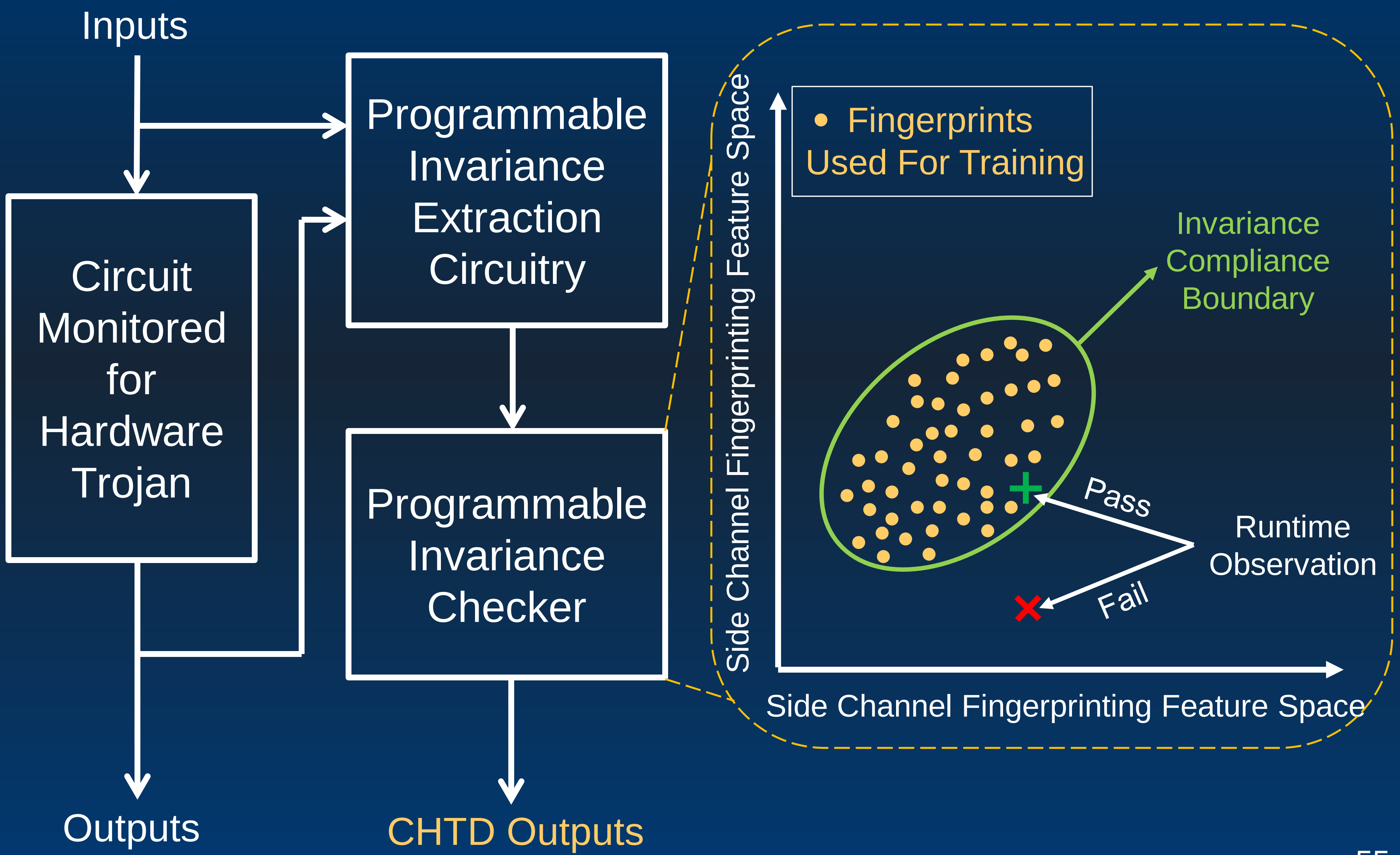
Concurrent Hardware Trojan Detection (ITC'15)



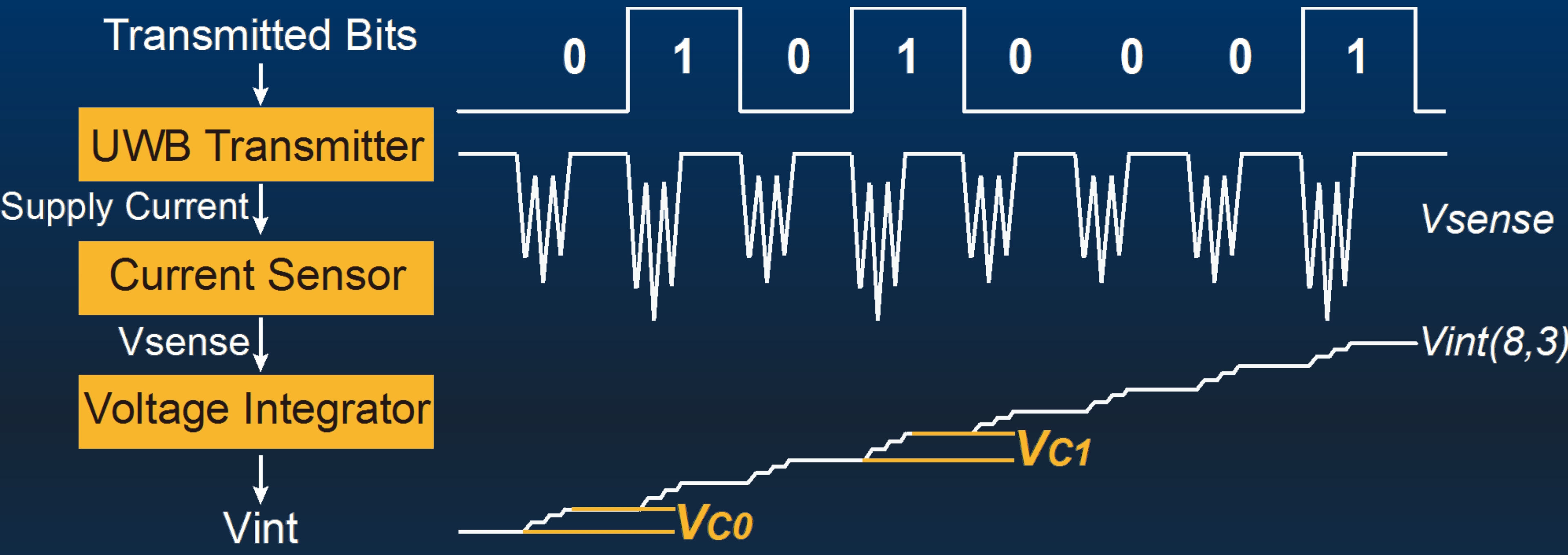
- Inspiration: Invariance-based Concurrent Error Detection
- Invariance: A property which holds true when a circuit operates correctly and is violated when it does not

- Challenge: Identify and check invariant property which holds true if and only if circuit in trusted operation region
  - Unknown, carefully hidden culprits, rather than modeled errors
  - Invariant property should be withheld from adversary: individualized to each chip after fabrication

Concurrent Hardware Trojan Detection



Invariant Property

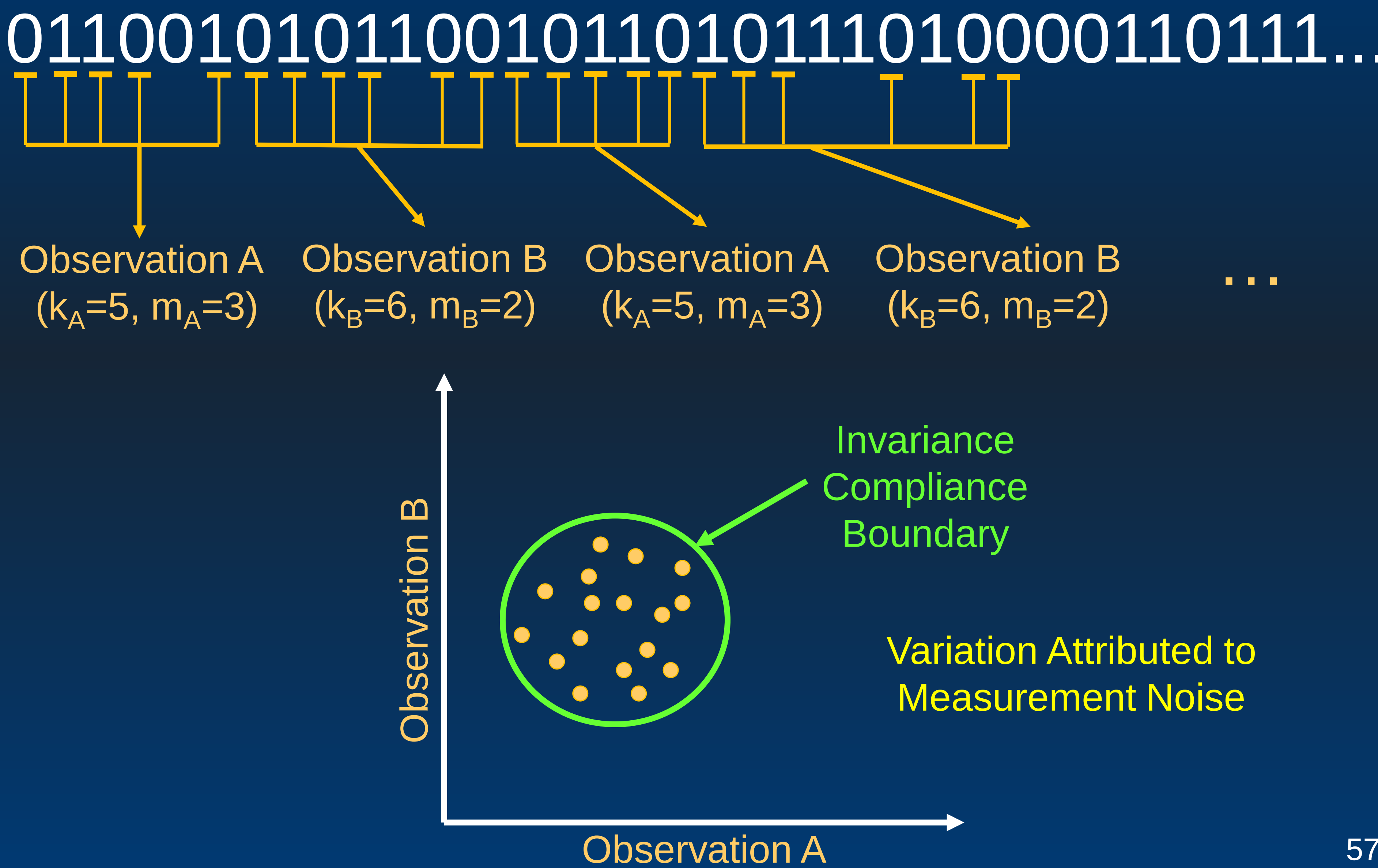


$$V_{int}(k,m) = m \cdot V_{C1} + (k-m) \cdot V_{C0} + \delta_{noise}$$

k: number of transmitted bits

m: number of $'1's$ in transmitted bits

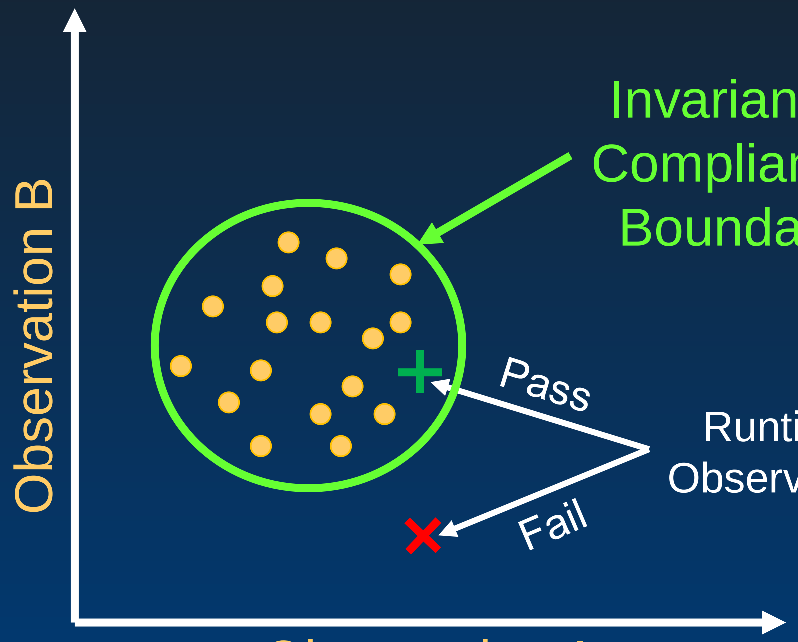
Training Phase



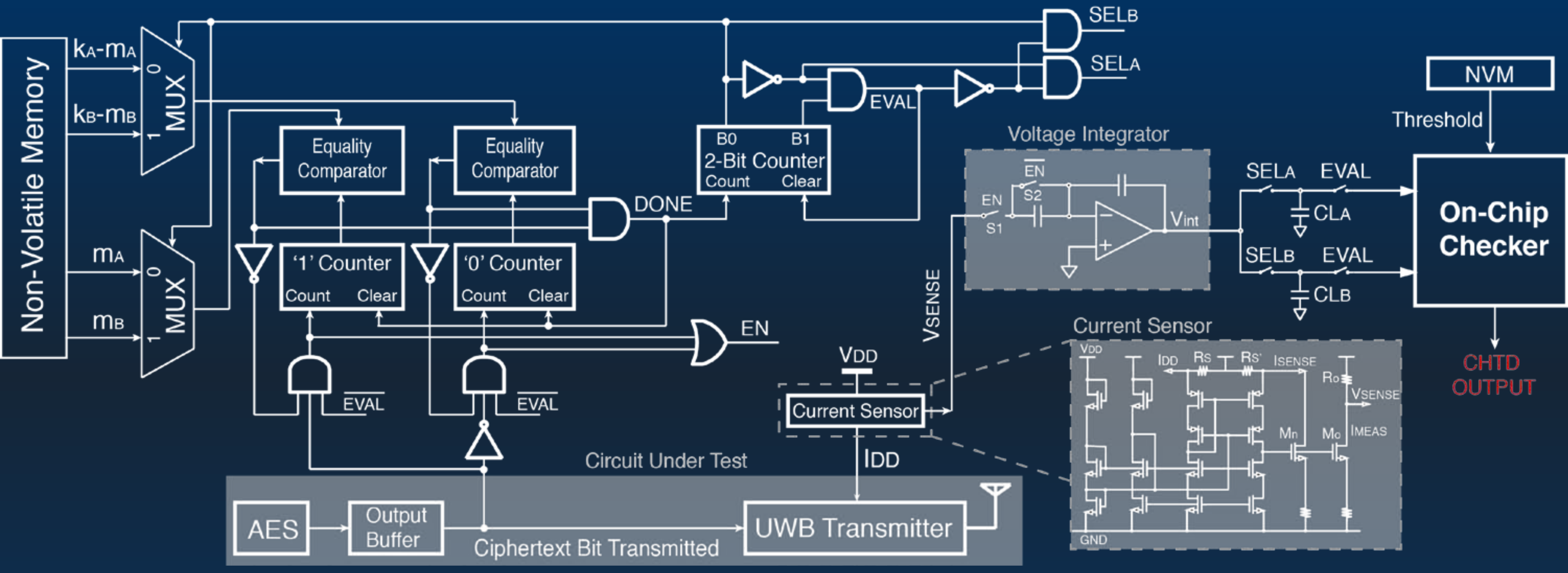
Monitoring Phase

1001101010100011011100101011010010...

Observation A (k_A=5, m_A=3) | Observation B (k_B=6, m_B=2) | Observation A (k_A=5, m_A=3) | Observation B (k_B=6, m_B=2)

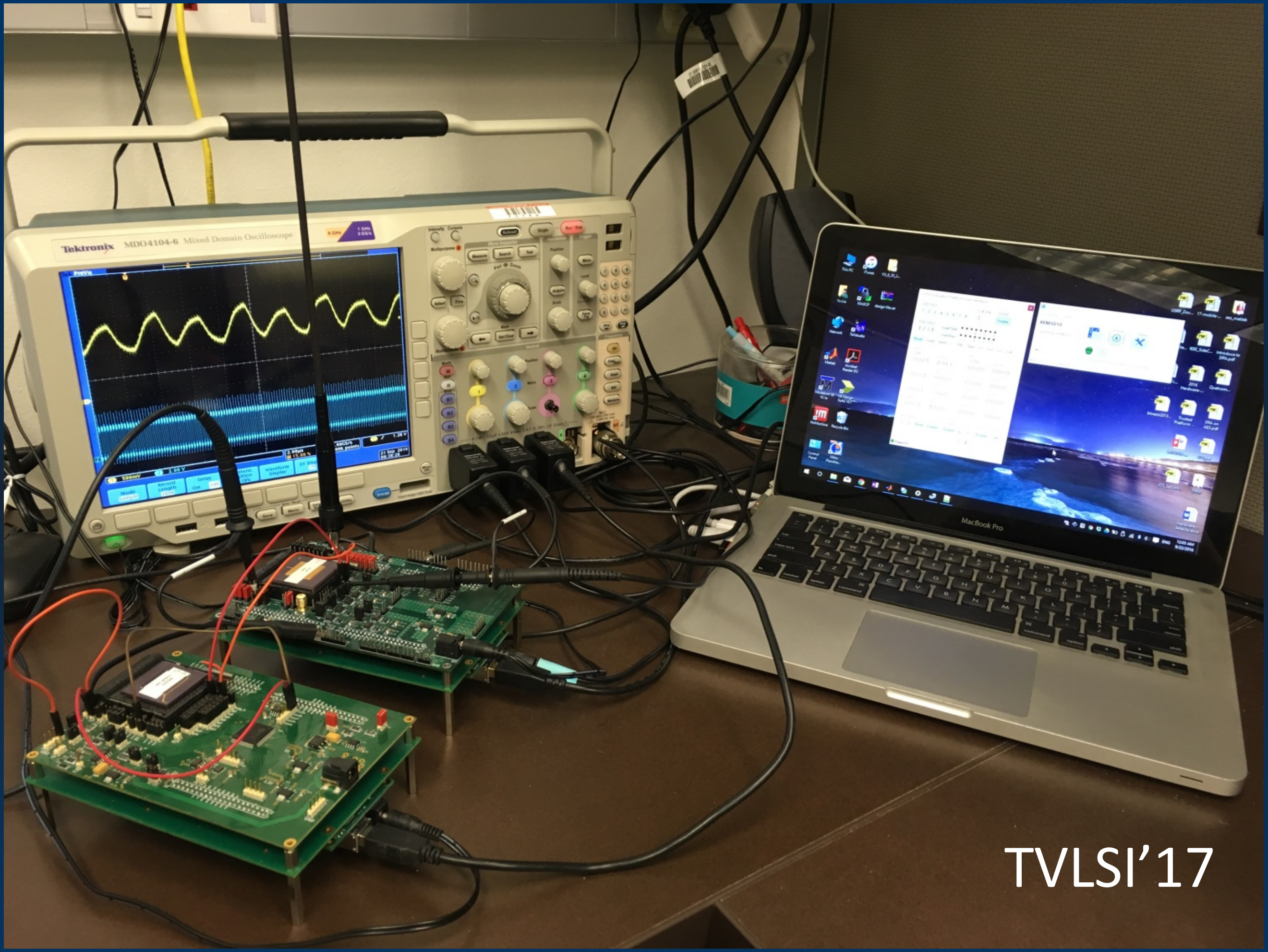


Invariant Property Extraction Circuit



- Non-volatile memory used to program invariance [ITC'15]

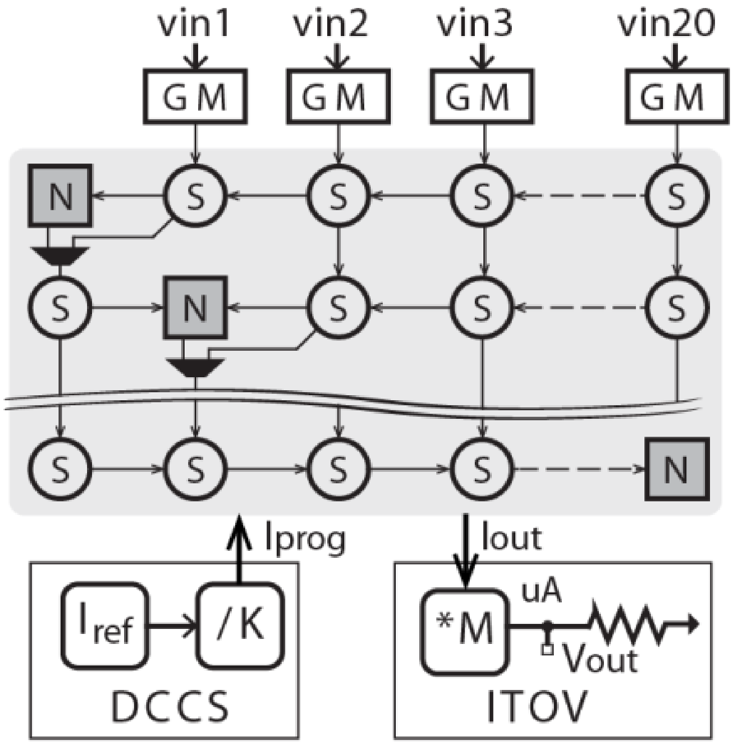
Experimentation Platform



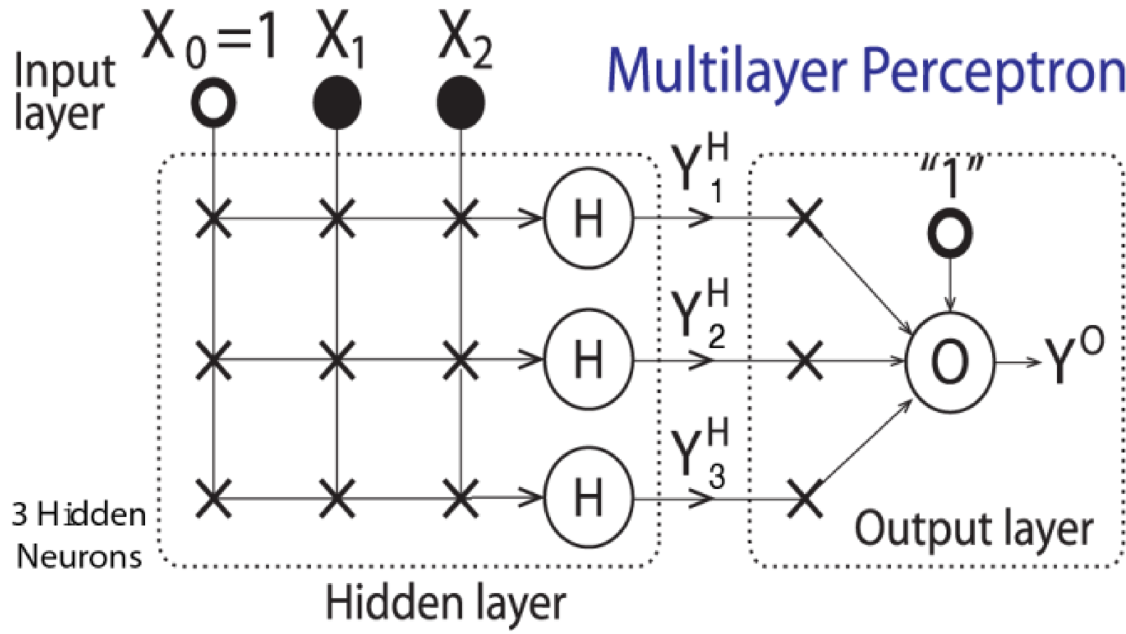
- All CHTD logic included in new version of wireless crypto IC
- First real-time hardware Trojan method demo in silicon

Programmable Analog Neural Network

Maliuk and Makris et al. IEEE TNNLS'15



(a)

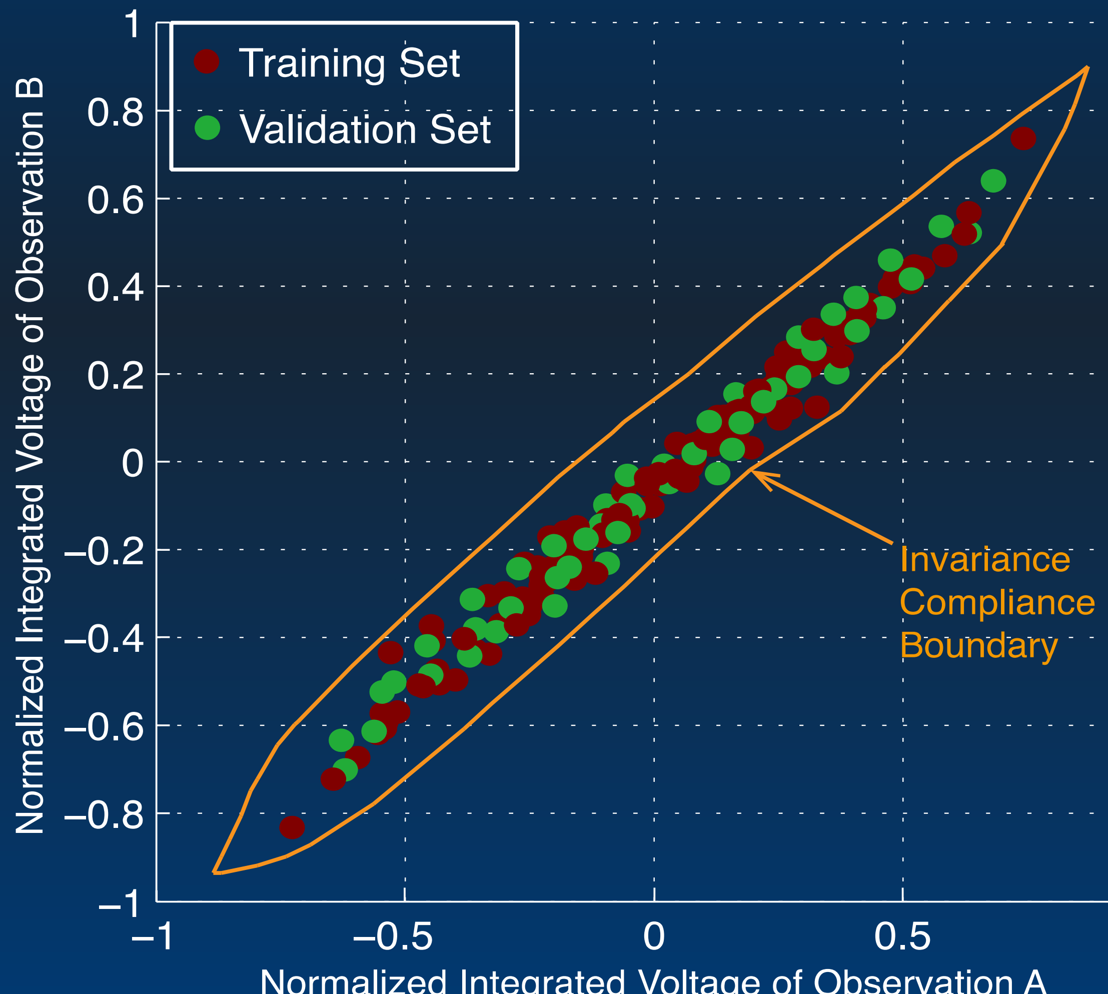


(b)

Technology	Chip Size	No. of inputs	No. of neurons	No. of synapses	Weight Resolution (dynamic mode)	Weight Resolution (non-volatile mode)
TSMC 0.35 µm	3x3 mm^2	20	30	600	>8 bits	>8 bits

Results (1/4): False Positives

- Trojan-free chip transmits randomly generated plaintext encrypted with randomly chosen 128-bit key.



Training Set Size: 50

Validation Set Size: 50

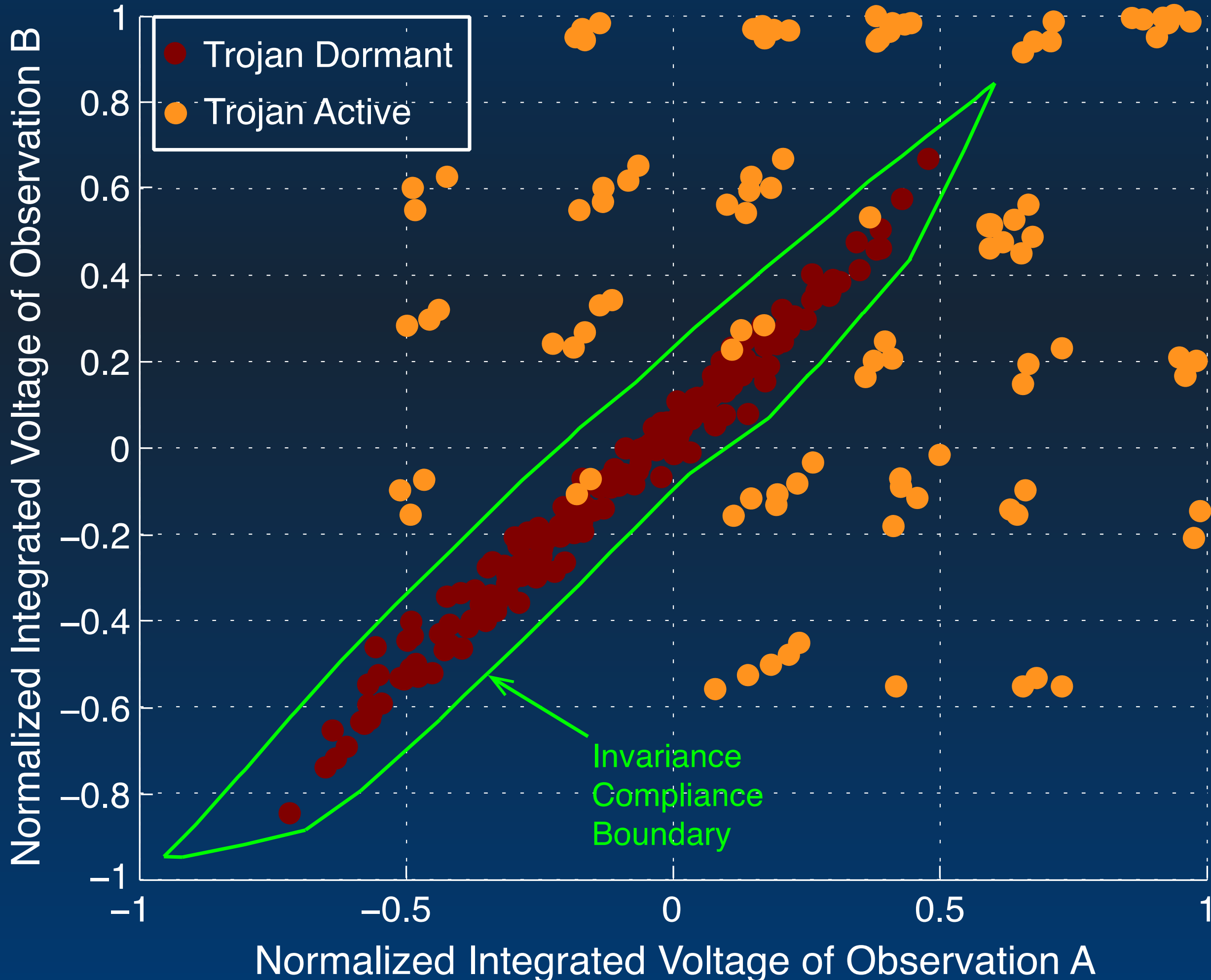
$k_A = 8, m_A = 2$

$k_B = 8, m_B = 4$

No False Positives

Results (2/4): Detecting Trojan Activation

- Trojan-I infested chip transmits randomly generated plaintext encrypted with randomly chosen 128-bit key



- Training Set:

  Trojan is *dormant*

  Sample Size: 100
- Validation Set:

  Trojan is *active*

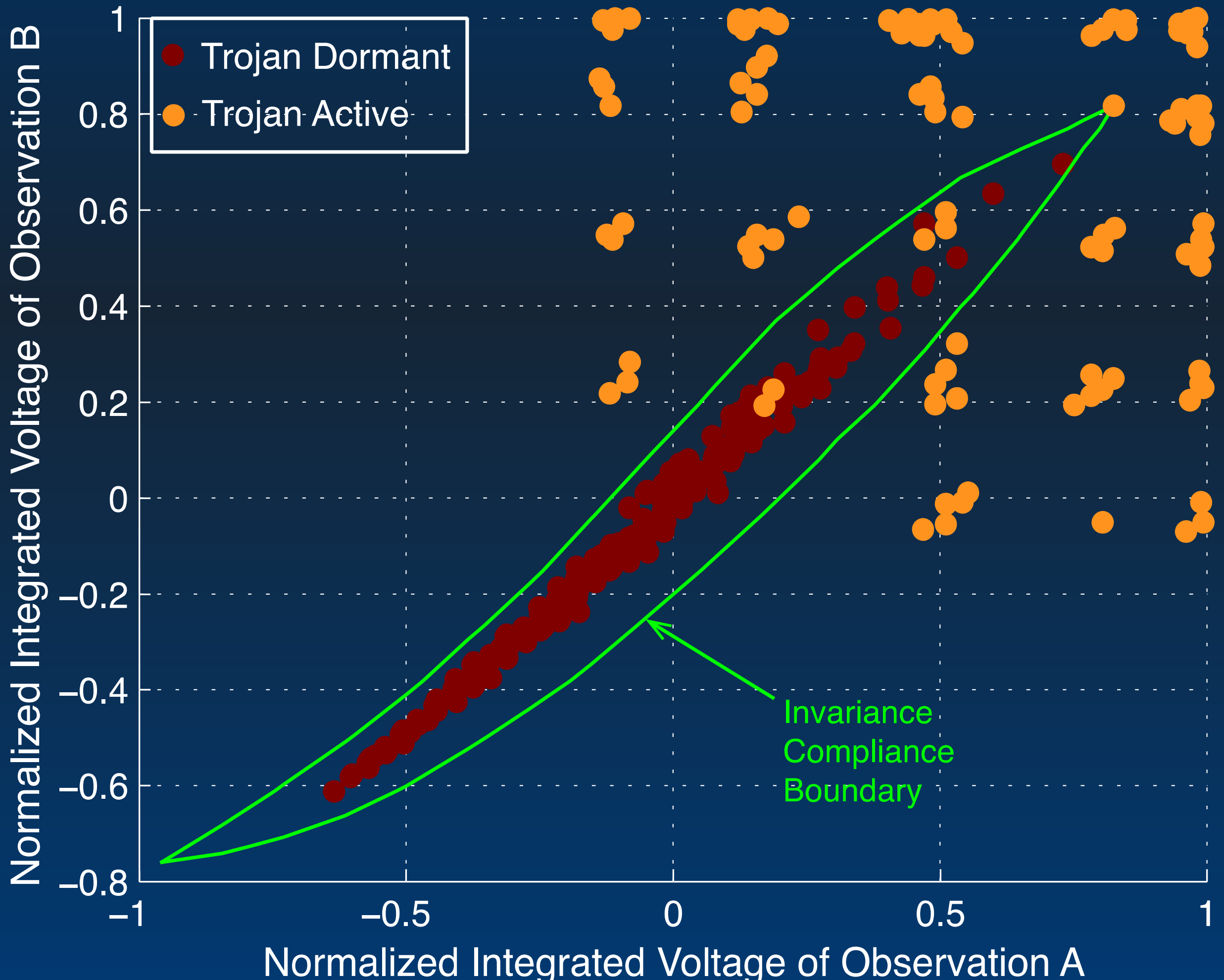
  Sample Size: 100
- Invariance:

  $k_A = 8, m_A = 2$

  $k_B = 8, m_B = 4$

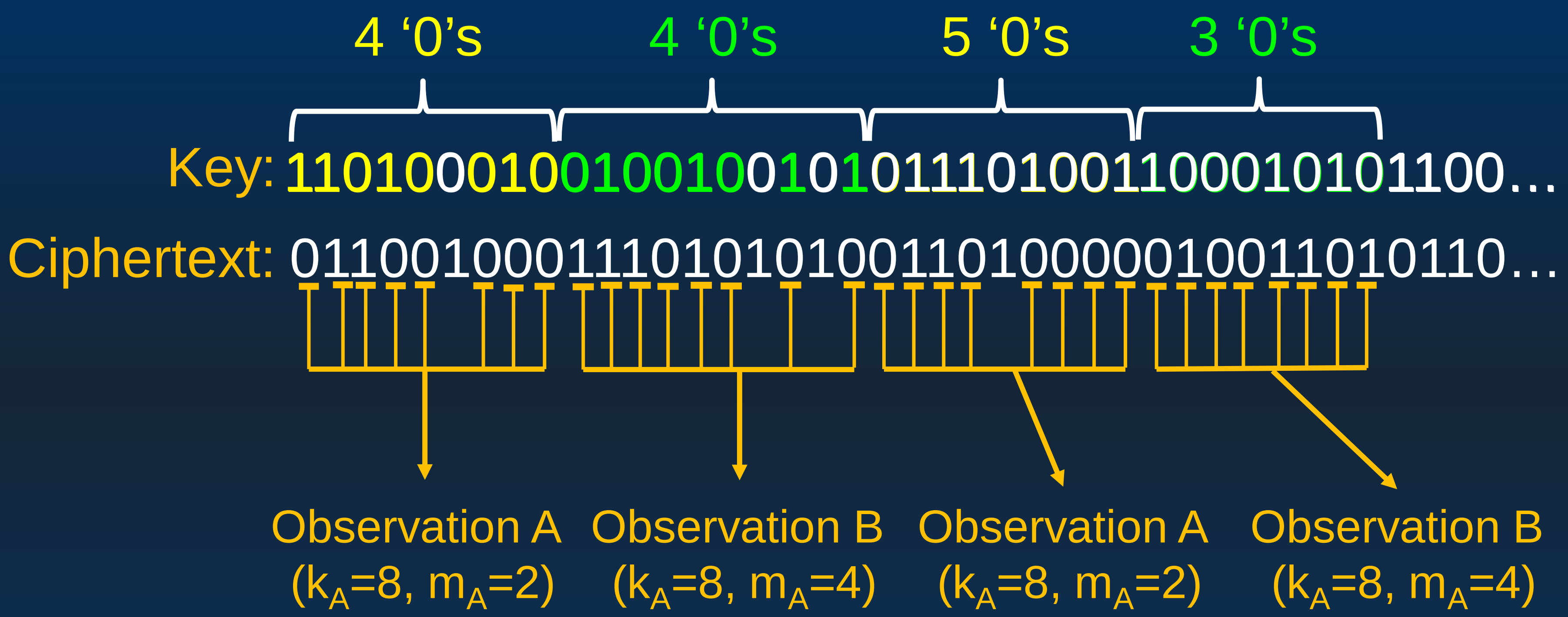
Results (3/4): Detecting Trojan Activation

- Trojan-II infested chip transmits randomly generated plaintext encrypted with randomly chosen 128-bit key



- Training Set:
  Trojan is *dormant*
  Sample Size: 100
- Validation Set:
  Trojan is *active*
  Sample Size: 100
- Invariance:
  $k_A = 8, m_A = 2$
  $k_B = 8, m_B = 4$

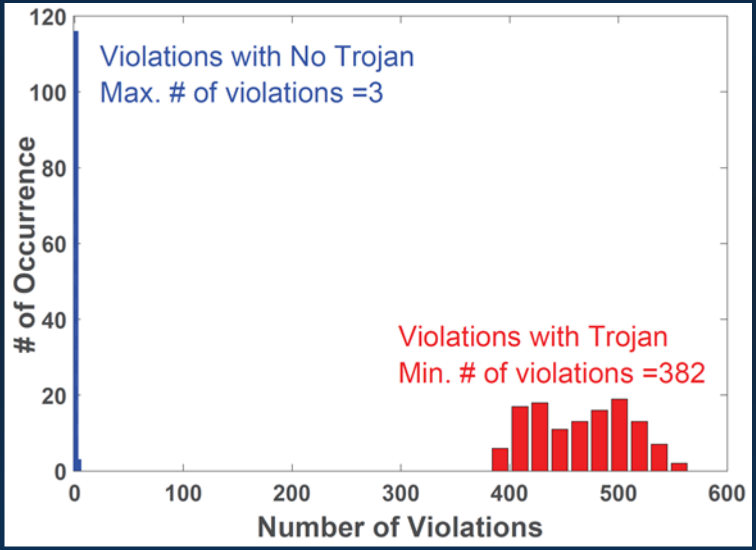
Results (4/4): Recovering False Negatives



- Aliasing caused by same number of leaked key ‘0s’
- Trojan detected in subsequent invariance check: Average latency: 23 cycles

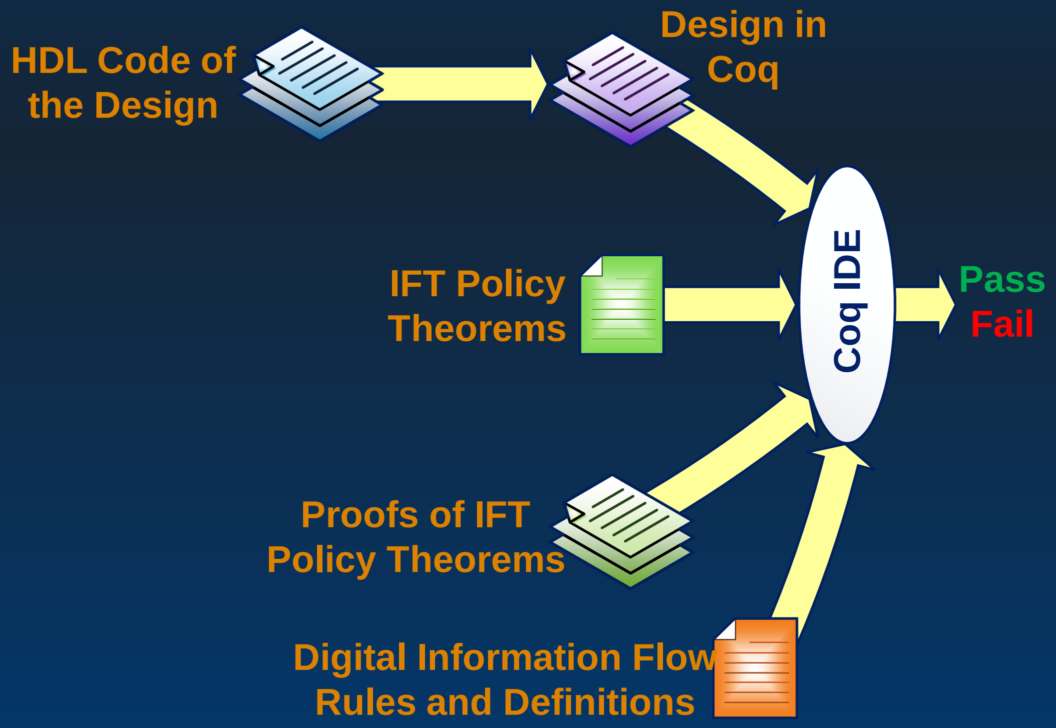
Statistical Methods

- Hardware Trojan detection in mobile platforms [ISQED'16]
  - Golden-chip free method
  - Detects Trojans operating below noise level
  - Threshold for noise referencing
  - Trojan distinguished from noise in the frequency domain
  - Number of violated frequency bins indicates Trojan activity

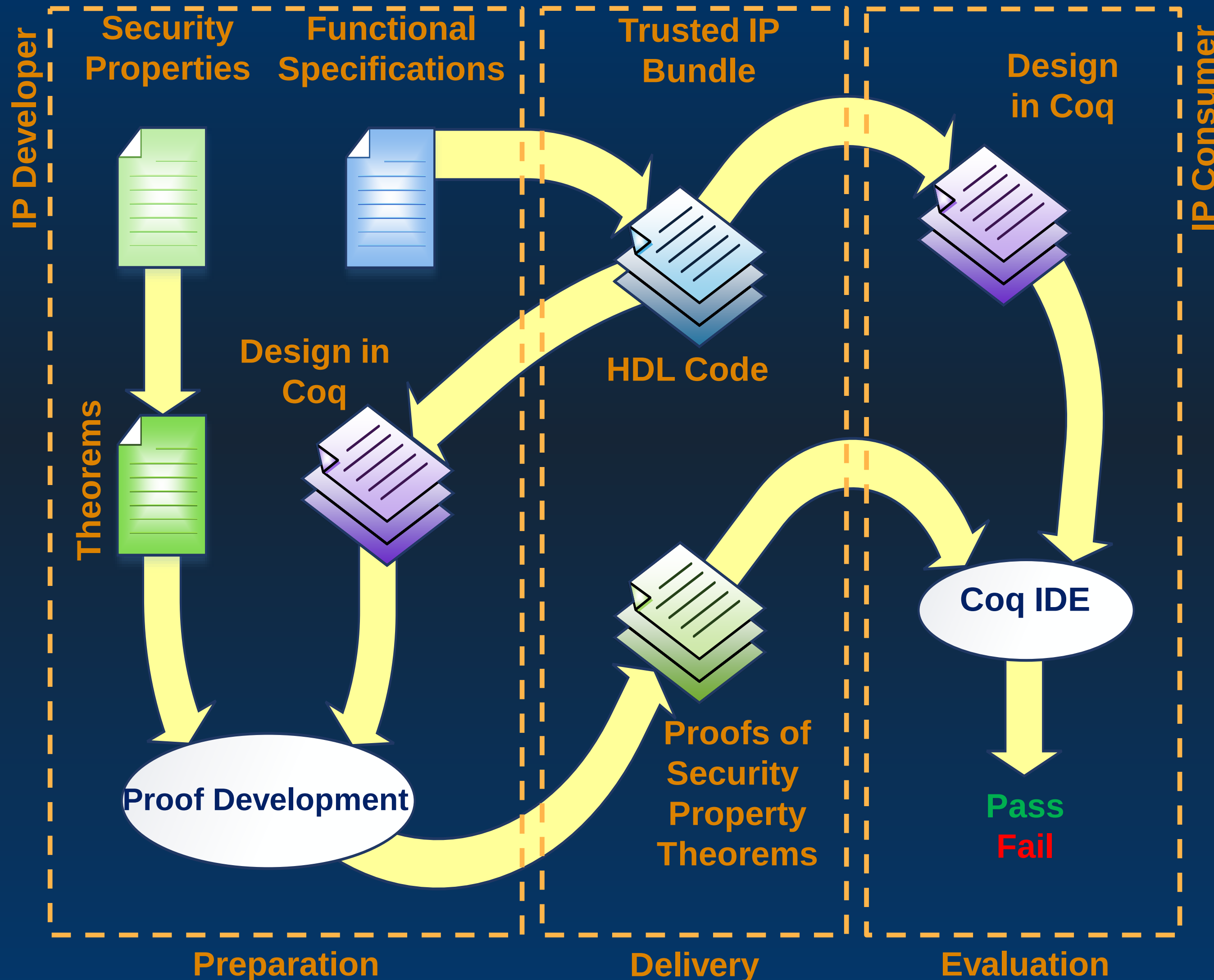


Formal Methods

- Information Flow Tracking in AMS Designs through Proof-Carrying Hardware IP [DATE’17]



Proof-Carrying Hardware IP (PCHIP)*



*[TIFS 2012]

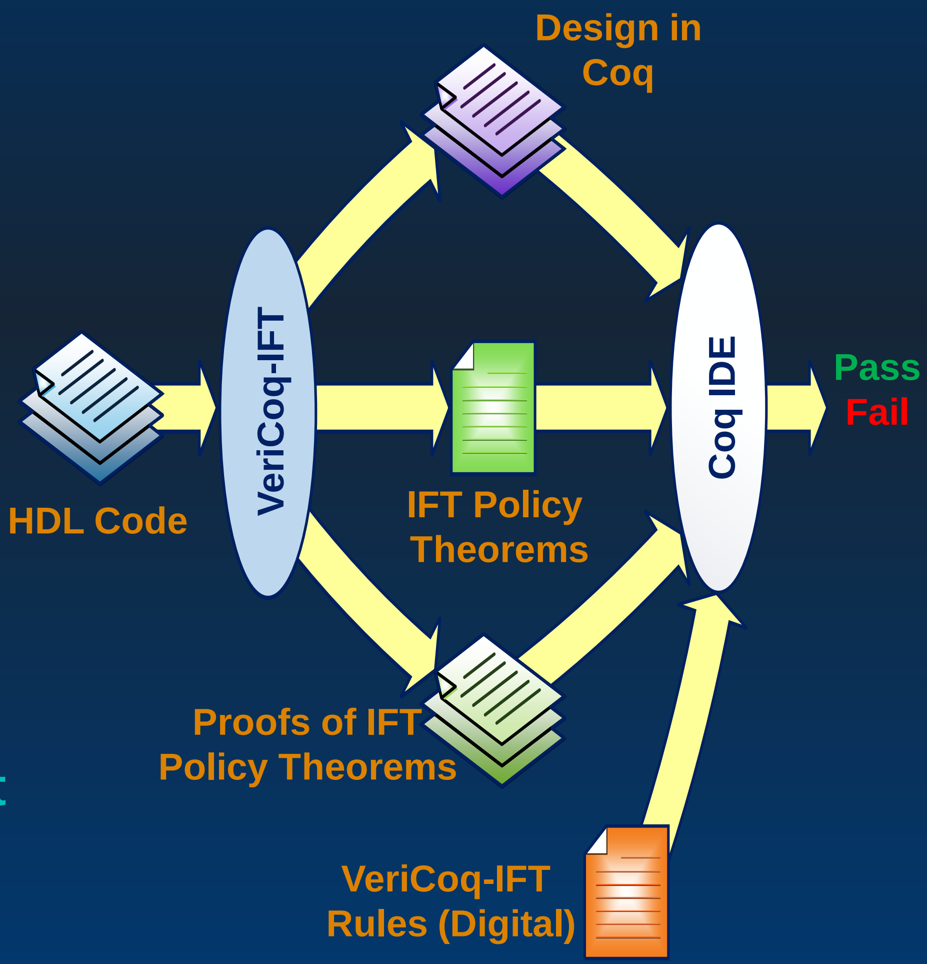
PCHIP-based IFT (HOST'13)

- **Ensures that no sensitive information is leaked through the outputs – mainly utilized for cryptographic hardware**
- **Assigns dynamic sensitivity level tags to each signal**
  - **Tracks the sensitivity levels through the design over time**
  - **Certain operations are marked as capable of reducing the sensitivity level**
  - **Functionality of operations is omitted**
- **Sensitivity levels are maintained in a list in Coq and their compliance with the security property is formally evaluated**

VeriCoq-IFT (HOST'15)

- **Fully automated PCHIP framework for information flow policies to prevent sensitive information leakage**

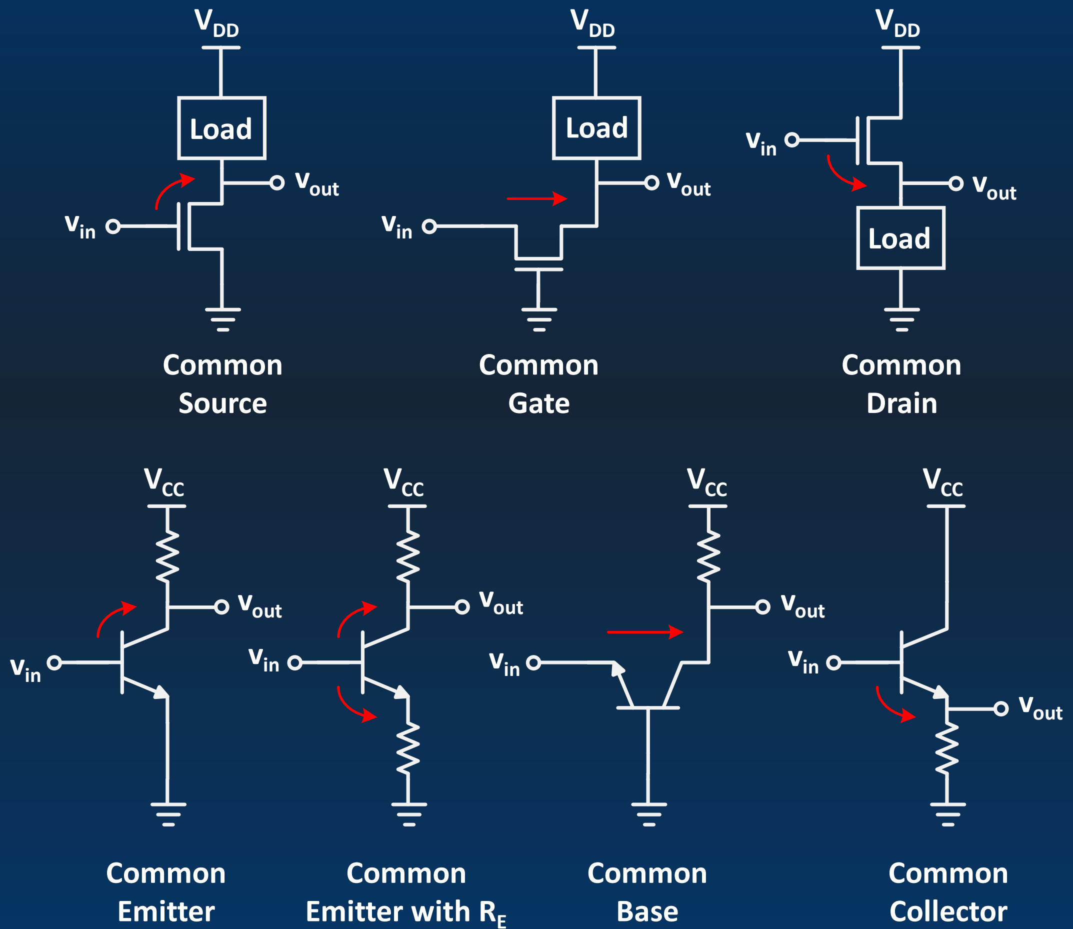
- **Conversion of Verilog code to Coq representation**
  - **Supports most Verilog synthesizable constructs**
  - **Special comments (pragmas) to gather the required information**
- **Security property theorems**
  - **Automatically generated for all outputs**
- **Proofs of theorems**
  - **Relies on stabilized sensitivity list**



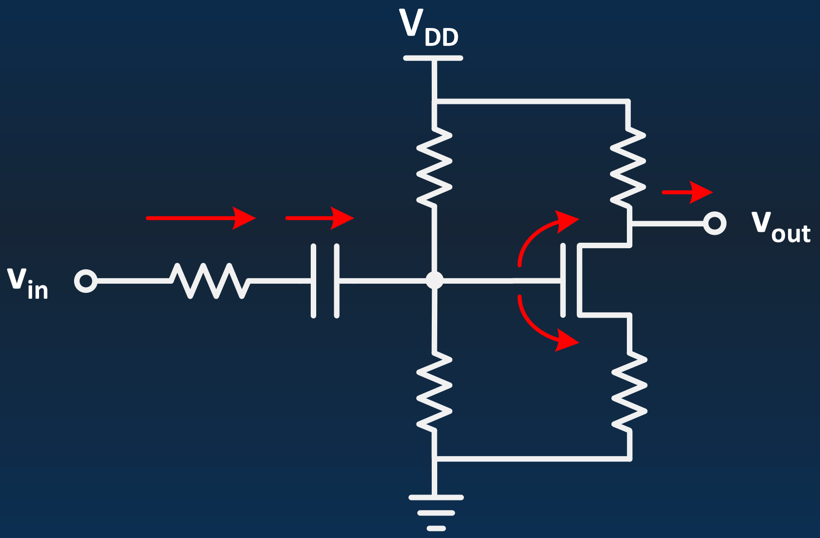
IFT in Analog Designs

Different from digital

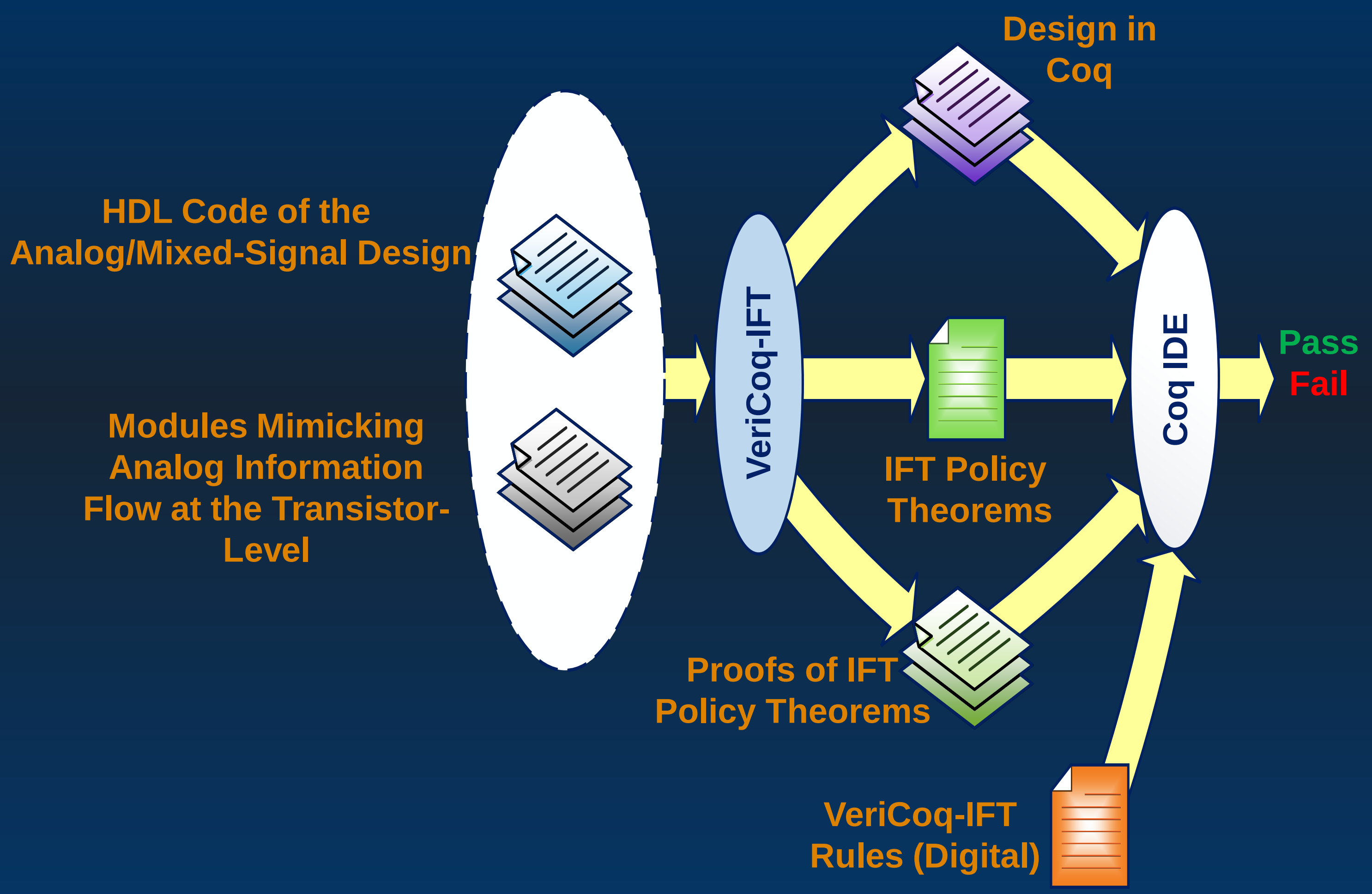
- Information carried through current as well as voltage
- Transistors used in various configurations
- Bulk terminal voltage manipulation can leak information
- Capacitors, resistors, and inductors should also be considered



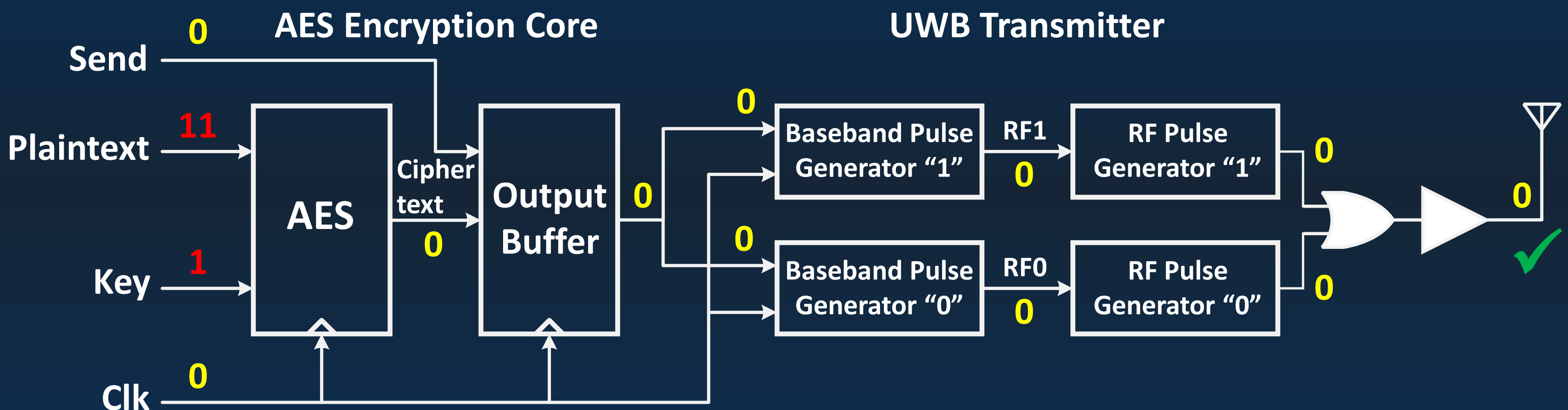
Transistor Level IFT Example



Analog Enabled VeriCoq-IFT (DATE'17)

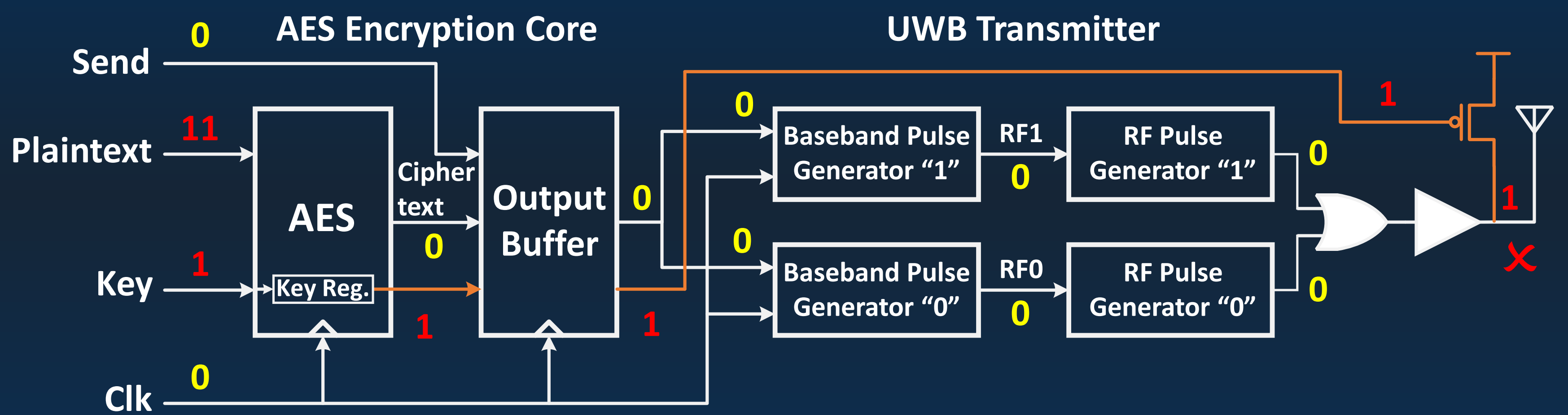


Genuine UWB Transmitter



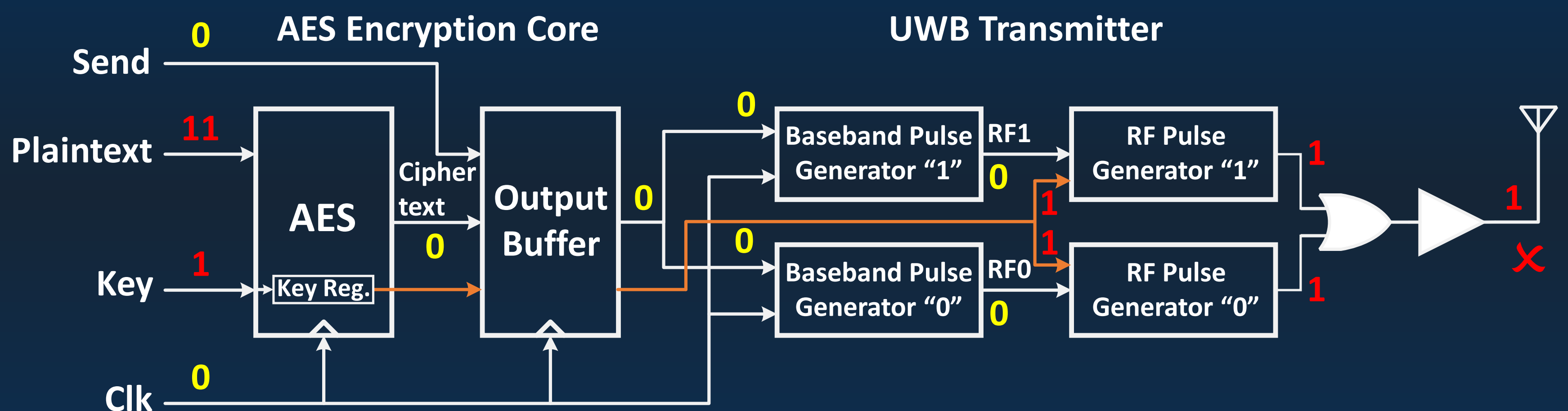
- Numbers represent sensitivity levels
- Proof of security theorem passes in Coq!

UWB Transmitter – Carrier Power Trojan



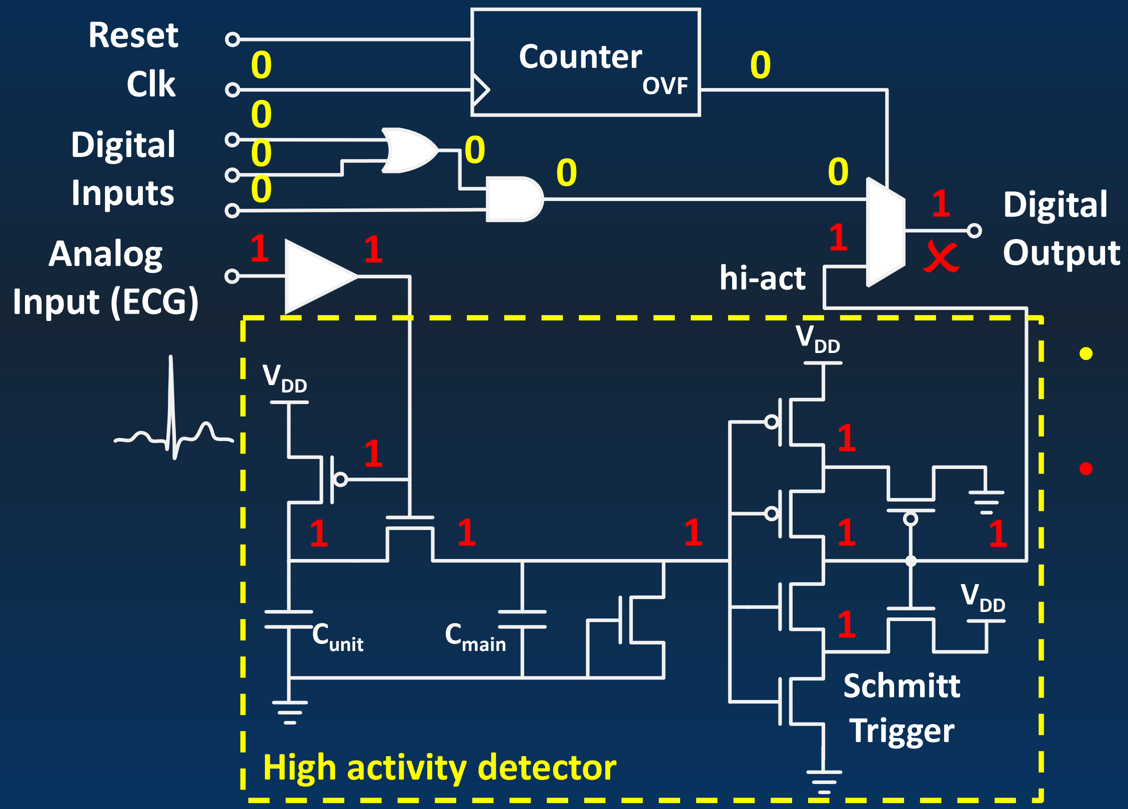
- Numbers represent sensitivity levels
- Proof of security theorem fails!

UWB Transmitter – Carrier Freq. Trojan



- Numbers represent sensitivity levels
- Proof of security theorem fails!

Analog to Digital Information Leakage



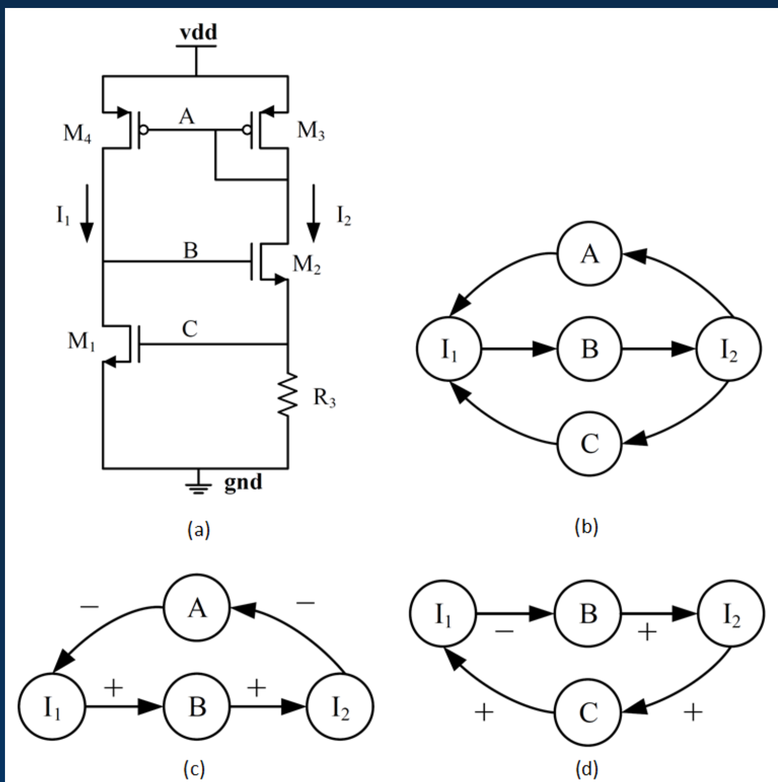
- Numbers represent sensitivity levels
- Proof of security theorem fails!

Homotopy Methods

- Has been long used for verification purposes
  - Define feedback loops
  - Annotate dependency signs
  - Determine positive feedback loops (even number of negative dependencies)
  - Apply continuation method (insert sources in the loop)
  - Sweep source and obtain output characteristics in order to determine undesired states

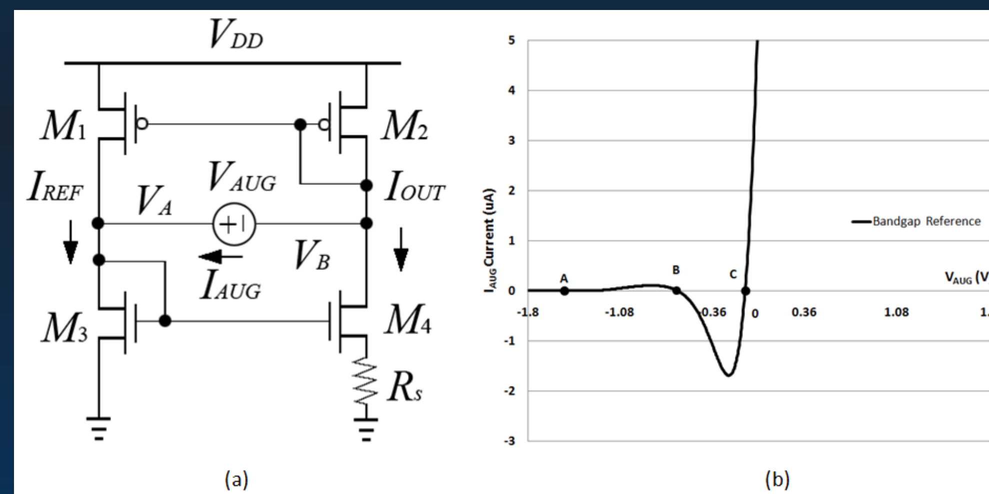
Homotopy Methods (2)

$I_1 \to B \to I_2 \to A \to I_1$



Vt reference circuit (ISCAS'14)

Continuation method:
C is the desired op. point
(all transistors in saturation)



Constant gm reference circuit

References – Part I

[1] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in IEEE International Workshop on Hardware-Oriented Security and Trust, pp. 51–57, 2008.

[2] Y. Jin and Y. Makris, "Hardware Trojans in wireless cryptographic ICs," IEEE Design and Test of Computers, vol. 27, pp. 26–35, 2010.

[3] Y. Liu, K. Huang, and Y. Makris, "Hardware Trojan detection through golden chip-free statistical side channel fingerprinting," in Proceedings of the 51st Annual Design Automation Conference on Design Automation Conference, pp. 1–6, 2014.

[4] Y. Liu, Y. Jin, and Y. Makris, "Hardware Trojans in wireless cryptographic ICs: silicon demonstration & detection method evaluation," in International Conference on Computer-Aided Design (ICCAD), pp. 399–404, 2013.

[5] Y. Liu, Y. Jin, A. Nosratinia, and Y. Makris, "Silicon demonstration of hardware Trojan design and detection in wireless cryptographic ICs," IEEE Transactions on VLSI, vol. 25, no. 4, pp.1506-1519, 2017.

[6] Y. Jin, D. Maliuk, and Y. Makris, "Post-deployment trust evaluation in wireless cryptographic ICs," in Design, Automation & Test in Europe Conference & Exhibition (DATE), 2012, pp. 965–970, 2012.

[7] Y. Liu, G. Volanis, K. Huang, and Y. Makris, "Concurrent hardware Trojan detection in wireless cryptographic ICs," in IEEE International Test Conference, pp. 1–8, 2015.

[8] D. Maliuk and Y. Makris, "An experimentation platform for on-chip integration of analog neural networks: A pathway to trusted and robust analog/RF ICs," IEEE Trans. Neural Networks and Learning Systems, vol. 26, no. 8, pp. 1721–1734, 2015.

References – Part I

[9] Y. Jin, N. Kupp, and Y. Makris, "Experiences in hardware Trojan design and implementation," in IEEE International Workshop on Hardware-Oriented Security and Trust, pp. 50–57, 2009.

[10] Y. Jin, M. Maniatakos, and Y. Makris, "Exposing vulnerabilities of untrusted computing platforms," in IEEE International Conference on Computer Design (ICCD), pp. 131–134, 2012.

[11] E. Love, Y. Jin, and Y. Makris, "Proof-carrying hardware intellectual property: A pathway to trusted module acquisition," IEEE Transactions on Information Forensics and Security, vol. 7, no. 1, pp. 25–40, 2012.

[12] E. Love, Y. Jin, and Y. Makris, "Enhancing security via provably trustworthy hardware intellectual property," in Proceedings of the 2011 IEEE Int. Symposium on Hardware-Oriented Security and Trust (HOST), pp. 12–17, 2011.

[13] Y. Jin, B. Yang, and Y. Makris, "Cycle-accurate information assurance by proof-carrying based signal sensitivity tracing," in IEEE Int. Symposium on Hardware-Oriented Security and Trust (HOST), pp. 99–106, 2013.

[14] Y. Jin and Y. Makris, "Proof carrying-based information flow tracking for data secrecy protection and hardware trust," in IEEE VLSI Test Symposium (VTS), pp. 252–257, 2012.

[15] Y. Jin and Y. Makris, "A proof-carrying based framework for trusted microprocessor IP," in Int. Conf. on Computer-Aided Design (ICCAD), pp. 824–829, 2013.

[16] M.-M. Bidmeshki, A. Antonopoulos, and Y. Makris, "Information flow tracking in analog/mixed- signal designs through proof-carrying hardware IP," in Design, Automation and Test in Europe (DATE), 2017 (to appear).

[17] M.-M. Bidmeshki and Y. Makris, "Toward automatic proof generation for information flow policies in third-party hardware IP," in IEEE Int. Symposium on Hardware-Oriented Security and Trust (HOST), pp. 163–168, 2015.

References – Part I

[18] M.-M. Bidmeshki and Y. Makris, "VeriCoq: A Verilog-to-Coq converter for proof-carrying hardware automation," in Int. Symposium on Circuits and Systems (ISCAS), pp. 29–32, 2015.

[19] H. G. Stratigopoulos and Y. Makris, "Error moderation in low-cost machine-learning-based analog/RF testing," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 27, no. 2, pp. 339–351, 2008.

[20] D. Maliuk, H. Stratigopoulos, H. Huang, and Y. Makris, "Analog neural network design for RF built-in self-test," in Proceedings of the IEEE International Test Conference (ITC), pp. 23.2.1–23.2.10, 2010.

[21] Y. Lu, K. S. Subramani, H. Huang, N. K. K. Huang, and Y. Makris, "A comparative study of one-shot statistical calibration methods for analog / RF ics," in IEEE International Test Conference, pp. 1–10, 2015.

[22] G. Volanis, D. Maliuk, Y. Lu, K. S. Subramani, A. Antonopoulos, and Y. Makris, "On-die learning--based self-calibration of analog/RF ICs," in IEEE VLSI Test Symposium, pp. 1–6, 2016.

[23] X. Cao, Q. Wang, R. L. Geiger, and D. J. Chen, "A hardware Trojan embedded in the Inverse Widlar reference generator," in IEEE 58th International Midwest Symposium on Circuits and Systems, pp. 1–4, 2015.

[24] Q. Wang, R. L. Geiger, and D. J. Chen, "Challenges and opportunities for determining presence of multiple equilibrium points with circuit simulators," in IEEE 57th International Midwest Symposium on Circuits and Systems, pp. 406–409, 2014.

[25] C. Cai and D. Chen, "Performance enhancement induced Trojan states in op-amps, their detection and removal," in IEEE International Symposium on Circuits and Systems, pp. 3020–3023, 2015.

References – Part I

[26] Q. Wang and R. L. Geiger, "Temperature signatures for performance assessment of circuits with undesired equilibrium states," Electron. Lett., vol. 51, no. 22, pp. 1756–1758, 2015.

[27] Q. Wang, R. L. Geiger, and D. Chen, "Hardware Trojans embedded in the dynamic operation of analog and mixed-signal circuits," in National Aerospace and Electronics Conference, pp. 155–158, 2015.

[28] N. Beringuier-Boher, M. Lacruche, D. El-Baze, J.-M. Dutertre, J.-B. Rigaud, and P. Maurine, "Body Biasing Injection Attacks in Practice," in Proceedings of the Third Workshop on Cryptography and Security in Computing Systems, pp. 49–54, 2016.

[29] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2 : Analog Malicious Hardware," in IEEE Symposium on Security and Privacy, pp. 18-37, 2016.

[30] N. Beringuier-Boher, K. Gomina, D. Hely, J. B. Rigaud, V. Beroulle, A. Tria, J. Damiens, P. Gendrier, and P. Candelier, "Voltage Glitch Attacks on Mixed-Signal Systems," in 17th Euromicro Conference onDigital System Design, pp. 379–386, 2014.

[31] A. Singhee and R. A. Rutenbar, "Statistical Blockade: A Novel Method for Very Fast Monte Carlo Simulation of Rare Circuit Events, and its Application," 2007 Design, Automation & Test in Europe Conference & Exhibition, 2007, pp. 1-6.

[32] H. G. Stratigopoulos, S. Mir and A. Bounceur, "Evaluation of Analog/RF Test Measurements at the Design Stage," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 28, no. 4, pp. 582-590, 2009.

[33] A. Antonopoulos, Y. Makris, "Security and Trust in the Analog/Mixed-Signal/RF Domain: A Survey and a Perspective," IEEE European Test Symposium (ETS), 2017 (to appear).

References – Part I

[34] E. Love, Y. Jin, Y. Makris, "Proof-Carrying Hardware Intellectual Property: A Pathway to Trusted Module Acquisition,"Special Issue on Integrated Circuits and System Security of the IEEE Transactions on Information Forensics and Security (TIFS), vol. 7, no. 1, pp. 25-40, 2012

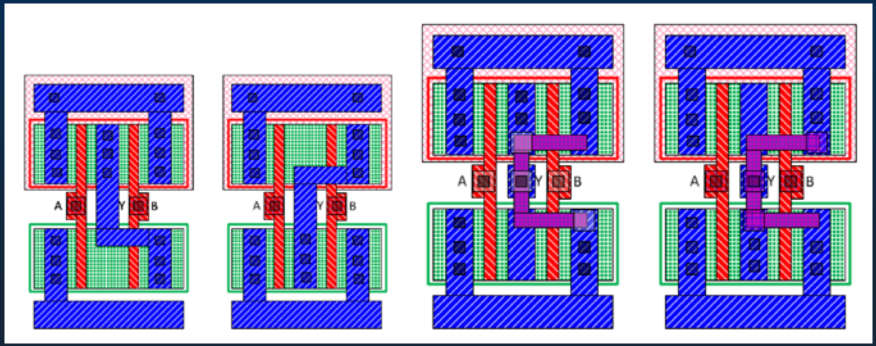
[35] Y. Jin, B. Yang, Y. Makris, "Cycle Accurate Information Assurance by Proof Carrying-Based Signal Sensitivity Tracing," Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 99-106, 2013

[36] M. Bidmeshki, Y. Makris, "Toward Automatic Proof Generation for Information Flow Policies in Third-Party Hardware IP," Proceedings of the IEEE Symposium on Hardware-Oriented Security and Trust (HOST), pp. 163-168, 2015

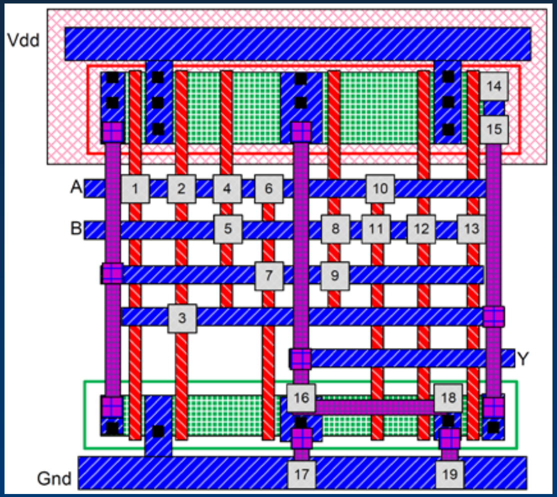
PART II:
Reverse Engineering and IP Theft

IC Camouflaging (CCS'13)

- Transform the design into one that is identical to the original but much more difficult to reverse engineer

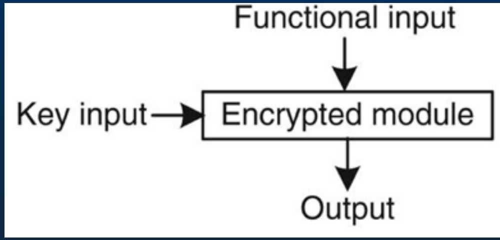


- Dummy contacts (XOR | NAND | NOR)

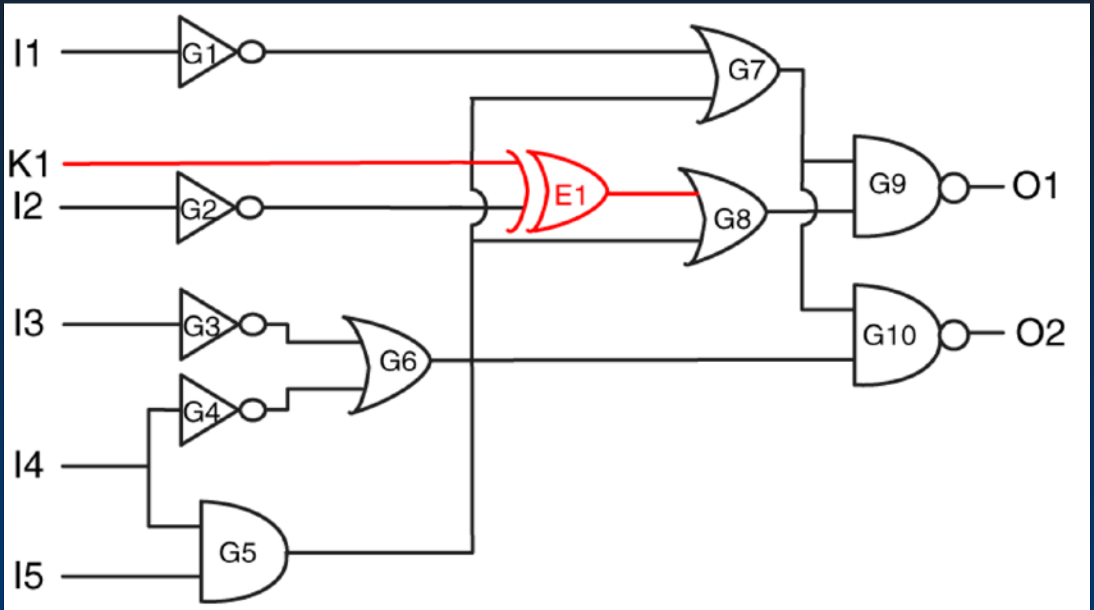


IC Logic Encryption (TCOMP'15)

- Encrypt logic by randomly inserting gates in the design



- Wrong keys corrupt the outputs



Limitations in the Analog Domain

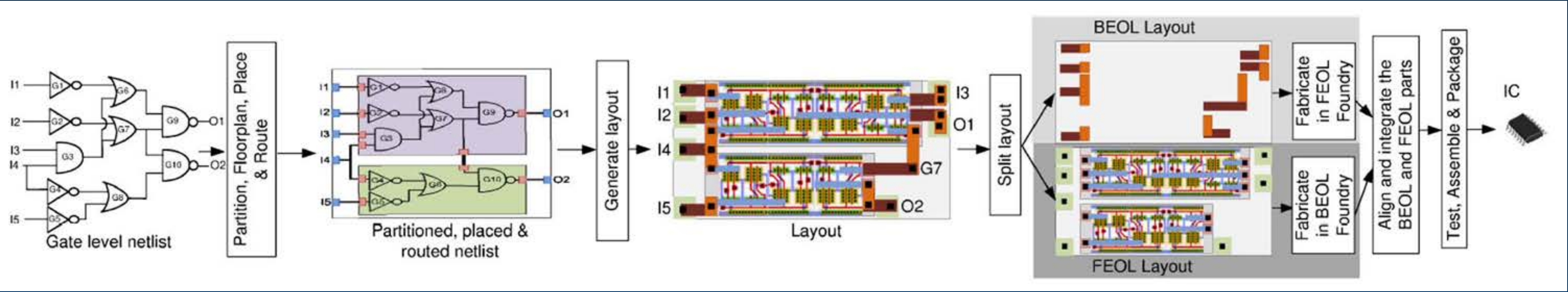
- Fewer components, layout additions will be detected by simple inspection
- Continuous values:
  - Design specifications will be shifted

[Protecting Analog Circuits with Parameter Biasing Obfuscation, HOST’17 poster]

Split Manufacturing

- Split design into front-end-of-line (untrusted foundry) and back-end-of-line (trusted foundry)
- Application on a power amplifier [Electronics'15]
- Top two metal layers were removed from front-end-of-line
  - Inductors and capacitors become invisible
  - Difficult to reverse engineer given the wide range of values and operating frequencies

[IEEE Proc.'14]



Layout Watermarking (ASIC/SOC'00)

- Parses the layout netlist
- Sorts transistors based on their type, width, shortest distance to input and output
- Uses the ordered outcome as a seed to generate the watermark through a PRNG
- Produced bitstream is embedded by using and odd (for '1') or even (for '0') number of fingers

Layout Watermarking (ASIC/SOC'00)

- Application in a two-stage Miller amplifier (0,25% area penalty)

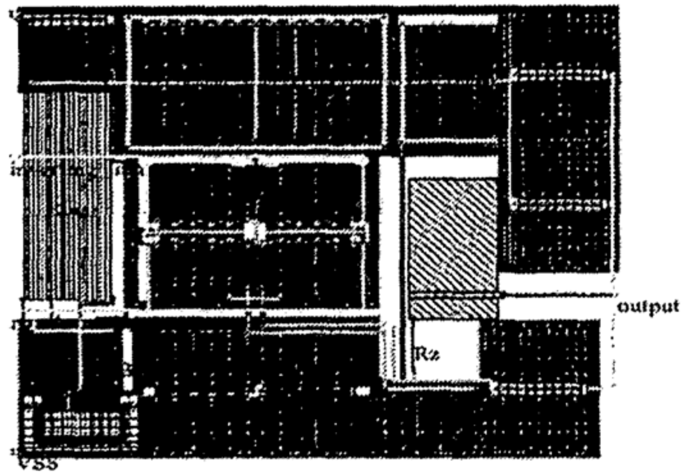


Figure 6. Unwatermarked operational amplifier.

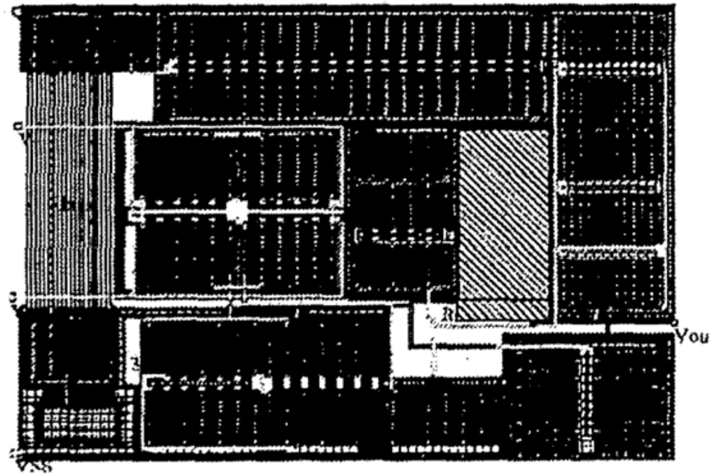


Figure 7. Watermarked operational amplifier.

References – Part II

[1] Y. Bi, J. S. Yuan, and Y. Jin, “Beyond the Interconnections: Split Manufacturing in RF Designs,” Electronics, vol. 4, no. 3, p. 541, 2015.

[2] J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, “Security Analysis of Integrated Circuit Camouflaging,” in Proceedings of the ACM SIGSAC Conference on Computer Communications Security, pp. 709–720, 2013.

[3] J. Rajendran, H. Zhang, C. Zhang, G. S. Rose, Y. Pino, O. Sinanoglu, and R. Karri, “Fault Analysis-Based Logic Encryption,” IEEE Trans. Comput., vol. 64, no. 2, pp. 410–424, 2015.

[4] R. D. Newbould, D. L. Irby, J. D. Carothers, J. J. Rodriguez, and W. T. Holman, “Mixed signal design watermarking for IP protection,” in Southwest Symposium on Mixed-Signal Design, pp. 110–115, 2001.

[5] Y. Bi, JS. Yuan, Y. Jin, “Split manufacturing in radio-frequency designs,” In Proceedings of the international conference on security and management (SAM), 2015.

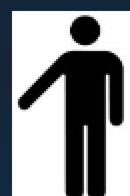
PART III:
Counterfeit Integrated Circuits

Do You Trust Your IC Supplier?

- Recycled ICs:
  Used ICs provided by untrustworthy suppliers, which are “scavenged” from used or defective circuit boards

Used or defective circuit boards

Malicious supplier



Recycled IC

Electronic supply chain

Danger !!!

- Other Counterfeit IC Types:
  Stolen/Reverse-Engineered IP, Over-production, Fake Parts

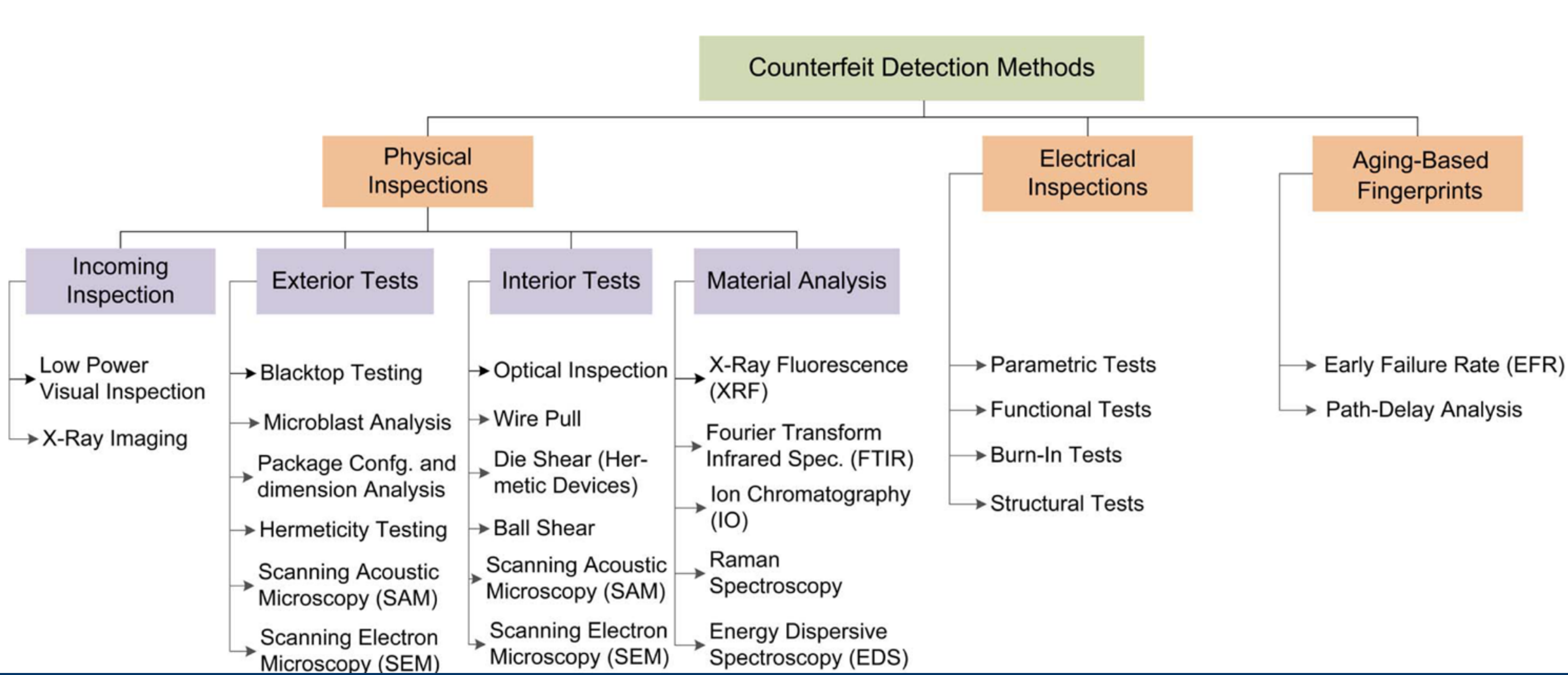
IC Recycling

Problem Growing in Magnitude

Top-5 most counterfeited semiconductors in 2011 [IEEE Proc.'14]		
Ranking	Component Type	% of reported incidents
1	Analog IC	25.2
2	Microprocessor IC	13.4
3	Memory IC	13.1
4	Programmable logic IC	8.3
5	Transistor	7.6

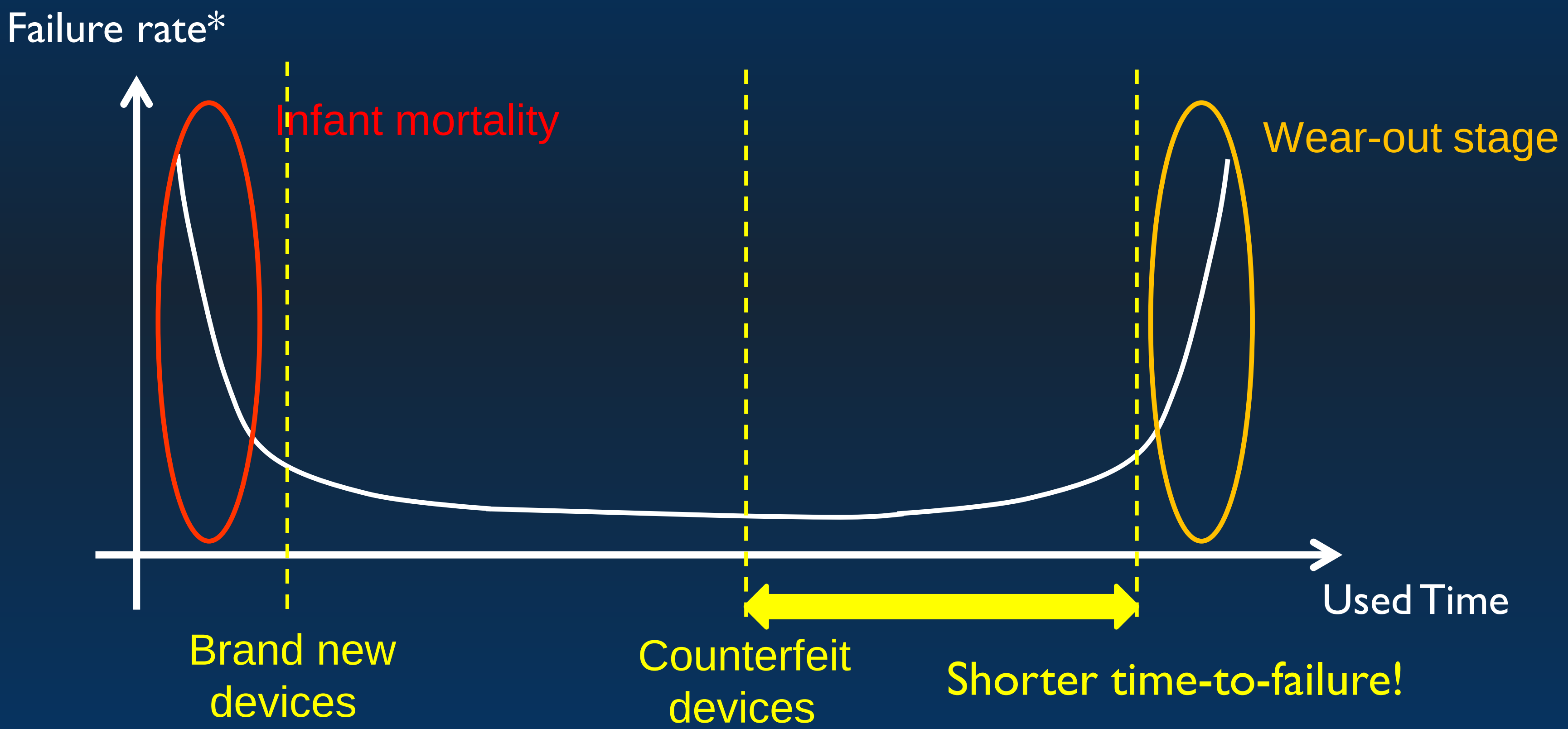
Counterfeit Detection Methods

[IEEE Proc.'14]



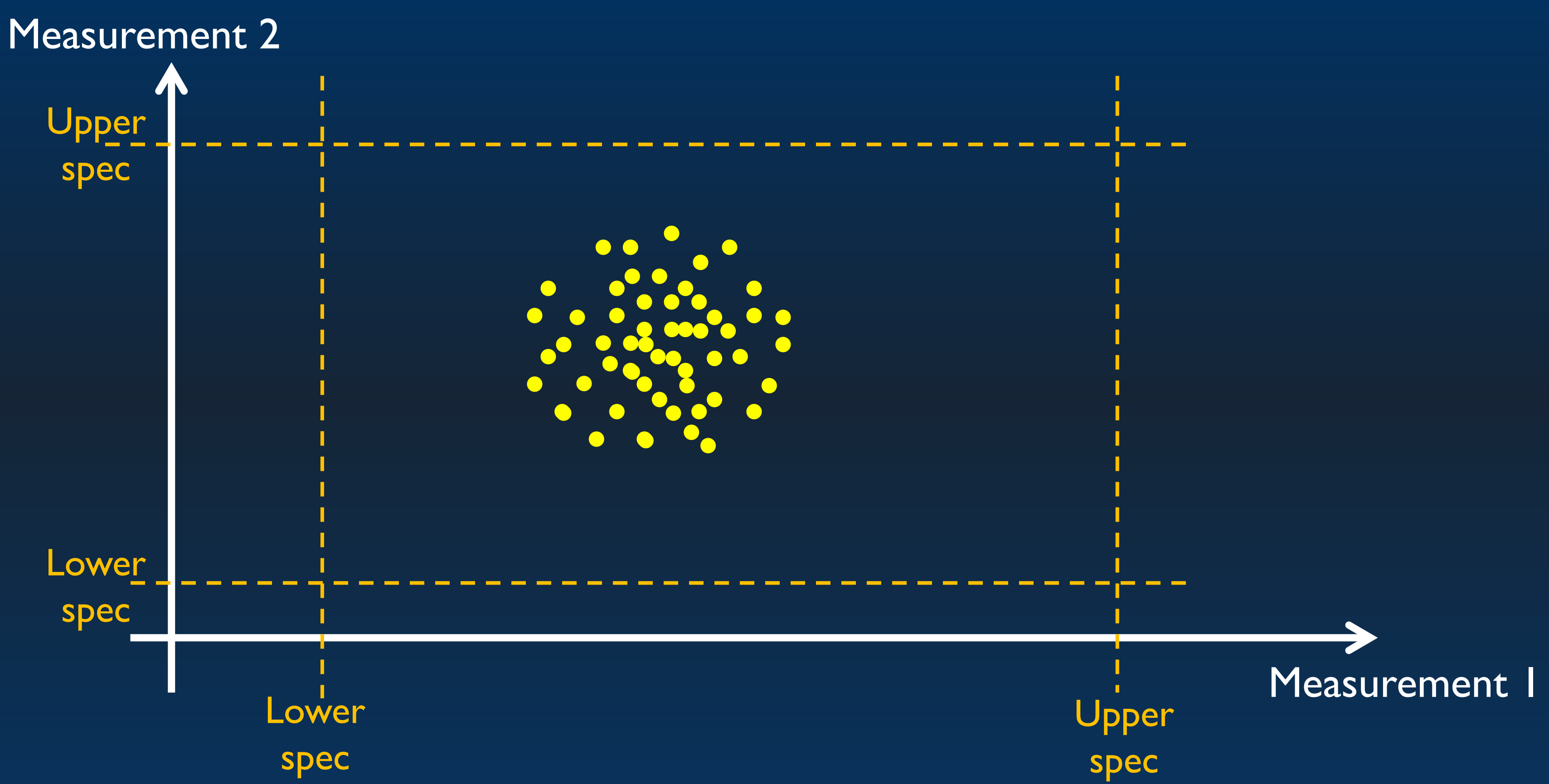
Problems of Recycled ICs

- Aging phenomena: NBTI, HCI, TDDB, Electromigration...
- Recycled ICs may work initially, but …

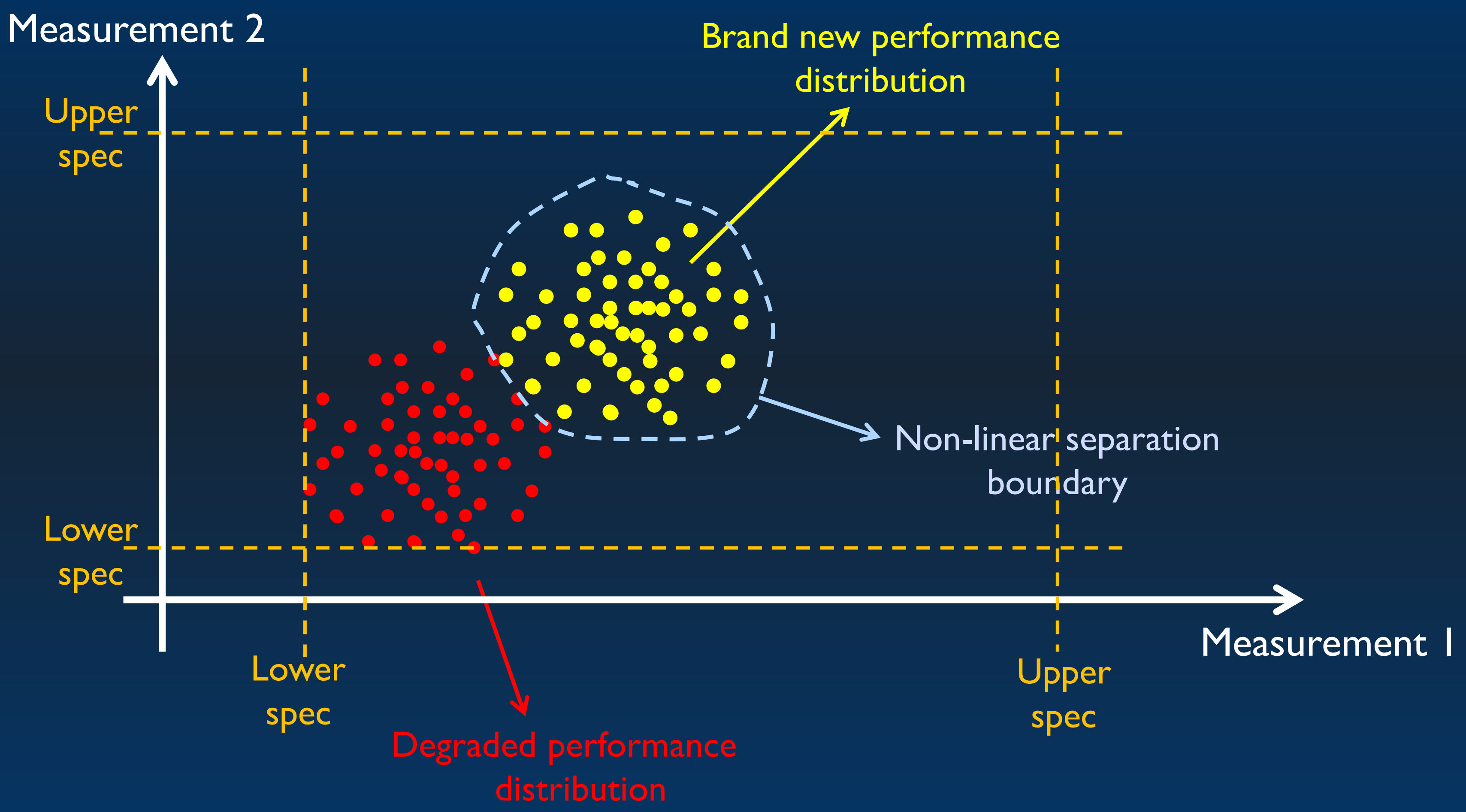


*Failure rate defined as the probability that a device will fail in the time interval between t and t+δt given that it has survived until time t
(Carulli and Anderson, "Test Connections – Tying Applications to Process", ITC'05)

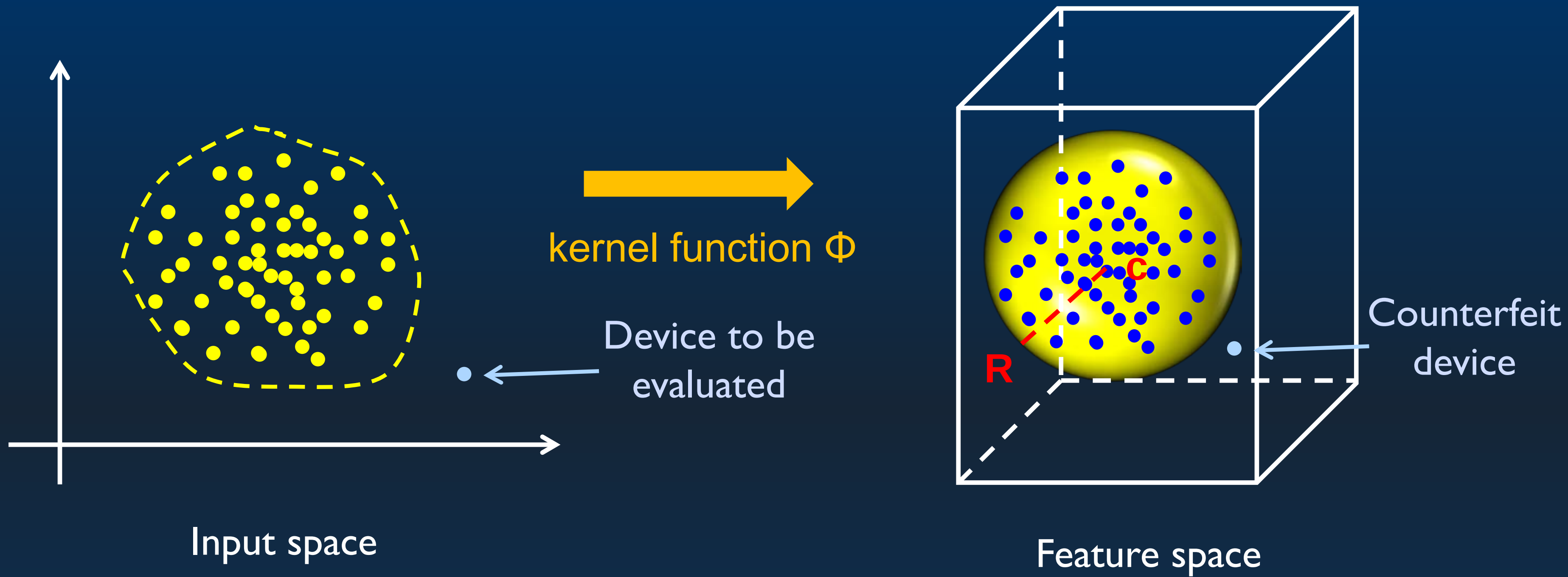
Idea: Examine Performance Degradation



Idea: Examine Performance Degradation



One-Class Support Vector Machine (SVM)

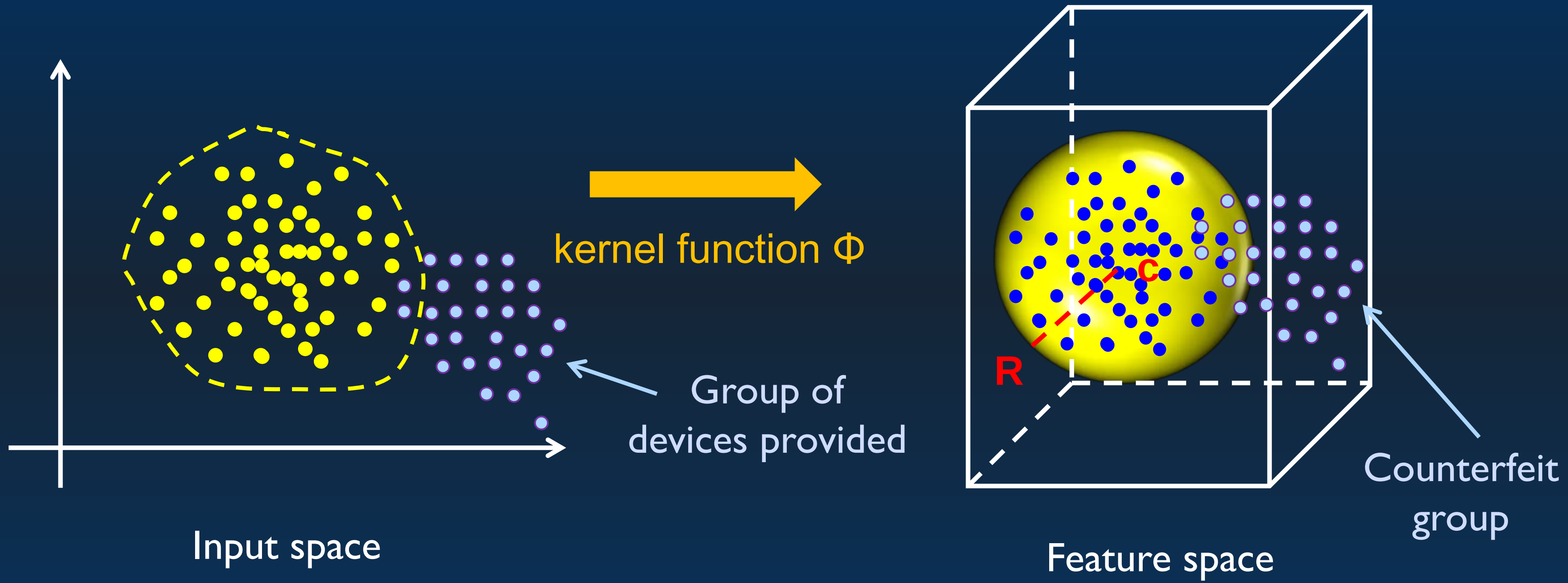


We use radial basis kernel function in this work:

$$k(x_1, x_2) = \exp(-\gamma |x_1 - x_2|^2)$$

- Train SVM to classify single chip as new vs. used

One-Class SVM: Group Classification



➢ Majority vote for group classification

- Train SVM to classify group of chips as new vs. used

Case Study

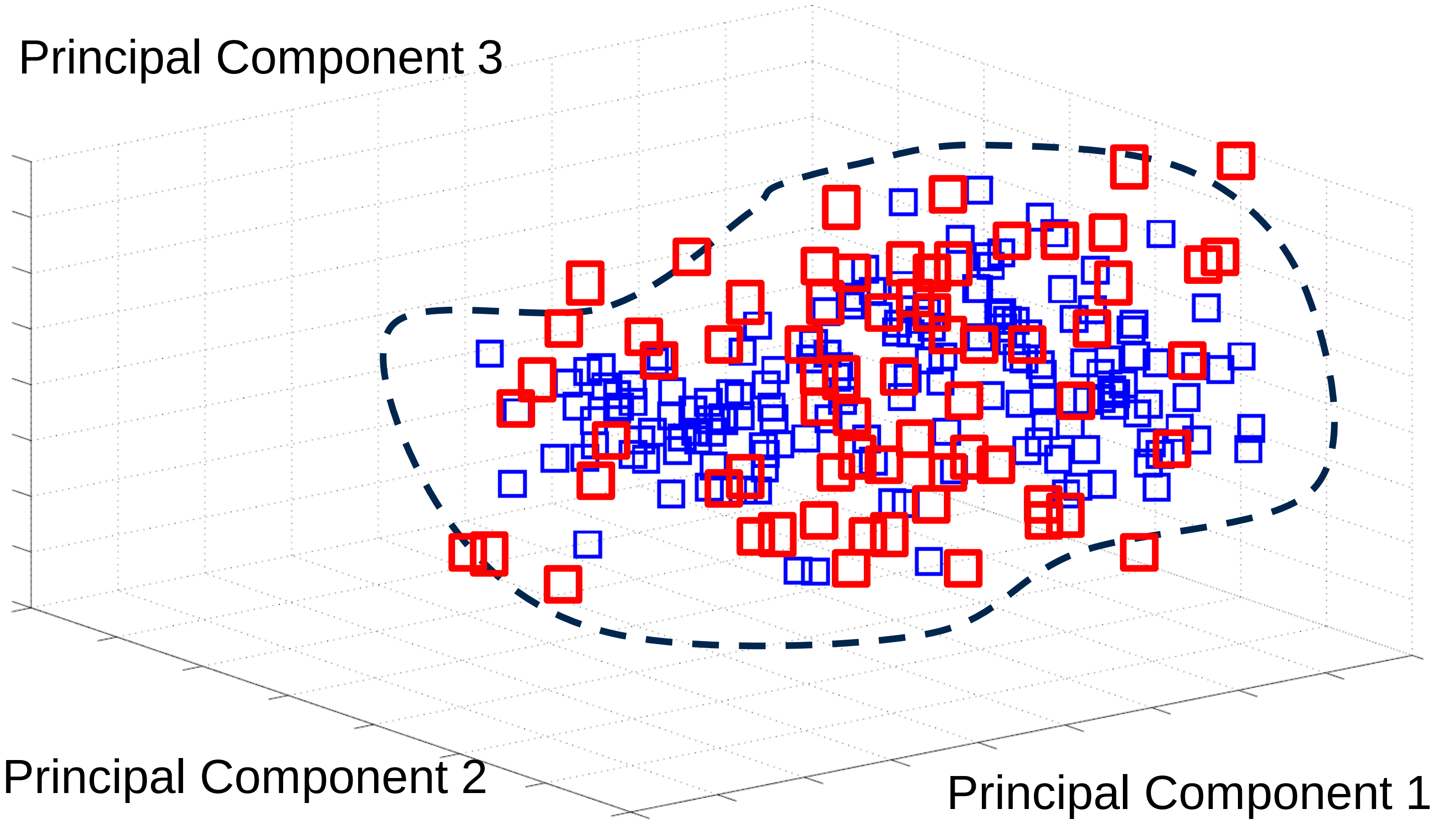
- Chip Population & Measurements:
  - ⇨ 313 devices (TI processor) from different lots in the fab
  - ⇨ 49 parametric measurements for each device (F*max* and/or V*min* of various blocks)
  - ⇨ 5 time read-points during burn-in failure analysis $t = t_0, t_1, t_2, t_3, t_4$

- Objective:
  Train an SVM to classify a chip (or a batch of chips) as brand-new or used

- Note:
  Only brand-new devices used for training (1-class SVM)

Training & Validation of Classifier

- Data from 157 out of 313 devices at t_0 used for training
- Classify remaining devices at t_0, one at a time



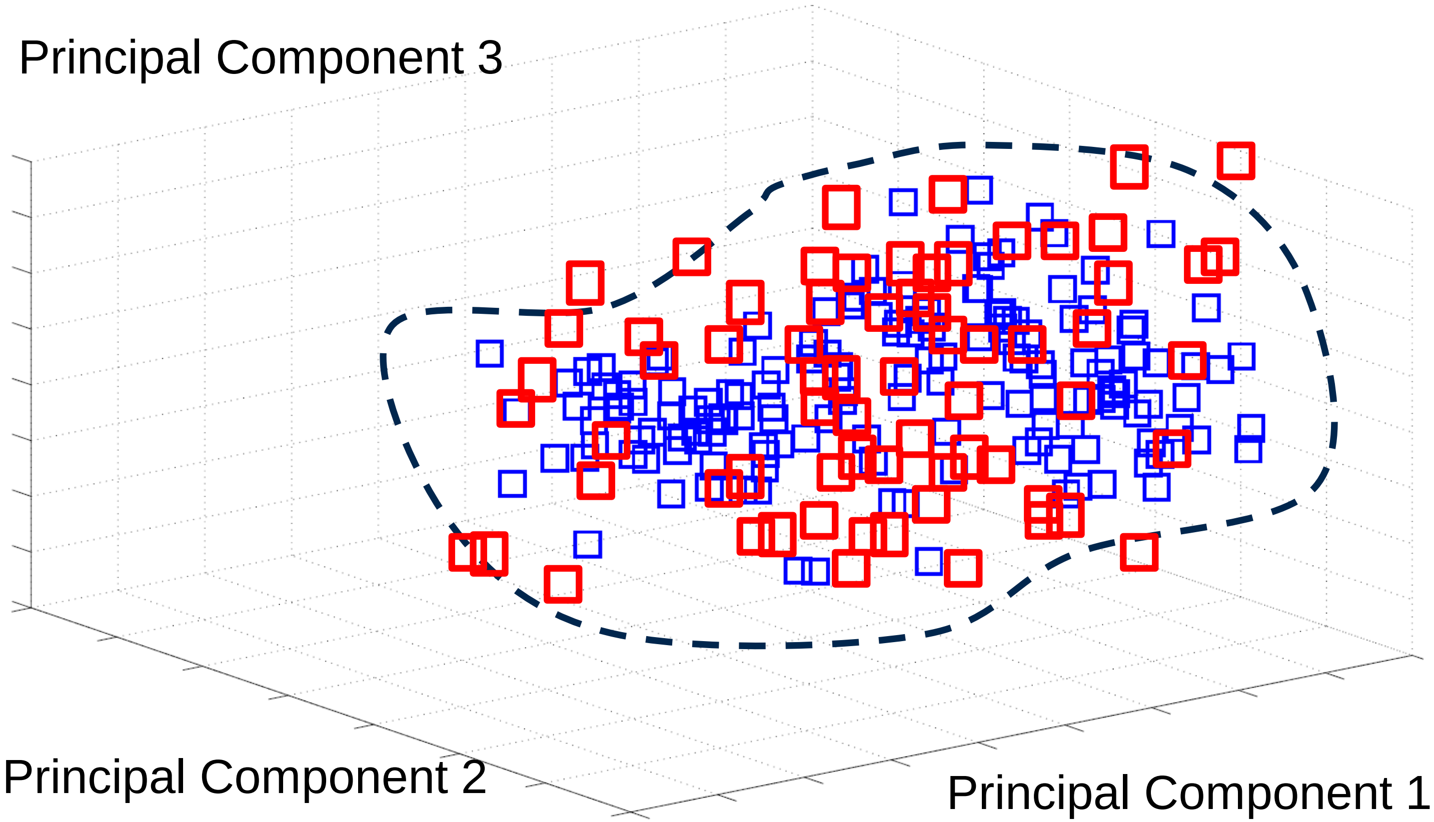
Correct Classification Rate

Group	Results
t_0	82.2%

- Note: Results averaged over 10 cross-validation runs

Training & Validation of Classifier

- Data from 157 out of 313 devices at t_0 used for training
- Performances gradually shift as device ages to $t=t_1$



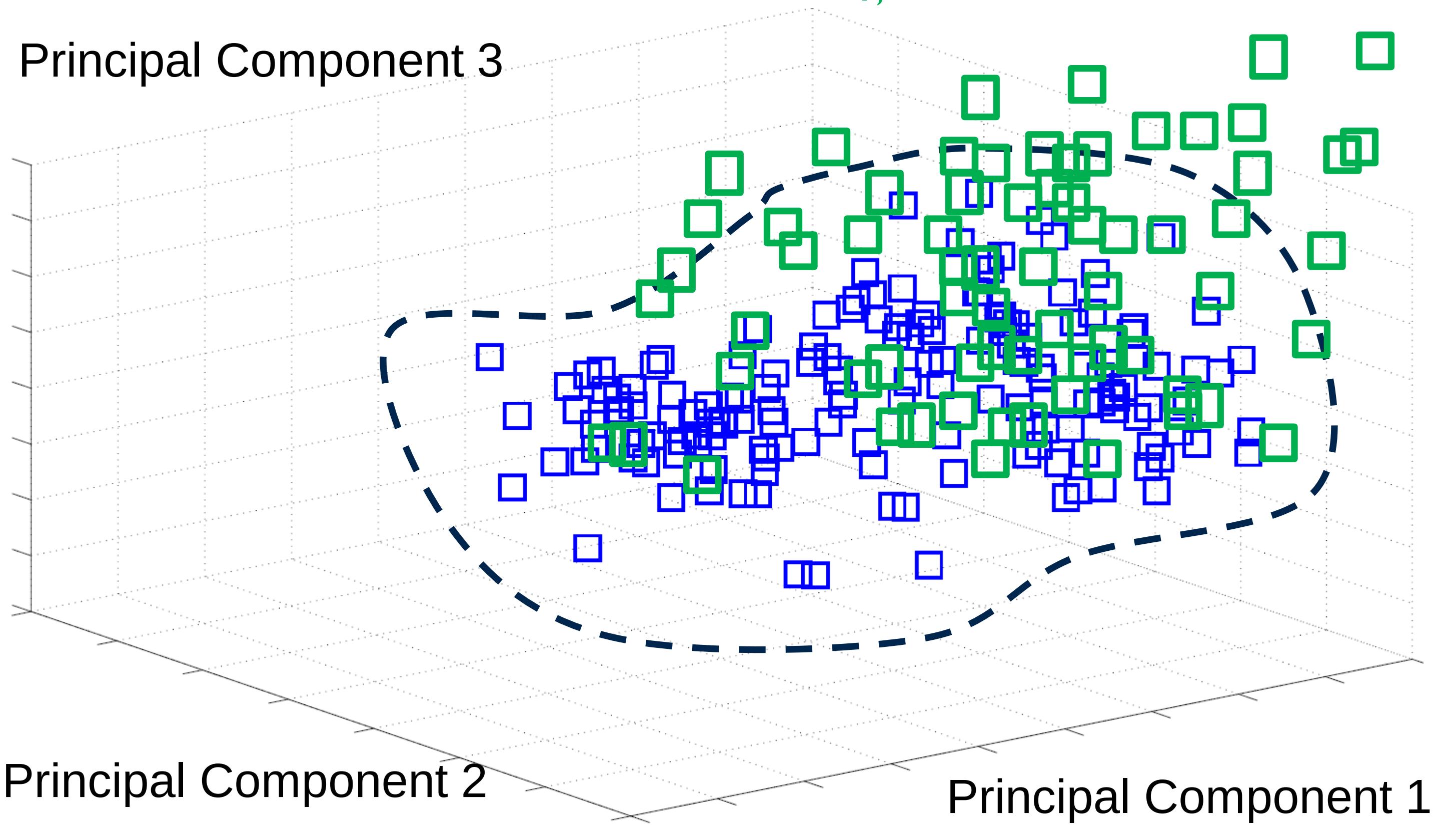
Correct Classification Rate

Group	Results
t_0	82.2%

- **Note:** Results averaged over 10 cross-validation runs

Training & Validation of Classifier

- Data from 157 out of 313 devices at t_0 used for training
- Classify validation set at $t=t_1$, one at a time



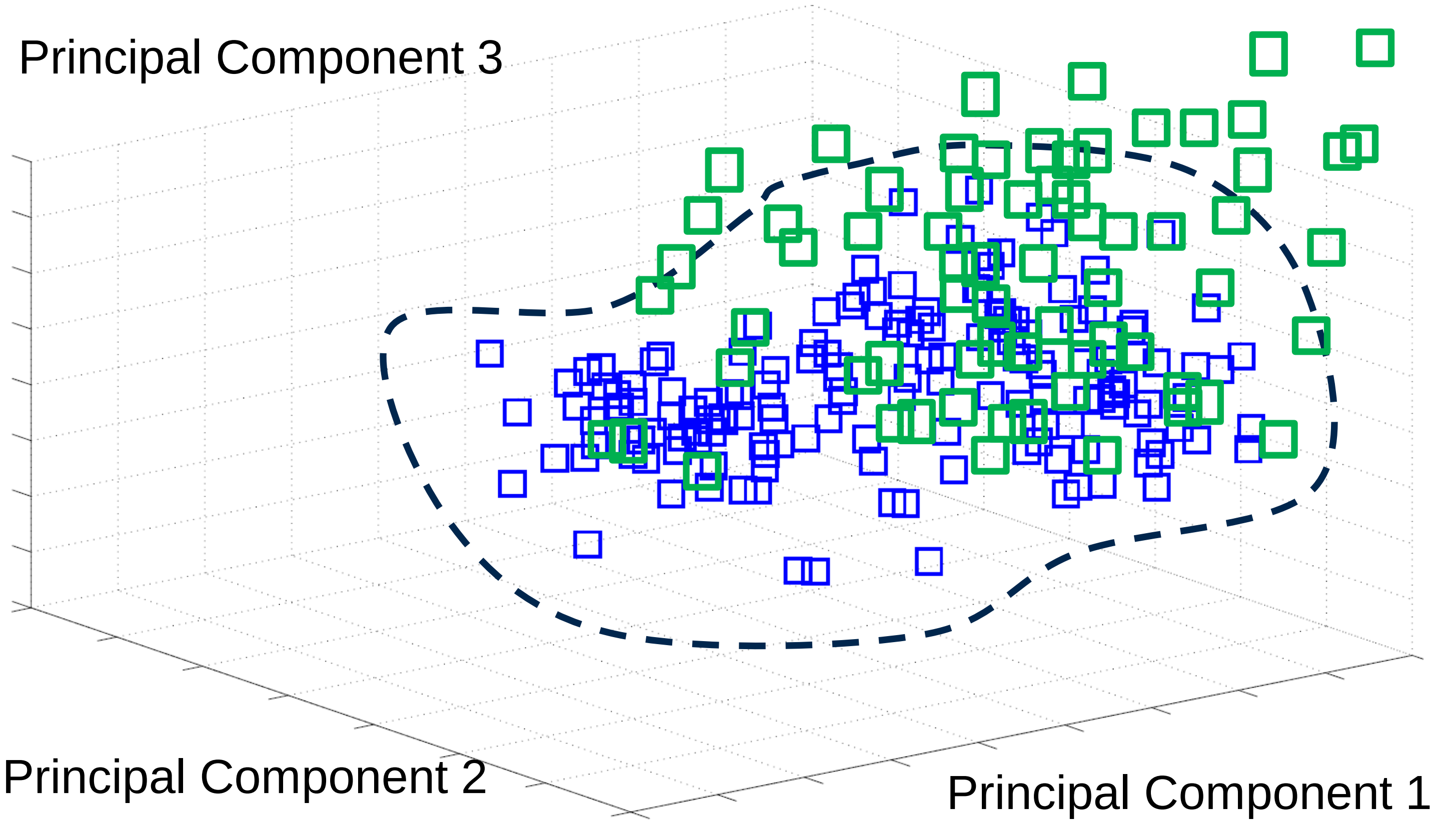
Correct Classification Rate

Group	Results
t_0	82.2%
t_1	69.2%

- **Note:** Results averaged over 10 cross-validation runs

Training & Validation of Classifier

- Data from 157 out of 313 devices at t_0 used for training
- Performances shift as device ages to $t=t_4$

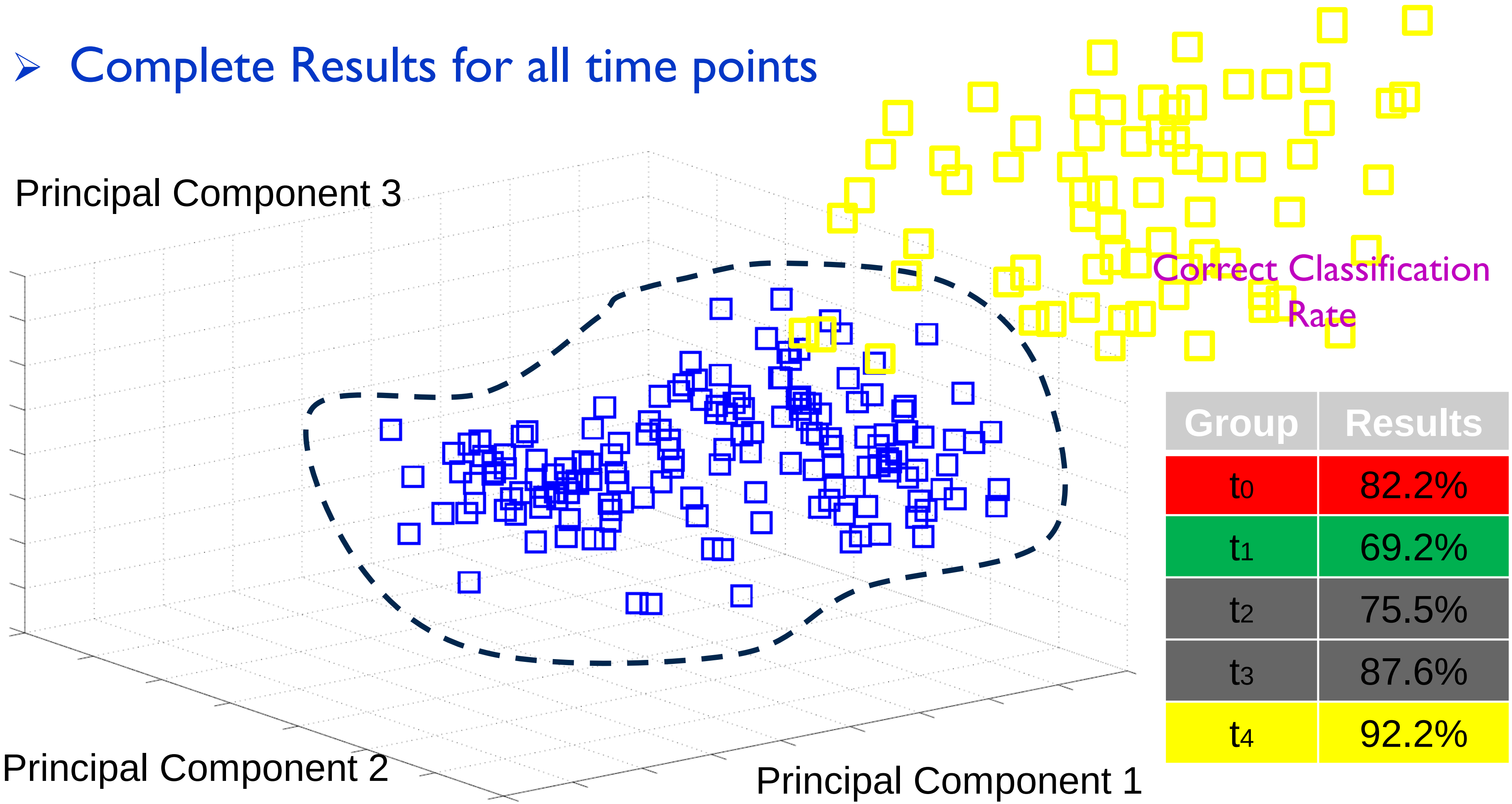


Correct Classification Rate

Group	Results
t_0	82.2%
t_1	69.2%

Training & Validation of Classifier

- Complete Results for all time points



Group	Results
t_0	82.2%
t_1	69.2%
t_2	75.5%
t_3	87.6%
t_4	92.2%

- Note: Results averaged over 10 cross-validation runs

Results for Various Group Sizes

Group/ Validation size	t_0	t_1	t_2	t_3	t_4
156	100%	100%	100%	100%	100%
80	100%	100%	100%	100%	100%
20	100%	96.2%	99.4%	100%	100%
10	100%	95.6%	98.4%	100%	100%
1	82.2%	69.2%	75.5%	87.6%	92.2%

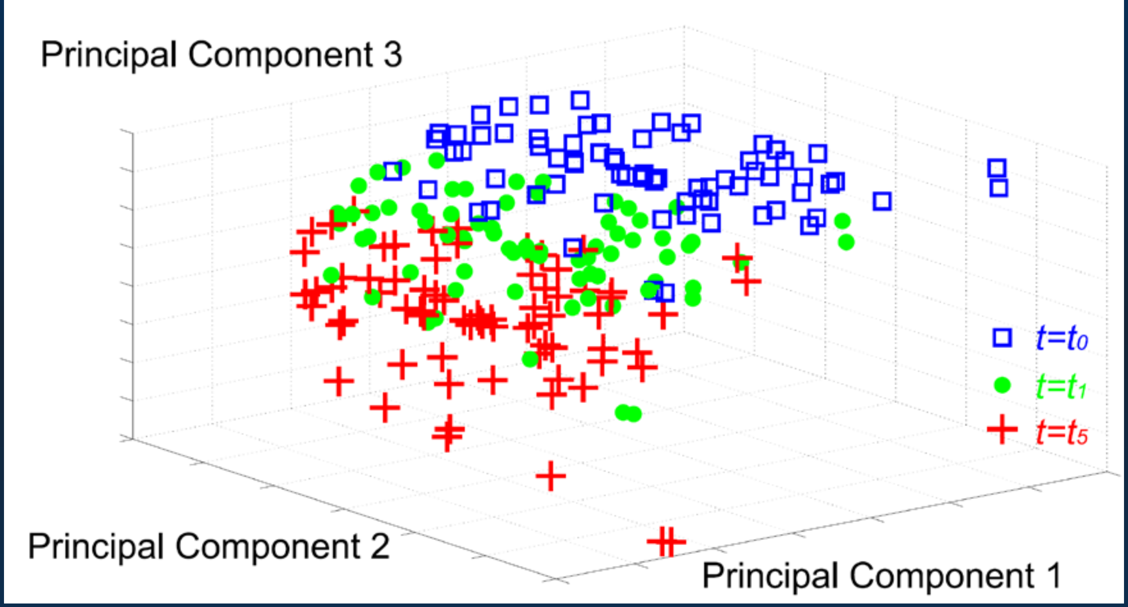
- Note: Results averaged over 10 cross-validation runs

Analog IC Case Study

- Analog Chip
  - Fully differential cascode amplifier in 45nm CMOS
  - 100 MC simulations
  - 4 parametric measurements (gain, phase margin, BW, I_{ddq})
  - NBTI and HCI aging effects
  - $[t_0, t_1, t_2, t_3, t_4, t_5]$ = [0, 1 month, 6 months, 1 year, 5 years, 10 years]

Analog IC Case Study

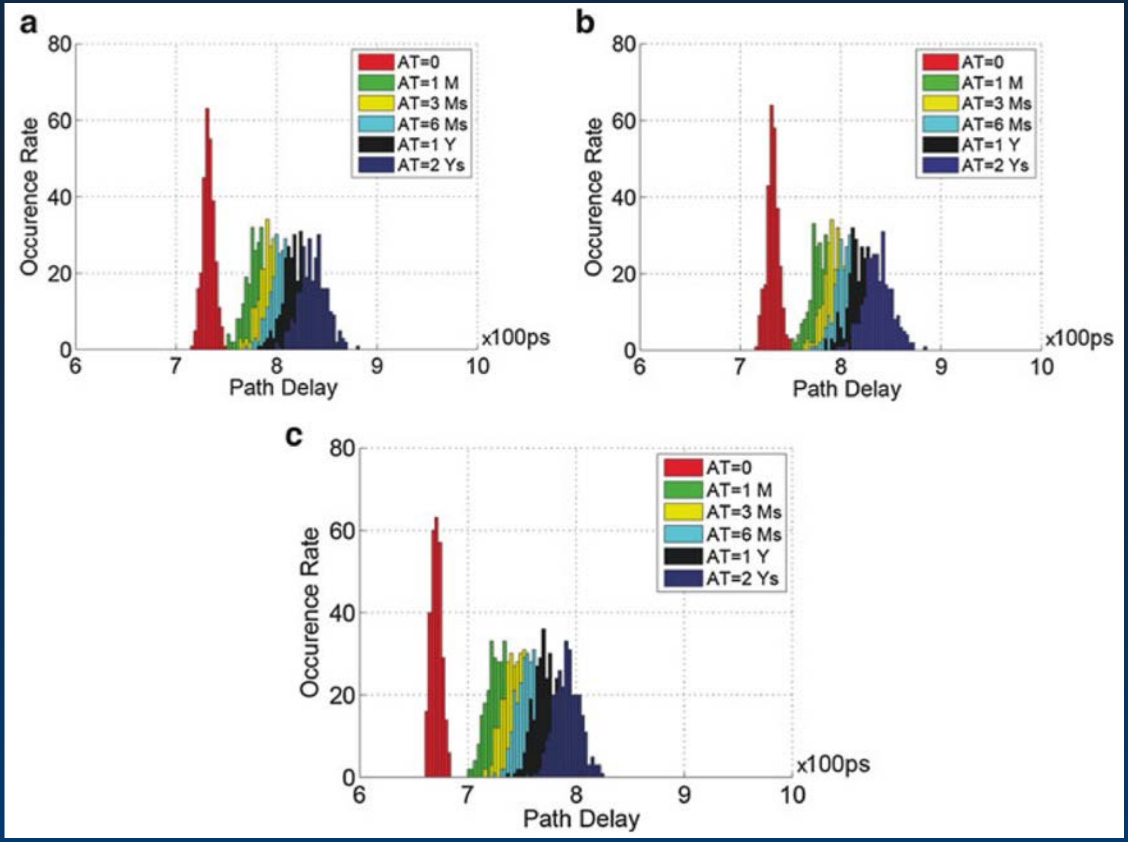
- Populations can be distinguished [TCAD'15]



Group\Validation size	t_0	t_1	t_2	t_3	t_4	t_5
50	100%	100%	100%	100%	100%	100%
20	100%	100%	100%	100%	100%	100%
10	100%	100%	100%	100%	100%	100%
1	100%	90%	100%	100%	100%	100%

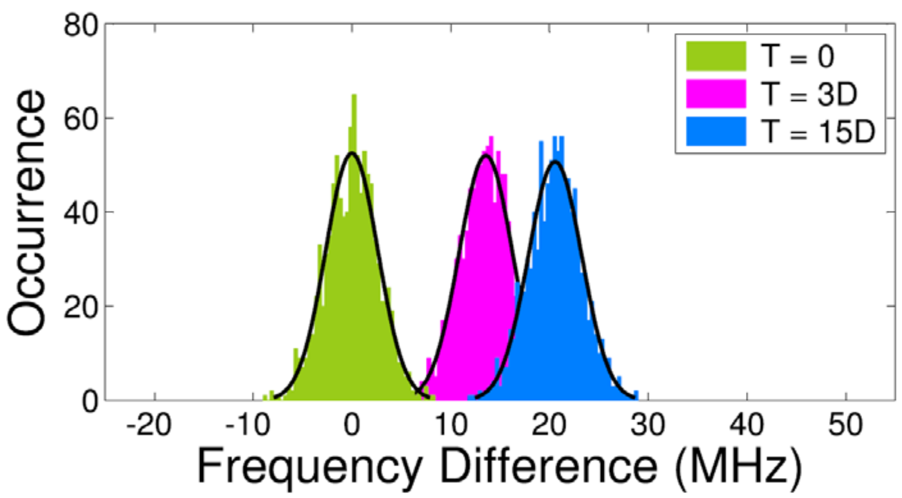
Other Aging Detection Methods

- Path delay at different aging times reveals recycled digital ICs [Springer'16]

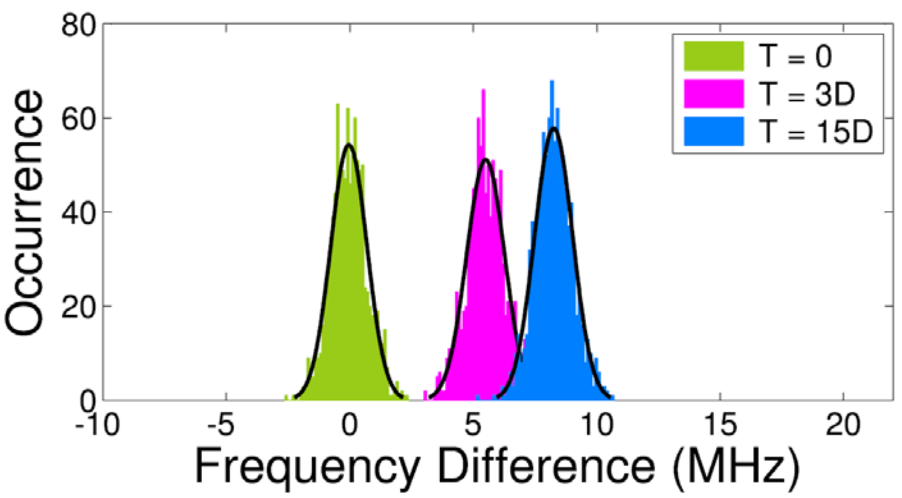


Other Aging Detection Methods

- On-chip ring oscillator sensor for detecting recycled ICs [TVLSI’16]
- Reference ring oscillator remains idle during stretch, sensor ring oscillator ages with IC usage



21-stage RO



51-stage RO

Physical Inspection

- Low power visual inspection [IEEE Proc.'14]

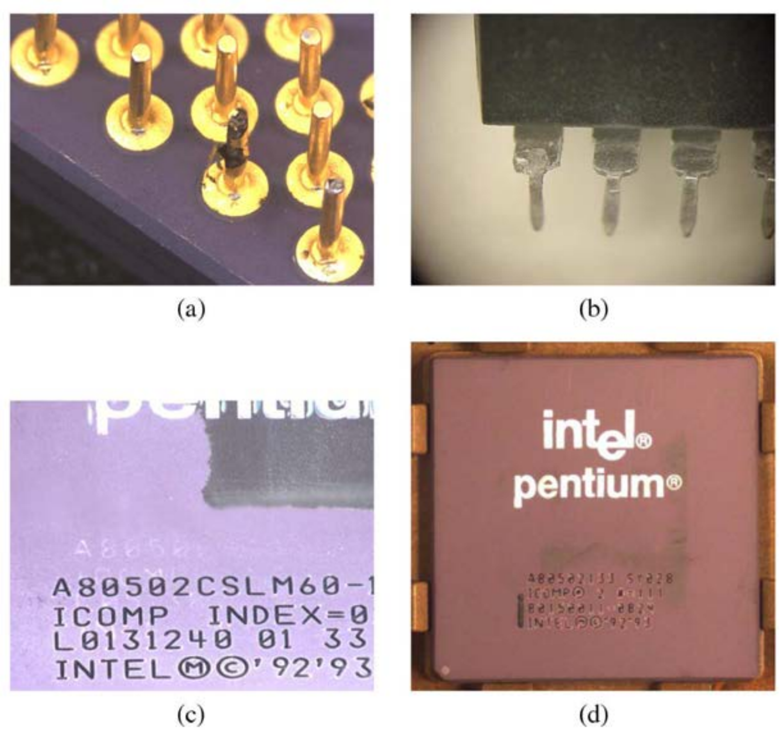


Fig. 5. *Counterfeit defects detected by LPVI (source: Honeywell). (a) Fake plating on leads. (b) Residual materials on leads. (c) Ghost marking on the package. (d) Heat sink mark on the package.*

Physical Inspection

- X-ray imaging [IEEE Proc.'14]

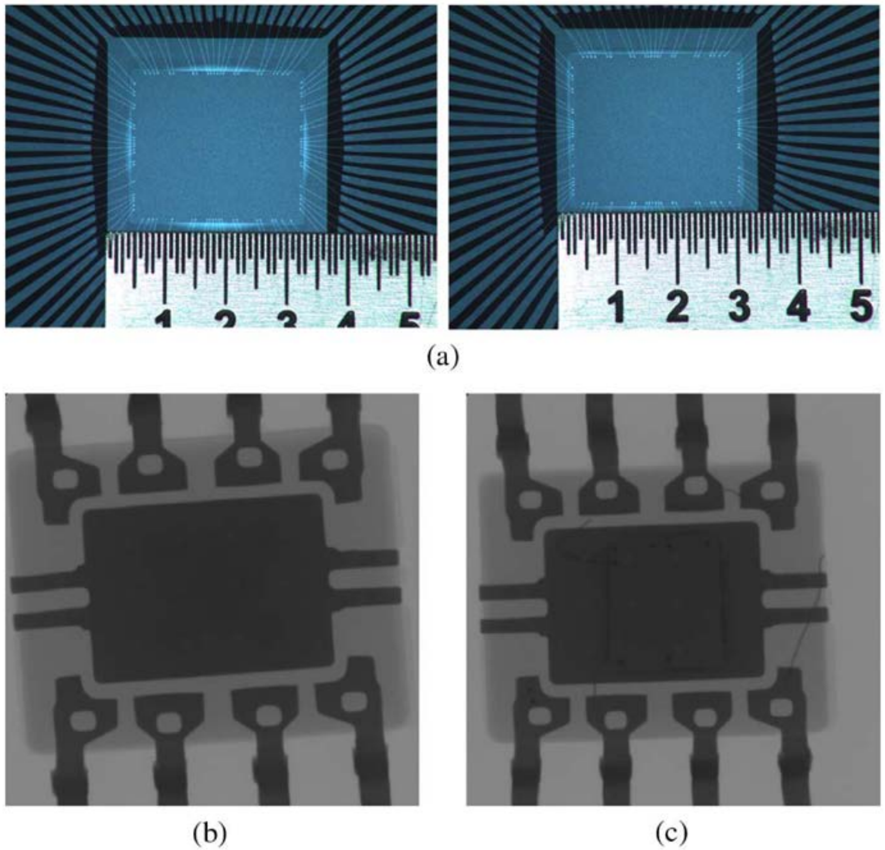
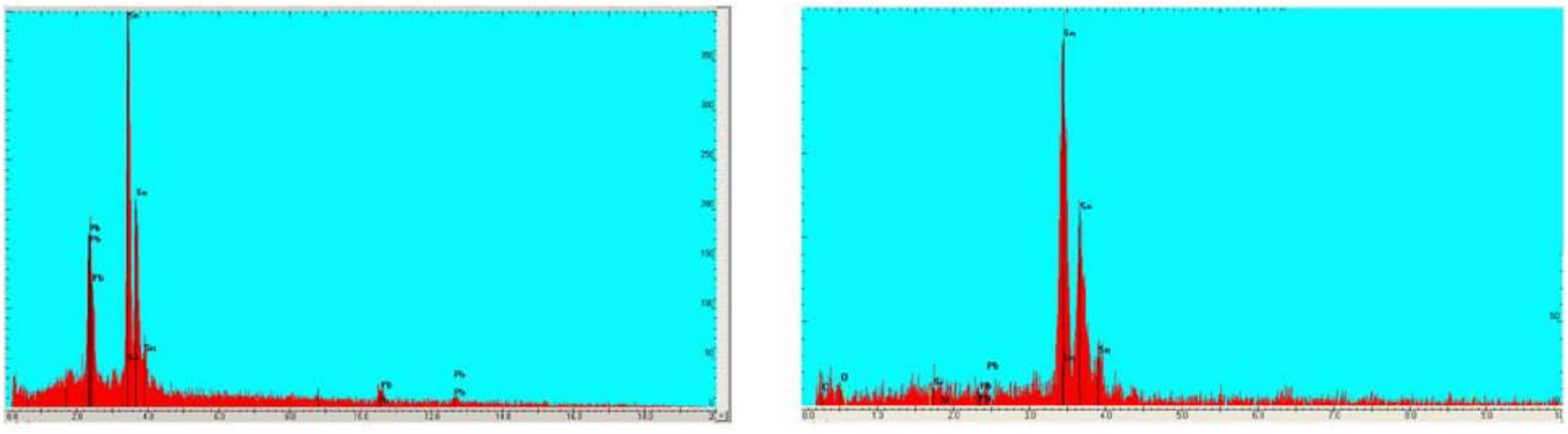


Fig. 6. ***Counterfeit defects detected by X-ray imaging (source: Honeywell). (a) Wrong Die. (b) Missing bond wires. (c) Broken bond wires.***

Physical Inspection

- Energy dispersive spectroscopy [IEEE Proc.'14]

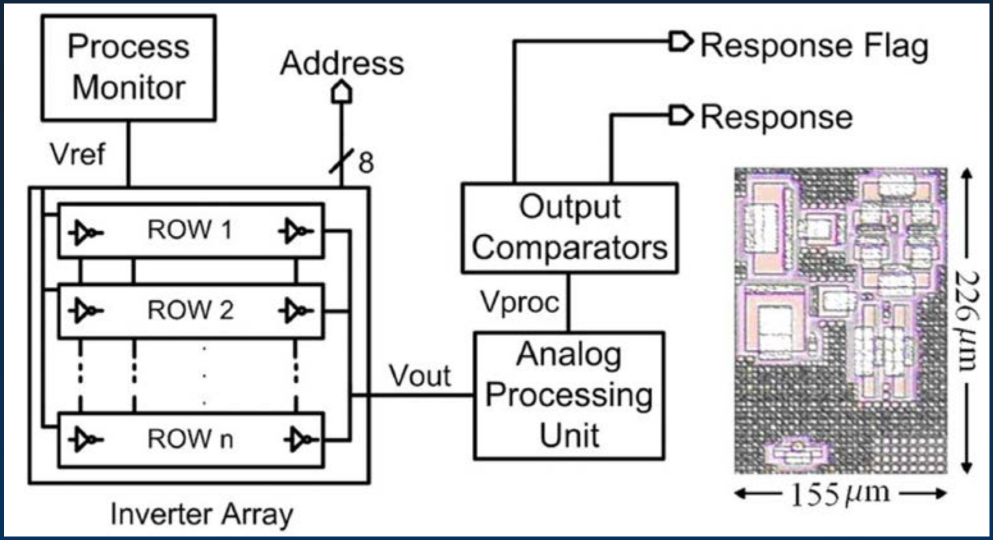


(a) (b)

Fig. 7. ***Counterfeit defects detected by EDS (source: Honeywell).***
(a) Counterfeit: element lead found in the leads of an IC.
(b) Genuine: No lead found.

Physical Unclonable Functions

- Silicon PUFs [JSSC'11]
- Exploit variability of MOSFET min. size V_t
- Generates a unique response to challenges



[A Stochastic All-Digital Weak Physically Unclonable Function for Analog/Mixed-Signal Applications, HOST'17]

References – Part III

[1] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, “Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain,” Proc. IEEE, vol. 102, no. 8, pp. 1207–1228, 2014.

[2] K. Xiao, D. Forte, and M. (Mark) Tehranipoor, “Circuit Timing Signature (CTS) for Detection of Counterfeit Integrated Circuits,” in Secure System Design and Trustable Computing, C.-H. Chang and M. Potkonjak, Eds. Cham: Springer International Publishing, pp. 211–239, 2016.

[3] K. Huang, Y. Liu, N. Korolija, J. M. Carulli, and Y. Makris, “Recycled IC Detection Based on Statistical Methods,” IEEE Trans. Comput. Des. Integr. Circuits Syst., vol. 34, no. 6, pp. 947–960, 2015.

[4] Z. Guo, T. Rahman, M. Tehranipoor, and D. Forte, "A Zero-cost Approach to Detect Recycled SoC Chips Using Embedded SRAM," IEEE Symposium on Hardware-Oriented Security and Trust (HOST), 2016.

[5] U. Guin, D. Forte, and M. Tehranipoor, "Design of Accurate Low-Cost On-Chip Structures for Protecting Integrated Circuits Against Recycling," IEEE Transactions on VLSI (TVLSI), 2015.

[7] S. Stanzione, D. Puntin and G. Iannaccone, "CMOS Silicon Physical Unclonable Functions Based on Intrinsic Process Variability," in IEEE Journal of Solid-State Circuits, vol. 46, no. 6, pp. 1456-1463, June 2011.

PART IV:
Limitations and Actions Needed

Limitations & Steps Forward

- In AMS circuits, security implications have only been shown in a few basic analog blocks
- All of the relevant work is based on simulations
- Demonstration and evaluation through actual silicon implementation is needed for drawing definitive conclusions
- No benchmark suite of circuits with hardware Trojans is available in the analog/mixed-signal/RF domain

Limitations & Steps Forward (2)

- Triggers for enabling hardware Trojans in AMS circuits and leading them to an undesired state are an open area
- Payload of AMS Trojan circuits and states, other than circuit malfunction or denial of service, needs further investigation and better understanding
- Most of the current incarnations of AMS Trojans are either too simplistic or too unrealistic to be considered a real threat

Limitations & Steps Forward (3)

- Trojan-agnostic, systematic and generalizable detection/prevention methods need to be developed for AMS/RF ICs – Current solutions are mostly ad-hoc
- Metrics for evaluating attack and defense effectiveness in the AMS domain are currently not available
- Formal, provably secure methods for protecting AMS/RF ICs/IPs are still at their infancy and are urgently needed
- Recent advances in analog formal verification may hold promise if applied to the security and trust domain

Perspective

- Despite the objective difficulties imposed by the continuous nature of AMS/RF ICs, the research community has realized the significant security and trustworthiness risk incurred
- Accordingly, there is a surge of activity in this area, seeking to develop security and trust solutions for AMS/RF ICs and IPs
- Extensive research effort, spearheaded by governmental and/or industrial support akin to that enjoyed by the digital domain over the last decade, has yet to materialize and is urgently needed in order for security and trustworthiness solutions for AMS/RF ICs and IPs to become up to par with their digital counterparts.

Questions?

yiorgos.makris@utdallas.edu