

Implementation Security In Cryptography

Lecture 01: Welcome!!

What to Expect from this Course

- Upon successful completion, you become...

A “mathematically and physically oriented” thief.



A person who know how to and (how not to) do practical cryptography

What ***not*** to Expect from this Course

Traditional mathematical cryptanalysis

Traditional (reduction-based) cryptographic proofs (except for a few cases...)



Prerequisites

A criminal mind — just joking

A bit of Boolean logic knowledge— gates, flip-flops etc

A bit of effort from your side to self-study and try a few things

A bit of courage to write C/C++/Python codes

What I Expect...

Please ask questions...

I will be more than happy if you are interested to do some advanced project — not as a part of these course though

You teach me — things that you have learnt and you think you can use here — e.g. machine learning, formal methods, crypto

Plan Ahead...

Programming Assignments	30% (best two among 3 will be considered)
Mid,End Semester	40%
Quiz	15% (best of 2)
Paper presentation	15% (group/individual)
Bonus Marks	+5—best presentation +5 — best assignment submission +5 — Extra “optional” coding assignment +2 — useful feedback

Jokes Apart: What to Expect from this Course

- Some basics of cryptographic algorithms
- Some basics on cryptographic hardware design
 - Very simple Verilog assignment
- Some exciting practical attacks
 - With hands-on
 - Attacks have theory — so there will be maths and stats...
 - Again, not to worry...will go slow..

Points to Remember

- Please take class notes — even if there are slides and online materials
- Please stop me — when I am going too fast
- Please stop me — when you have any question

Lecture Formats

- Traditional
- Some components will be **math heavy** at the beginning — so pay attention
- Later part of the course will have components directly from papers
 - So, if you think video lectures/ uploaded slides will save you, you are wrong.
- In the later part of the course, you will be given some papers to read
 - You have to present them in groups
 - Be prepared to do some **Google search** to understand them.
 - Not all papers are equally hard
 - We shall take care :)

Home Rules

- No cheating please!! — it will be reported
- No open-screen during lecture
- Group activity needed

TAs



- Kalind Karia (kalind.karia@iitb.ac.in)



- Giriraj Singh (23m0815@iitb.ac.in)

Course Modules

- Module 1: Some Crypto Algorithms and Their Implementation
 - A bit theoretical
- Module 2: Power Attacks on Block Ciphers
 - The real fun begins here — some maths, not too hard
 - Python based attack codes
- Module 3: Power Attack Countermeasures
 - Short module
 - Optional assignment — you may give a try if interested
- Module 4: Fault Attacks
 - Another source of fun
 - Python based attack codes

Implementation Security: Why?

- Let's start from stories...

IoT Goes Nuclear: Creating a ZigBee Chain Reaction

Eyal Ronen(✉)*, Colin O'Flynn†, Adi Shamir* and Achi-Or Weingarten*

*Weizmann Institute of Science, Rehovot, Israel

{eyal.ronen,adi.shamir}@weizmann.ac.il

†Dalhousie University, Halifax, Canada

coflynn@dal.ca

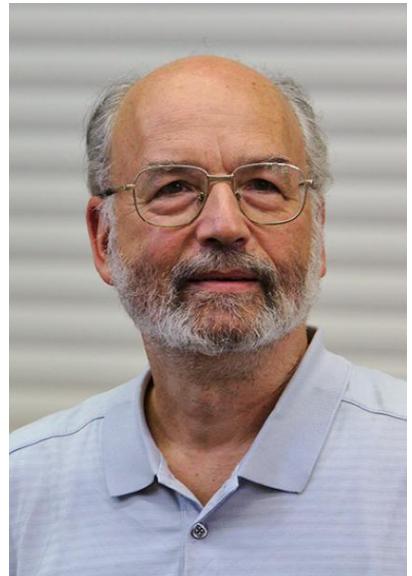


Figure 9. ZigBee warflying scenario



Implementation Security: Why?

- Another real story...

Israel concealed explosives inside batteries of pagers sold to Hezbollah, Lebanese officials say



By [Tamara Qiblawi](#), [Eliza Mackintosh](#), [Wayne Chang](#), [Eric Cheung](#), [Yong Xiong](#), [Kara Fox](#), [Gianluca Mezzofiore](#) and [Balint Bardi](#), CNN

⌚ 11 minute read · Updated 11:05 AM EDT, Fri September 27, 2024

The New York Times reported that the [Israeli intelligence](#) operated BAC Consulting and created two other unnamed [shell corporations](#) to hide their involvement.^[33] The pagers produced for Hezbollah had batteries that integrated 3 grams (0.11 ounces) of the explosive [PETN](#) in such a way that it would have been extremely difficult to detect.^[74] Israeli officials believe that Hezbollah did in fact disassemble the pagers for inspections, and may have even scanned them with x-rays, yet were unable to detect the explosive materials.^[59] The explosive could not be detected by an airport security check.^[75]



Serious Security: Rowhammer returns to gaslight your computer

Gaslights produce a telltale flicker when nearby lamps are lit; DRAM values do something similar when nearby memory cells are accessed.

Written by Paul Ducklin

JULY 10, 2023

NAKED SECURITY • DATA LEAKAGE • ROWHAMMER • SERIOUS SECURITY

You're probably familiar with the word *gaslighting*, used to refer to people with the odious habit of lying not merely to cover up their own wrongdoing, but also to make it look as though someone else is at fault, even to the point of getting the other person to doubt their own memory, decency and sanity.

You might not know, however, that the term comes from a 1930s psychological thriller play called *Gas Light* [spoiler alert] in which a manipulative and murderous husband pretends to spend his evenings out on the town

Crypto Keys Could Be Compromised by Intel and AMD 'Hertzbleed' Chip Vulnerability

2 mins

By Martin Young

Updated by Geraint Price
16 June 2022, 07:40 GMT+0000



Intel ups protection against physical chip attacks in Alder Lake

Repurposes logic originally used for spotting variations in voltage, timing in older circuits to help performance

Dan Robinson

Fri 12 Aug 2022 15:00 UTC

BLACK HAT Intel has disclosed how it may be able to protect systems against some physical threats by repurposing circuitry originally designed to counter variations in voltage and timing that may occur as silicon circuits age.

The research was presented by Intel at the Black Hat USA 2022 cybersecurity conference this week, and details logic inside the system chipset that is intended to complement existing software mitigations for fault injection attacks, the chipmaker said.

It makes use of a Tunable Replica Circuit (TRC), logic developed at Intel Labs to monitor variations such as voltage droop, temperature, and amino acids in circuits to improve



AI power analysis breaks post-quantum security algorithm

Technology News | February 19, 2023

By Nick Flaherty

AUTHENTICATION & ENCRYPTION

TRENDING: Maingear MG-1 AMD PC Build • GeForce RTX 4070 • Radeon RX 7900 XTX • Ryzen 7 7800X3D • Alienware Area-51m

HOME NEWS

AMD And Intel CPUs Rocked By New Speculative Execution Attack With A Huge Performance Hit

by Zak Killian — Wednesday, July 13, 2022, 05:08 PM EDT



BECOME A PATRON



Technology

Using just a \$25 device a researcher hacked into Elon Musk's Starlink system

What will the technology mogul have to say about this?

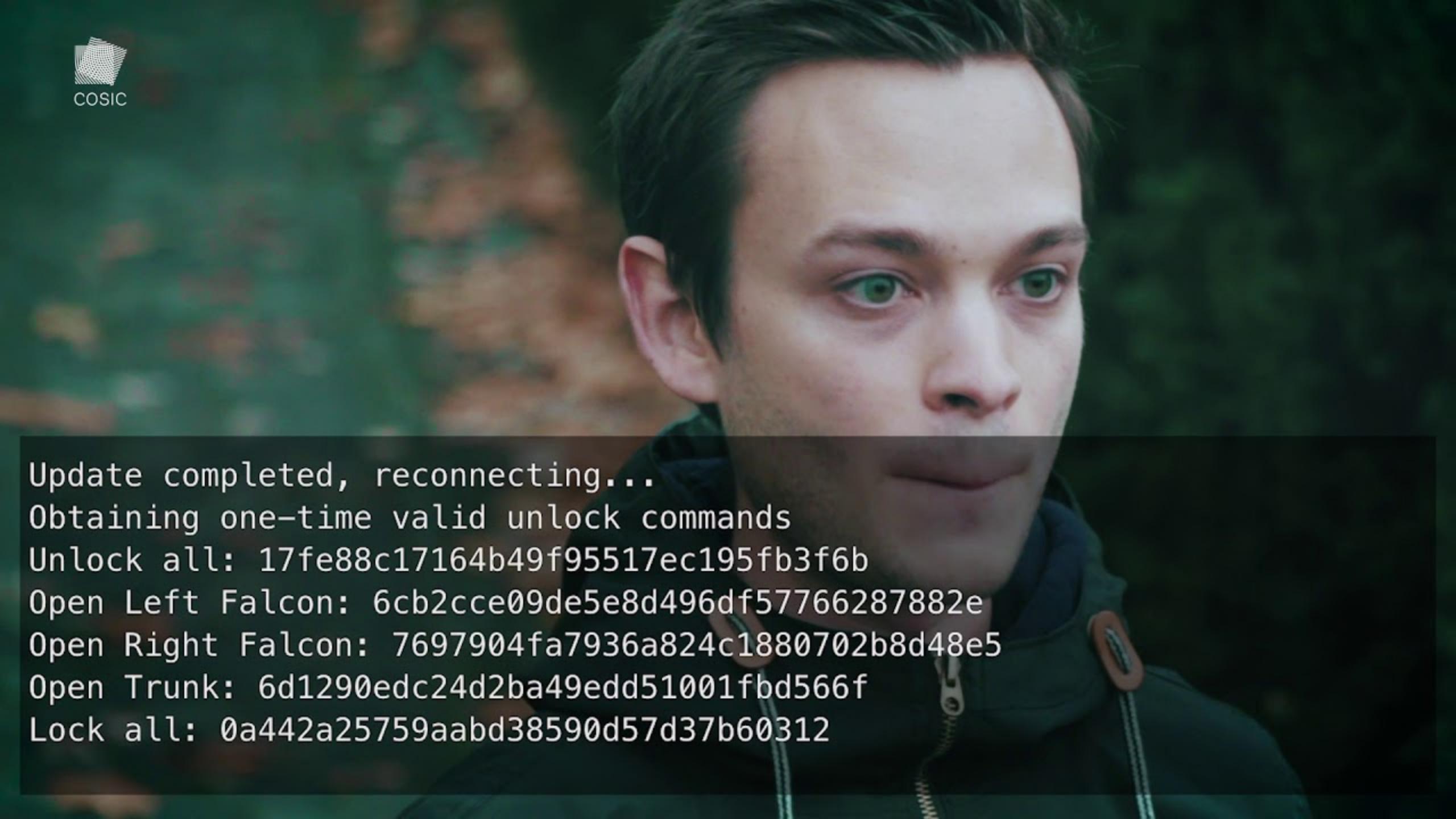


This NXP side-channel attack can clone Google Titan 2FA keys

Charlie Osborne 12 January 2021 at 13:28 UTC
Updated: 30 June 2021 at 16:34 UTC

Google • Hardware • 2FA





```
Update completed, reconnecting...
Obtaining one-time valid unlock commands
Unlock all: 17fe88c17164b49f95517ec195fb3f6b
Open Left Falcon: 6cb2cce09de5e8d496df57766287882e
Open Right Falcon: 7697904fa7936a824c1880702b8d48e5
Open Trunk: 6d1290edc24d2ba49edd51001fb566f
Lock all: 0a442a25759aab38590d57d37b60312
```

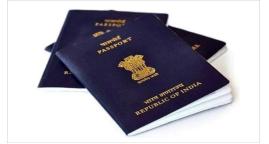
Why Crypto??

- Hacking chips is a fashion now...
- But where is crypto here?? I came here to learn some crypto!!!
 - Every device in this room is running some crypto



Cryptology

- Objectives: Aims at design and analysis of algorithms to ensure:
 - Confidentiality — No one **reads** your message
 - Integrity — No one **modifies** your message
 - Availability — Your system must not get too **slow**
- Recent days there has been humongous advancement in cryptology.
- New primitives developed giving us additional capabilities:
 - Performing operations on encrypted databased in cloud.
 - Post-quantum Cryptography
 - Homomorphic encryption, multi-party computatio



- Embedded/IoT devices
- Typically in-order pipeline; limited memory (SRAM/Flash)
- Not typically multi-user
- **Physical Access**



- Modern high end processors; Intel, AMD, Apple
- Co-processors, e.g. GPUs
- **Remote Access**

Software Crypto

Implementation	FIPS 140-2 mode	FIPS 140-2 validated	FIPS 140-3 validated
Botan	No	No	No
Bouncy Castle	Yes	Yes ^[30]	In process ^[31]
BSAFE	Yes	Yes ^{[32][33]}	Yes ^[34]
cryptlib	Yes	No	No
Crypto++	No	No ^[a]	No
GnuTLS	No	Yes ^{[35][b]}	In process ^[36]
Java's default JCA/JCE providers	No	No ^{[37][c]}	No
Libgcrypt	Yes	Yes ^{[38][d]}	In process ^[36]
libsodium	No	No	No
Mbed TLS	No	No	No
NaCl	No	No	No
Nettle	No	No	No
Network Security Services (NSS)	Yes	Yes ^{[39][e]}	In process ^[36]
OpenSSL	Yes	Yes ^{[40][f]}	In process ^[36]
wolfCrypt	Yes	Yes ^[41]	Yes ^[42]



GitHub

<https://github.com>

:

[mupq/pqm4: Post-quantum crypto library for the ARM ...](#)

The pqm4 build system is designed to make it very easy to add new schemes and implementations, if these implementations follow the NIST/SUPERCOP/PQClean API.



Cryptography ePrint Archive

<https://eprint.iacr.org>

:

[pqm4: Benchmarking NIST Additional Post-Quantum ...](#)

by MJ Kannwischer · 2024 · Cited by 15 — In this paper, we study the suitability and performance of said candidates on the popular Arm Cortex-M4microcontroller. We integrate the ...



National Institute of Standards and Technology (.gov)

<https://csrc.nist.gov> PDF

:

[pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4](#)

by MJ Kannwischer · Cited by 132 — The pqm4 framework investigates the feasibility and performance of the proposed PQC solutions on microcontrollers by focusing on a specific ...

22 pages

Need for Speed...

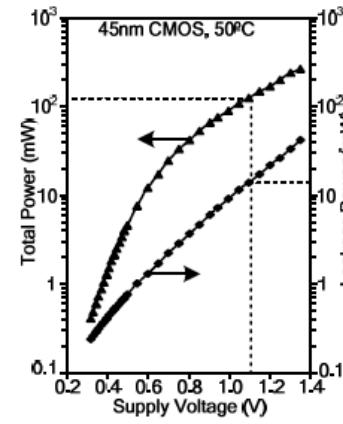
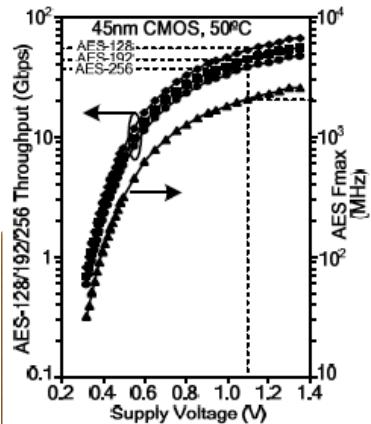
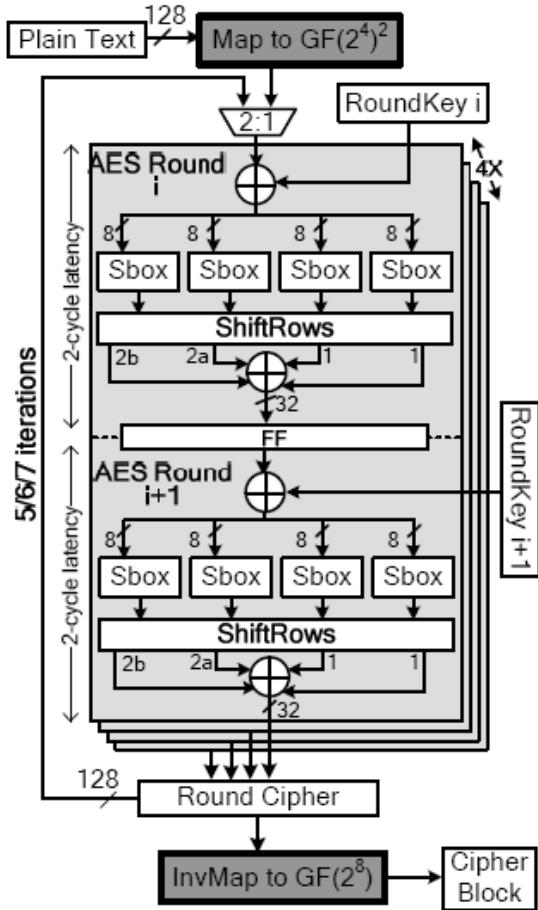
- Hardware vs Software speeds:

- Sensitive operations in the internet is becoming very important aspect of web applications.
- E-commerce and net-banking require transfer of sensitive information and are protected by Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols.
- Open SSL is an open source implementation of SSL and TLS, and accompanying cryptographic algorithms.
- OpenSSL has implementations of symmetric ciphers, asymmetric ciphers, hash functions, etc.
 - However, they are time consuming in software!

Cryptographic Co-processors

- Cryptographic algorithms can be accelerated by providing customized instruction in the processor Instruction Set Architecture (ISA):
 - AES-NI: Special Instruction in Intel ISA for performing AES operations.
 - PCLMULQDQ: Special Instruction in Intel ISA for carry less multiplication of 2 64-bit operands.
 - Every STM32 processor these days have a crypto accelerator
- Advantages:
 - Speed: Hardware offers speed, dedicated processing, parallelism.
 - Security: Can rule out many attacks which are possible on pure software. — **this is a sweeping statement to some extent**

Intel's AES-NI: Instruction for AES Operations



Reference: S. Mathew, 53Gbps Native $GF(2^4)^2$ Composite Field AES-Encrypt/Decrypt Accelerator for Content Protection in 45nm High Performance Microprocessors, VTS 2010

A Case Study of ECC Co-processors

- Elliptic Curve Cryptography (ECC) is an efficient public key cipher.
 - Elliptic Curve Scalar Multiplication



Reference: <https://www.youtube.com/watch?v=2RVLBUncHJk&list=PL71FE85723FD414D7&index=34>

A Case Study of ECC Co-processors (Contd.)

- Elliptic Curve Cryptography (ECC) is costly:
 - For n-bit key for characteristic 2 curves (n could be 163 or 233), number of finite field operations are roughly:
 - #Inv: $2n$, #Mul: $2n$, #Add: $4n$, #Sqr: $2n$ (for affine co-ordinate implementations).
- On Intel Core II Duo with 2.93 GHz and OpenSSL 1.0.1c, average time for 10000 scalar multiplications is 8.891 s.
- A hardware accelerator prototyped on Altera Cyclone IV FPGA requires around 4.397 s (double speed up!)

Reference: Debapriya Basu Roy, Shubham Agrawal, Chester Rebeiro, Debdeep Mukhopadhyay:
Accelerating OpenSSL's ECC with low cost reconfigurable hardware. ISIC 2016: 1-4

Ok...But So What...

- Ok, crypto is some sort of math-heavy algorithm, that people sometimes implement in hardware...but then?



Crypto can be attacked...

IoT Goes Nuclear: Creating a ZigBee Chain Reaction

Eyal Ronen(✉)*, Colin O'Flynn†, Adi Shamir* and Achi-Or Weingarten*

*Weizmann Institute of Science, Rehovot, Israel

{eyal.ronen,adi.shamir}@weizmann.ac.il

†Dalhousie University, Halifax, Canada

coflynn@dal.ca

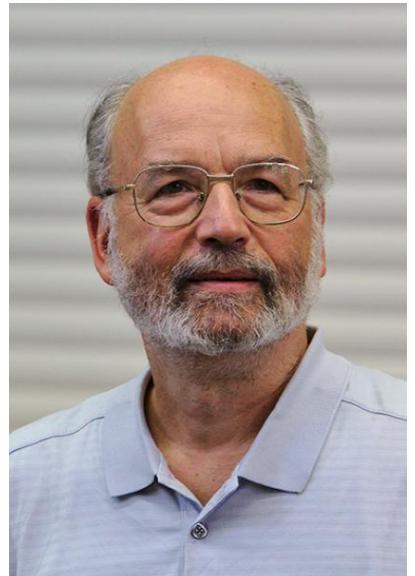


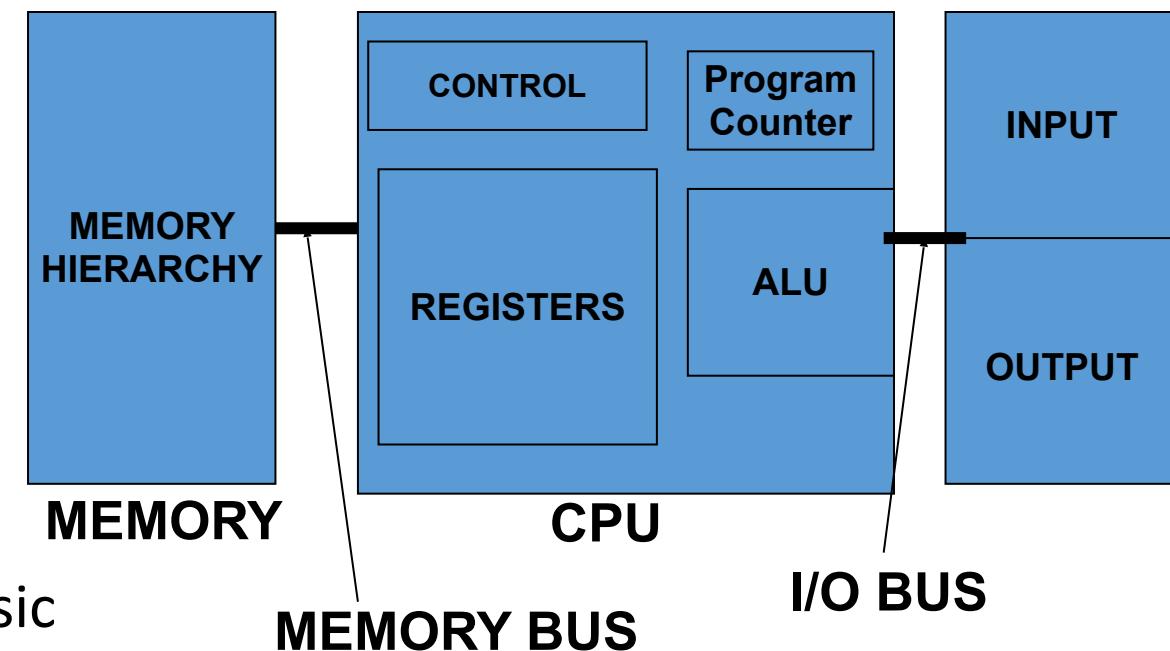
Figure 9. ZigBee warflying scenario



- “if you think your problem can be solved by cryptography, then you do not understand cryptography and you do not understand your problem”-[Bruce Schneier]

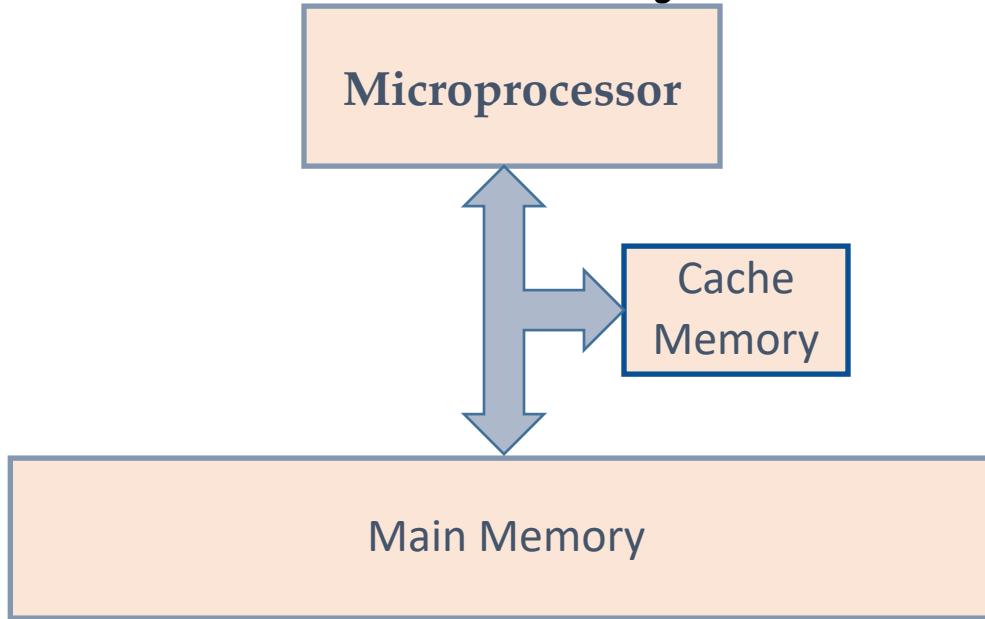
Crypto and Attacks

- **Software Attacks:** Present day computing systems are naturally vulnerable.



- Von Neumann (1903-1957)
- Contributed to give a very basic model, often referred to as Von Neumann model

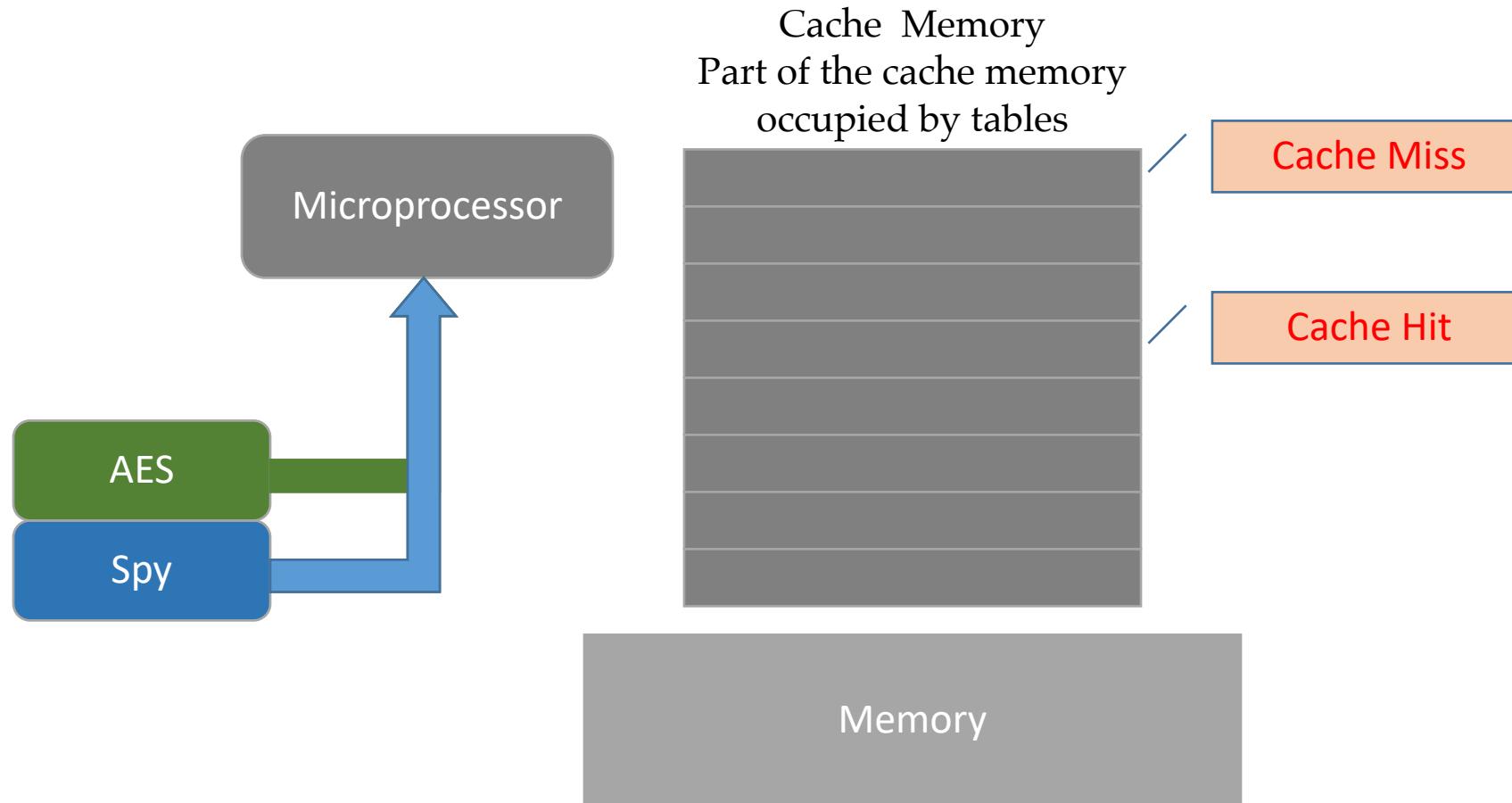
Attacks due to Memory Wall



- If there is a *Cache Hit*
 - Access time is less
 - Power Consumption is less
- If there is a *Cache Miss*
 - Access time is more
 - Power Consumption is more

Timing Attacks due to Cache Memory

- Uses a spy program to determine cache behavior



Micro-architectural Attacks: Design for Security

Computer Architecture has been designed with performance as a primary design criteria.

Security has been an after thought.

For example:

Speculative execution is an optimization technique where a computer system performs some task that may not be needed.

This has been the basis of the recently discovered attacks: **Spectre and Meltdown**.

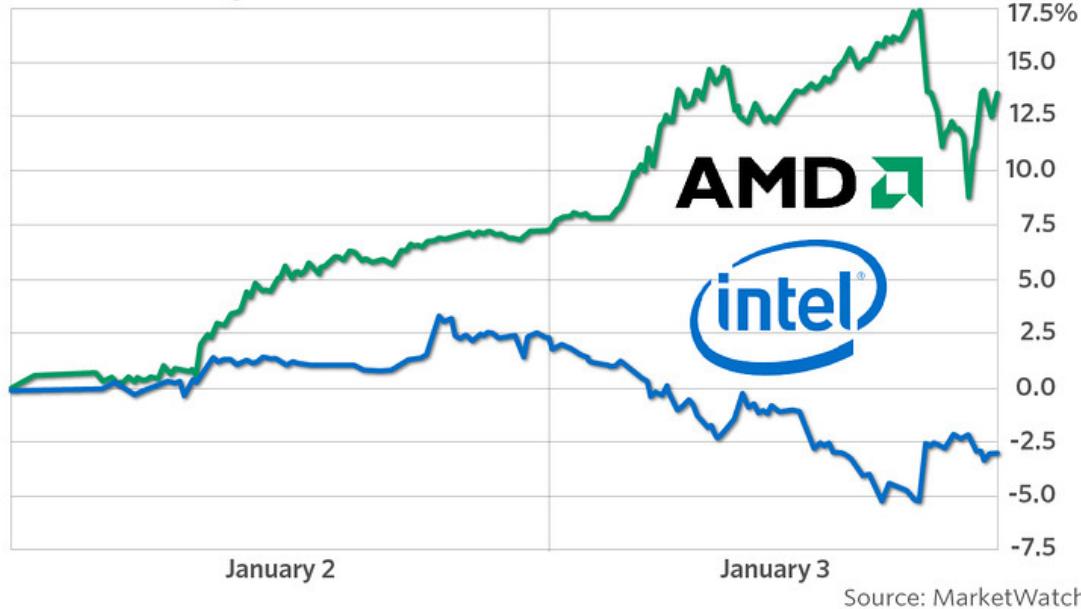
To quote Bruce Schneier, “**Fixing them either requires a patch that results in a major performance hit, or is impossible and requires a re-architecture of conditional execution in future CPU chips.** It shouldn't be surprising given that microprocessor designers have been building insecure hardware for 20 years. What's surprising is that it took 20 years to discover it.”

Reference: *Spectre and Meltdown*, Daniel Gruss, Moritz Lipp, Yuval Yarom, Paul Kocher, Daniel Genkin, Michael Schwarz, Mike Hamburg, Stefan Mangard, Thomas Prescher and Werner Haas, Google Ground Zero Project

Security can be a game changer

Intel stock drops after report of security flaw

Intel shares had their worst day in eight months, but pared deeper earlier losses, while rival AMD gained



Although the vulnerabilities, called **Meltdown** and **Spectre**, affected leading processors in many devices, **Intel** is bearing most of the fallout **after** rival AMD distanced itself from the bulk of the issues. **Intel shares** were down nearly 5 percent, around \$43 apiece, **after** posting a 3 percent decline on Wednesday.

Reference: <https://www.cnbc.com/2018/01/04/intel-stock-down-intc-could-meltdown-spectre-exploit-benefit-amd.html>

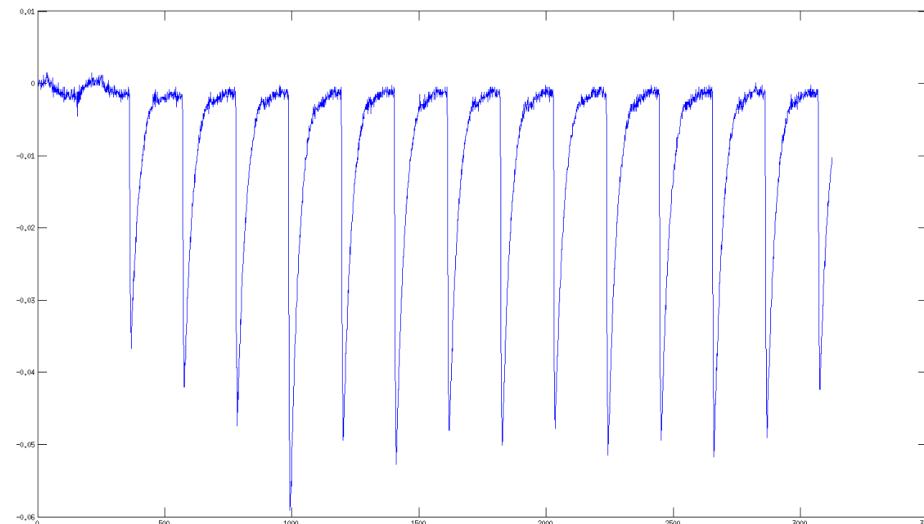
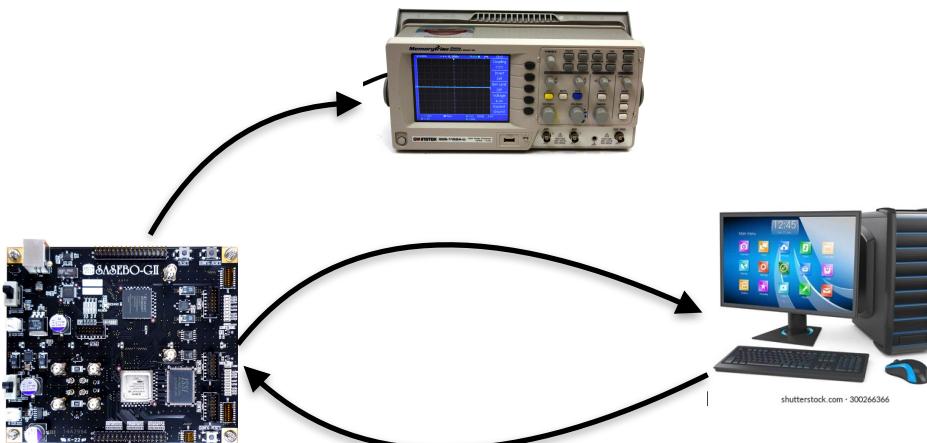
Ok...But So What...

- Ok, that was about crypto software...
- I will make hardware crypto...then?
- Also, my device is not multi-user



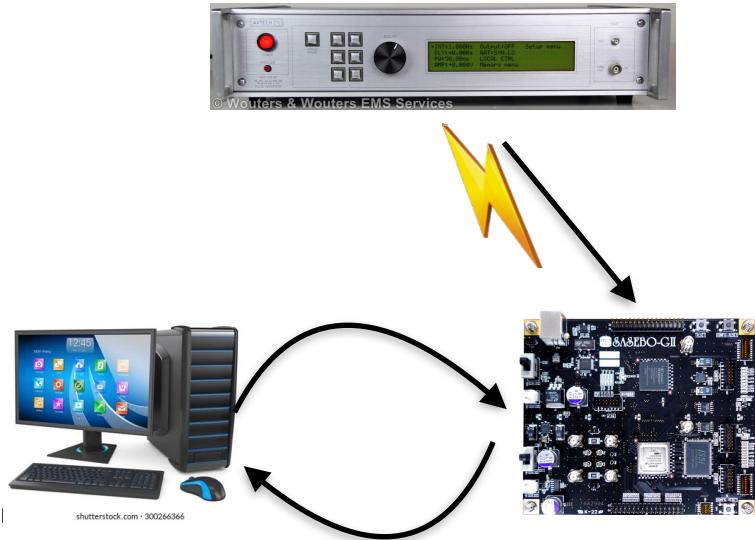
It is Impossible to Cheat Physics

- The physical channels are correlated with the information being processed
- Let us consider the power consumption from a chip performing AES
- Fundamental cause: power consumption is correlated with switching of CMOS transistors (0->1, 1->0)
 - Typically it is assumed that power consumption is correlated with the Hamming Weight/Distance.
- If some internal state is exposed, the key of AES can be recovered in seconds.



Source: Testbed for Side Channel analysis and security evaluation

It is Impossible to Cheat Physics



- The computation can be disturbed with “faults”...
- Once again, you can break AES...

Ok...So Everything is Vulnerable

- What is the point of studying then....Let's go home and sleep.
 - The attacks are not straightforward...needs maths and “criminal mind”..
 - We shall learn these attacks here in this course....and some ways to prevent them....



Who Cares...?



Rambus



synopsys®



THALES