A Novel Approach to Detect Hardware Trojan Attacks on Primary Data Inputs

Taimour Wehbe^°, Vincent J. Mooney[#&°], David C. Keezer*° and Nicholas B. Parham^°

*Professor, ^School of Electrical and Computer Engineering
[#]Associate Professor, School of Electrical and Computer Engineering
[&]Associate Professor, School of Computer Science
°Institute for Information Security and Privacy

Georgia Institute of Technology, Atlanta, Georgia, USA

Georgia Tech Institute for Information Security & Privacy

Outline

- Introduction
- Background
- Prior Work
- Threat Scenario
- Architecture and Approach
- Specific Hardware Trojan Attacks
- Experimental Results
- Discussion and Conclusion

Outline

- Introduction
- Background
- Prior Work
- Threat Scenario
- Architecture and Approach
- Specific Hardware Trojan Attacks
- Experimental Results
- Discussion and Conclusion

Introduction

- Disaggregation of the chip manufacturing process
  - HDL & Design For Test (DFT)
  - Synthesis
  - Placement & routing
  - Pre-fabrication testing
  - Fabrication
  - Post-fabrication testing
- Attacker skill levels
  - Common thief
  - Technically sophisticated hacker
  - Industry
  - Government

Introduction

- Recent threats and attacks
  - In 2002, two University of Cambridge security researchers performed an inexpensive attack to extract secret information contained in widely used smart cards. *(Markoff, J. Vulnerability Is Discovered In Security for Smart Cards. The New York Time. May 13, 2002)*
  - In 2010, the U.S. Navy discovered fake microchips with a "back door" which could have disarmed missiles. *(Johnson, R. The Navy Bought Fake Chinese Microchips That Could Have Disarmed U.S. Missiles. Business Insider. July 27, 2011)*

Outline

- Introduction
- Background
- Prior Work
- Threat Scenario
- Architecture and Approach
- Specific Hardware Trojan Attacks
- Experimental Results
- Discussion and Conclusion

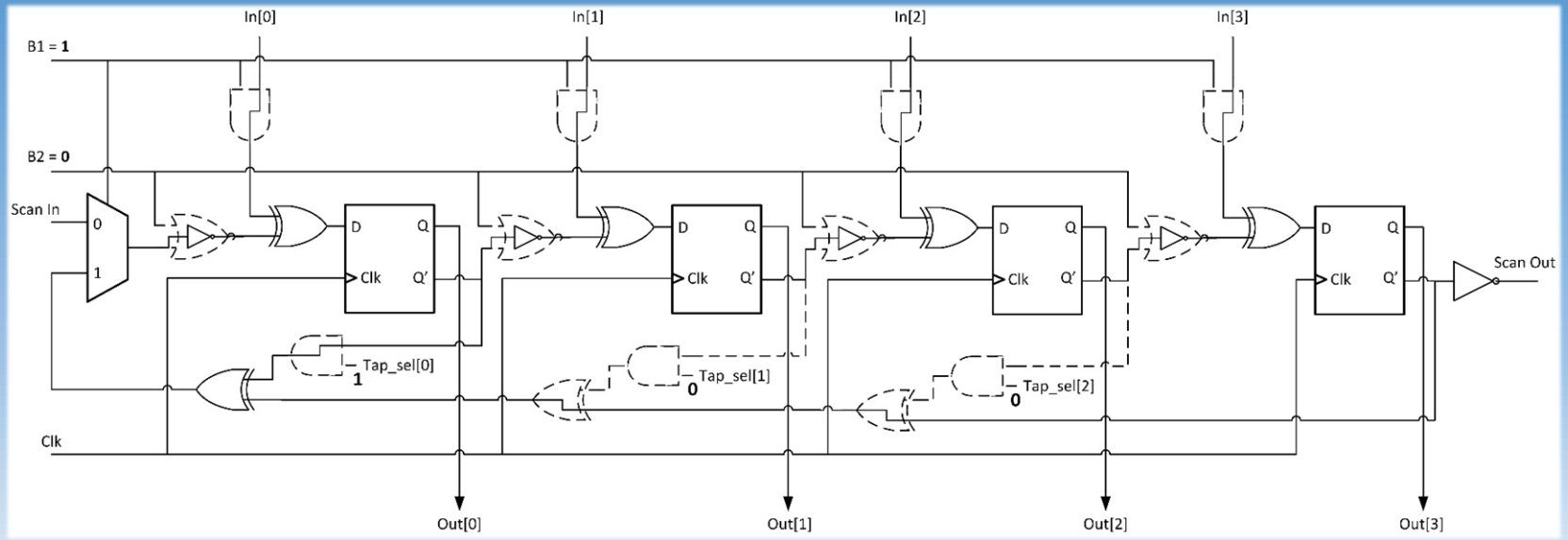
Background

- Hardware Trojans can be classified by [3,4]:
  - Physical attributes (related to chip layout)
  - Activation characteristics (how HT is triggered)
  - Action taken (what the HT tries to accomplish)
- Signature Generation
  - Message Authentication Codes (MACs)
    - Hash-based (HMACs) and Cipher Block Chaining-based (CBC-MACs)
  - Multiple Input Signature Register (MISR)
    - Built-in Logic Block Observer (BILBO) MISR

Secure Hash Algorithm (SHA)

- Create signatures using the Secure Hash Algorithm (SHA)
- Cryptographic hash security properties:
  - Pre-image resistance
  - Second pre-image resistance
  - Collision resistance
- High security but significant layout area and power consumption
  - Area of full implementations of 256-bit SHA-3 ranged between 39k Gate Equivalents (GE) and 80kGE [14-15]
  - Area of lightweight implementations were around 15kGE [16]

BILBO MISR



- MISRs are typically used in digital systems test
- For built-in self tests, BILBO MISRs are used
- We take advantage of the pre-existing BILBO registers in the design and program them to operate in MISR mode

Outline

- Introduction
- Background
- Prior Work
- Threat Scenario
- Architecture and Approach
- Specific Hardware Trojan Attacks
- Experimental Results
- Discussion and Conclusion

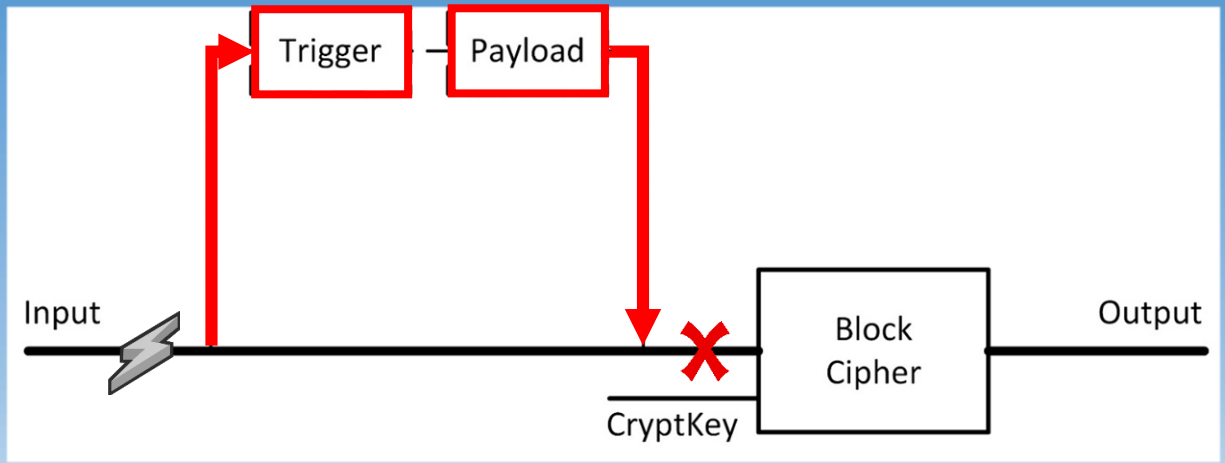
Prior Work

- Variety of research work targeting HTs inside the chips [3,4,8,9,10,11]
  - An HT triggers an internal node which rarely toggles
- A recent study (2015) conducted at Stanford University [11] prevents a wide variety of HT attacks during both IC testing and system operation in the field
- In our previous work (2014) [7], we studied the effects of HTs attacking internal modules of transmitter and receiver circuits and designed necessary circuitry to combat these HTs
- No prior research that addresses HT attacks on input values as they initially appear on a chip

Outline

- Introduction
- Background
- Prior Work
- Threat Scenario
- Architecture and Approach
- Specific Hardware Trojan Attacks
- Experimental Results
- Discussion and Conclusion

Threat Scenario

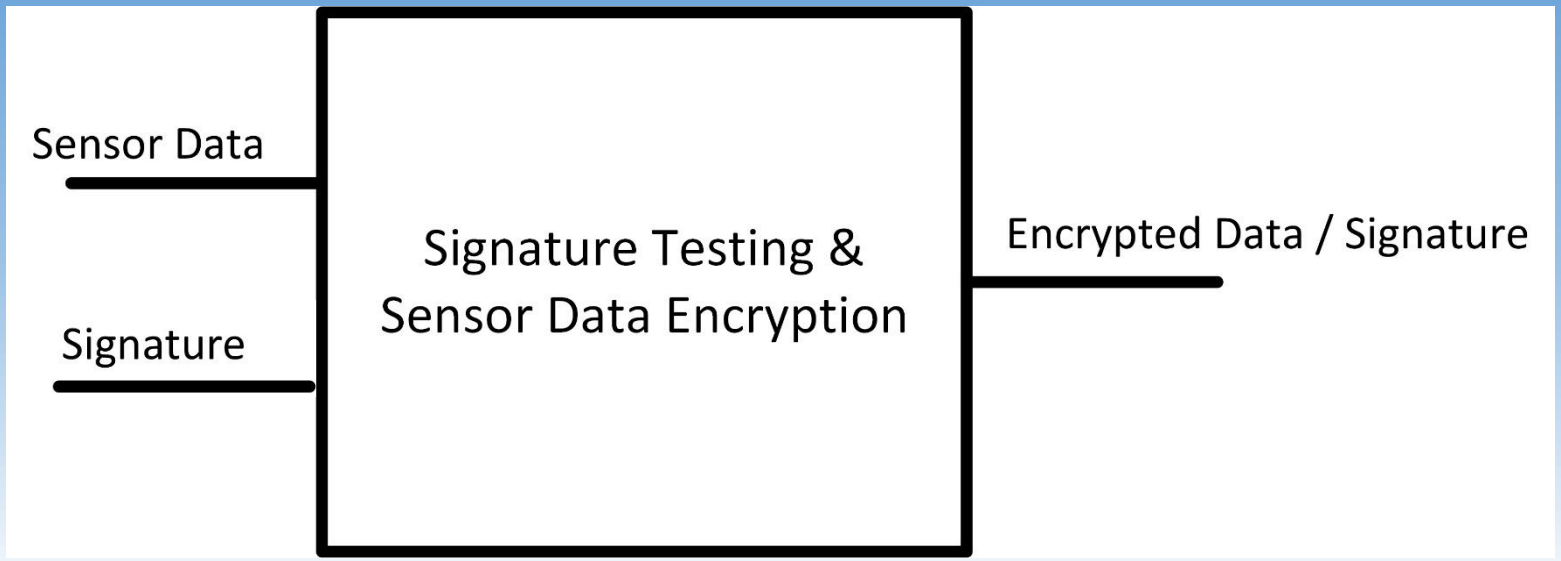


- We focus on:
  - Extremely small HT logic inserted in the chip fabrication process, which when triggered, attempts to corrupt functionality
  - Attack on primary input of a chip
  - HT triggers a payload which modifies the input value
  - Data is affected before any encryption or signature generation

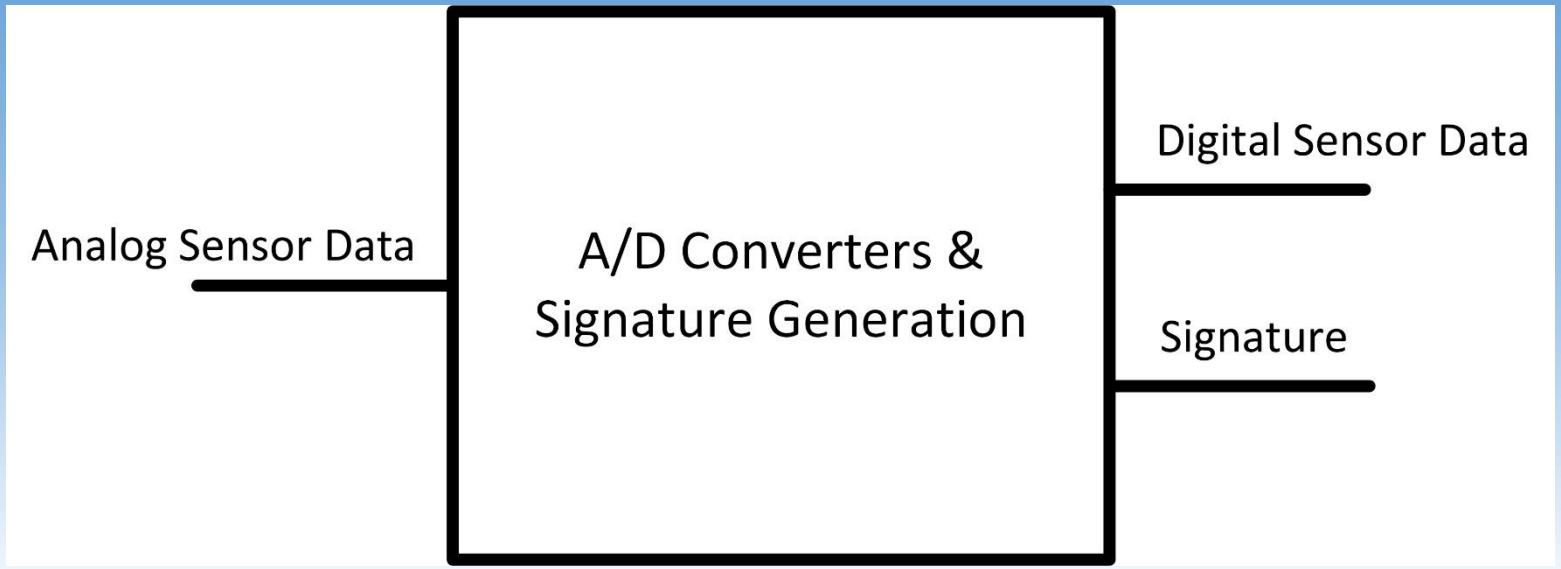
Outline

- Introduction
- Background
- Prior Work
- Threat Scenario
- Architecture and Approach
- Specific Hardware Trojan Attacks
- Experimental Results
- Discussion and Conclusion

Approach



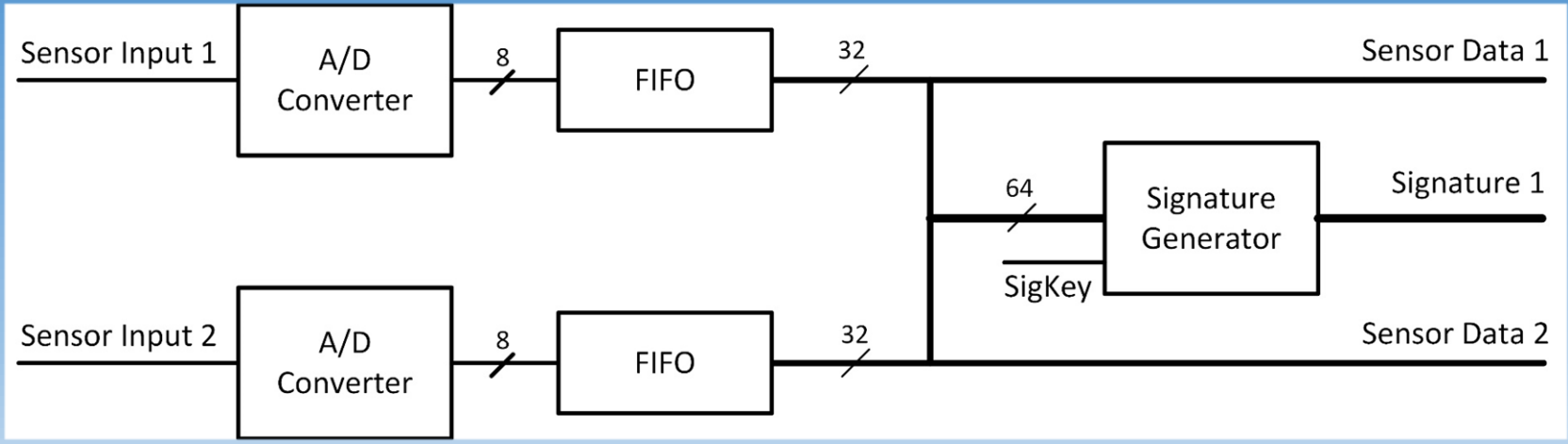
Approach (cont'd)

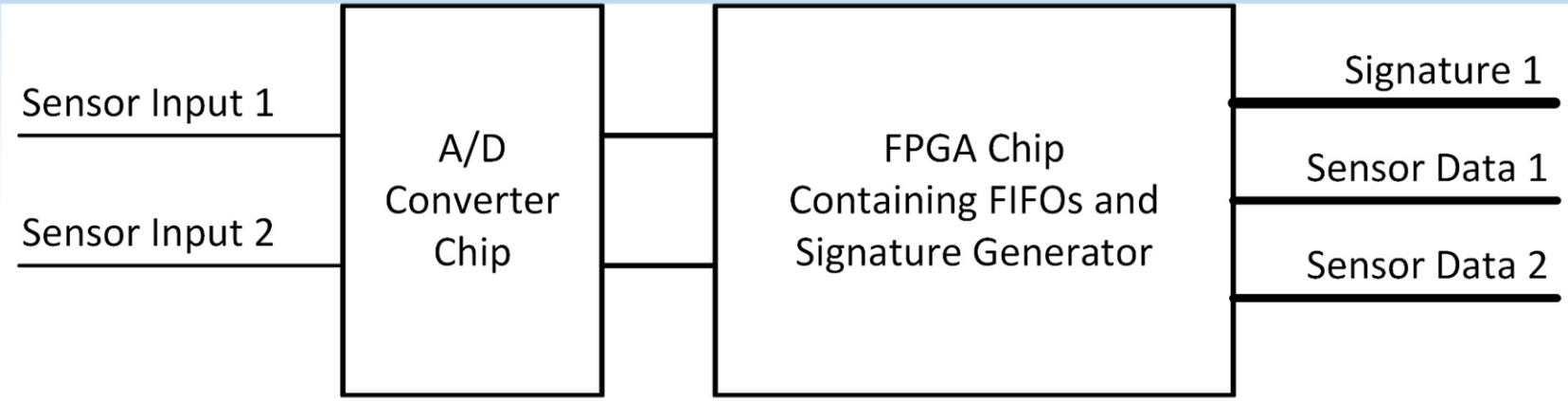


Architecture

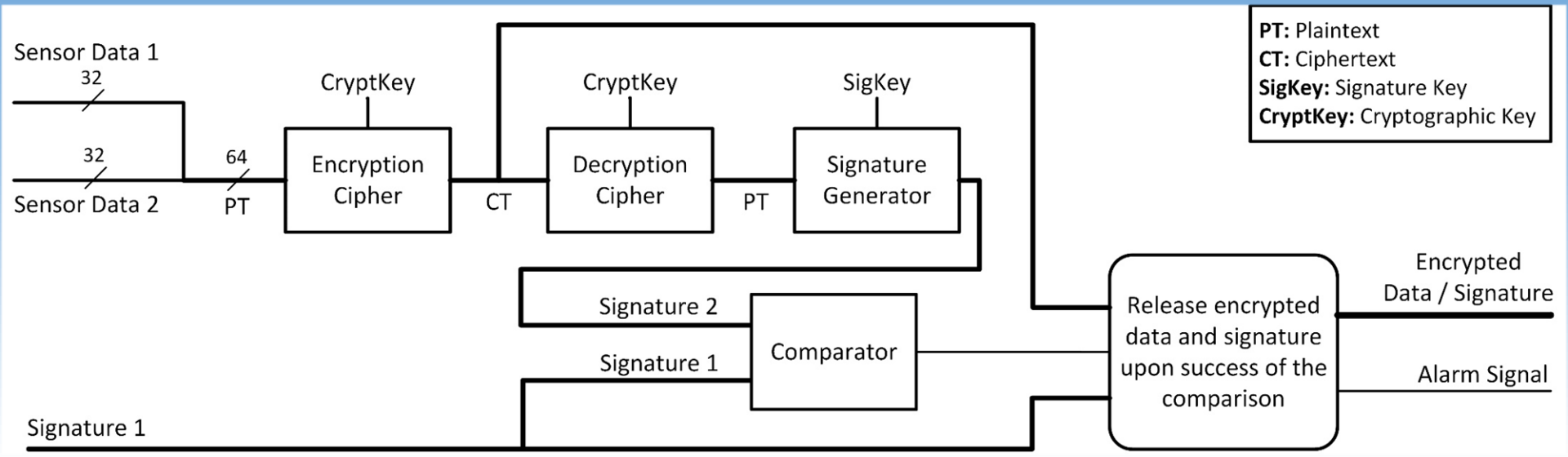
- Chip 1: A/D & Signature Generation
  - Using FPGAs and commercial of-the-shelf (COTS) components
  - Using ASICs
- Chip 2: Signature Test & Sensor Data Encryption

Chip 1: A/D & Signature Generation





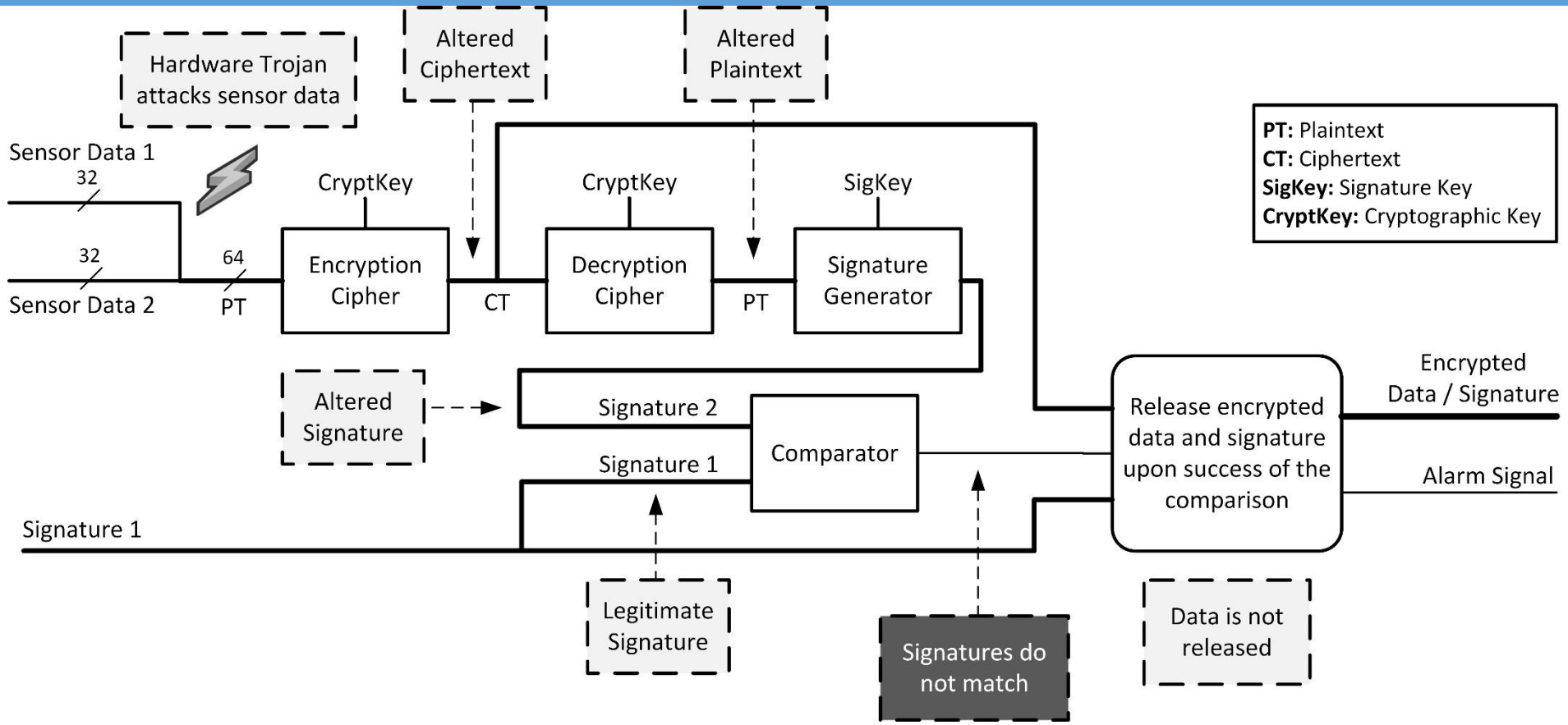
Chip 2: Signature Test & Sensor Data Encryption



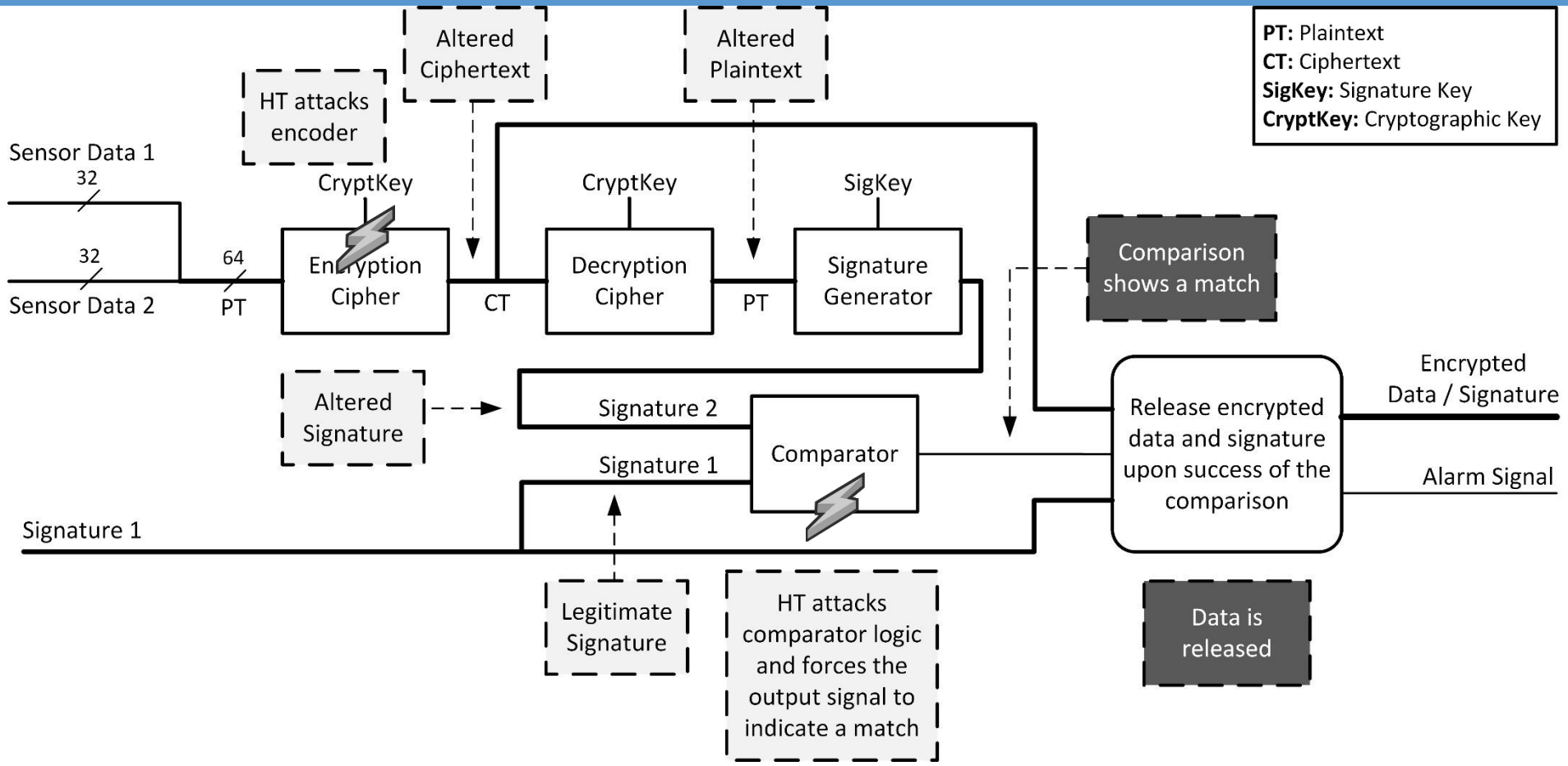
Outline

- Introduction
- Background
- Prior Work
- Threat Scenario
- Architecture and Approach
- Specific Hardware Trojan Attacks
- Experimental Results
- Discussion and Conclusion

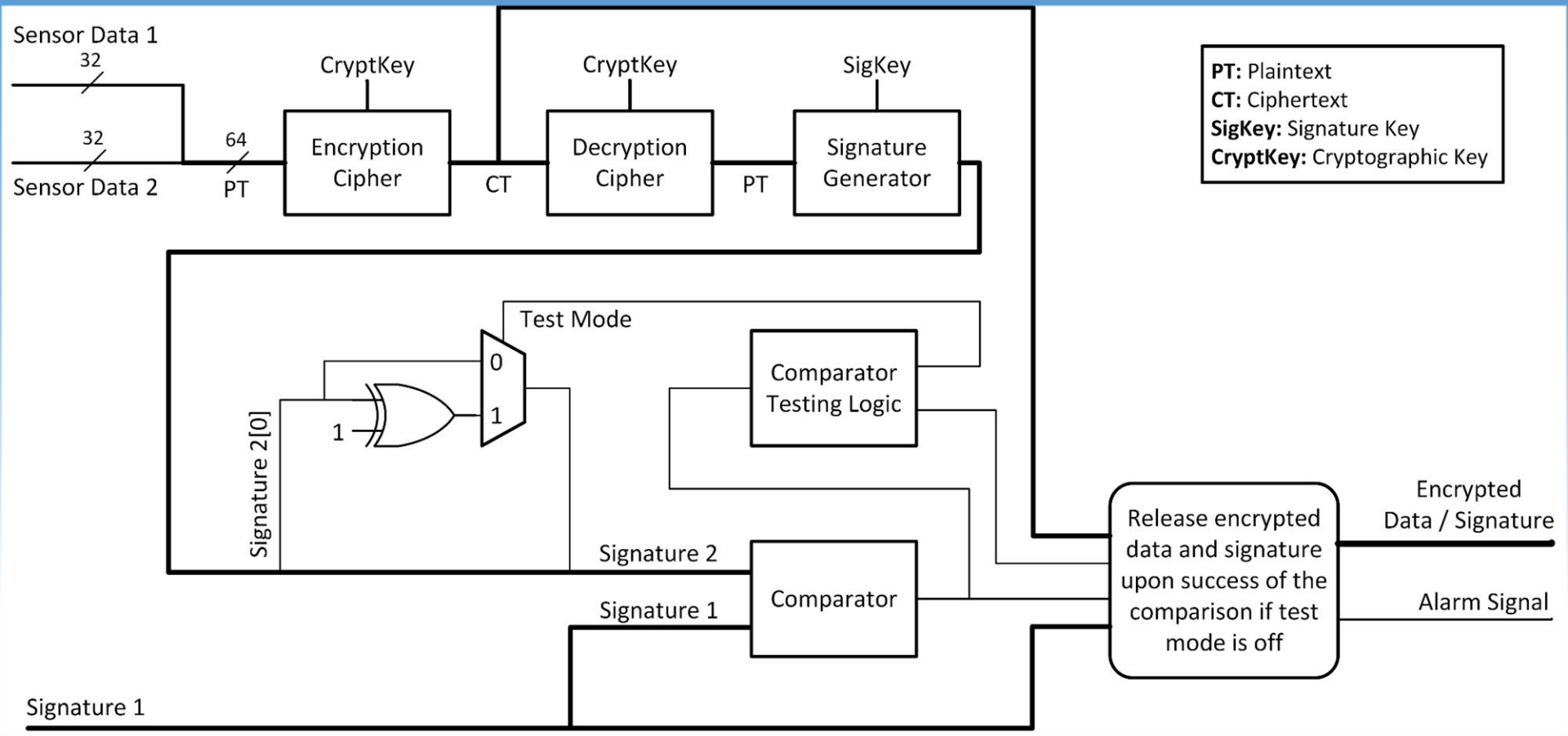
Input Attack Scenario



Comparator Attack Scenario



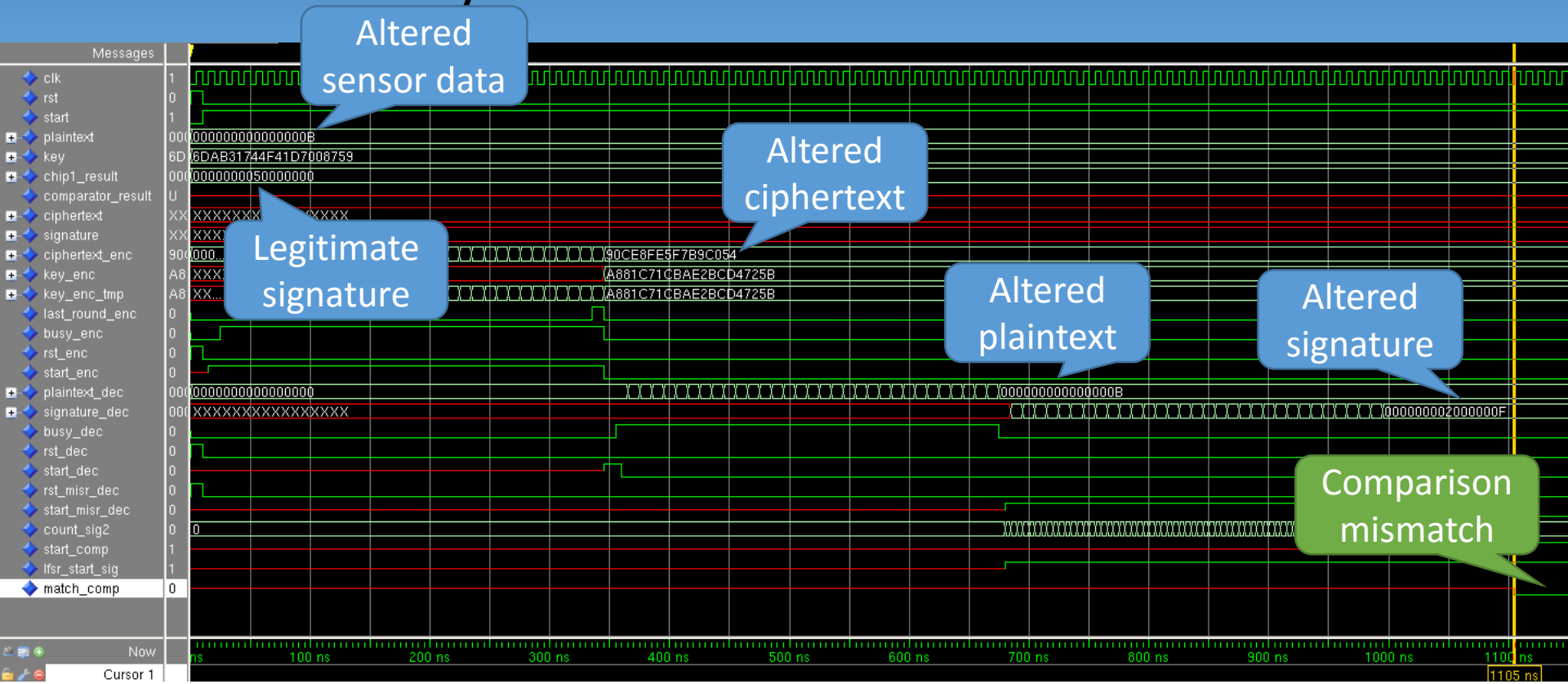
Comparator Testing Logic



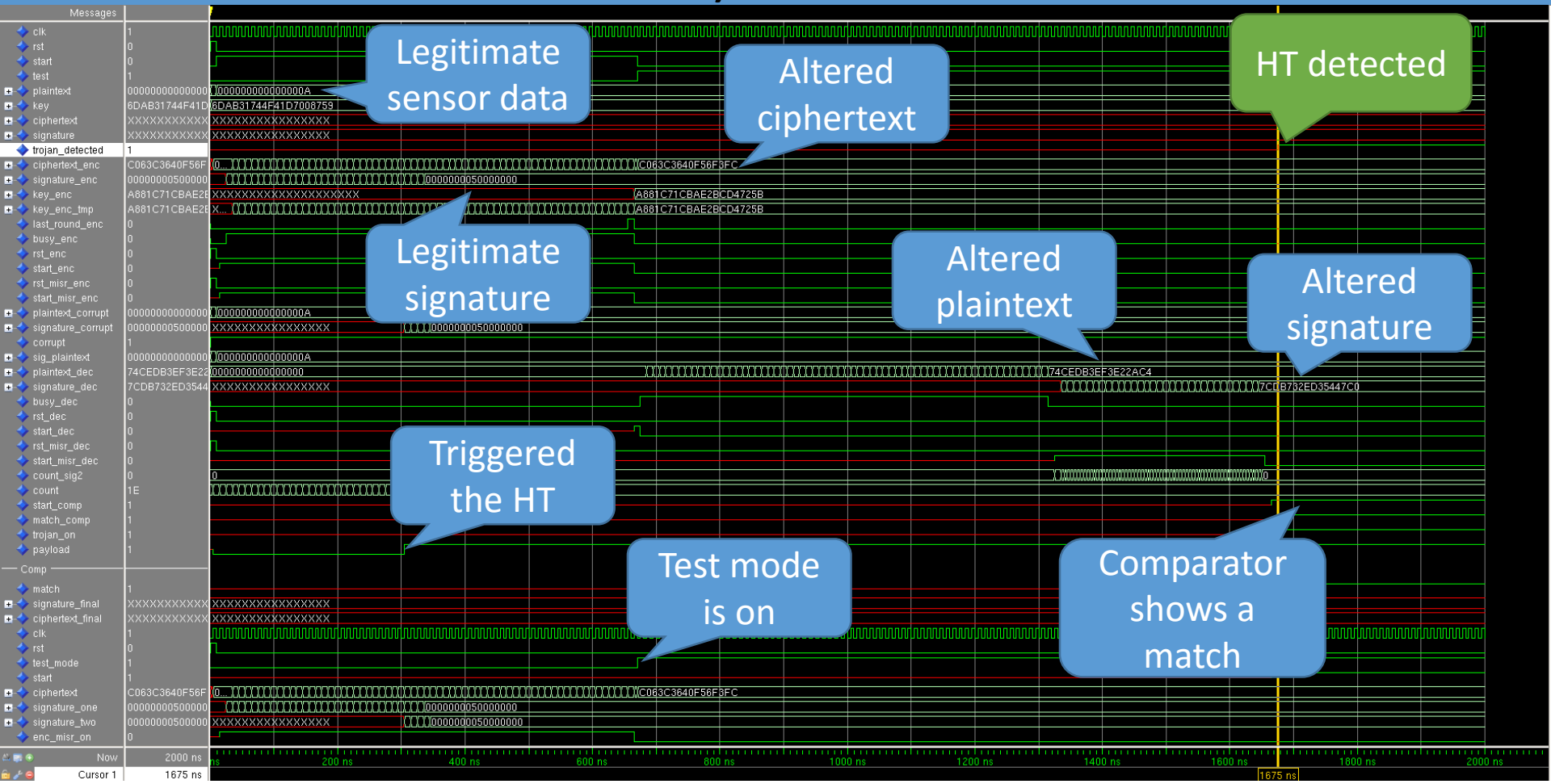
Outline

- Introduction
- Background
- Prior Work
- Threat Scenario
- Architecture and Approach
- Specific Hardware Trojan Attacks
- Experimental Results
- Discussion and Conclusion

Simulation Results (Input Attack Scenario)



Simulation Results (Comparator Attack Scenario)



Synthesis Results

Area Resources

Module	Area (square microns)
80-bit PRESENT Encryption Cipher	6819
80-bit PRESENT Decryption Cipher	7860
64-bit MISR	2597
Comparator	3575
Comparator Testing Logic	44

Area Overhead

Design	Area (square microns)	Overhead (%)
No HT Detection	14679	---
HT Detection (64-bit MISR as a signature generator)	20895	42.34
HT Detection (64-bit MISR embedded in BILBO logic)	18298	24.65
HT Detection (256-bit SHA-2 as a signature generator)	65755	347.95

Fault Coverage Results

Module	Fault Coverage (%)
80-bit PRESENT Encryption Cipher	93.45
80-bit PRESENT Decryption Cipher	91.12
64-bit MISR	99.98
Comparator	100
Comparator Testing Logic	100

- All modules have high fault coverage
- More importantly, the ones responsible for HT detection have 99.98% (MISR) and 100% (comparator and comparator testing logic) coverage

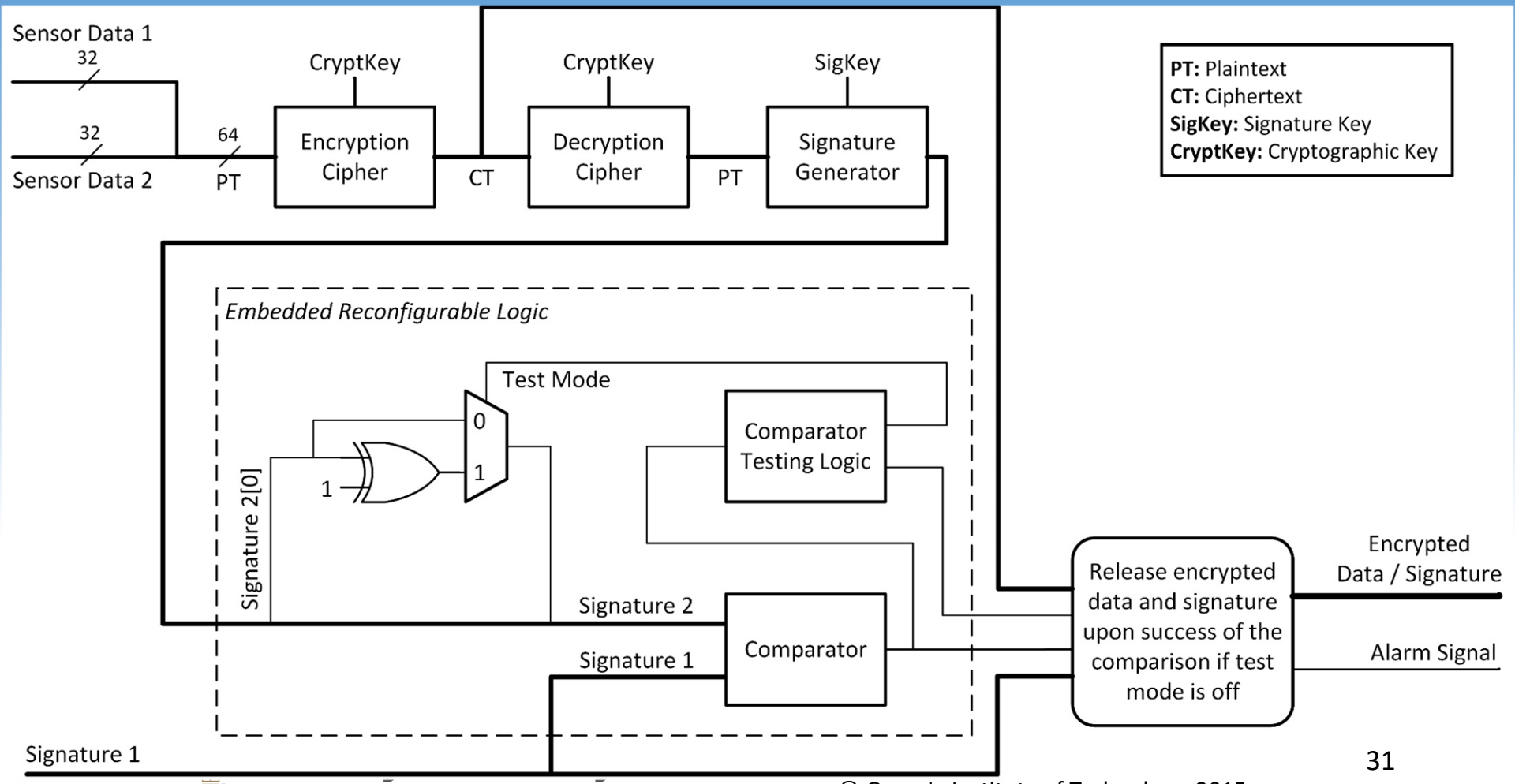
Outline

- Introduction
- Background
- Prior Work
- Threat Scenario
- Architecture and Approach
- Specific Hardware Trojan Attacks
- Experimental Results
- Discussion and Conclusion

Discussion and Conclusion

- Cheaper microchip technology for A/D converters
  - Less than state-of-the-art fab with more reliable security measures
- Advantage of using COTS components
- Use of reconfigurable embedded logic to combat the attack on the comparator testing logic

Comparator Testing Logic Implemented in Embedded Reconfigurable Logic



THANK YOU

Presented by:
Taimour Wehbe, Ph.D. Student
Hardware/Software Codesign Group
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia, USA
taimour.wehbe@gatech.edu
http://users.ece.gatech.edu/~twehbe3/
http://codesign.ece.gatech.edu/flash.html