ISC 2018 ISC互联网安全大会 | 360互联网安全中心

从集成电路芯片角度看物联网和系统安全

金意儿　　佛罗里达大学副教授兼IoT冠名教授

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China

IOT AND SYSTEM SECURITY: FROM THE VLSI PERSPECTIVE

Yier Jin

Associate Professor
Endowed IoT Term Professor
University of Florida

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China

Contents

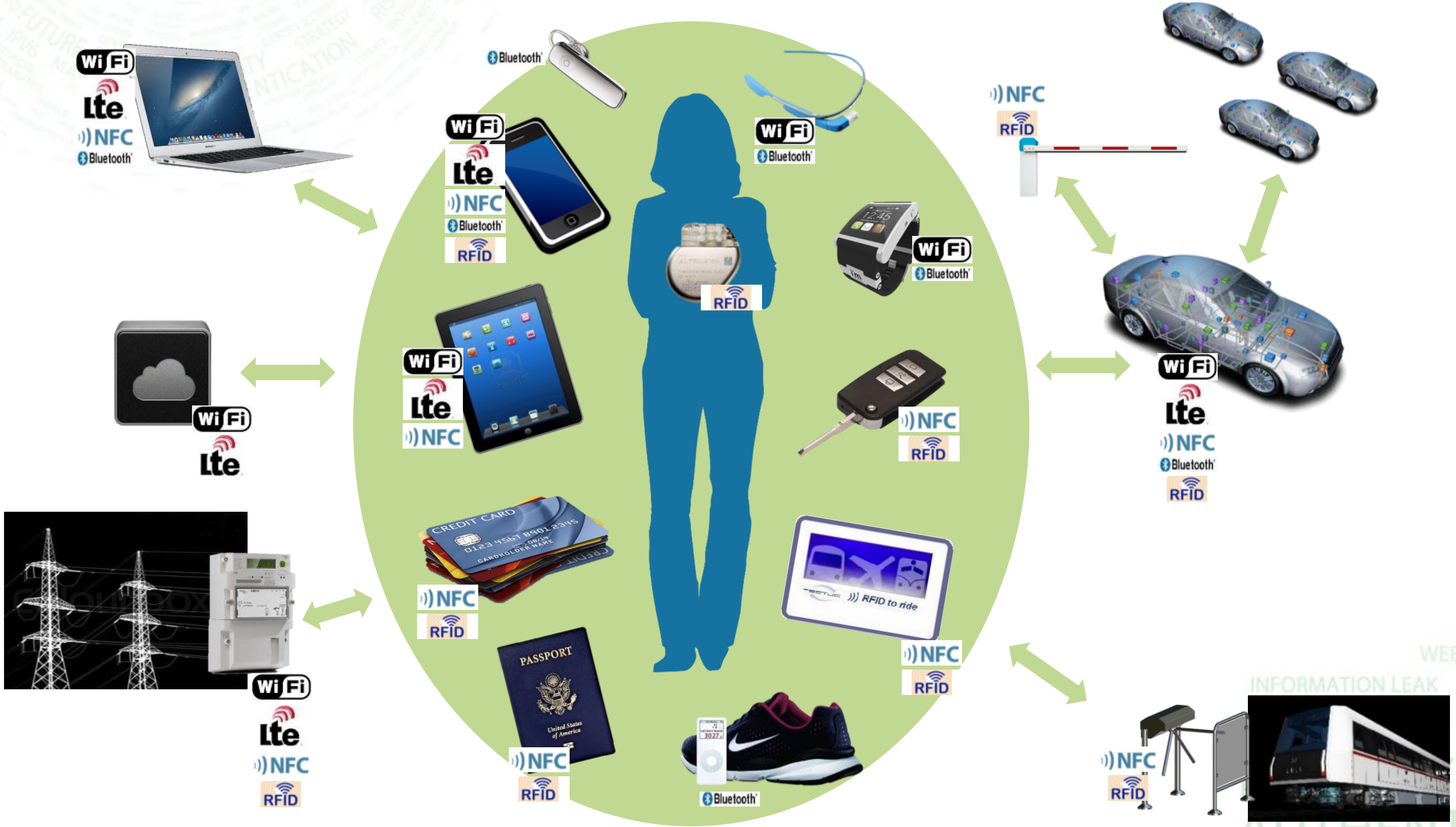
INTRO TO IOT

VLSI ATTACKS

REVERSE ENGINEERING

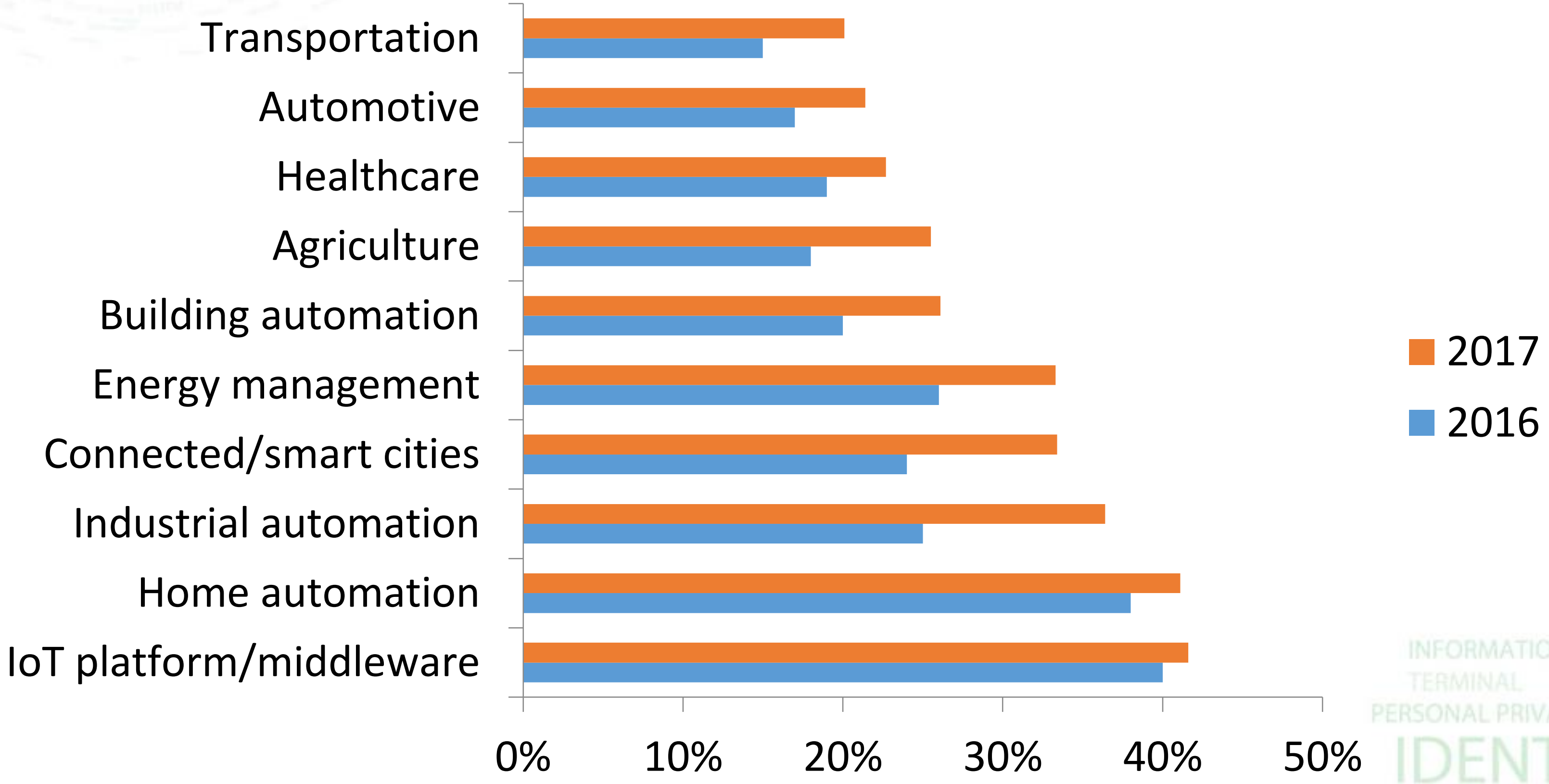
CASE STUDY

Internet of Things (IoT)

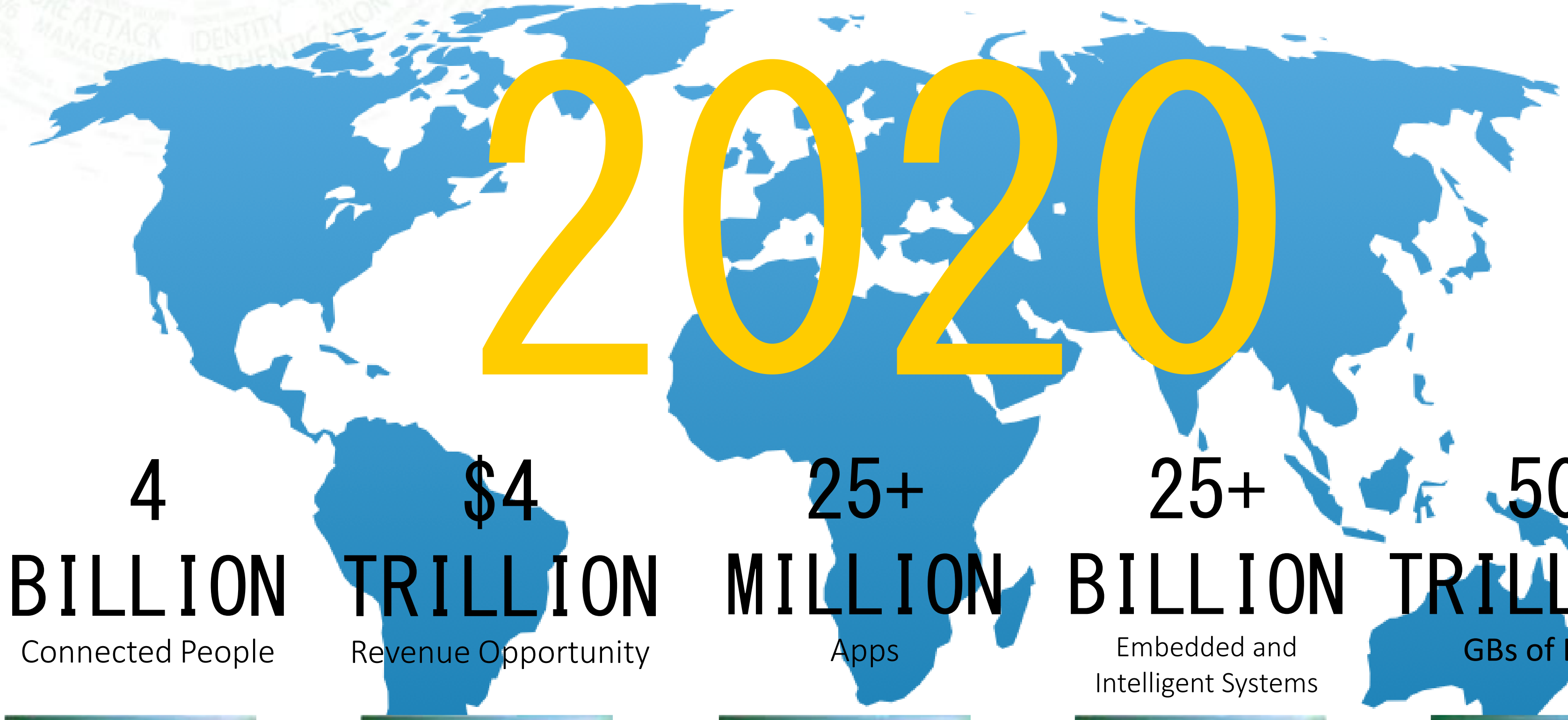


Expanding Adoption of IoT

A Recent Survey of IoT Adoption



Internet of Things (IoT) by 2020



2020

4 BILLION
Connected People

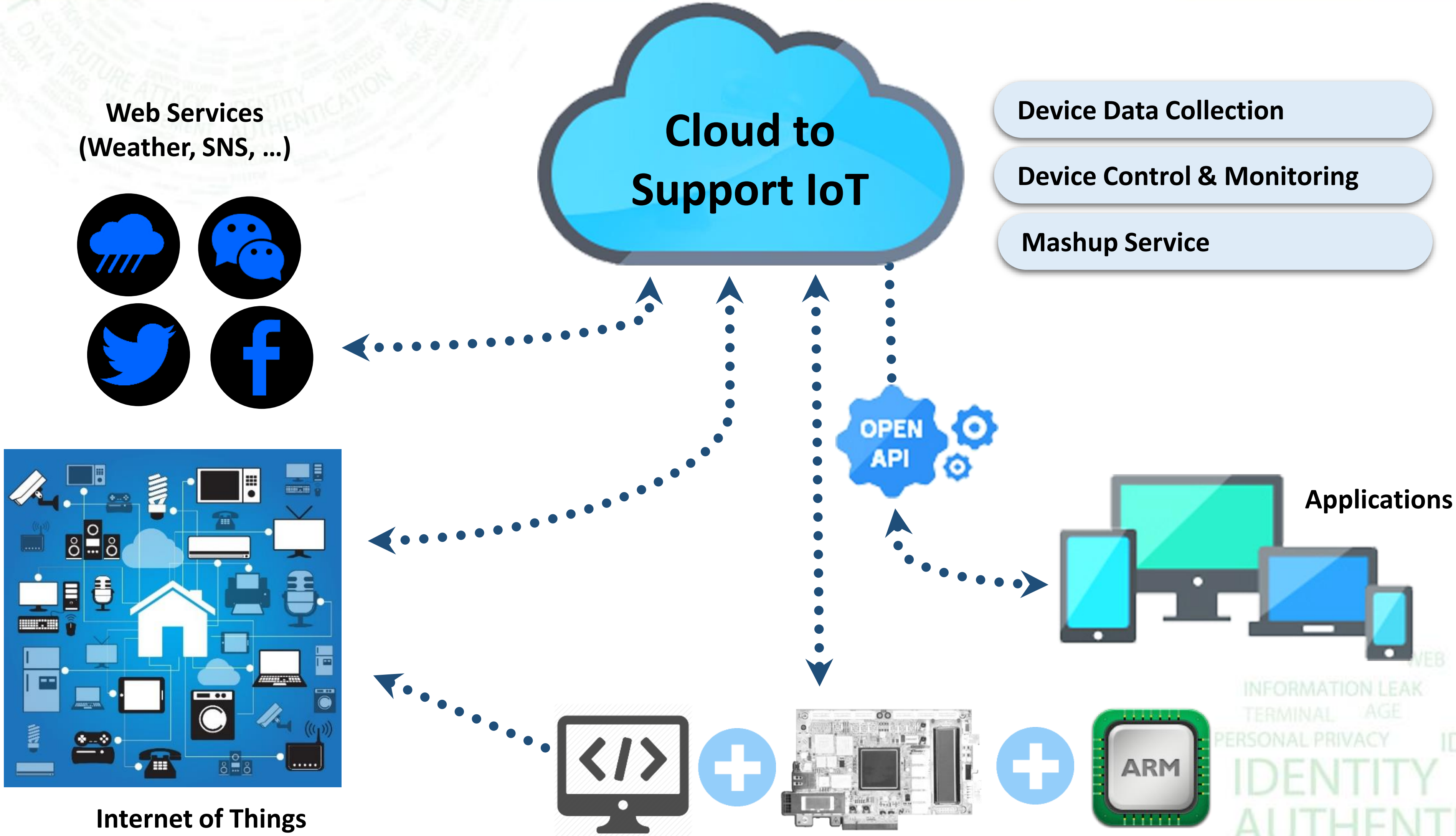
$4 TRILLION
Revenue Opportunity

25+ MILLION
Apps

25+ BILLION
Embedded and
Intelligent Systems

50 TRILLION
GBs of Data

IoT Design and Structure



Cloud to Support IoT

Device Data Collection

Device Control & Monitoring

Mashup Service

Web Services (Weather, SNS, ...)

Internet of Things

Applications

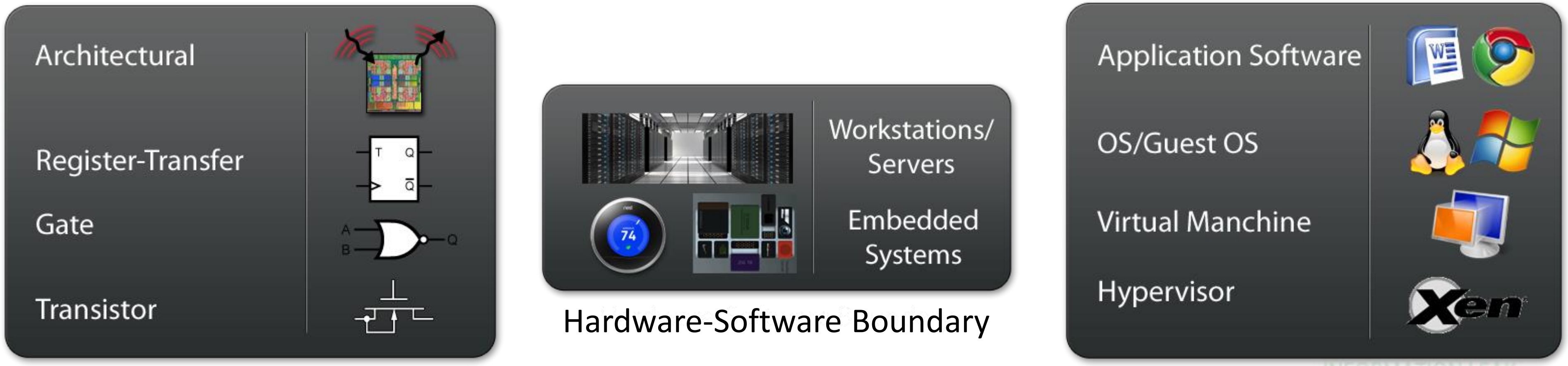
Software Code

Hardware Platform

Microprocessor

How To Ensure IoT Security?

Cross-Layer: Technical cybersecurity solutions should take various layers of computing systems into consideration.



Architectural

Register-Transfer

Gate

Transistor

Hardware Layers

Workstations/ Servers

Embedded Systems

Hardware-Software Boundary

Application Software

OS/Guest OS

Virtual Manchine

Hypervisor

Software Layers

Layered View of Computing Systems

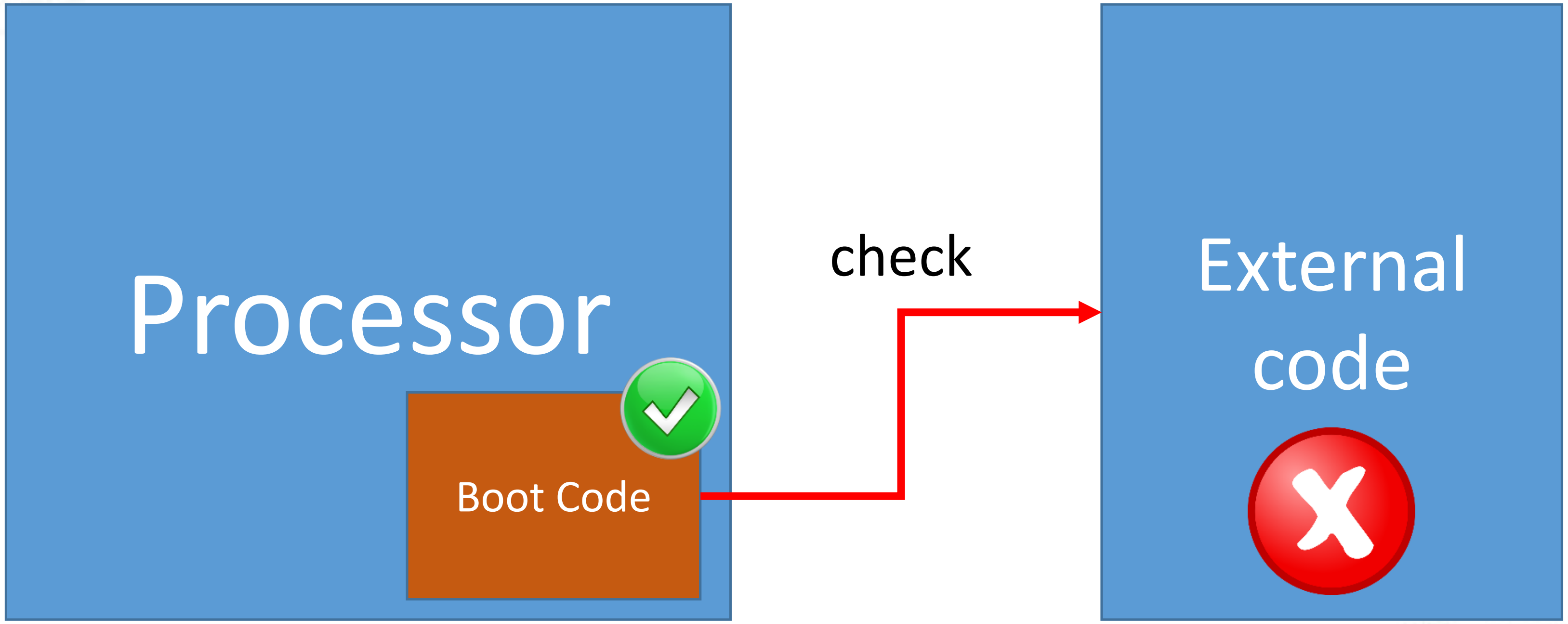
WHY INTEGRATED CIRCUITS (IC, AKA VLSI) SECURITY

Introduction to Secure Boot

Establish a root of trust

➔Start code execution from a trusted source

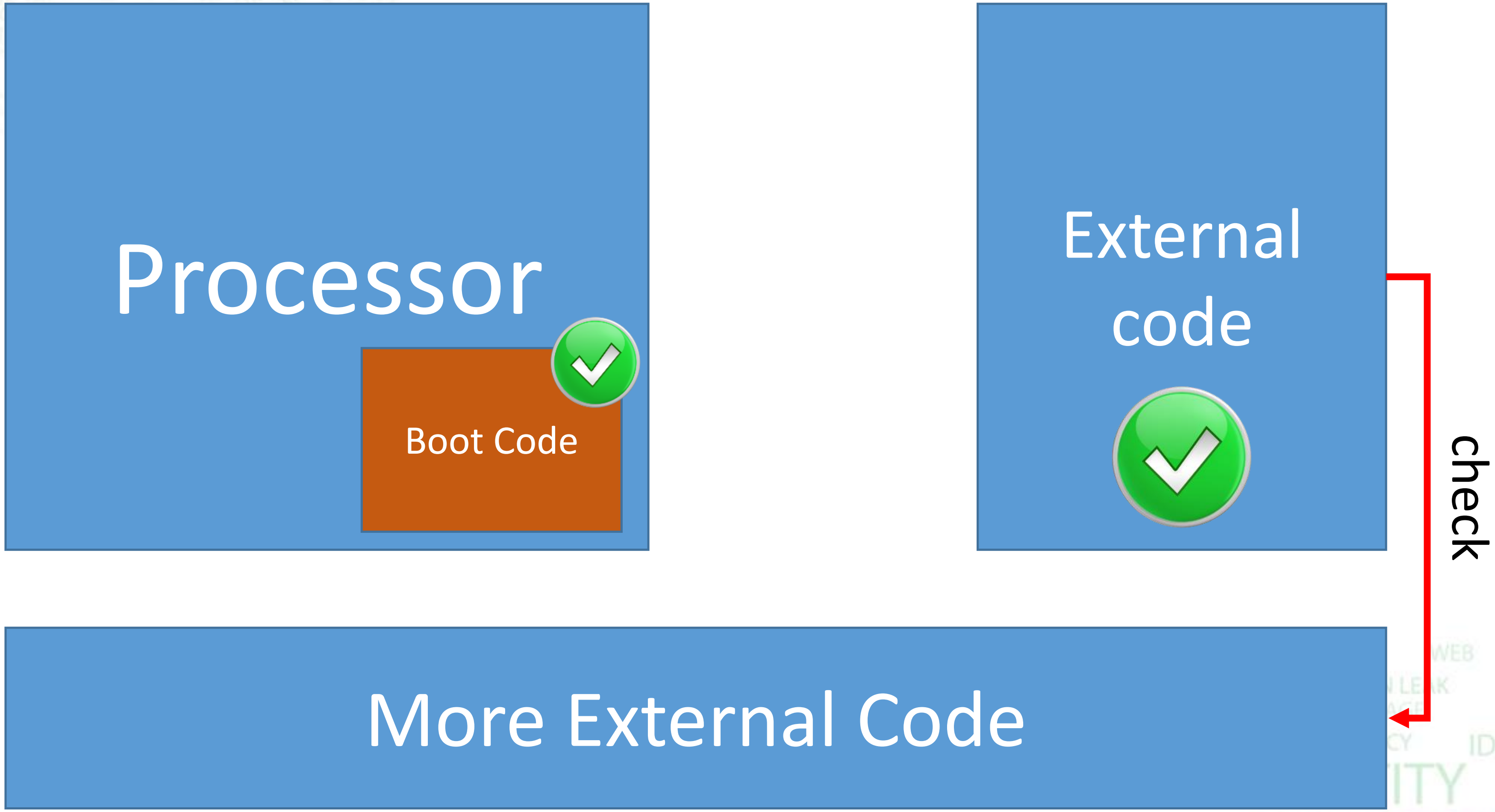
➔Have trusted source check next step of the code chain



Pass: execute

Fail: panic()

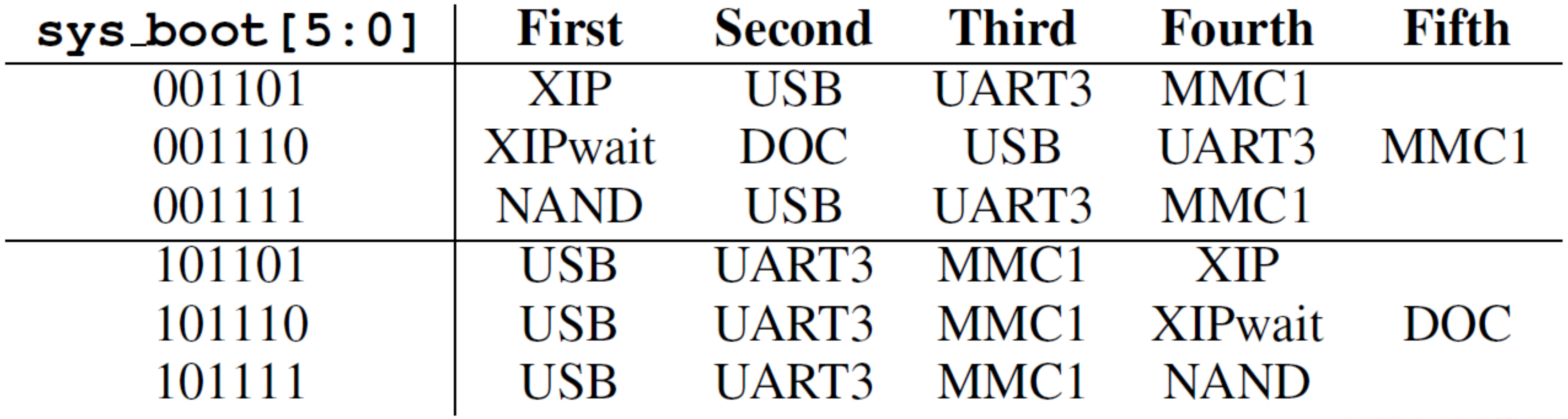
Secure Boot Chain



Bypassing Boot Process

Boot Process Security Validation

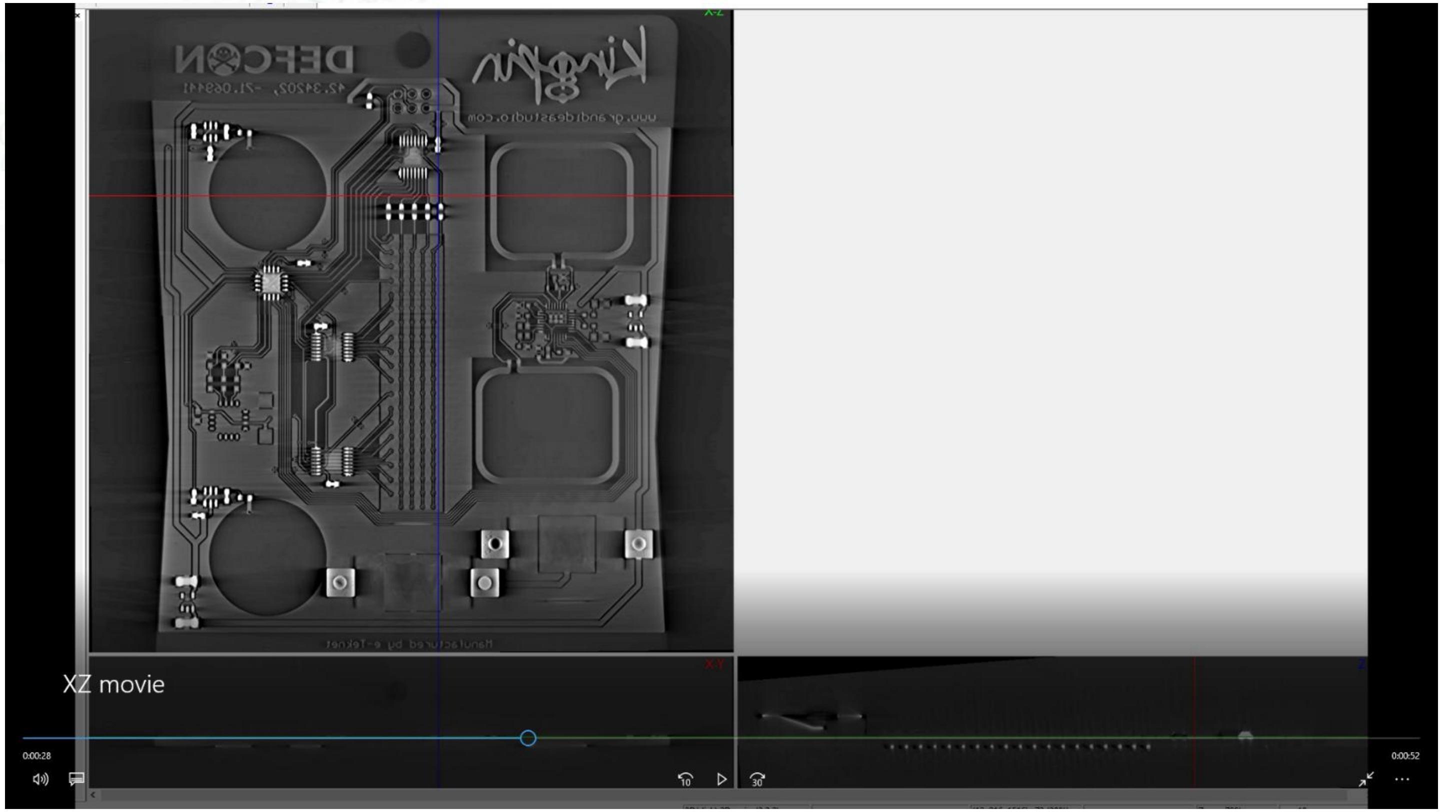
- Modern SoCs are designed to provide high flexibility
- Dilemma: Flexibility vs security
- Task: Evaluate the security implications of all possible boot configurations
- Case study: TI Sitara AM3703 SoC



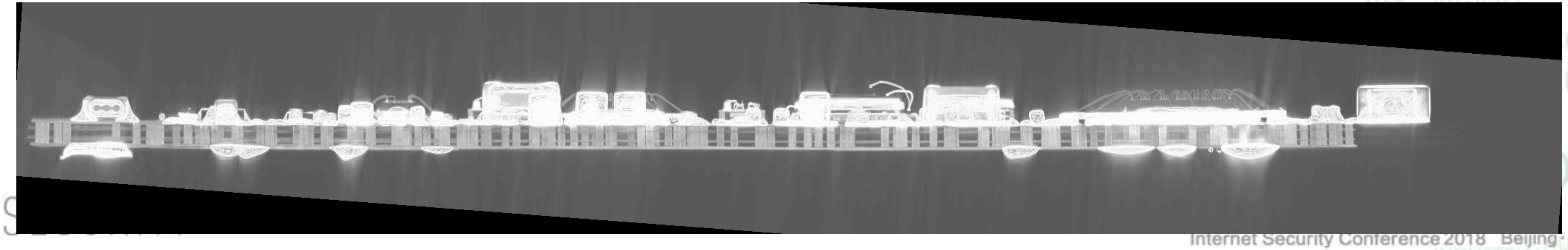
sys_boot[5:0]	First	Second	Third	Fourth	Fifth
001101	XIP	USB	UART3	MMC1	
001110	XIPwait	DOC	USB	UART3	MMC1
001111	NAND	USB	UART3	MMC1	
101101	USB	UART3	MMC1	XIP	
101110	USB	UART3	MMC1	XIPwait	DOC
101111	USB	UART3	MMC1	NAND	

PCB Reverse Engineering

Top view



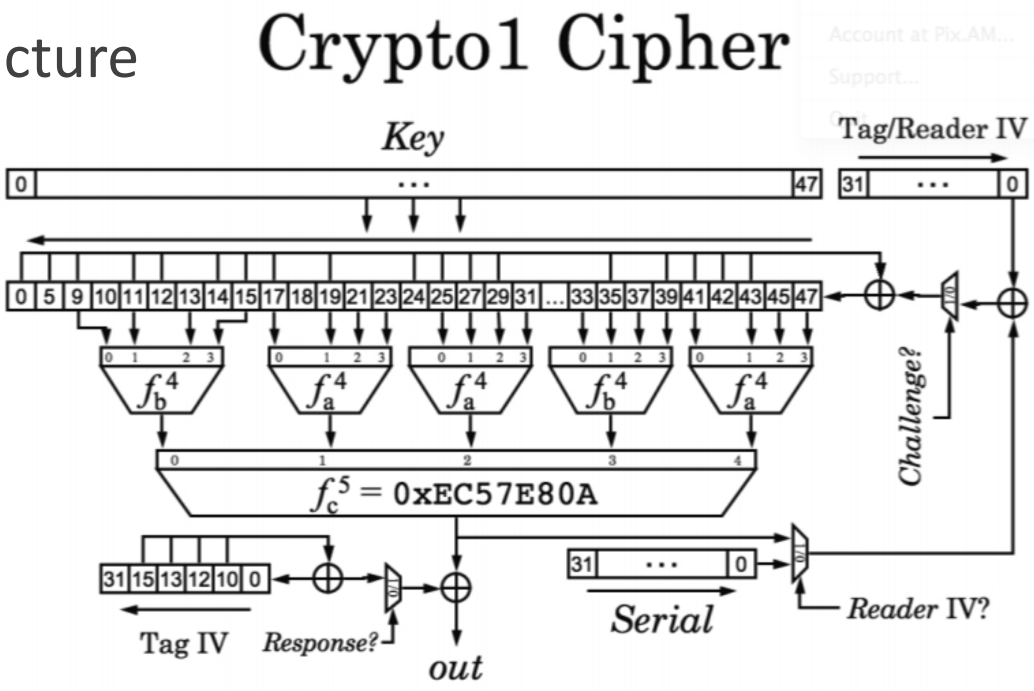
Side view



Chip Reverse Engineering

NXP Mifare

- Proprietary cryptographic algorithm: CRYPTO-1
- Reverse engineering: Algorithm and LFSR structure
- Widely used in ID cards



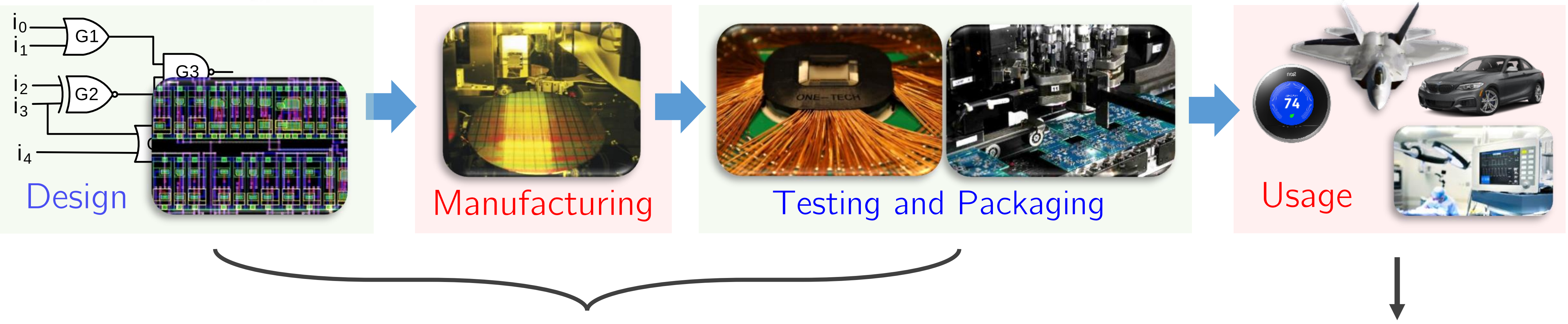
f_a^4 = 0x9E98 = (a+b)(c+1)(a+d)+(b+1)c+a

f_b^4 = 0xB48E = (a+c)(a+b+d)+(a+b)cd+b

Tag IV ⊕ Serial is
loaded first, then
Reader IV ⊕ NFSR

IC Supply Chain

Global Integrated Circuit (IC) Supply Chain



Design

Manufacturing

Testing and Packaging

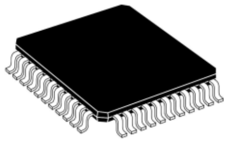
Usage

What hardware developers see.

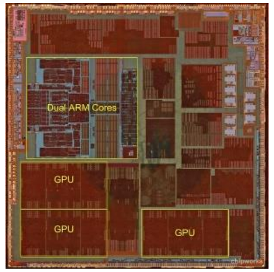
What software developers see.

Integration Circuit (IC) Reverse Engineering

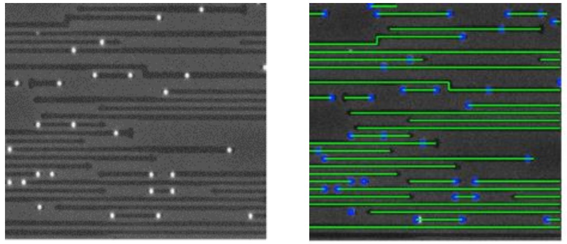
- Netlist recovery by a foundry or end-user threatens intellectual property and facilitates system level exploitation.



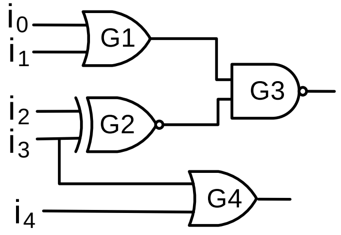
Packaged IC



Die



Delayering, Imaging, Recognition

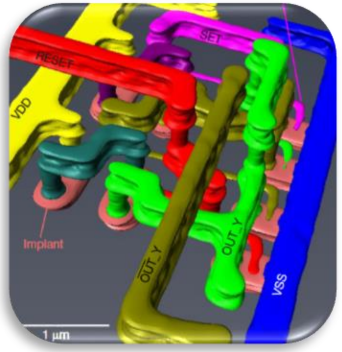


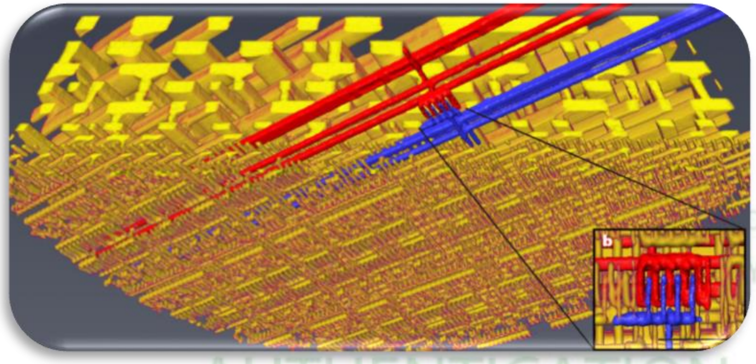
Netlist

- The technology is advancing…

High-resolution non-destructive three-dimensional imaging of integrated circuits

Mirko Holler[1], Manuel Guizar-Sicairos[1], Esther H. R. Tsai[1], Roberto Dinapoli[1], Elisabeth Müller[1], Oliver Bunk[1], Jörg Raabe[1] & Gabriel Aeppli[1,2,3]





FICS Research SeCurity and AssuraNce (SCAN) Lab

Courtesy of FICS @ UF

Imaging and Circuit Edit Capabilities

2000 µm³/s 200 µm³/s 20 µm³/s Milling rate

Nondestructive

Destructive

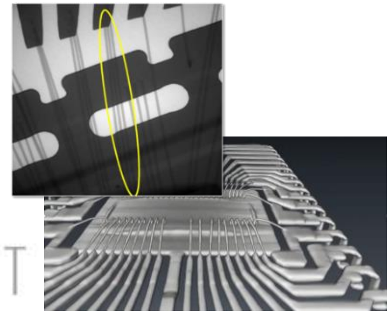
Skyscan 2211
(X-ray Micro CT)

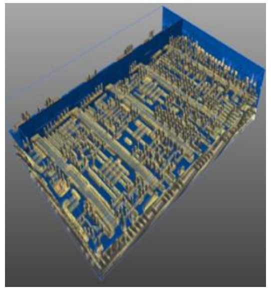
FERA3-GMH
(Plasma FIB-SEM)

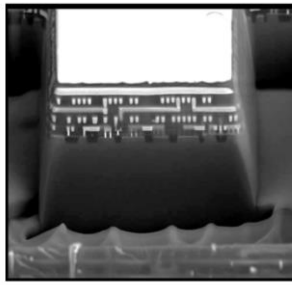
LYRA-3 XMH
(Gallium FIB-SEM)

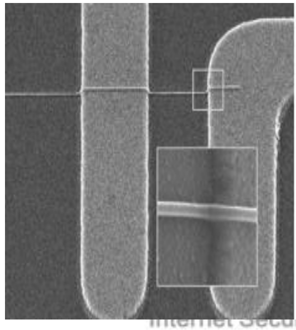
Orion NanoFab
(He-Ne FIB)

100 µm 1 µm 100 nm 10 nm 1 nm Imaging Resolution









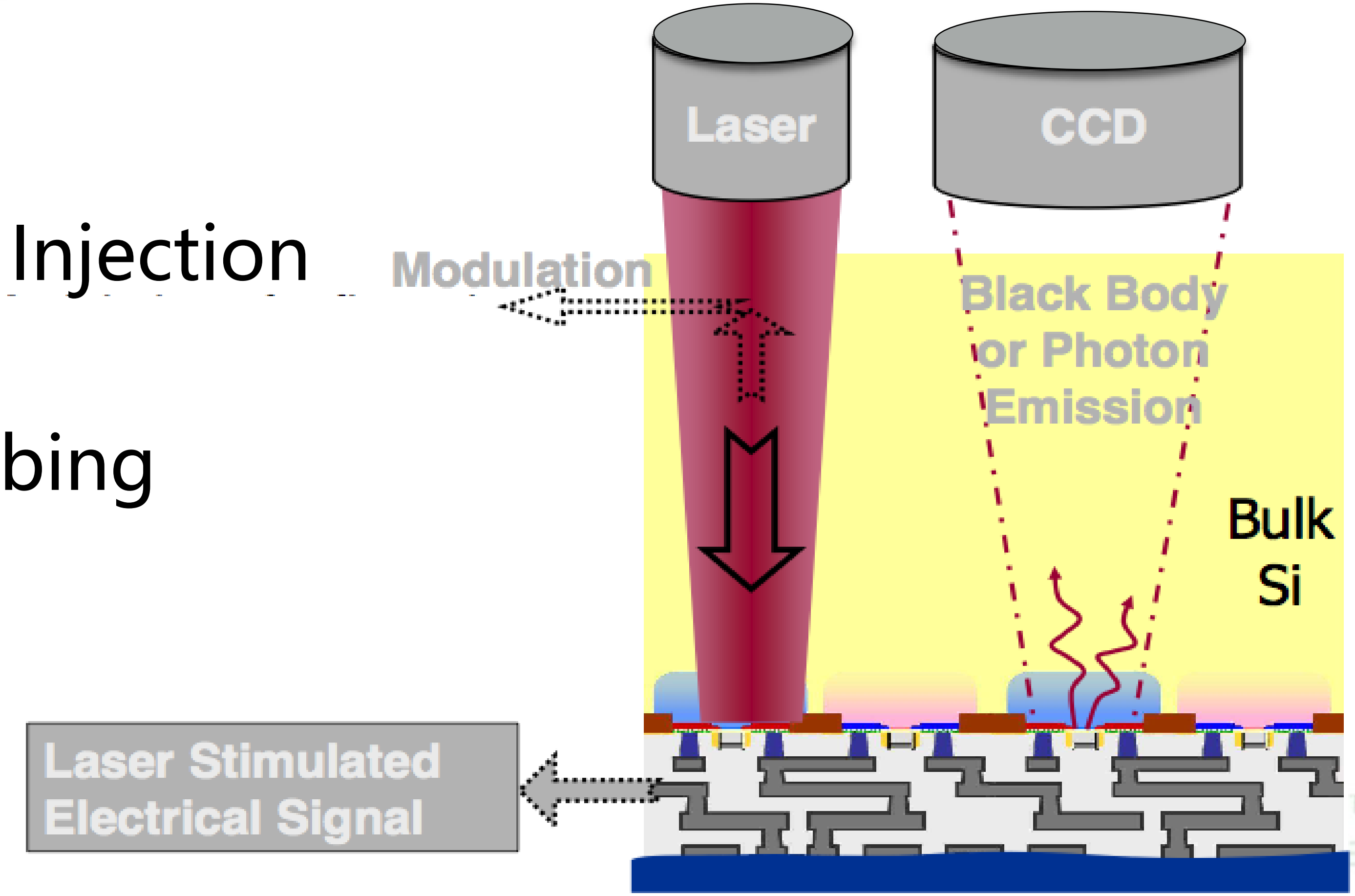
Courtesy of FICS @ UF

Optical Backside Analysis

Photon Emission

Laser Stimulation/Fault Injection

Optical Contactless Probing


Laser
CCD
Modulation
Black Body or Photon Emission
Bulk Si
Laser Stimulated Electrical Signal

Courtesy of Shahin Tajik @ FICS

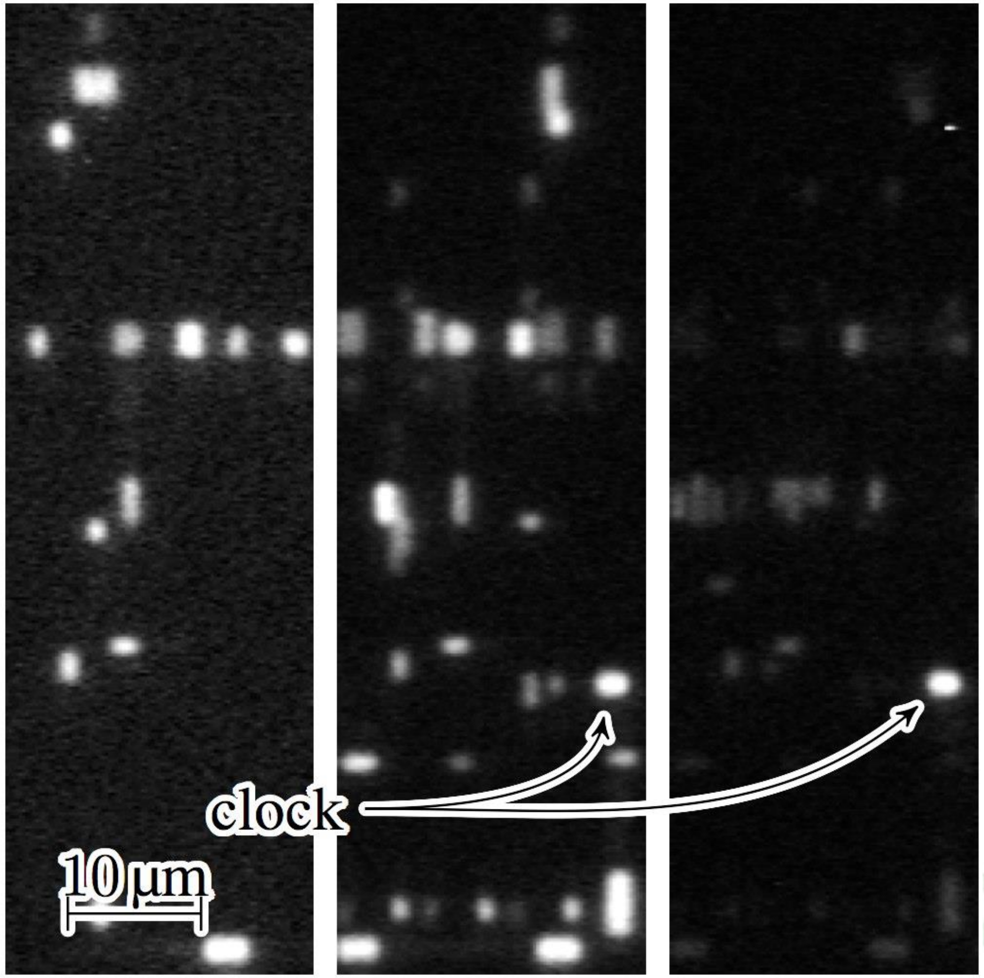
PHOTON EMISSION ANALYSIS (PEM)

Combinatorial vs. Sequential Logic

Combinatorial Logic: AND, OR, NOT, XORs, etc.

Sequential Logic: Counter, Shift Register, State Machines, etc.

Presence of Clock in Sequential Logic



Altera MAX V (180 nm)

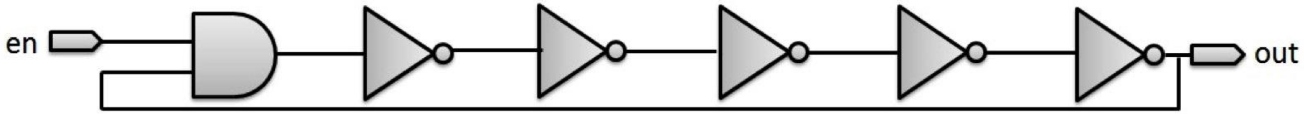
Courtesy of Shahin Tajik @ FICS

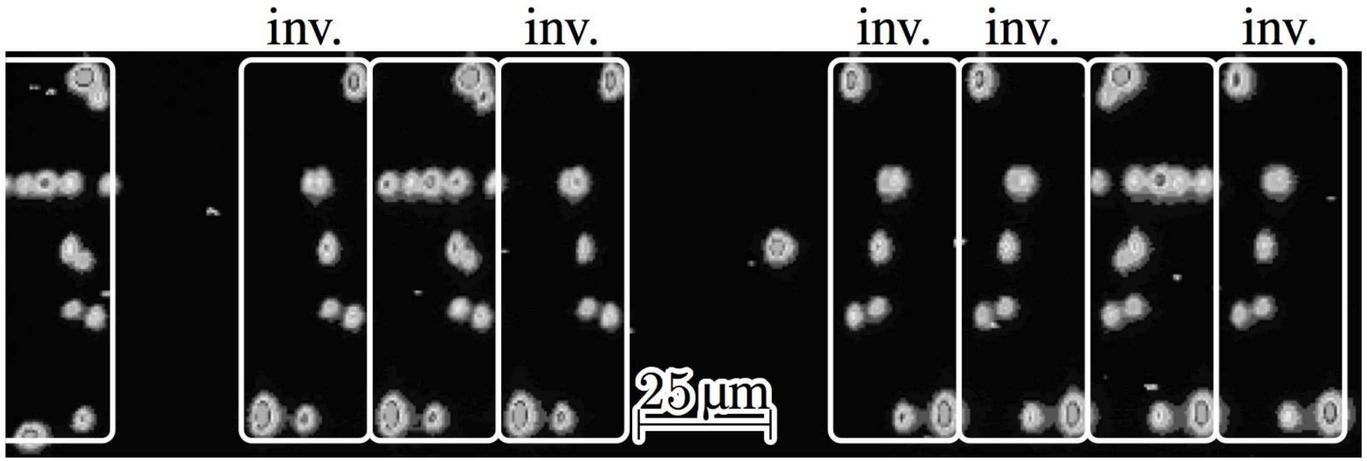
Ring-Oscillator Emission

Identical Switching Frequency by all LEs

Switching frequency independent and generally higher than clock frequency

Applications: TRNG and Internal Clocks





Altera MAX V (180 nm)

Courtesy of Shahin Tajik @ FICS

Conclusions

IC SECURITY

REVISITING IOT SECURITY

WORKFORCE GENERATION

HARDWARE FOR SOFTWARE

ISC 2018
ISC 互联网安全大会

360互联网安全中心

THANKS

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China