A Signature Based Architecture for Trojan Detection

Aderinola Gbade-Alabi*, David Keezer*, Vincent Mooney*,&, Axel Poschmann#, Marc Stöttinger+ and Kshitij Divekar*

*School of Electrical and Computer Engineering, Georgia Institute of Technology, Georgia, USA

&School of Computer Science, Georgia Institute of Technology, Georgia, USA

+Temasek Laboratories, Nanyang Technological University, Singapore

#NXP Semiconductors, Germany

OUTLINE

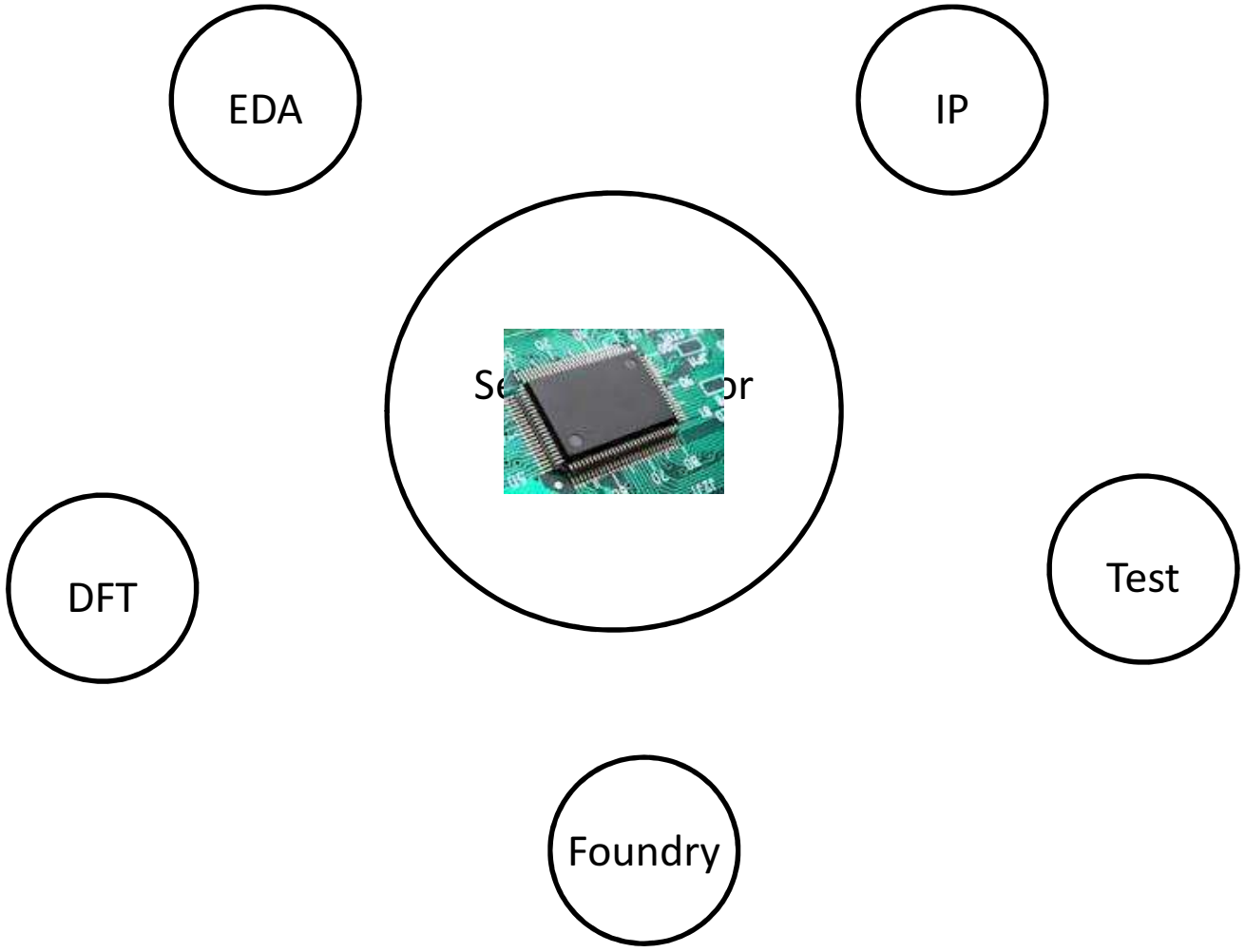
- Background
- Prior work
- Threat scenarios
- Architecture
- Experimental Results
- Conclusion and Future Work

OUTLINE

- Background
- Prior work
- Threat scenarios
- Architecture
- Experimental Results
- Conclusion and Future Work

Background

Disaggregation of Semiconductor companies



Background

- Result:

I. Less control over the chip fabrication process

II. Possibility of malicious hardware being inserted into chips

- Different Levels of Skill:

I. Common thief

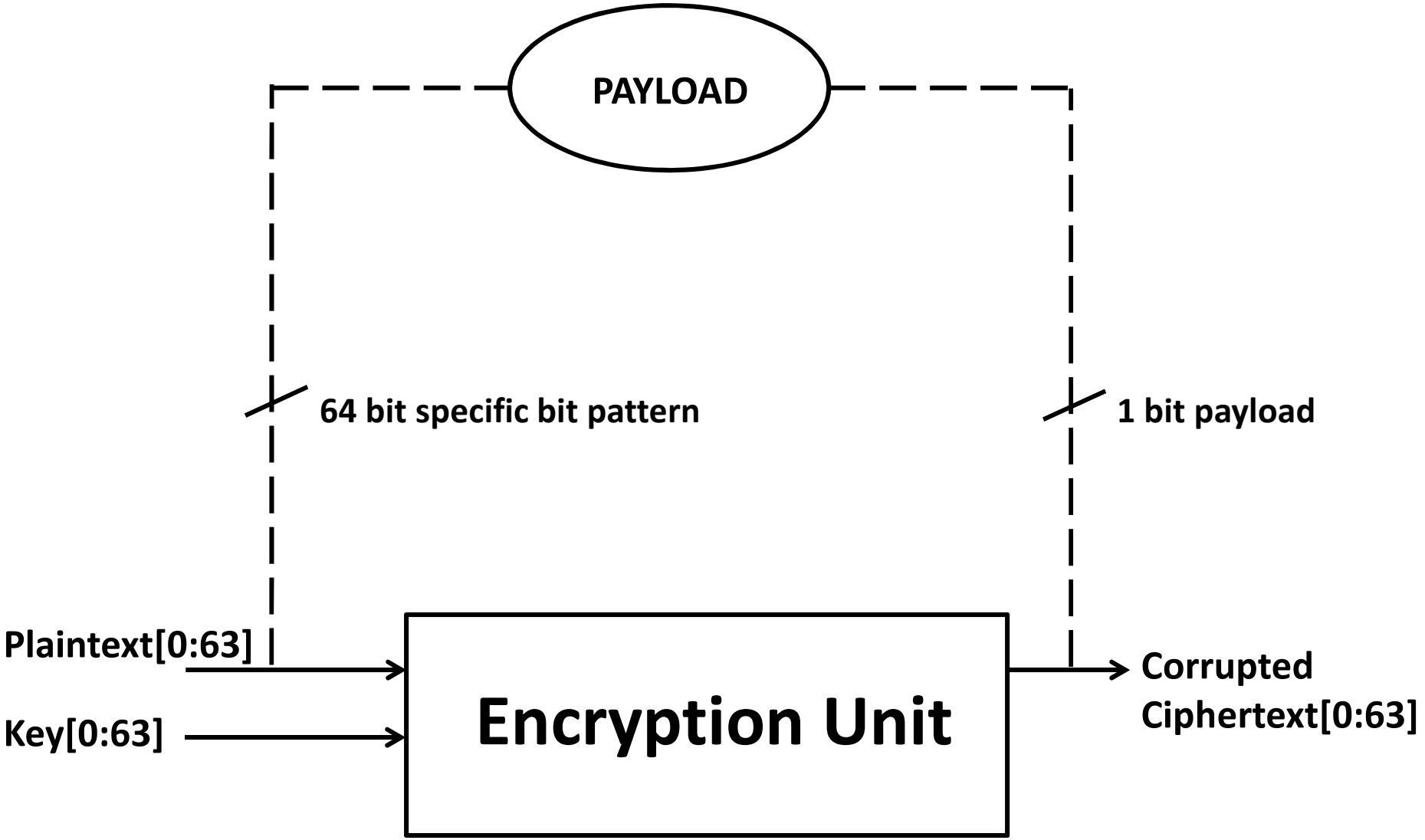
II. Technically sophisticated hacker

III. Industrial Espion

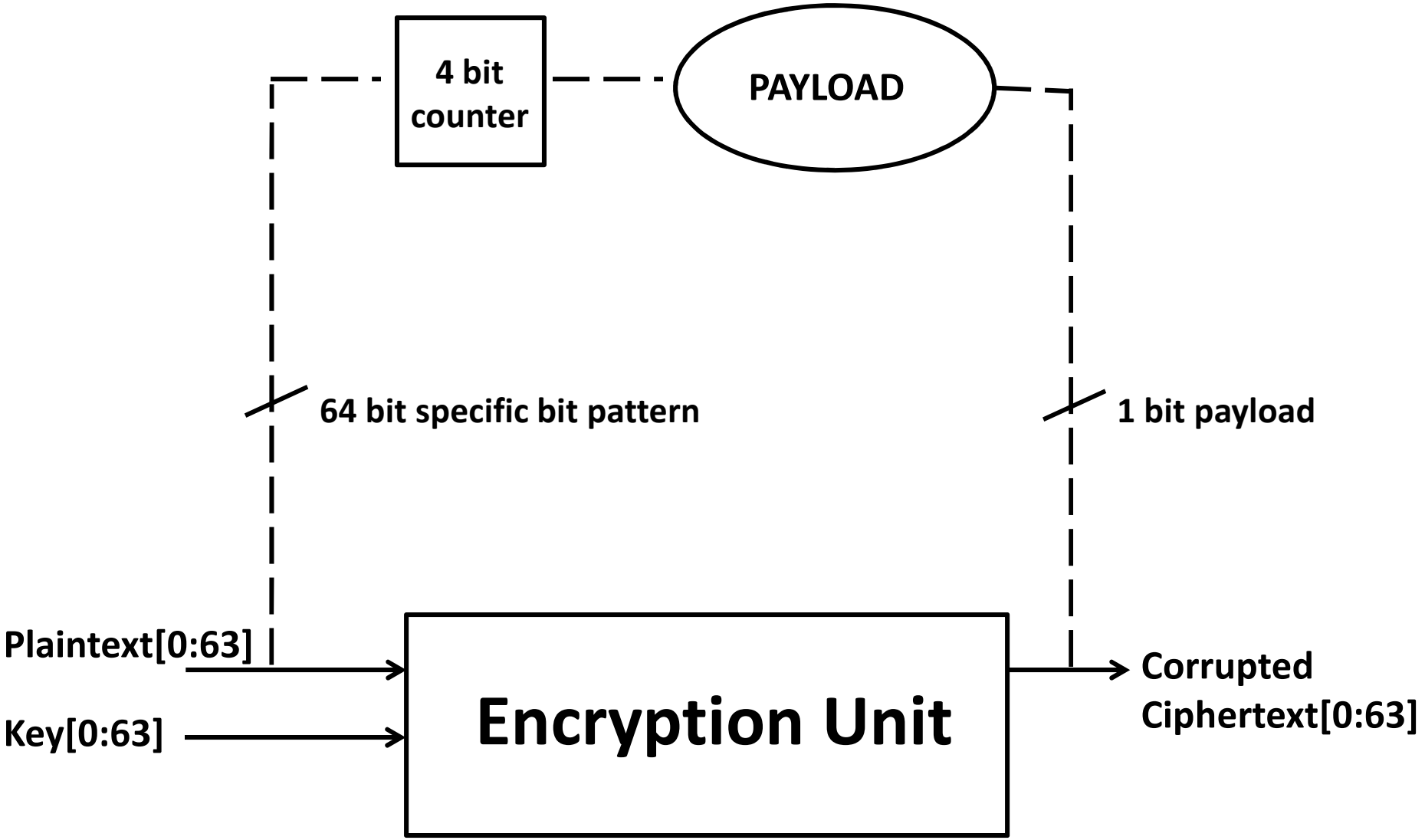
IV. Government

HT found in counterfeit chips supplied to the government : (http://www.businessinsider.com/navy-chinese-microchips-weapons-could-have-been-shut-off-2011-6)

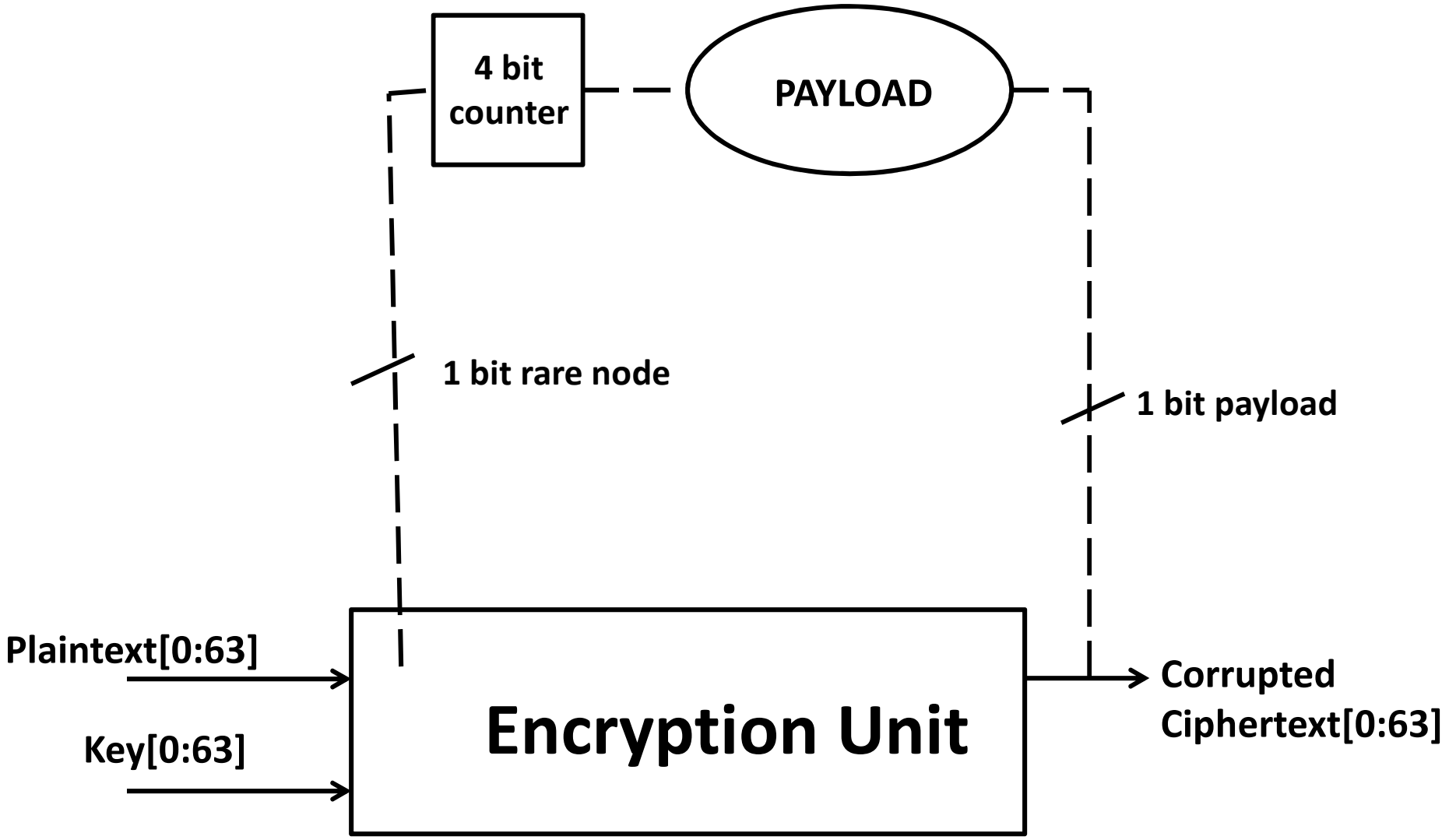
Hardware Trojan Attacks



Hardware Trojan Attacks



Hardware Trojan Attacks



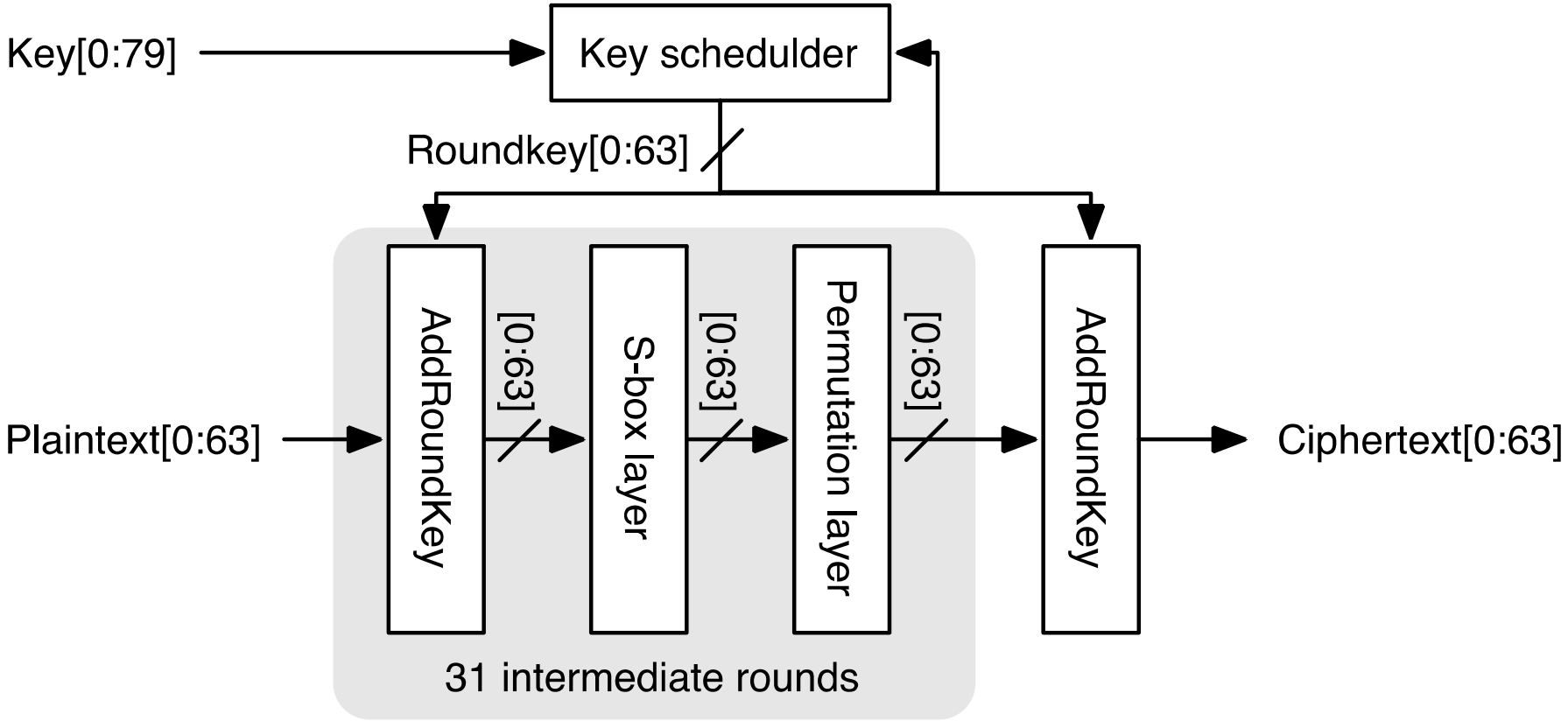
OUTLINE

- Background
- Prior work
- Threat scenarios
- Architecture
- Experimental Results
- Conclusion and Future Work

Prior Work in Hard to Detect Tiny Hardware Trojans

- S. Wei, K. Li, F. Koushanfar and M. Potkonjak, “Hardware Trojan Benchmark via Optimal Creation and Placement of Malicious Circuitry,” Design Automation Conference (DAC'12), pp. 90-95, June 2012

Prior Work: Block Cypher **PRESENT**



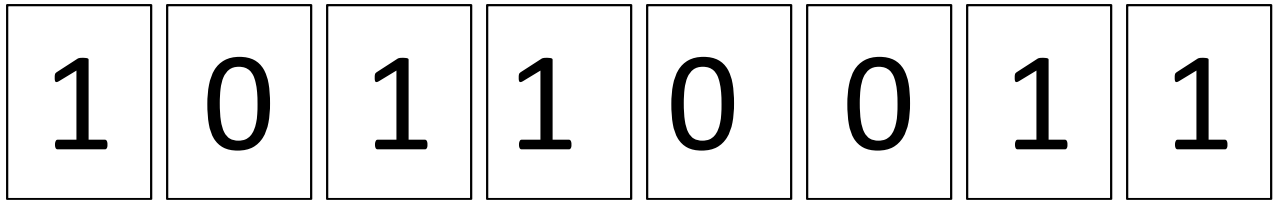
PRESENT

- Plain-text (64 bit): $b_{63} \ldots b_0$
- Round-key (64 bit): $\kappa_{63} \ldots \kappa_0$

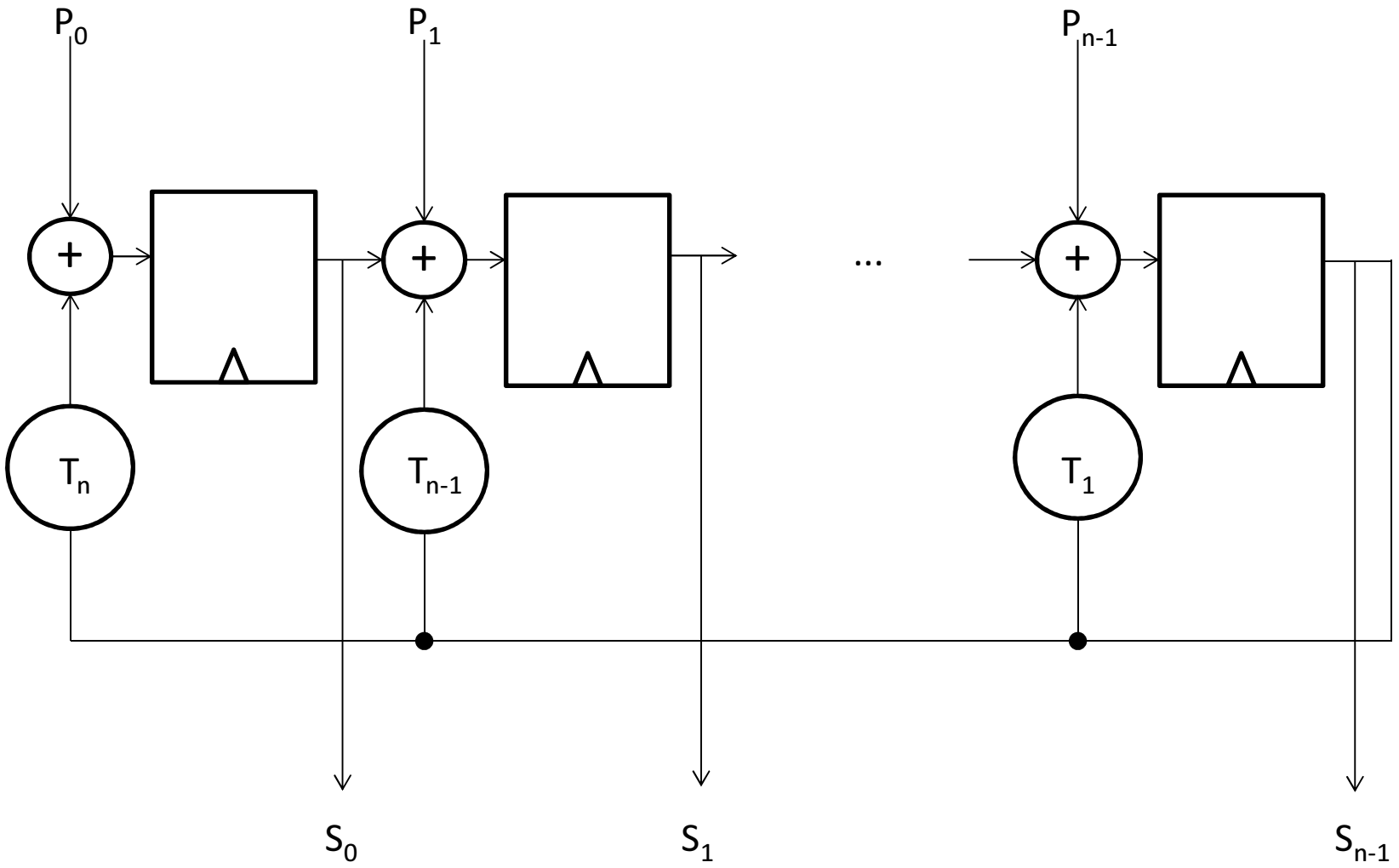
  $bj \rightarrow bj \text{ xor } \kappa ji$
- sBoxLayer:

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[X]	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

- pLayer:



Prior Work: Signature Generation Using a Multiple-Input Shift Reg (MISR)

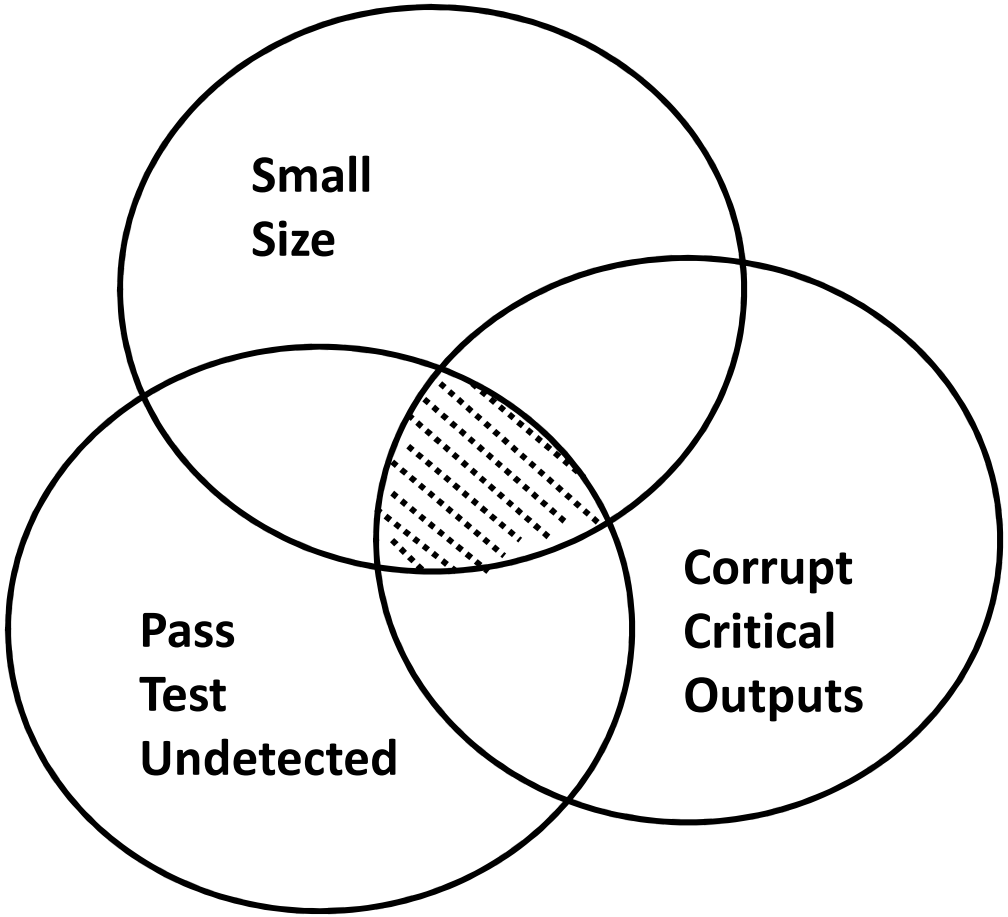


OUTLINE

- Background
- Prior work
- Threat scenarios
- Architecture
- Experimental Results
- Conclusion and Future Work

Threat Scenarios

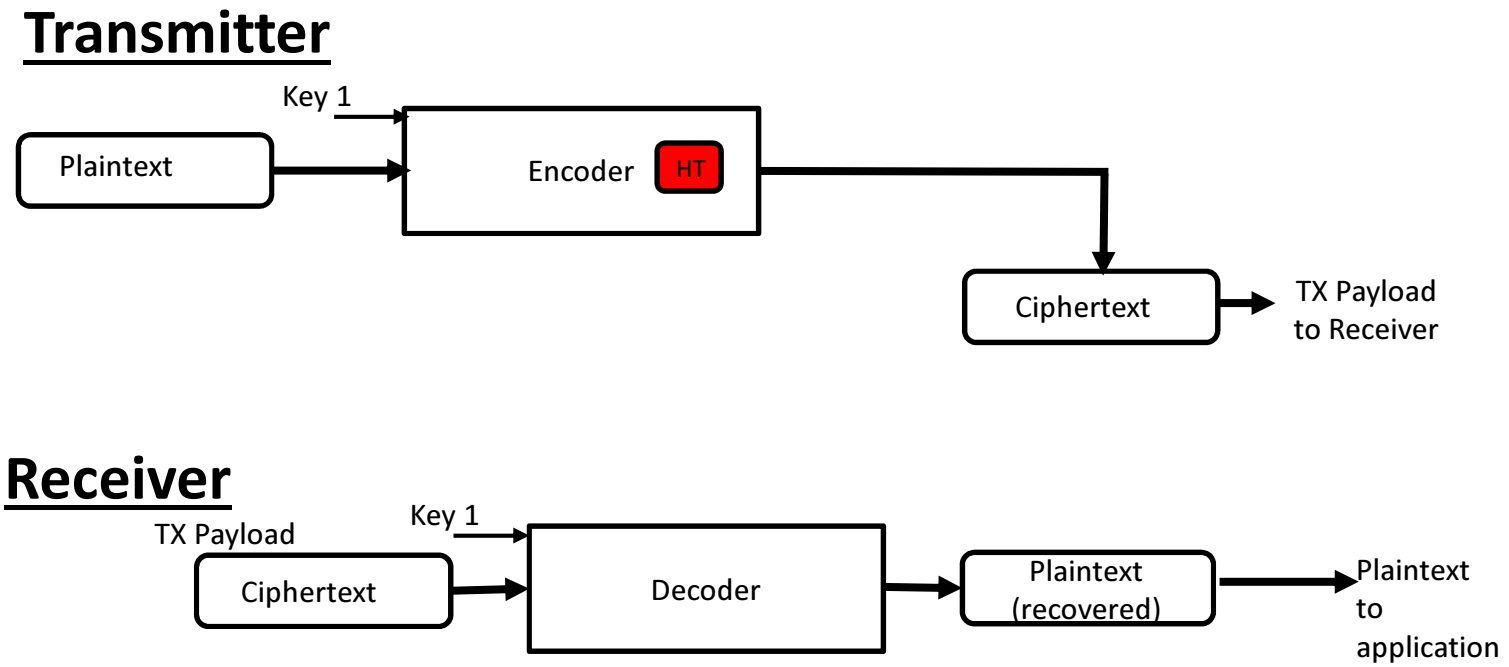
- Focus is on tiny HTs which affect functionality
- We do not discuss what to do after detection



- Side channel attacks are not considered

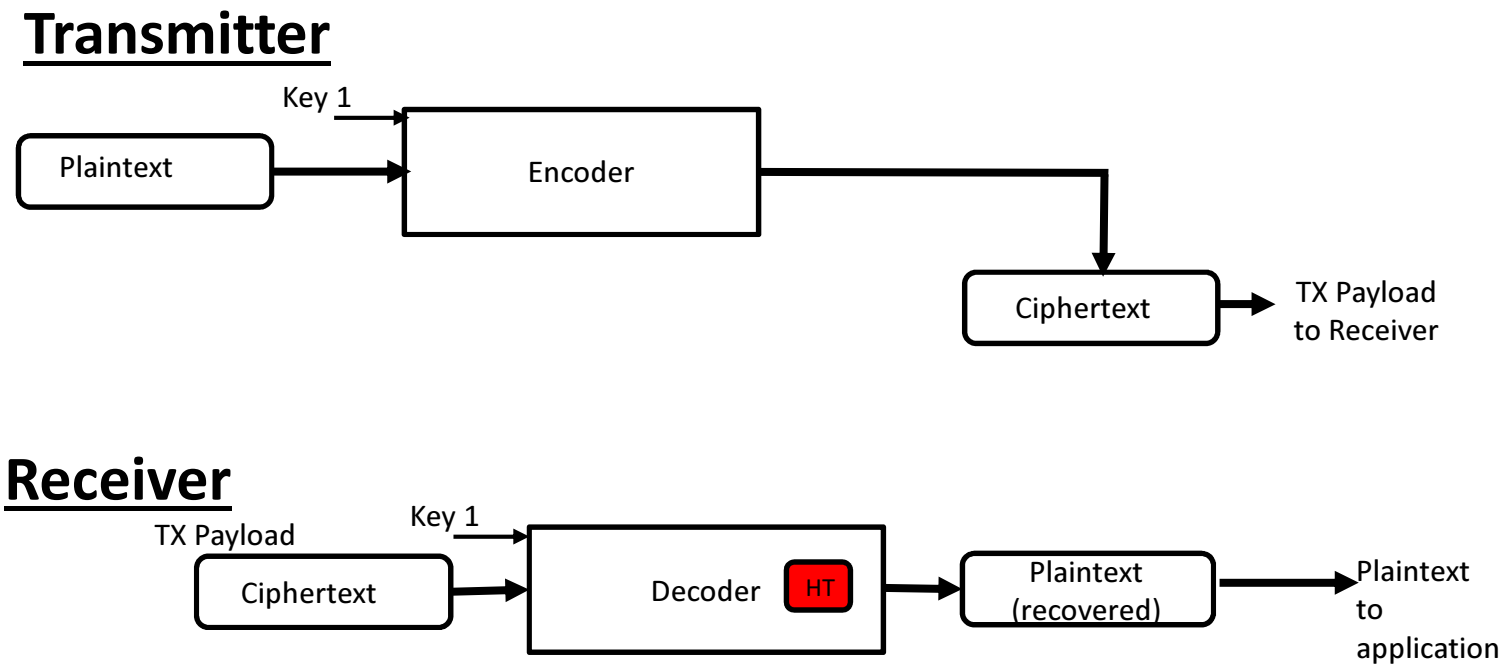
THREAT SCENARIO (a)

a) HT in encoder



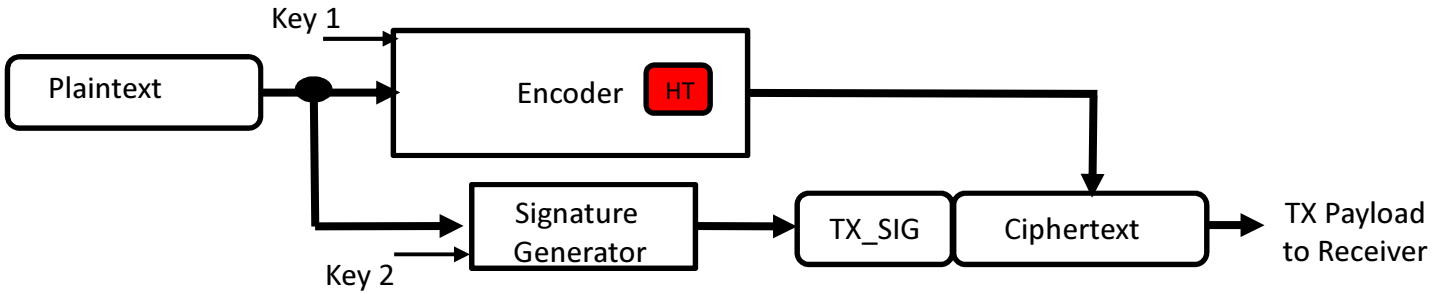
THREAT SCENARIO (b)

b) HT in decoder

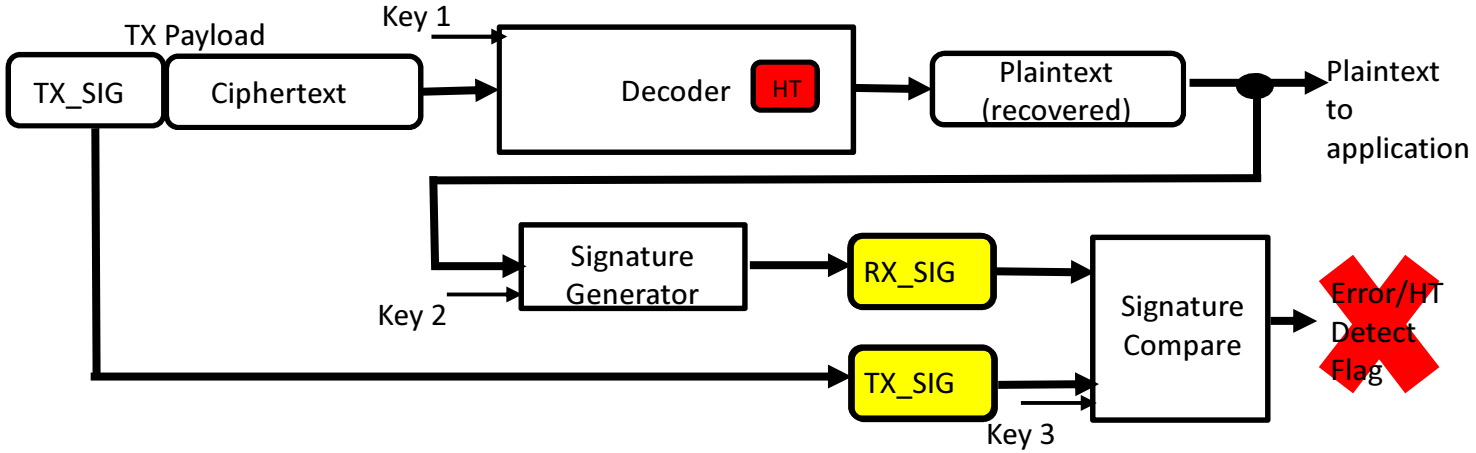


ARCHITECTURE

Transmitter



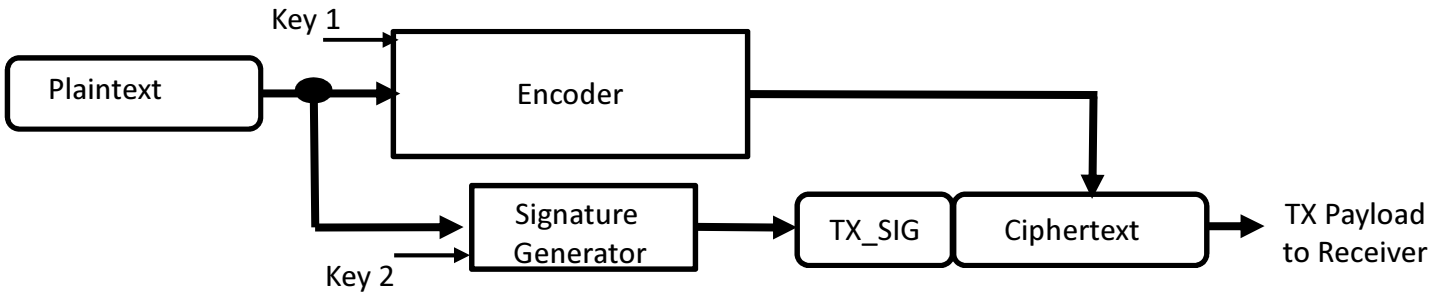
Receiver



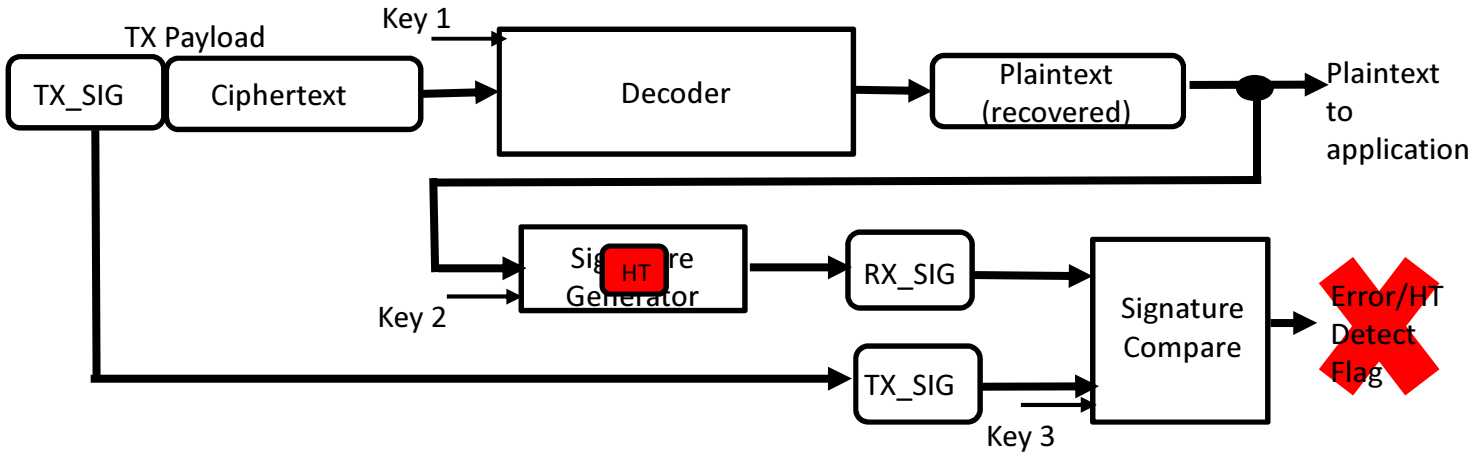
THREAT SCENARIO (c)

c) HT in Signature Generator

Transmitter



Receiver



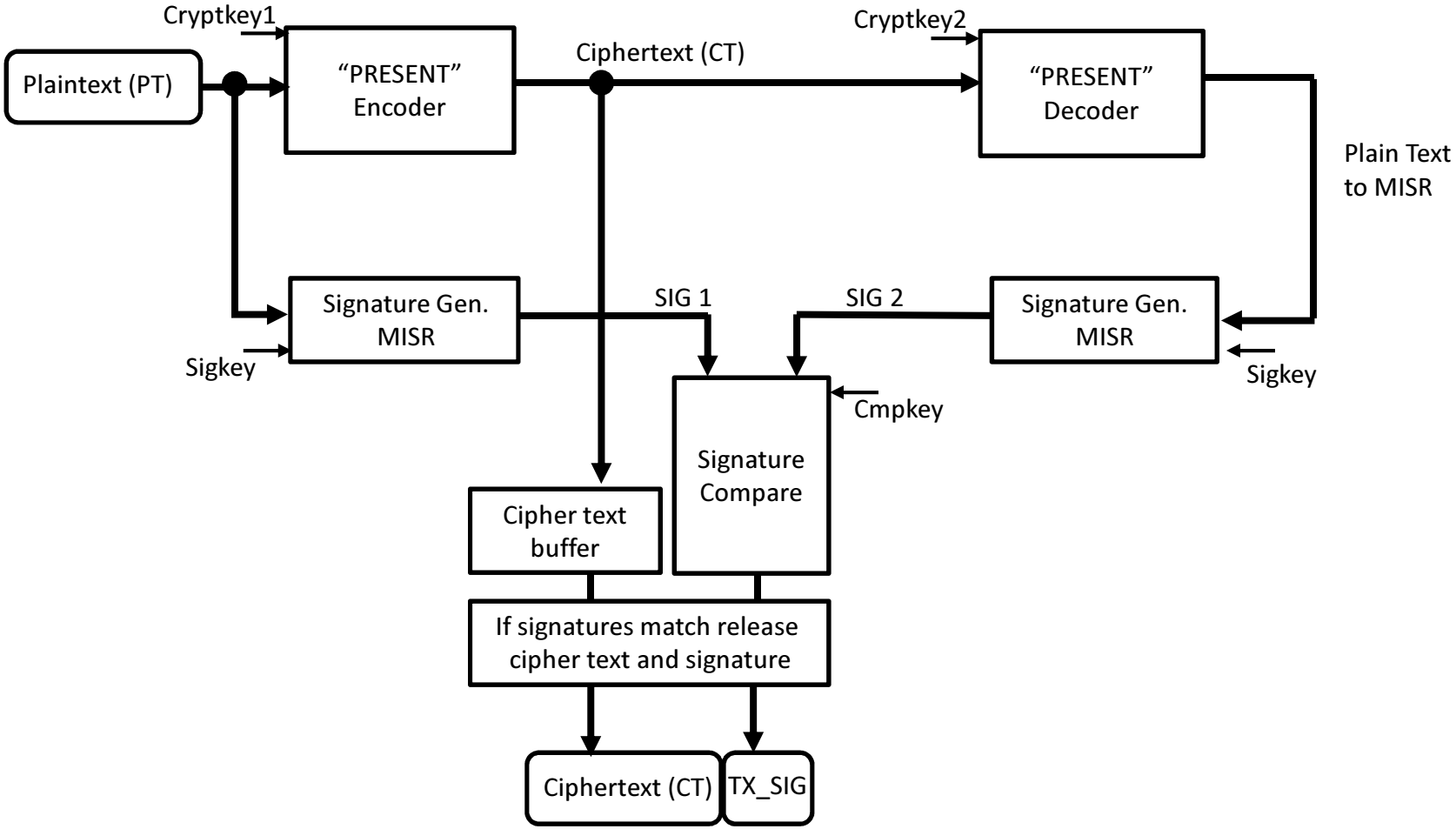
Scenario not Considered a Threat

- Simultaneous alteration of encrypted text & associated signature
- Mathematics for this not published
  - Any such approach likely to require a large hardware footprint

OUTLINE

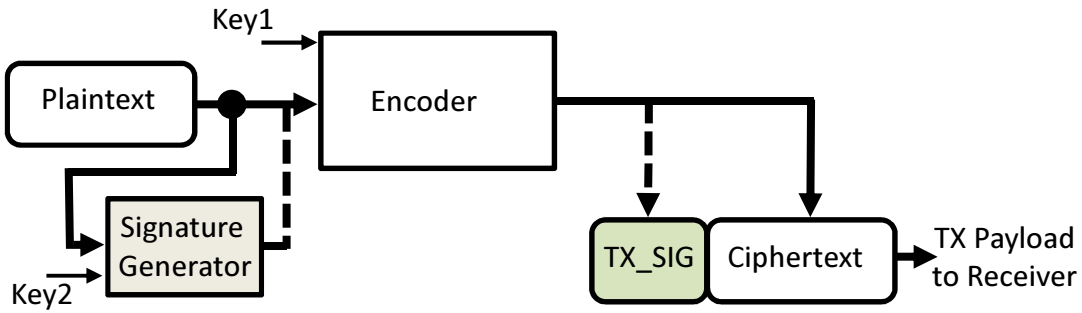
- Background
- Prior work
- Threat scenarios
- Architecture
- Experimental Results
- Conclusion and Future Work

Transmitter with HT detection

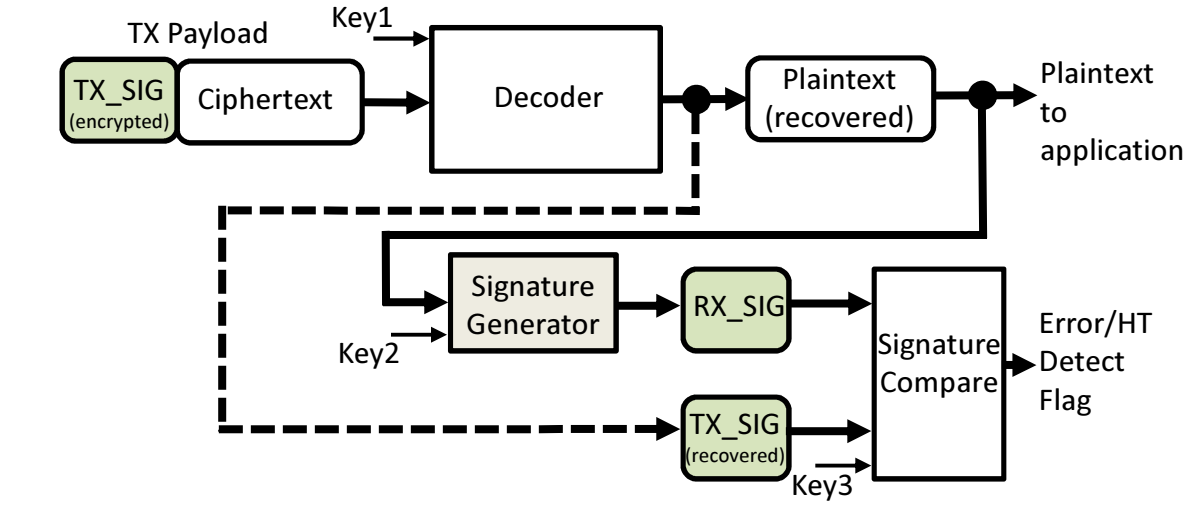


Architecture Modification with Encrypted Signature

Transmitter



Receiver



OUTLINE

- Background
- Prior work
- Threat scenarios
- Architecture
- Experimental Results
- Conclusion and Future Work

Simulation Results

- Used Mentor Graphics ModelSim PE 6.6b
- Clock Period of 10ns (100 MHz)
- HTs in encoder were triggered by:

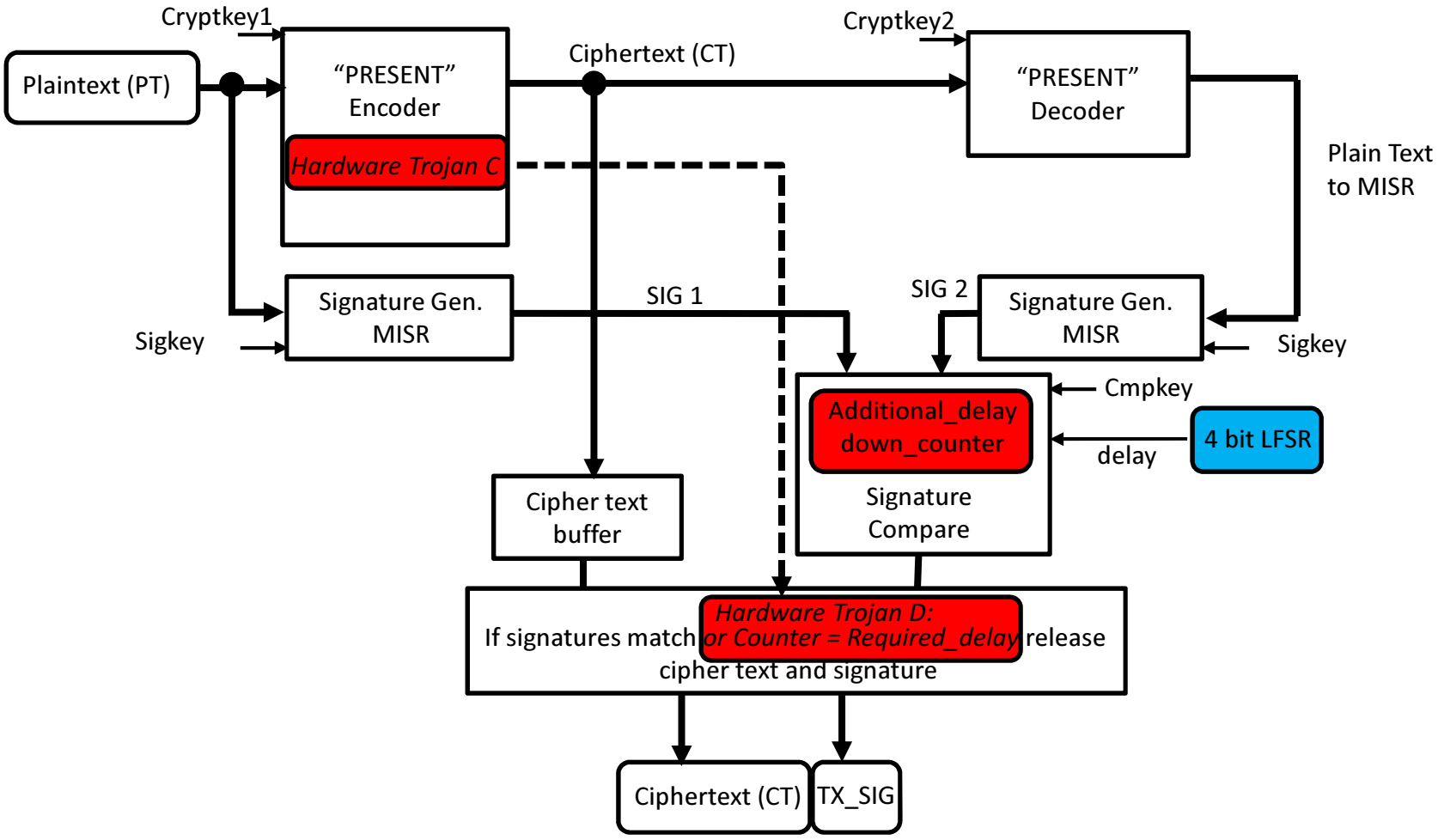
a) 64 bit plain-text (0x0123456789ABCDEF)

b) Multiple occurrences (2, 4 and 8) of a 64 bit plain-text

c) Sensitization of a rare node multiple times

d) Co-ordinated Attack between HT c) in encoder and an HT in the signature comparator

Co-ordinated Hardware Trojan Attack



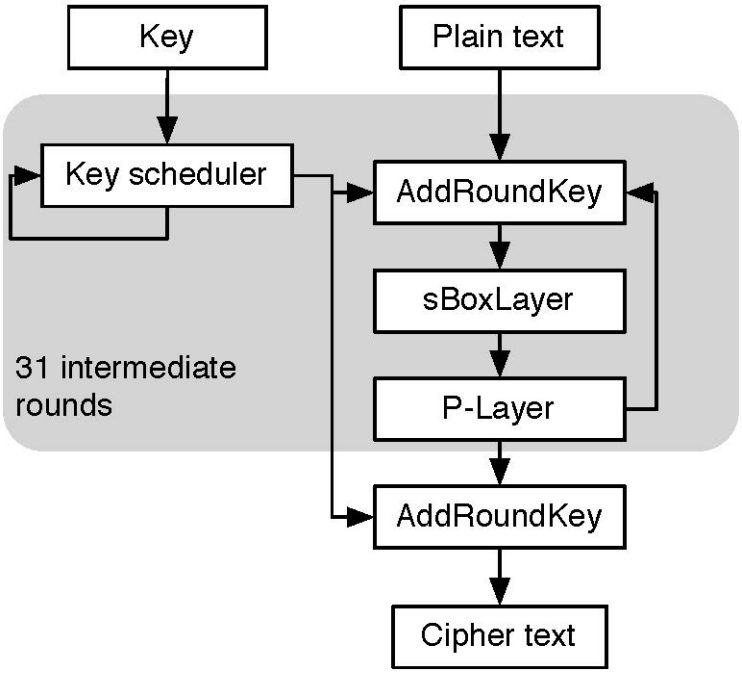
Synthesis Results

- Synthesized using Synopsys Design Compiler version 2010.12-SP3 for Linux and the NCSU 45nm Base Kit

COMPONENT	AREA(sq. micron)
DECODER	6906
ENCODER	5784
SIGNATURE GENERATOR	2524
COMPARATOR	764

- Original design area = 12690
- Area of proposed design = 18502
- 45.79984% increase in area

Test Coverage (No Scan Reg)



Logic Block	Fault Coverage
Controller	98.45%
Datapath	100.00%
Key Scheduler	96.81%
pLayer	100.00%
sBox	100.00%
PRESENT encoder	91.86%

Table 1. Fault Simulation Results – Encoder.

OUTLINE

- Background
- Prior work
- Threat scenarios
- Architecture
- Experimental Results
- Conclusion and Future Work

Conclusion and Future Work

- The proposed architecture can detect any HT in encoder and also a coordinated HT attack between encoder and signature comparator
- We need to look into the following:

a) Aliasing effect and how it can be exploited for a coordinated attack between encoder and decoder
b) Other coordinated attacks between different components
c) Choosing the optimum MISR configuration to strike a balance between test, area overhead and functionality
d) Replacing the MISR with a less HW intensive signature generator
e) Testing the comparator at run-time by knowingly using non-matching signatures
f) Input signatures in analog