Hardware Security in the Connected World:
An Overview on Side Channels and PUFs

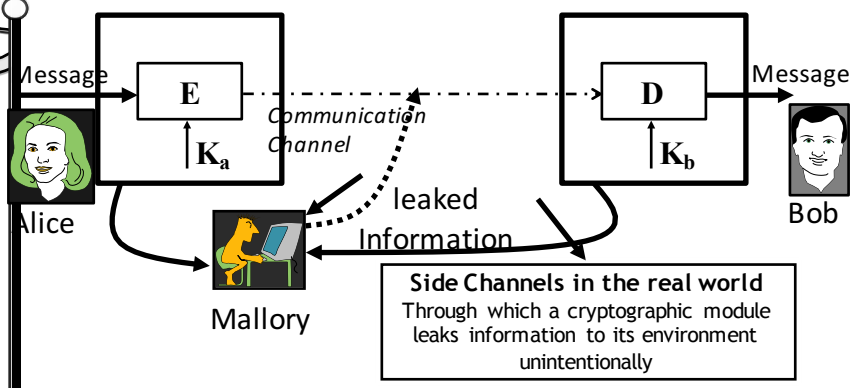
Professor
Debdeep Mukhopadhyay

Secured Embedded Architecture Laboratory (SEAL)
Department of Computer Science and Engineering
IIT Kharagpur
debdeep@cse.iitkgp.ac.in, debdeep.mukhopadhyay@gmail.com

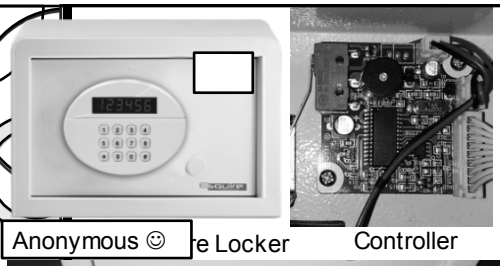
Agenda for the Talk

- Introduction to SEAL, IIT Kharagpur
- Internet of Things and Side Channel Analysis
  - Power & Fault Attacks
- Lightweight Authentication of Devices

Embedded Security:
The Gap between Theory and Practice

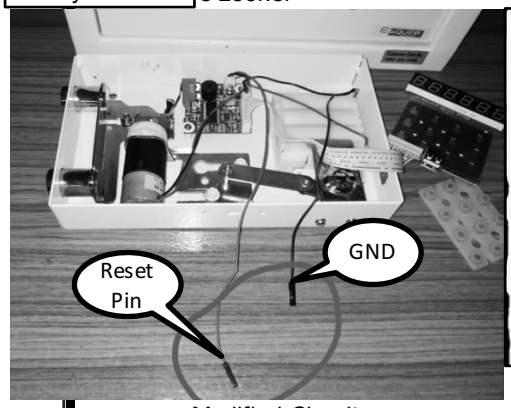


Cryptographic Theory has limitations.
There is an absence of theory for the reality!
Even mathematically strong ciphers leak in the real world!

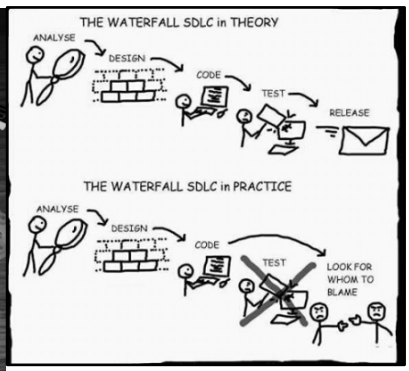


Anonymous ☺ e Locker Controller

**"In theory there is no difference between theory and practice.
In practice there is"**



Modified Circuit



Professor-in-Charge

Debdeep Mukhopadhyay
(Professor)

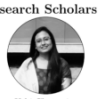
Associated Faculty Members

Rajat Subhra Chakraborty
(Associate Professor)

Soumyajit Dey
(Associate Professor)

Aritra Hazra
(Assistant Professor)

Research Scholars



Urbi Chatterjee

Mansar Alam

Sayandeep Saha

Rajat Sadhukhan

Arnab Bag

Boyapally Harishma

Anirban Chakraborty

Durba Chatterjee

Akashdeep Saha

Siddhartha Chowdhury

Soumyadyuti Ghosh

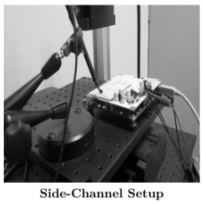
Kuheli Pratihar

Lab Attendant

Joydeep Chowdhury

The Seal Family

Laser Injection System

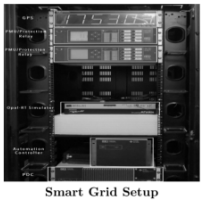


Side-Channel Setup

Temperature Chamber

Crossbeam-340 Setup

IoT Setup



Smart Grid Setup

Instruments ... putting "Life" into our Research

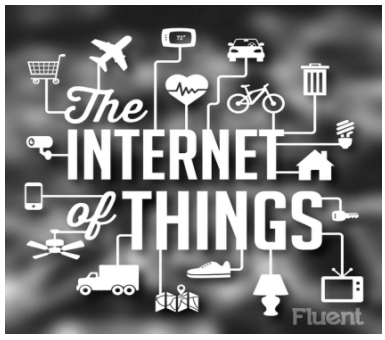
Side Channels
IoT Security
CPS Security
Hardware Forensics

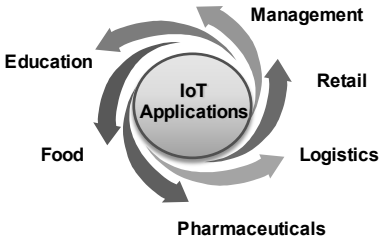
Agenda for the Talk

- Introduction to SEAL, IIT Kharagpur
- Internet of Things and Side Channel Analysis
  - Power & Fault Attacks
- Lightweight Authentication of Devices

Internet of Things (IoT): Next Generation Networks

- IoTs will extend today's internet much further, connecting a wide spectrum of devices.
- It is estimated that by 2020, 21 billion devices will be internet connected, which includes critical device, like cars, pacemakers, electrical grids.





IoTs can revolutionize quality of life
However, commercial IoT devices lack security measures!
Can have catastrophic consequences to mankind.

Applications of IoT: Indian Context

- **Nano-sensors** can be used to monitor water quality at reduced cost
- Nano-membranes can assist in the treatment of waste-water.
- **Food Control:** Control geographical origin, Food production management, Nutrition calculations

- Sensor technologies can monitor vulnerable environments and limit **natural disasters.**
- **E-governance:**
  - Warehouse, management
    - Inventory control
  - Port management
    - Ships, boats, containers, etc.
- **Pharmaceuticals:**
  - Intelligent tags for drugs
  - Drug usage tracking, Pharmaceuticals: Product websites
  - RFIDs can be used to track the origin of safe drugs thereby reducing counterfeits.

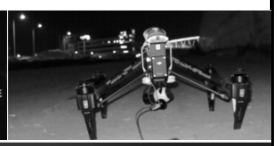
→ Enable the emergency treatment to be given faster and more correct.

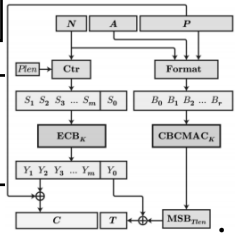
Need to integrate security into the IoT by developing novel secured protocols for interactions of multiple components, which are secured against these menacing threats.

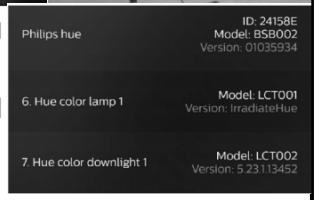
Side Channel Analysis(SCA)- A Powerful Method to Break Cryptographic Keys

Introduction

- Industry standard cryptographic techniques can be disrupted
- Breaking the key does not require physical access to secure memory area of device



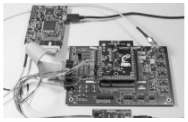


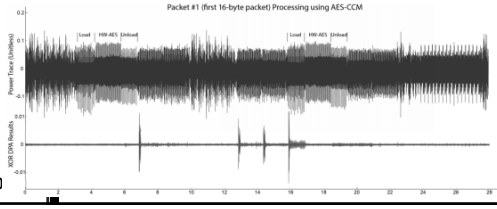


Demonstration

- A Correlation Power Analysis (CPA) attack against the AES-CCM mode used to encrypt and verify firmware updates, allowing adversary to encrypt, sign and upload malicious OTA updates to infect Philips Hue lamps

Experimental Setup



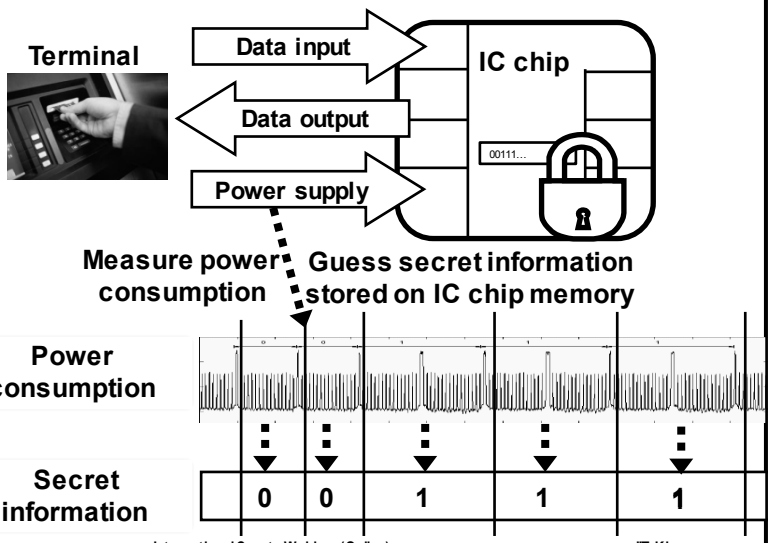


Results

- The modified firmware by the adversary was accepted by the Hue light (the version number is modified to IrradiateHue)
- Recover complete original Bootloader by the manufacturer
- A self-spreading worm was spread using the combined ability to sign and encrypt arbitrary binaries- long-range take-over attack

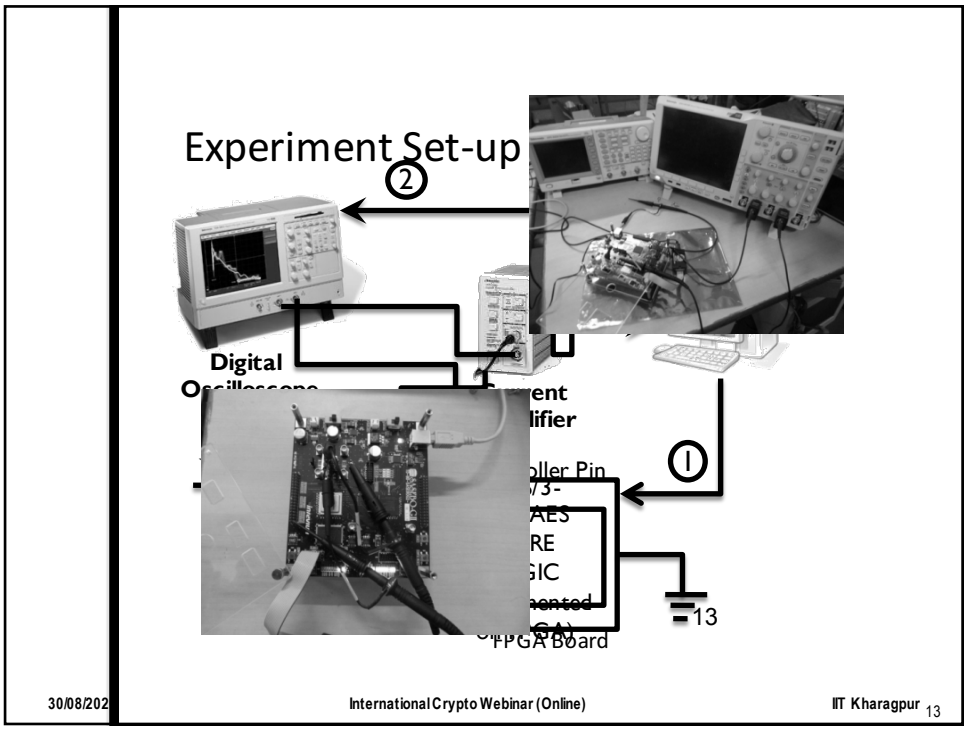
E. Ronen, A. Shamir, A. Weingarten and C. O'Flynn, "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2017, pp. 195-212. doi: 10.1109/SP.2017.14

Strong cryptographic algorithms are just the beginning!



What are Side Channels?

- These are covert channels which leak information which the designers of cryptographic algorithms did not consider.
- Information is leaked because of the implementation:
  - optimization leads to information leakage
  - example: **an if-else statement in a programming language**

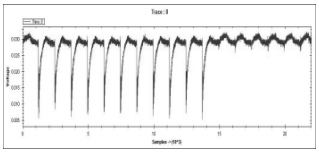


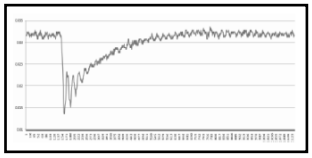
Power Attacks

- SPA – Simple Power Analysis attacks
  - Fact exploited - Power consumption at an instant of time is a function of the operation being carried out by the device
- DPA – Differential Power Analysis
  - Fact exploited - Power consumption of the same operation at different instants of time depends on the data being processed.

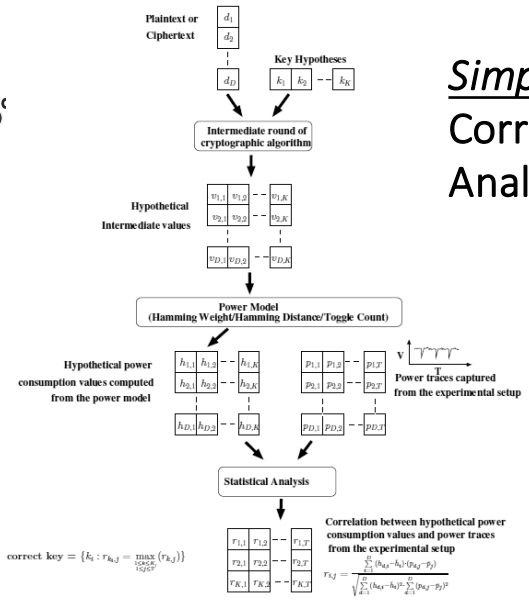
Paul C. Kocher, Joshua Jaffe, Benjamin Jun: Differential Power Analysis. CRYPTO 1999: 388-397

A Power Trace

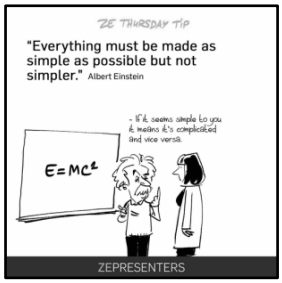




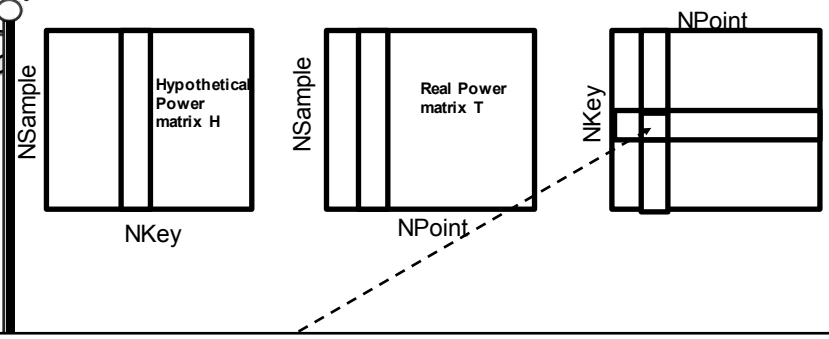
- Power Trace of a round of AES.
- Observe the variation of power values.
- The variations occur because of the operation dependence of power: leads to SPA.
- The variations also occur because of data dependence of power: leads to DPA.



Simple illustration of Correlation Power Analysis



Correlation Matrix



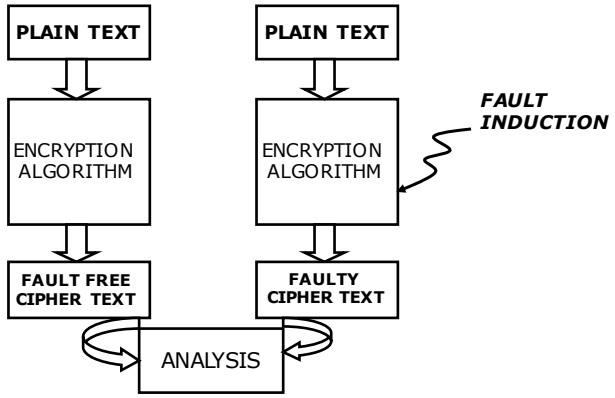
$$C[i][j] = \frac{\Sigma_{k=0}^{NSample}(hPower[i][k] - meanH[i])(trace[j][k] - meanTrace[j])}{\Sigma_{k=0}^{NSample}(hPower[i][k] - meanH[i])^2 \Sigma_{k=0}^{NSample}(trace[j][k] - meanTrace[j])^2}$$

ESP-Anweshak: Side Channel Evaluator & Analyzer

ESP

- Built on Open Source Platforms
- Combined Analyzer for both Power and Fault
- Entirely built using Python
- Take care of Handshaking between FPGA and PC
- Oscilloscope can be controlled using the tool: Allowing Remote Access

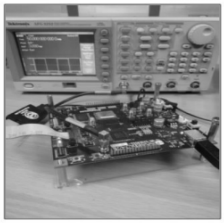
Fault Attacks: Differential Fault Analysis (DFA)



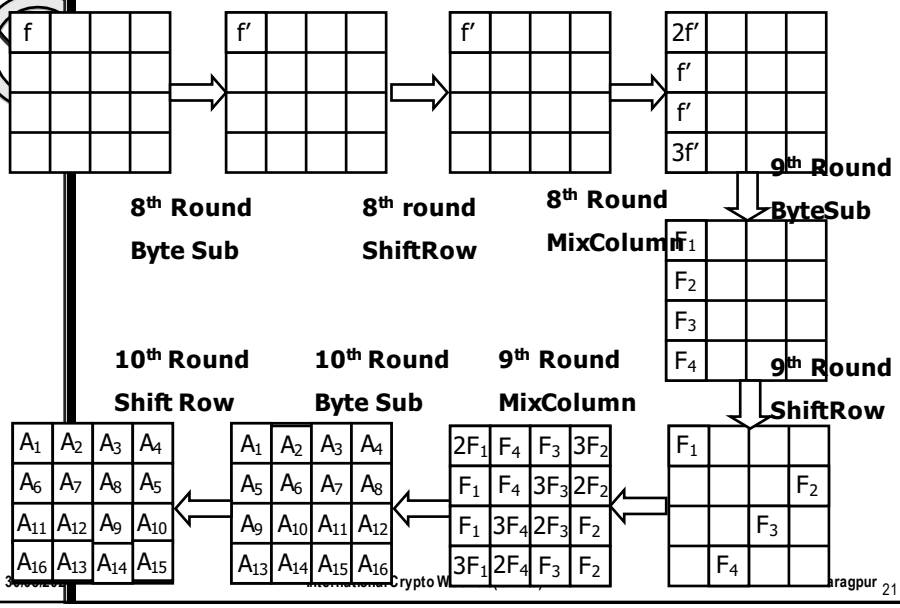
19

Fault Injection Techniques

- Clock Glitches
- Voltage Glitches
- Electromagnetic Attacks
- Optical attacks
- Laser Guns



Propagation of Fault Induced



DFA on AES

A Single Fault can reduce the AES Key Size to around 2^8 values.

- **Time Complexity~2^{30}**

A double fault uniquely retrieves the Key!

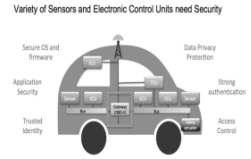
Michael Tunstall, Debdeep Mukhopadhyay: Differential Fault Analysis of the Advanced Encryption Standard using a Single Fault. IACR Cryptology ePrint Archive 2009: 575 (2009)

Michael Tunstall, Debdeep Mukhopadhyay, S,Ali, Differential Fault Analysis of the Advanced Encryption Standard using a Single Fault, Cryptology ePrint Archive: Report 2009/575, WISTP 2011

https://www.youtube.com/watch?v=y67QwAuKV6E&list=PLbRMhDVUMngfulSvKL0cT-tn8ULtERsWk&index=49&t=0s

Fault Injection on Automotive Chips

- MCUs are foundational units for the modern car.
- Reliability and safety is a major concern:
  - ISO 26262: framework for the development of safe automotive electronic systems.
  - Defines the Automotive Security Integrity Level (ASIL) [levels A to D]
- Protect against faults during normal operations.
- Many of these protections are also suggested in security literature, like duplication.
- **Taken for granted that MCUs implementing ISO 26262 recommendations are protected against Fault Attacks!**



A Case Study to Show the Myth

- ASILD1: Implements an ARM Cortex-R4 core
- ASILD2: Implements a PowerPC e200
  - Two of the most prevalent architectures in the safety electronic industry.
- In both these targets mechanisms include a dual core CPU for Simple Time Redundancy with Comparison and memories with error correction codes (ECC) and parity bits, as recommended by ISO 26262 part 5.

- Fault Injection Tools:
  - VC Glitcher
  - FPGA enabled generator of voltage glitches (2 ns precision), and input to an EM pulse emitter device (for EM glitching)
  - Target has a pin to trigger the glitch generator.
  - A device analyzes the power consumption of the target, and generates a trigger signal when a programmable reference pattern is detected.

Glitching

- Effectiveness depends on time of glitch, shape of glitch.
- These can be modeled though glitch length, glitch intensity (voltage or EM field), time offset from the trigger signal.
  - For EM signal, the point on the chip surface is also crucial.
- Objective: Glitches which creates an error and bypass the check.

Experiment 1: unroll

```
trigger_up( )
 asm(add r1 #1)
 asm(add r1 #1)
...
 asm(add r1 #1)
 asm(add r1 #1)
trigger_down()
send_serial(r1)
```

Experiment 2: auth

```
flag=1
trigger_up()
If(flag==0)

send_serial_authenticated
()
 else
    send_serial_denied()
trigger_down()
```

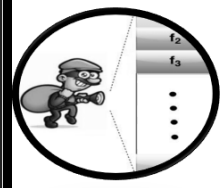
Experiment: A total of ~720,000, ~550,000 glitches were injected on ASILD1 and ASILD2 for 3 weeks.

	unroll		auth	
	Voltage	EM	Voltage	EM
ASILD1	87%	0.2%	60%	0.2%
ASILD2	0%	18%	N/A	57%

Post-Mortem

- ASILD-1 reports the fault detection mechanisms (unlike ASILD-2):
  - 84%-98% of detected glitches were due to output comparisons, across experiments
  - The next frequent detection was based on Flash and RAM parity bits (around 18 to 25%).
  - Note that a glitch can trigger several detections simultaneously.
- **A single glitch more effective!:**
  - A possible analysis (we don't have accurate information) is that the glitch affects the same instruction but in different stages of pipeline, resulting in similar output signals, and is thus missed!

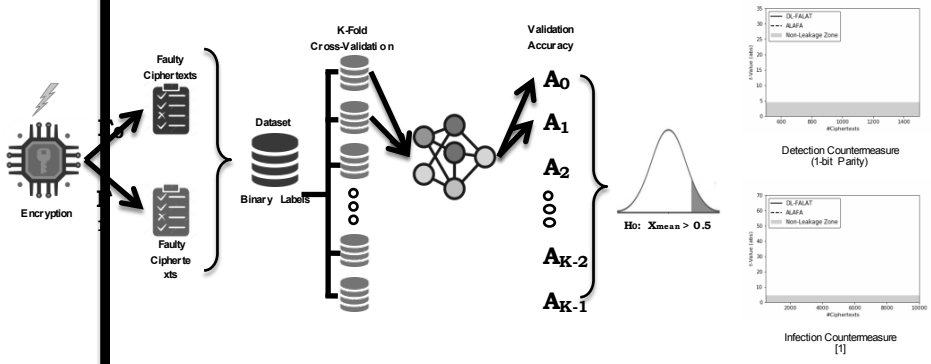
Testing Block Ciphers for Fault Attacks



Securing cryptographic devices against fault attacks

- Several countermeasures exist :
  - Either extremely resource hungry
  - Or not robust against all possible faults
    - Broken!!!
- Malicious faults are highly repeatable.
- Different fault models.
- **How do we know what is secure and what is not?**

DL-FALAT: Overview of the Methodology



[1] B. Gierlichs, J. Schmidt, and M. Tunstall. Infective computation and dummy rounds: fault protection for block ciphers without check-before-output. In LatinCrypt'12, pages 305–321. Springer, 2012.

Demonstration on SCA Tools

https://www.youtube.com/watch?v=j5ISb-JCeUQ&feature=share&fbclid=IwAR3APYaQ6l2X6eAyAZP5RLAvOQvs44vXsSAMTqmSOWnlQjj7URizqKbmBHc

Agenda for the Talk

- Introduction to SEAL, IIT Kharagpur
- Internet of Things and Side Channel Analysis
  - Power & Fault Attacks
- Lightweight Authentication of Devices
  - Physically Unclonable Functions (PUFs)
  - Authentication using PUFs

Security and Privacy in Context to IoT

- **The IoT has no protection against attacks**
- **Seamless information** exchange without user intervention implies need for adequate security measures
- But this ease-of-use and seamlessness should not facilitate certain classes of **implementation-specific attacks:**
  - **Side-channel attacks** (which utilize leaked information to compromise the security of secure systems)
- Design **low-overhead** IoT that are sufficiently robust against side-channel attacks:
  - IoT subsystems are **resource constrained**!
  - **Need light-weight** solutions.

Debdeep Mukhopadhyay, PUFs as Promising Tools for Security in Internet of Things. IEEE Design & Test 33(3):103-115(2016)

A Case Study of Security Weakness: A Simple Eavesdrop Attack on Philips Hue Wireless Lighting System

- **Allows the user to wirelessly control the lighting system in home via Philips Hue App for Android and iOS.**

•When the app was launched, the hashed value of the MAC address of the device was used to create the username and was "white-listed" in the bridge.

•If the attacker knows the MAC address of the device, she can easily retrieve the username of the device.

• Later, this mechanism was changed.
•But the communication is now in plain text!

If the attacker can capture traffic between a legitimate user and Hue bridge, then it can be used to extract the bridge's IP and all "white-listed" usernames using a python script.

1: User name is time of reg

2: While sending anycomm in W

3: Using IP Address of the Bridge and the username, entire white-list of the Bridge is exposed.

Fortifying IoTs through Key-less Crypto

- Side Channel Analysis is an extremely important topic!
  - It is an art and works in the real scenarios.
- Side Channels make conventional cryptography challenged:
  - Overheads are huge.
  - Counter-measures against one side channel can aid other side-channels.
- Cryptographic keys are stored in memory, which could be a point of attack: Row-hammer bugs.
- With more advancement in computer architecture, more vulnerabilities are introduced.
- What would be the way ahead?

Debdeep Mukhopadhyay, PUFs as Promising Tools for Security in Internet of Things. IEEE Design & Test 33(3):103-115(2016)

Physically Unclonable Function (PUF)

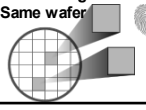
Silicon PUF exploiting CMOS process in defining **device-specific** (**unique**) random mapping

PUF Overview → Our contributions

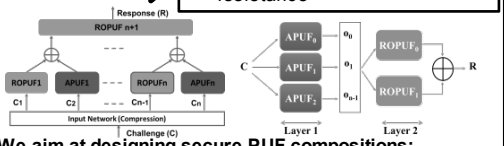
Composite PUF [HOST 2014]:
- A composition of primitive PUFs
- Achieved improved modeling resistance

Physically Unclonable Function:

Same design
Same wafer



Chips with unique and (physically) unclonable fingerprints



Applications:
1) **On-the-fly** private key generation (an alternative for non-volatile key storage)
2) Hardware authentication (**anti-counterfeiting**)

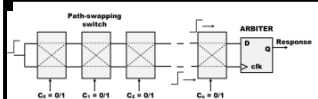
We aim at designing secure PUF compositions:

2013-14
- Design of Low Area-overhead Ring Oscillator PUF with Large Challenge Space [**ReconFig 2013**]
- Composite PUF: A New Design Paradigm for Physically Unclonable Functions on FPGA [**HOST 2014**]

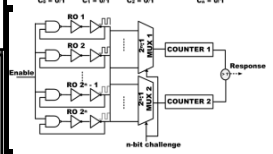
2015
- A Case of Lightweight PUF Constructions: Cryptanalysis and Machine Learning Attacks [**IEEETCAD 2015**]
- Efficient Attacks on Robust Ring Oscillator PUF with Enhanced Challenge-response Set [**DATE 2015**]

2016
- Security Analysis of Arbiter PUF and Its Lightweight Compositions Under Predictability Test [**ACM TODAES 2016**]
- Fault Tolerant Implementations of Delay-based Physically Unclonable Functions on FPGA [**FDTC 2016**]

Arbiter PUF [Lim 2002, MIT]



ROPUF [Suh, 2007]

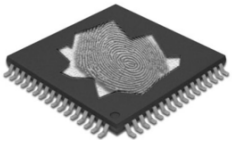


Challenges
- **Model-building and side channel resistant reliable PUF designs on ASICs**
- **ASIC designs need to be experimented with large number of instances of the same PUF design.**
- **Fault Tolerance of PUF ASICs**
- **Test Strategies for PUFs: metrics for assessing architectures of PUFs**

Reliability and Model building attacks are main issues.

What is a PUF?

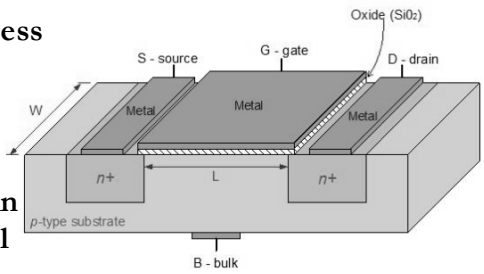
- Fingerprint of Devices



- A challenge-response mechanism in which the mapping between an applied input ("challenge") and the corresponding observed output ("response") is dependent on the complex and variable nature of a physical material
- The challenge-response mapping is unclonable (ideally) and instance-specific (depends on manufacturing process variations evident in ASICs)

Source of variations in MOS devices

- Scaling in CMOS process technology (< 22nm)
- Lack of efficiency in fabrication process
- Introduces variations in MOS device's physical parameters:
  - Gate length (L)
  - Gate width (W)
  - Threshold Voltage (Vth)
  - Oxide thickness (Tox)

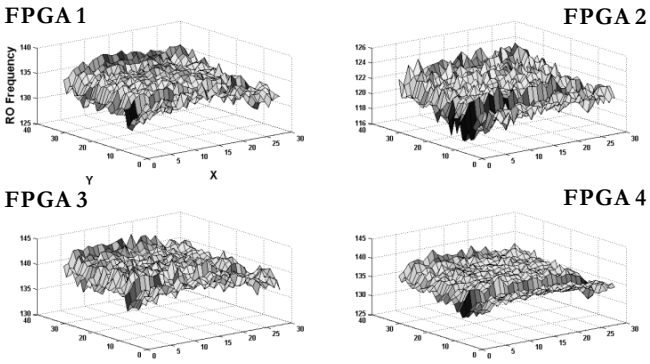


$$i_D = \mu_n C_{ox} \frac{W}{L}[(v_{GS} - V_t)v_{DS} - \frac{1}{2}v_{DS}^2]$$

CMOS scaling → Limitation in fabrication process → Variation in MOS device's physical parameters → Variation in Circuit parameters (e.g., propagation delay, leakage current, etc) → Existence of randomness

Distinguishable variations in CMOS circuit behavior

- Ring Oscillator



Device-unique behavior ➔ Device fingerprint

Advantage PUF!!

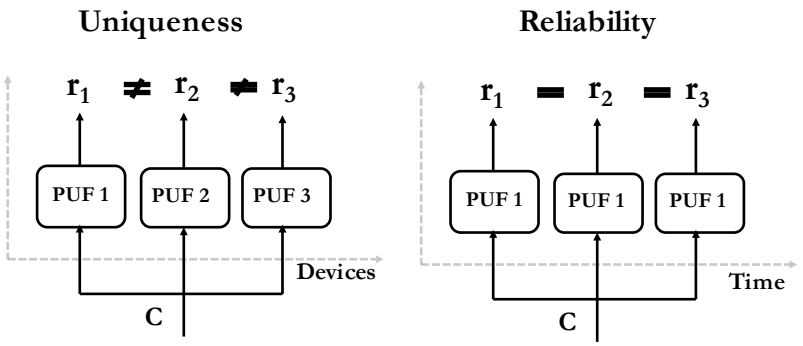
World without PUF

- Trusted party embeds and tests secret keys in a secure non-volatile memory (NVM)
- EEPROM adds additional complexity to manufacturing
- Adversaries may physically extract secret key from non-volatile memory

World with PUF

- Intrinsic properties of device is used to generate secret key.
- Key never leaves the IC's cryptographic boundary, nor be stored in a non-volatile memory.
- Key is deleted after usage in de- or encryption process

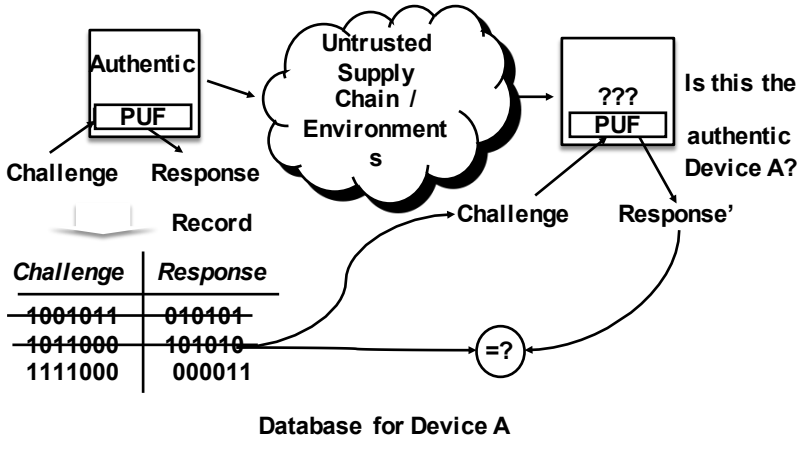
Quality Metrics for PUF



- Uniformity: ratio of 0's and 1's in response
- Bit-dependency: autocorrelation coefficient of response

PUF in Use: Low-cost HW authentication

- Protect against IC/FPGA substitution and counterfeits without using cryptographic operations



Naïve Authentication

Limitations:

1. **The bare CRPs are used.**
2. **If adversary can collect the CRPs, then she can imitate a legal client.**

Authentication using PUFs

- Enrolment Phase:

Node A

CA

RA

CA, CS, a, B

PA=H1(RA)
PS=H2(CS, KS)
B=PA-a.PS

Security Credential Generator

KS (verifier key) Stored in a tamper proof memory

Verifier S

Verification Step

- Verification Phase:

R1=PUF(CA)
PA=H1(R1)
PS'=QA-PA
VA'=e(PA,PS')

Node A

VA'

CA,CS,a,B

<CA,QA>

PS=H2(CS,KS)
PA=a.PS+B
QA=PA+xPS, VA=e(PA,xPS)

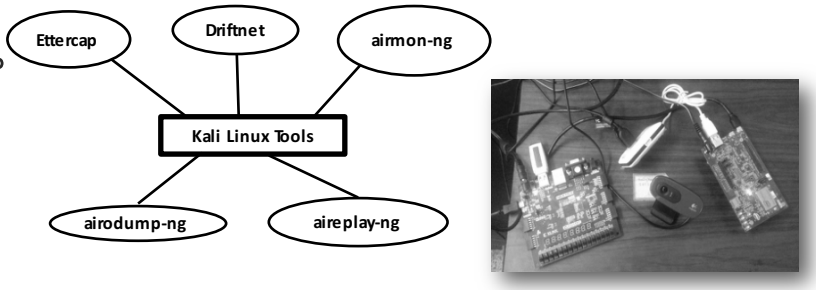
KS (verifier key) Stored in a tamperpro of memory

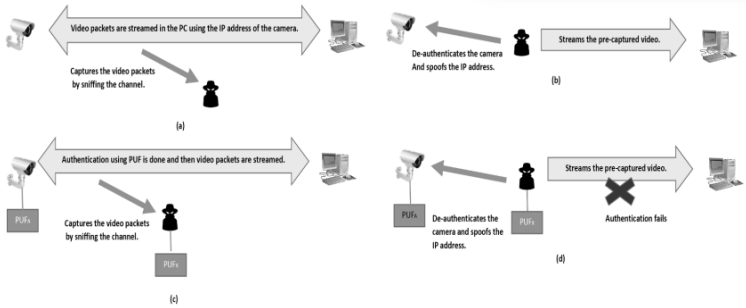
VA==VA' ??

Verifier S

Urbi Chatterjee, Vidya Govindan, Rajat Sadhukhan, Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, Debashis Mahata, Mukesh Prabhu:
PUF+IBE: Blending Physically Unclonable Functions with Identity Based Encryption for Authentication and Key Exchange in IoTs. IACR Cryptology ePrint Archive 2017: 422 (2017)[Accepted in IEEE TDSC]

Attack on a Video Surveillance Camera and PUF based Protection





Overheads: Does it fit the Budget?

Hardware Overhead	
Tool	Xilinx ISE 14.2
Slices	547
Registers	288
LUTs	1347
Power (Xilinx XPower Analyzer)	0.044 W

Software Overhead	
Tool	MIRACL Crypto SDK
Executable Size	512 kB
Latency	480.11 ms

Specification of the Elliptic Curve	
512 bit prime number p	8D5006492B424C09D2FEBE717EE382A57EBE3A352FC383E1AC79F21DDB43706CFB192333A7E9CF644636332E83D90A1E56EFBAE8715AA07883483F8267E80ED3
order r	80000000000000000000000000000000020001
curve	$y^2 = x^3 + Ax + B$ where: A=-3 and B=6099938373679980001C95B87A6BA872135E26906DB4C192D6E038486177A3EDF6C50B9BB20DF881F2BD05842F598F3E037B362DBF89F0A62E5871D41D951BF8E

Protocol Demonstration

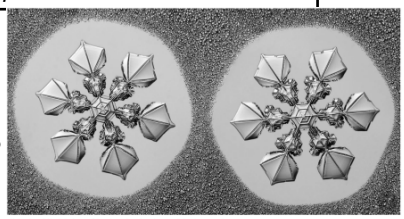
A Hardware Countermeasure of KRACKs in WPA2 using Physically Unclonable Functions

Urbi Chatterjee, Rajat Sadhukhan, Debdeep Mukhopadhyay, Rajat Subhra Chakraborty, Debashis Mahata, Mukesh M. Prabhu:Stupify: A Hardware Countermeasure of KRACKs in WPA2 using Physically Unclonable Functions. WWW (Companion Volume) 2020: 217-221

Cryptophasia of Hardware Circuits

- **New properties:** efficient key exchange which is seamless and is intrinsic to the device?

At the Horticultural Gardens of Calcutta, this Mad Tree represents a strange variety where every leaf is a different shape

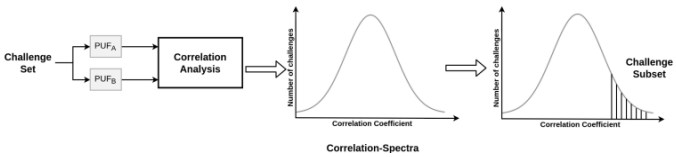


Snow Flakes: No two alike? Not any more...

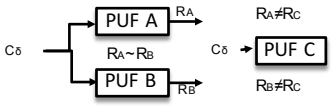
http://www.snowcrystals.com/identicaltwins/identicaltwins.html

Physically Related Functions (PReF): Keyless Crypto?

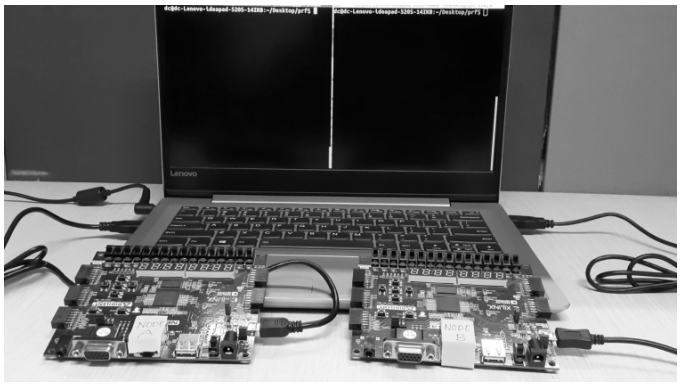
- Dependency on challenge set:



- For a PReF (P_A, P_B) and PUF P_C



Demonstration of Protocol



Features of the Protocol

- No Third Party requirement
- No secure key- storage
- Hardware root of trust
- Light-weight operations
- Unlimited authentications per Challenge-Response Pair
- New edges between two nodes can be formed without calling the node back to the server
- Secure against Replay and MITM attacks

Conclusions

- Security of IoT is of utmost importance in modern society
  - Develop expertise in Security, Embedded Systems, VLSI, Architecture, Networks, ML
- IoT constituents are varied:
  - Resource Constrained "things" to pervasive clouds
  - Offers different attack surfaces: side channels, inability to support costly ciphers, eavesdropping, replay, masquerade, poisoning, coalition, etc.
- We strive to develop novel tools and solutions for side channel security, designing new hardware primitives for end-end IoT security.
- The heterogeneous nature of IoT motivates developing end-end security aware designs:
  - ***"A Chain is no stronger than its weakest link…"- William, American philosopher and psychologist***

SPACE 2020: Tenth International Conference on Security, Privacy and Applied Cryptographic Engineering

December 17-21, 2020, Virtual Conference

SPACE-2020 | Call For Papers | Members | Invited Speakers | Last 3 Years Conferences

SPACE-2020
Virtual Conference

Check previous SPACE proceedings on SpringerLink

Topics

We invite authors to submit previously unpublished original research.Topic include but are not limited to:

Cryptographic Engineering

- Design of Cryptographic Primitives
- Random Number Generators and PUF
- Cryptographic Hardware
- Cryptographic Software
- Cryptographic Protocols
- Formal Methods in Cryptographic Engineering
- Evaluation of Cryptosystems
- Attacks and Countermeasures

Security and Privacy

- Security of Cyber-Physical Systems
- Secure Networking Protocols
- Securing Human-in-the-loop Systems
- Data privacy
- Authentication
- Botnets and Malware
- Anonymization Techniques and Attacks
- Intrusion Detection

Side-channel Analysis and Countermeasures

- Fault Analysis and Countermeasures
- Reverse Engineering and Tampering
- Hardware Trojans and Counterfeit Detection
- Cryptanalysis

To be Co-located with AsianHOST 2020

Important Dates

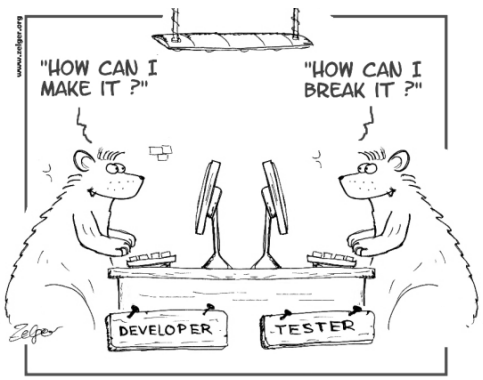
- Paper submission deadline: Aug. 07, 2020 23:59:59 EDT (~~Jul. 24, 2020 23:59:59 EDT~~)
- Notification of Acceptance: Sep. 25, 2020
- Camera-ready Version: Oct. 11, 2020
- Conference: Dec. 17-21, 2020

Selected papers to be invited for Journal of HASS, Springer.


Keynote Speakers
Tutorial Speakers
Ahmad-Reza Sadeghi
TU Darmstadt, Germany
Personal Website
Joan Daemen
Radboud University, The Netherlands
Personal Website
Lejla Batina
Radboud University, The Netherlands
Personal Website
Patrick Longa
MSR Redmond, USA
Personal Website
Ingrid Verbauwhede
KU Leuven, Belgium
Personal Website
Peter Schwabe
Radboud University, The Netherlands
Personal Website
Stjepan Picek
TU Delft, The Netherlands
Personal Website
Yuval Yarom
University of Adelaide, Australia
Personal Website


Online Course on Hardware Security
YouTube
hardware security
NPTEL
Swayam
NPTEL Online Certification Courses
on
Hardware Security
By
Prof. Debdeep Mukhopadhyay
Department of Computer Science & Engineering
IIT Kharagpur
Play (k)
0:03 / 6:29
Hardware Security
3,226 views
9
2
SHARE
SAVE
IIT Kharagpur July 2018
Published on 14 Nov 2018
SUBSCRIBE 29K

Thank You for your attention!!



They weren't so much different, but they had different goals

https://gabysurianosj.github.io/the_importance_of_testing

Email: debdeep@esp-research.com

Email: debdeep@cse.iitkgp.ac.in
debdeep.mukhopadhyay@gmail.com