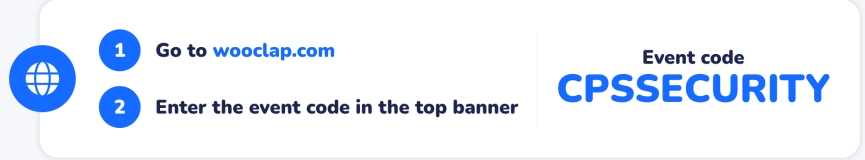
CE/CZ4055 Cyber Physical System Security

Micro-Architectural Security

Anupam Chattopadhyay

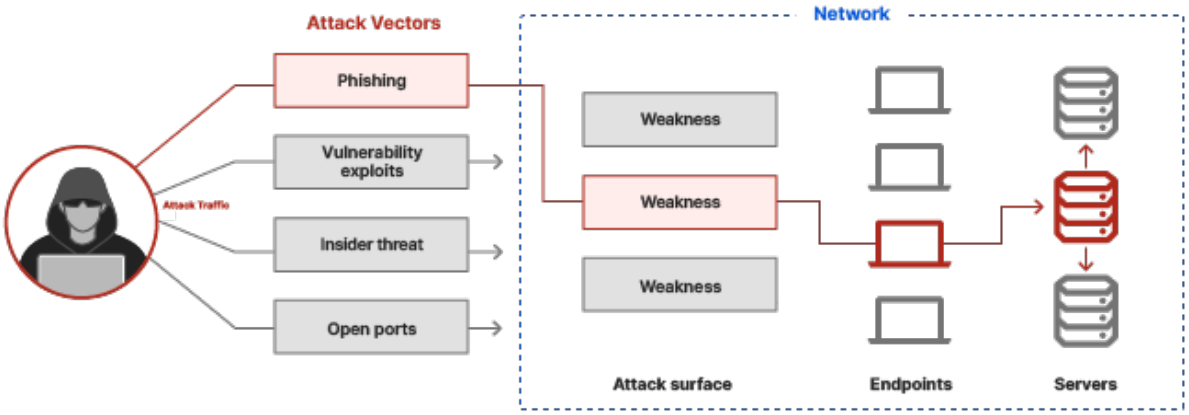
SCSE, NTU



NANYANG TECHNOLOGICAL UNIVERSITY

Discussions from Last week

- ***Attack vectors*** are the ways an attacker can breach sensitive data or compromise an organization
- ***Attack Surface*** is the collection of all attack vectors
- ***Attack Path*** is the path from attack source to attack target

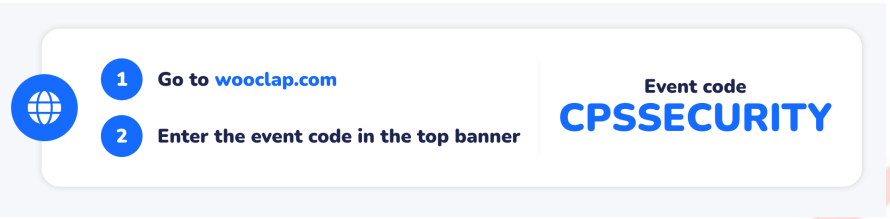


NANYANG TECHNOLOGICAL UNIVERSITY

Source: Cloudflare

Contents

- *Side Channel Attacks*
  - Timing Attack
  - Power Attack
  - Attacks on ‘Secure’ Processor
  - Discussion



NANYANG TECHNOLOGICAL UNIVERSITY

Side Channel Attacks Classification

- Passive Attacks:
  - Observe the target such as computer
  - Gain the “additional” information leaked from the physical devices caused by any operation i.e. timing information, power consumptions, electromagnetic leaks, voices/sounds

- Active Attacks:
  - Add “additional” inputs
  - Change the environment or target itself to let abnormal operations or change the program flow, i.e. add voltage, clock glitching, or tempest virus

SCA: Real World Examples

- KEELOQ
  - Keyless Car Entry
  - Successful CPA in 10 traces
  - Manufacturer's key extracted
- MiFARE DESFire (NXP)
  - Access Card/Public Transport with HW 3-DES
  - Successful CPA in 250K traces
  - Allows Cloning
  - NXP discontinued
- Virtex-II Pro (Xilinx)
  - FPGA with HW 3-DES for bitstream encryption
  - Successful CPA in 25K traces
  - Allows Cloning/ Bitstream Modfiication
- ProASIC (Actel)
  - FPGA with HW AES for bitstream encryption
  - Successful attack in 0.01s
  - Allows Cloning/ Bitstream Modification

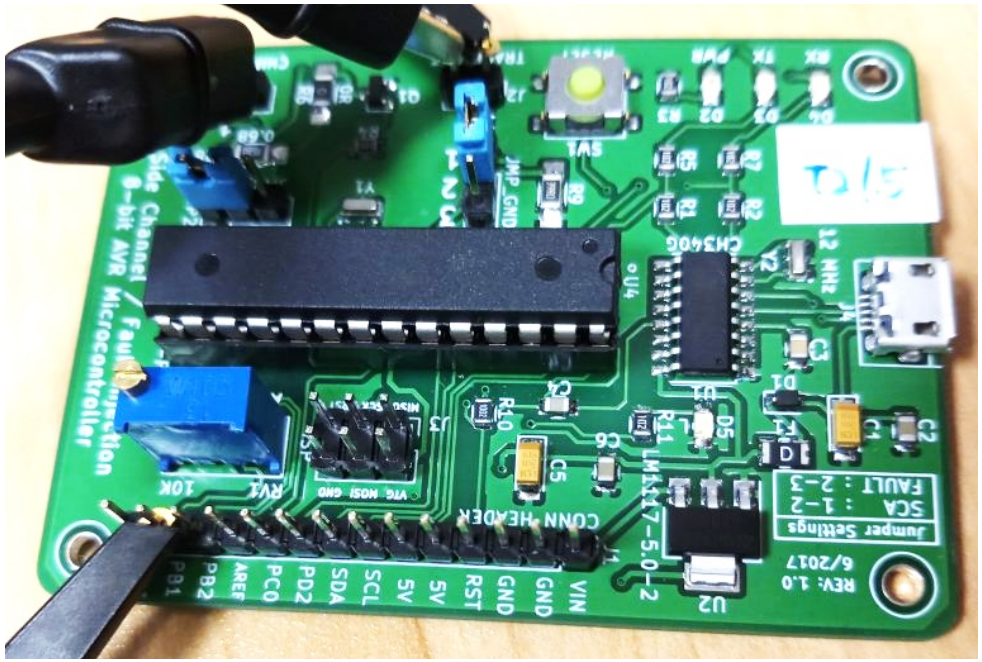
Security Attacks Classification

- **Passive Attacks**
- Active Attacks

Timing Attack

- Timing attack is an example of an attack that exploits the implementation rather than the algorithm itself
- Measure the time it takes for a certain unit to perform an operation
- Keep the input, output, and consumed time
- Check the correlation between time measurements of guess key or input and empirical result (often statistically)

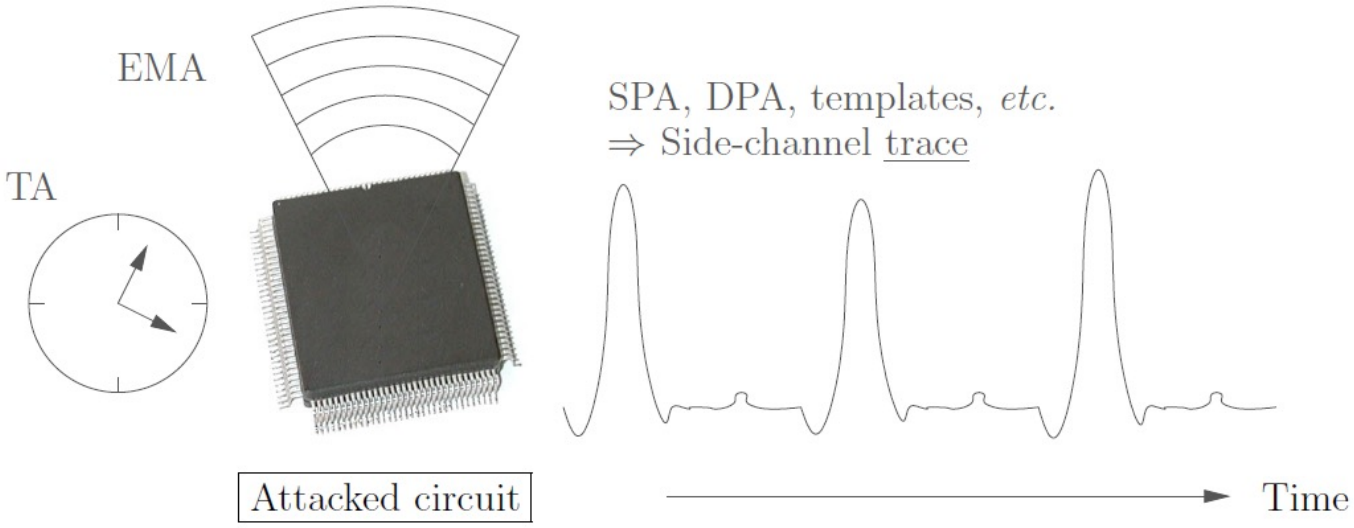
Threat: Power Analysis Attack



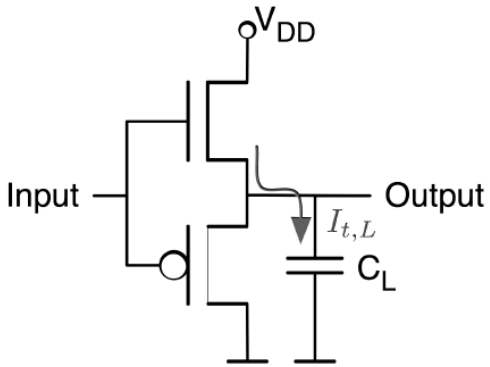
Setup: CZ/E4055 Labs

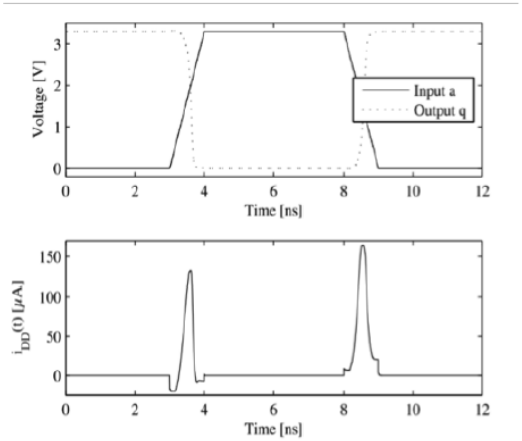
NANYANG TECHNOLOGICAL UNIVERSITY

Threat: Power Analysis Attack



Why does Power Analysis Attack work?





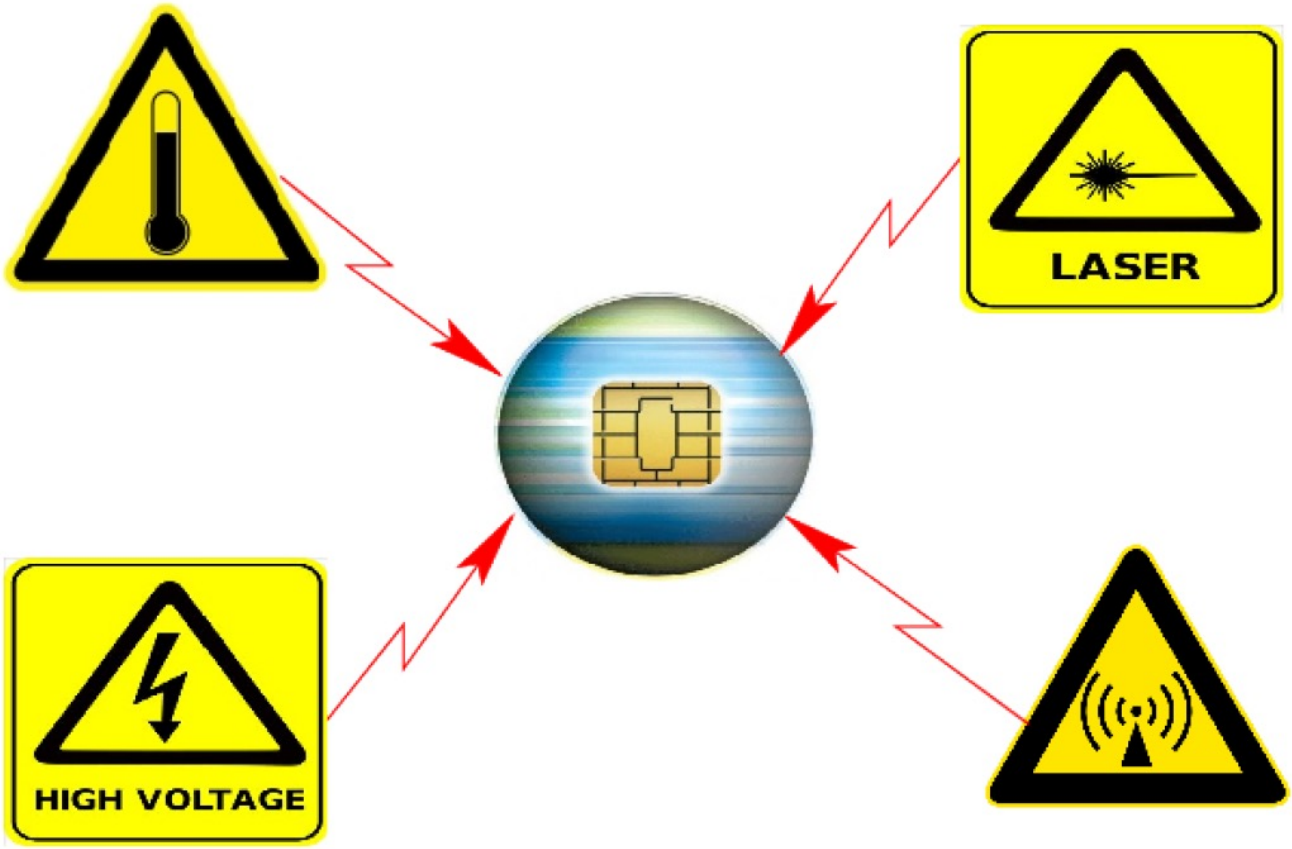
- CMOS cell is building block of almost every electronic system
- CMOS consumes power when input transition occurs
- This transition is observable through side-channels
- Thus the secret data processed by CMOS gate is observable

NANYANG TECHNOLOGICAL UNIVERSITY

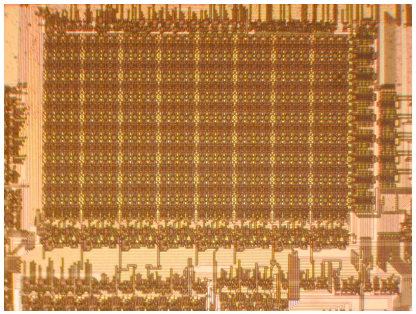
Security Attacks Classification

- Passive Attacks
- **Active Attacks**

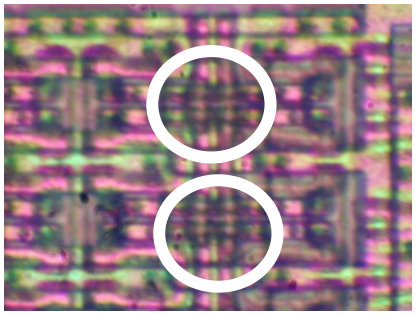
Threat: Fault Injection Attacks (FIA)



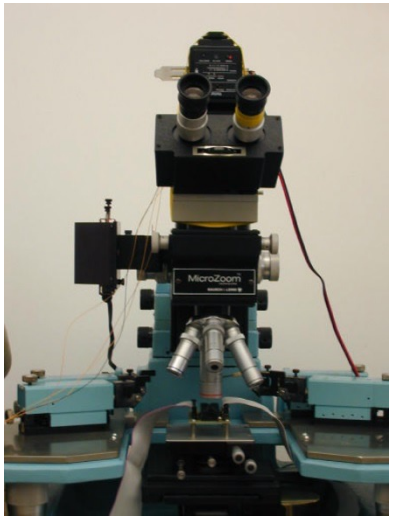
Example: Physical Attack (Fault)



80X



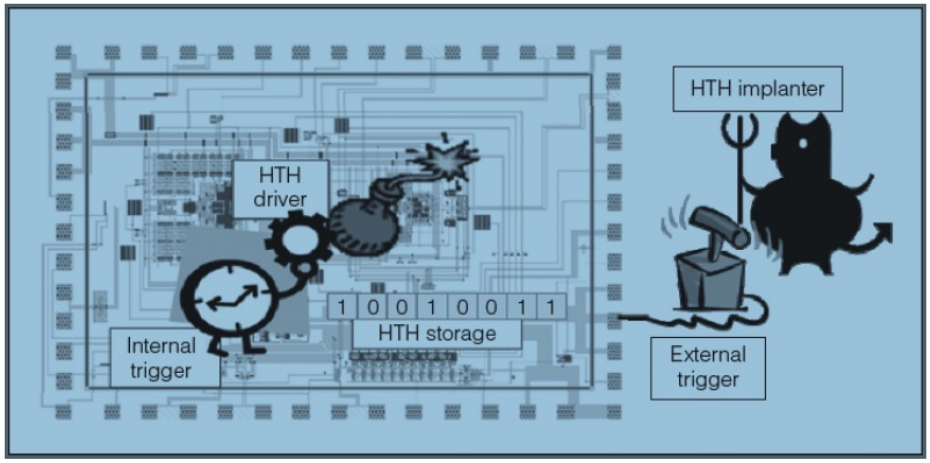
1500X

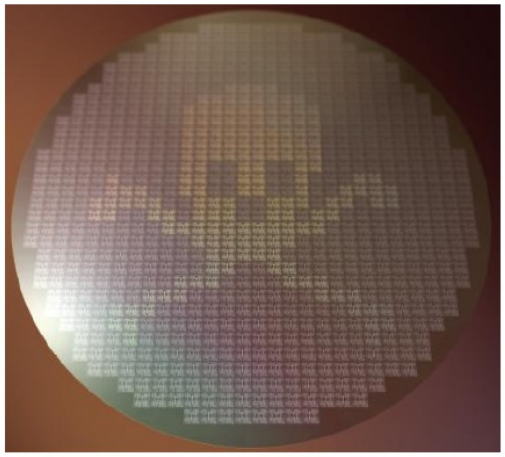


- With cheap laboratory equipment, memory states can be altered or damaged permanently
- Attack precision improves with sophisticated equipment
- Other forms of attack rely on the mode of information storage
  - e.g., magnetic storage can be attacked with strong magnetic field

S. Skorobogatov et al, "Optical Fault Induction Attacks", CHES, 2002

Example: Hardware Trojan Horse (HTH)





- Malicious modifications in Integrated Circuits (ICs).
- Realize malicious functions (Leakage of sensible information, alteration of IC behaviours, etc.).
- HTH was born because of outsourcing design/fabrication process.

Contents

- Side Channel Attacks
- *Timing Attack*
- Power Attack
- Attacks on ‘Secure’ Processor
- Discussion

NANYANG TECHNOLOGICAL UNIVERSITY

1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
CPSSECURITY

RSA Revisit

- **Encryption** (with public key): $C = M^e$
- **Decryption** (with private key): $M = C^d$

- $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+h\varphi(n)} \equiv M \pmod{n}$

- We have $ed \equiv 1 \pmod{\varphi(n)}$. Hence we can write $ed = h(p-1)(q-1) + 1$ for some (non negative) integer h
- Now, $(M^e)^d = M^{ed} = M^{ed-1}M = M^{h(p-1)(q-1)}M = (M^{p-1})^{h(q-1)}M$.
- Fermat's Little Theorem → $M^{p-1} \equiv 1 \pmod{p}$

- $(M^e)^d = \cdots \equiv 1^{h(q-1)}M \pmod{p} = M \pmod{p}$
- $(M^e)^d = \cdots \equiv 1^{h(p-1)}M \pmod{q} = M \pmod{q}$

→ $(M^e)^d = M \pmod{pq} = M \pmod{n}$ [Euler's Lemma]

Modular Exponentiation

- The way of attacks depend on the details of modular exponentiation
- For efficiency, modular exponentiation is done via:
  - ✓ Simple multiplication
  - ✓ Repeated squaring
  - ✓ Chinese Remainder Theorem (CRT)
  - ✓ Montgomery multiplication
  - ✓ Sliding window
  - ✓ Karatsuba multiplication

Simple Multiplication

- The simplest case, the modular exponentiation is done by multiplying the number as many as the values of exponent such as
  - $2^{13} = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times \cdots$
- Therefore, the execution time is directly proportional to the exponent value (key value)

Simple Multiplication: Attack

- An attacker eavesdrops the decryption operation, where (s)he gets *a plaintext* and *its computation time* (the decryption key is 13 which is hidden from the attacker)

- Attacker guesses the key is 12, decrypts with the guess key and it returns ***smaller*** computation time

- Then, attacker guesses the key is 14 and returned computation time is ***greater*** than empirical data

→ the key is between 12 and 14

Prevention: Constant Time Calculation

- In this strategy, the time it takes to do any operation must be independent from input and key (constant and equal at every time)
- Thus, every operation takes the slowest operational time by waiting
- However, this strategy raises the execution time dramatically (corresponding to the worst case)

Prevention: Random Time Calculation

- In this strategy, the time it takes to do any operation changes every operation at each time
- It is done by waiting a random time before going to the next execution
- However, this strategy also raises the execution time and its random variance must be large

Contents

- Side Channel Attacks
- Timing Attack
- *Power Attack*
- Attacks on ‘Secure’ Processor
- Discussion

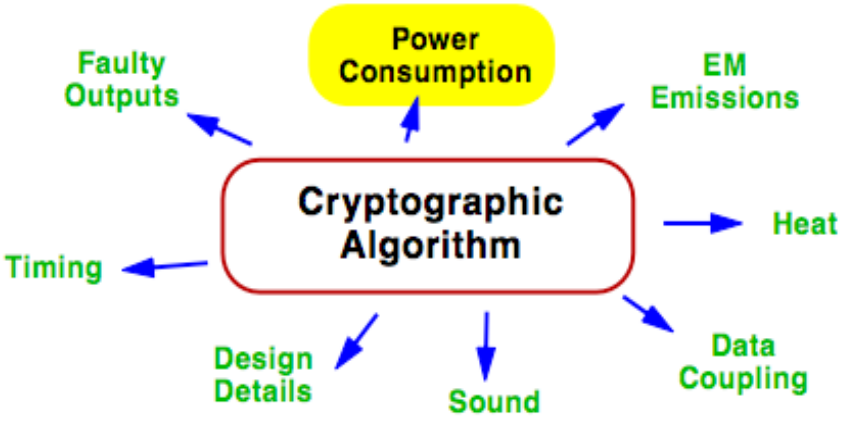
NANYANG TECHNOLOGICAL UNIVERSITY

1 Go to wooclap.com

2 Enter the event code in the top banner

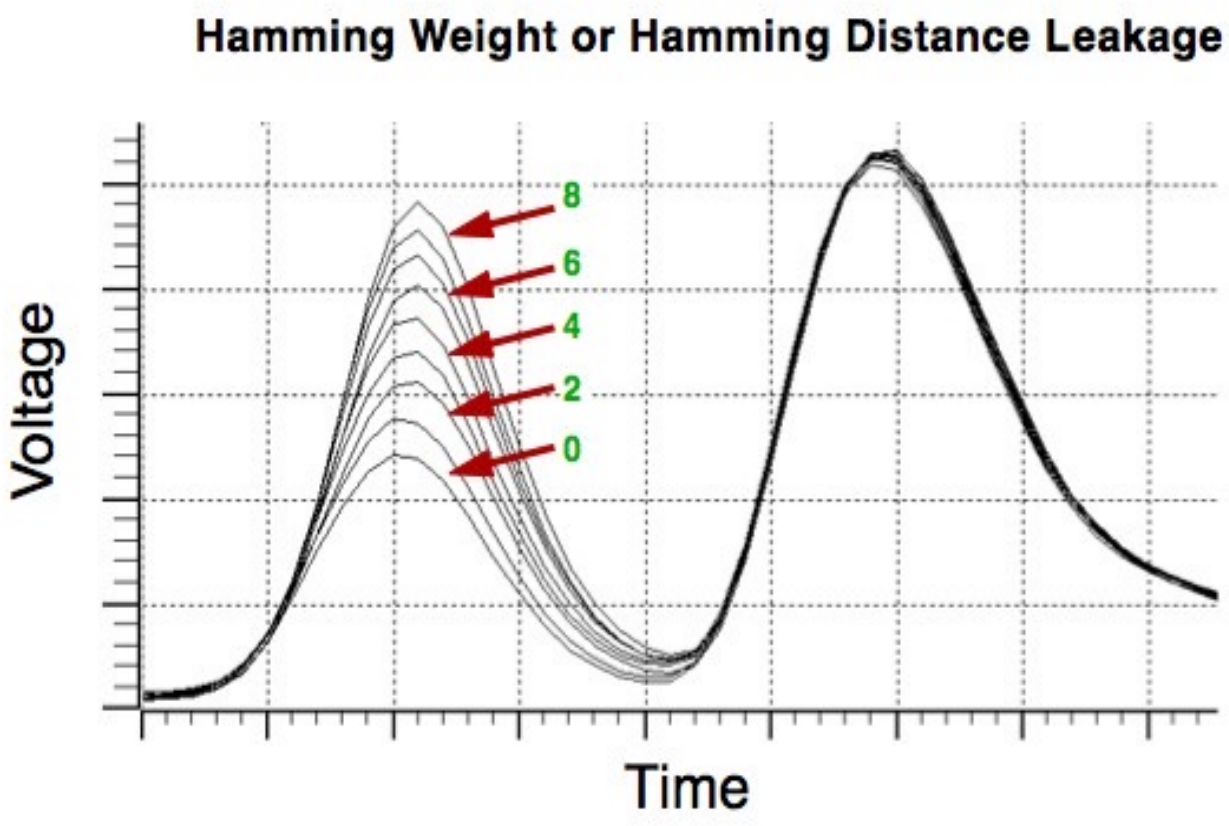
Event code
CPSSECURITY

Side Channels



- Kocher et al., June 1998: Measure instantaneous power consumption of a device while it runs a cryptographic algorithm
- Different power consumption when operating on logical ones vs. logical zeroes.

Information Leakage



Systems under Threat

- Implementations of Cryptographic Algorithms
  - On smart cards
  - On general/specific purpose hardware
  - On software

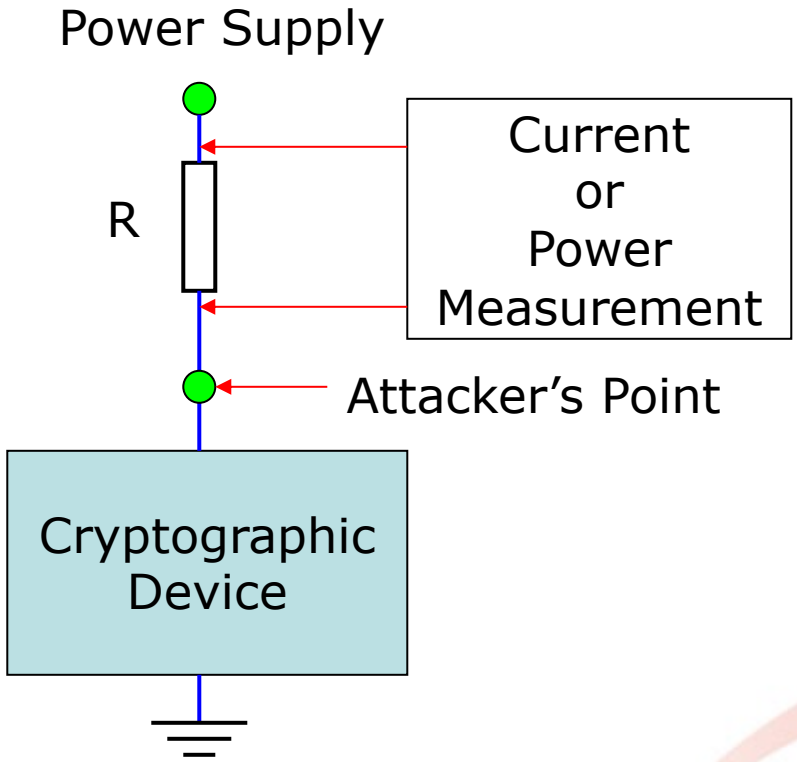
Power Attacks

- **Power Attacks are powerful and generic**
  - Based on statistical processing of observed data
  - Known random messages
  - Targeting a known algorithm
  - Running on a single smart card

- **Attack performed in 2 steps**
  - Acquisition phase: on-line with the smart card
  - Analysis phase: off-line on a PC (hypothesis testing)

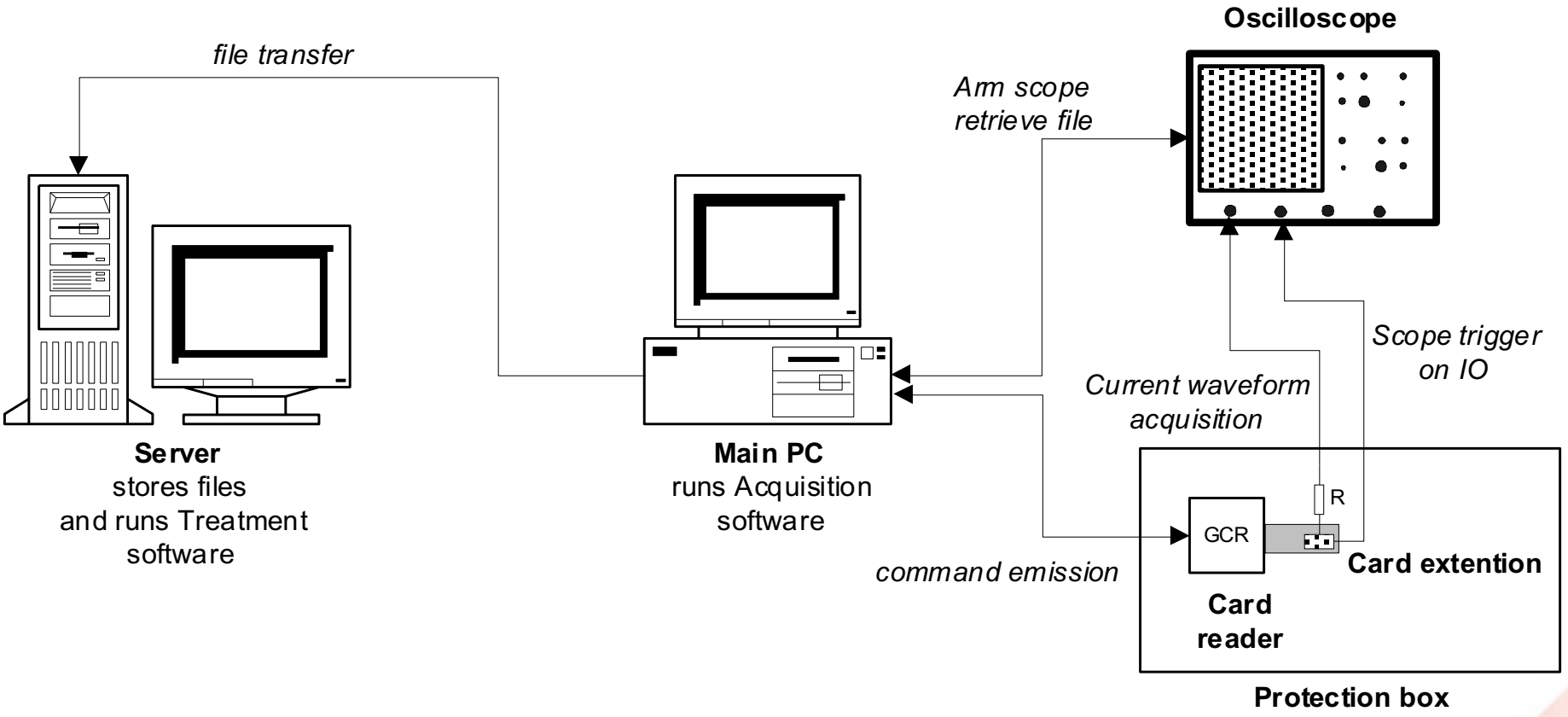
What is a Power Analysis Attack?

Side-channel attacks exploit correlation between secret parameters and variations in timing, power consumption, and other emanations from cryptographic devices to reveal secret keys



NANYANG TECHNOLOGICAL UNIVERSITY

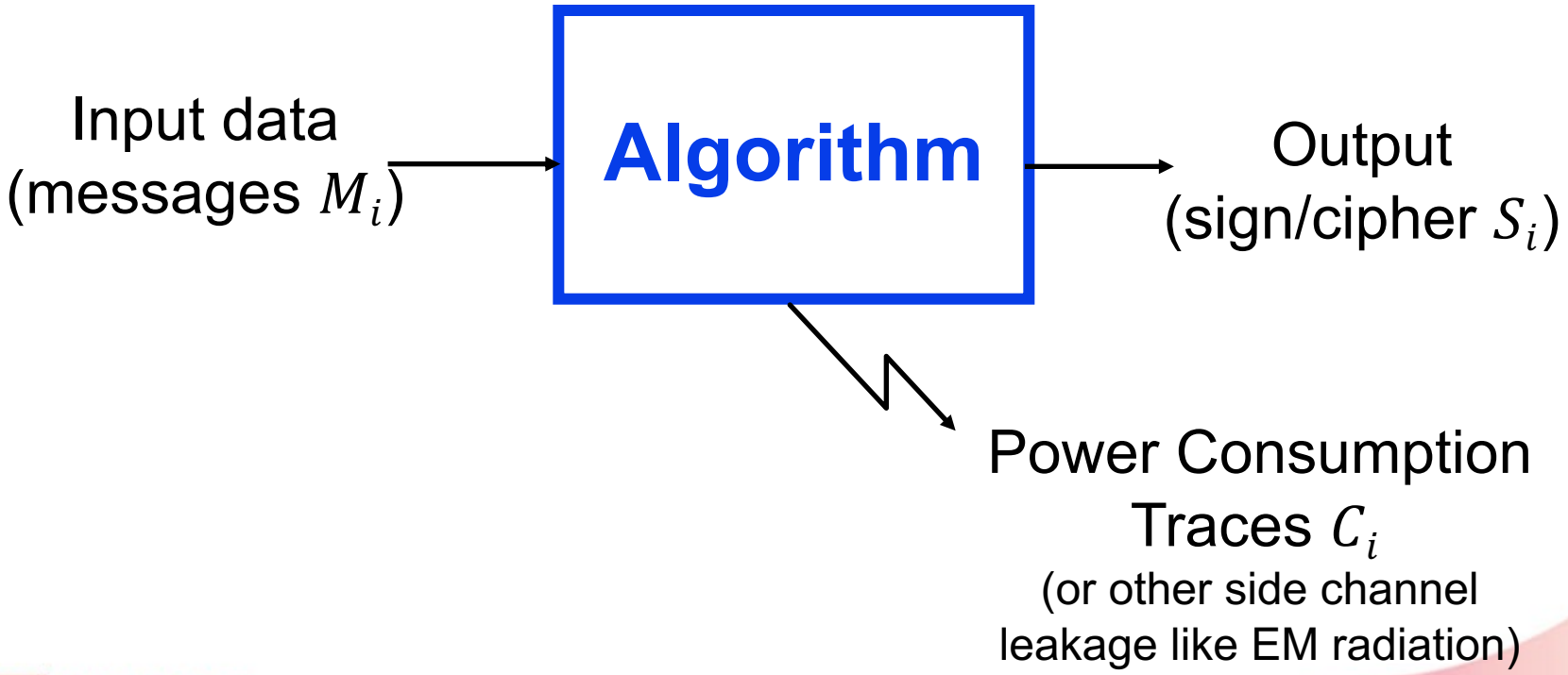
Acquisition Procedure



NANYANG TECHNOLOGICAL UNIVERSITY

Acquisition Procedure

Play the algorithm N times



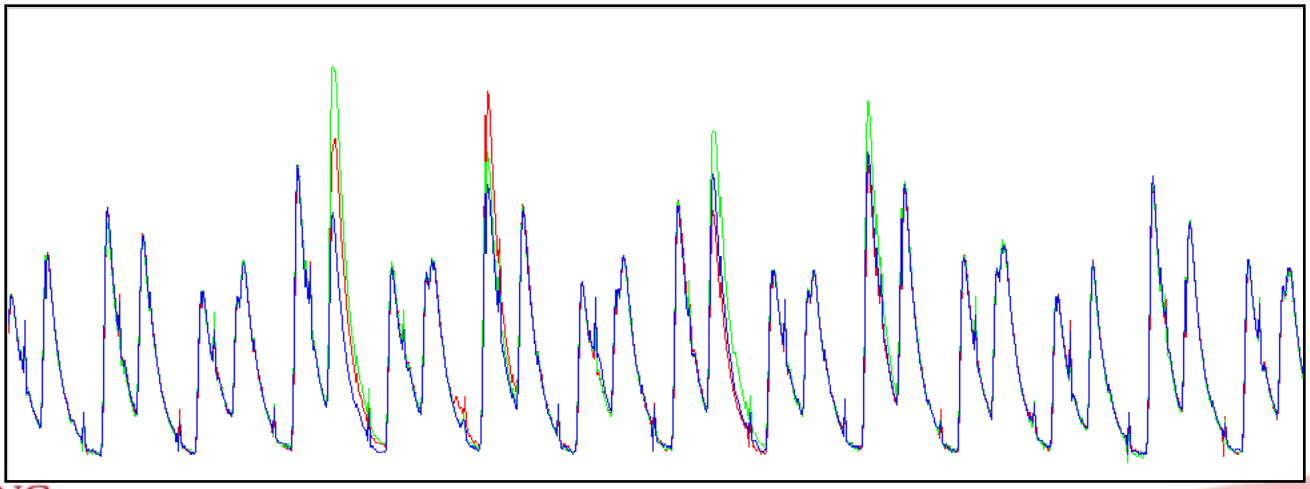
Acquisition Procedure

- After data collection, what is available ?
  - N plain and/or cipher random texts

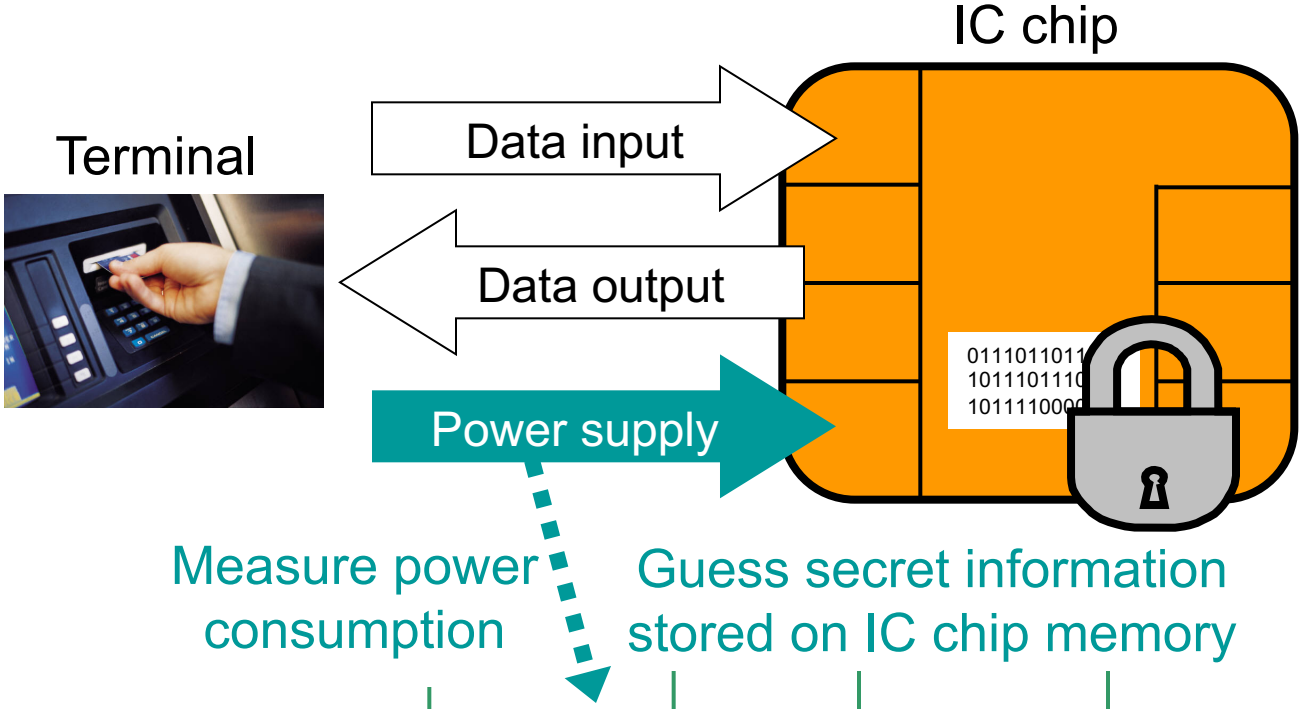
    00 B688EE57BB63E03E

    01 185D04D77509F36F

    02 C031A0392DC881E6 …
  - N corresponding power consumption waveforms



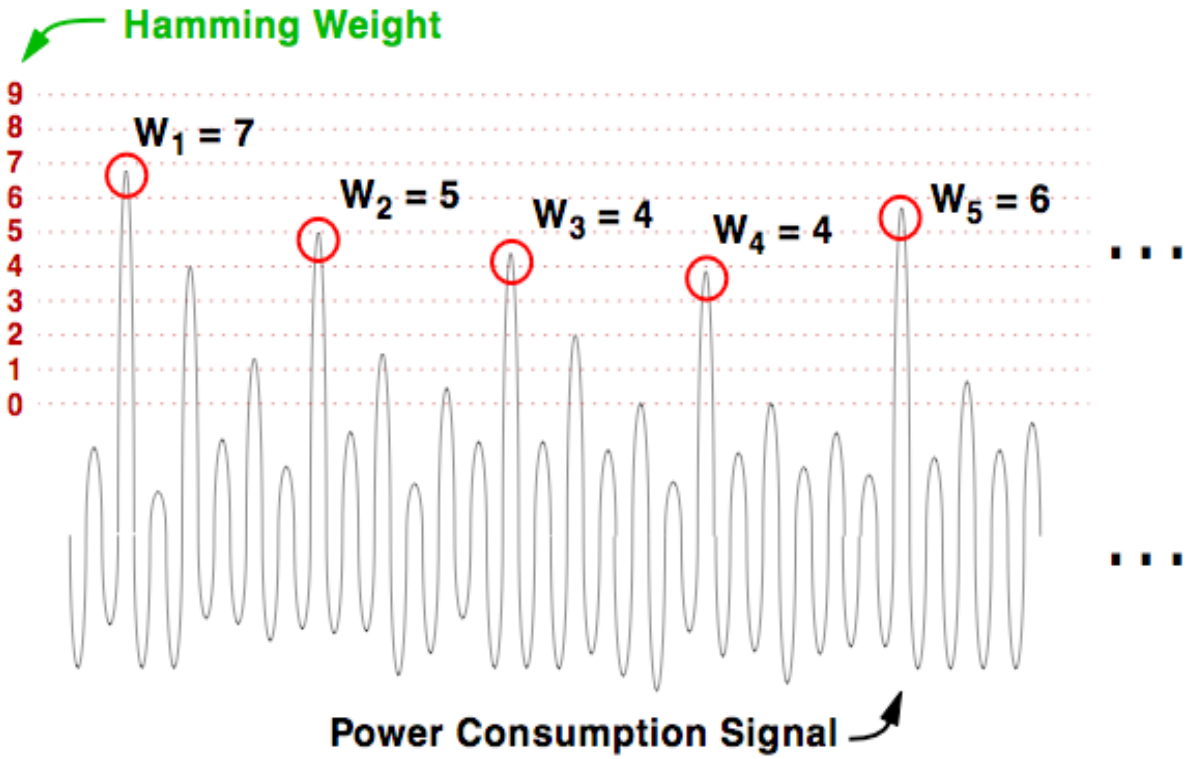
Simple Power Analysis



NANYANG TECHNOLOGICAL UNIVERSITY

Simple Power Analysis

- Simple attack, needs a few seconds
- Direct observation of a system‘s power consumption
- Can gain very useful information



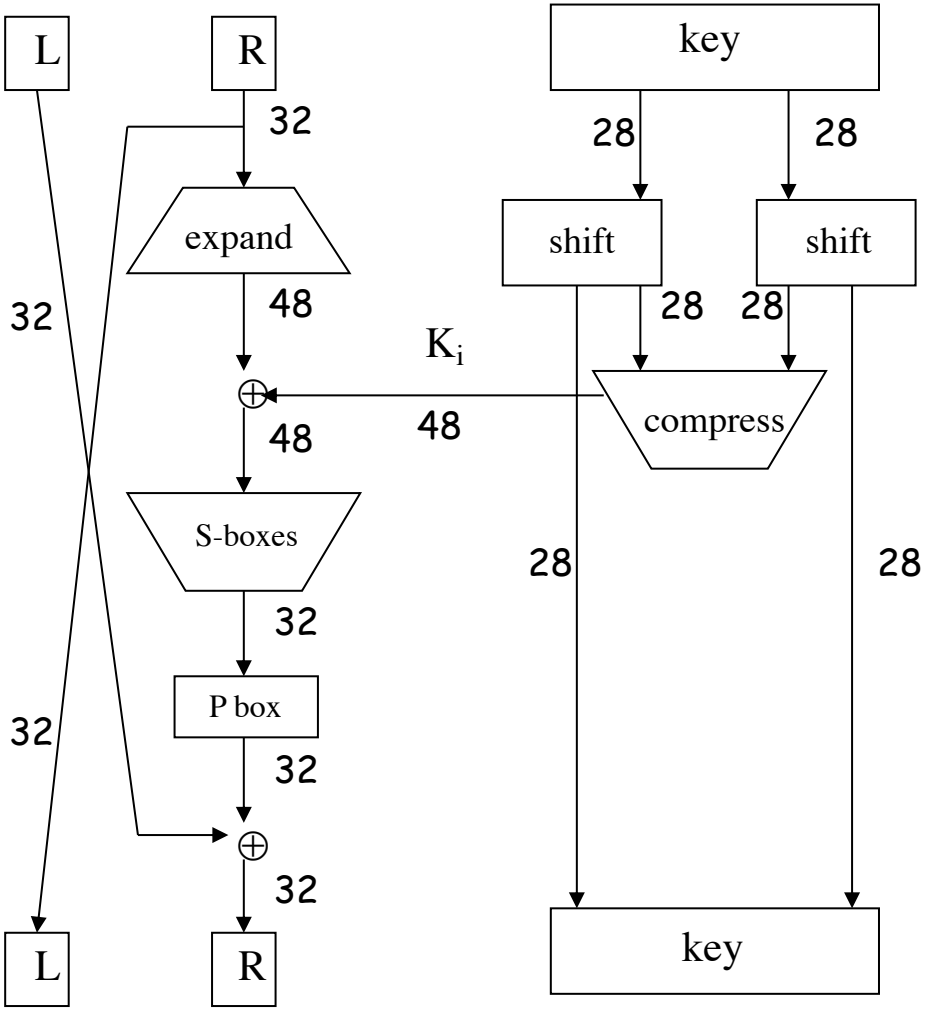
Simple Power Analysis (SPA)

- Directly interprets the power consumption of the device
- Looks for the operations taking place and also the key!
- Trace: A set of power consumptions across a cryptographic process
- 1 millisecond operation sampled at 5MHz yield a trace with 5000 points

Example: DES

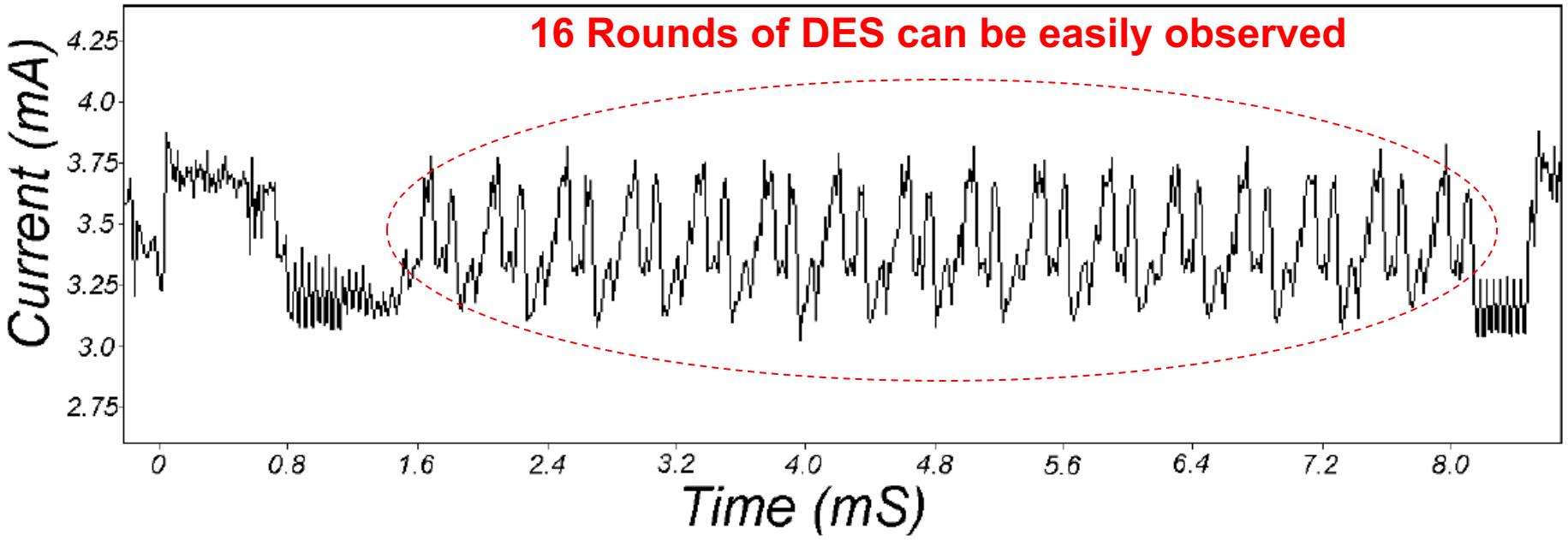
- DES is a block cipher
- 64 bit block length
- 56 bit key length
- 16 rounds
- 48 bits of key used each round (subkey)
- Each round is simple (for a block cipher)
- Security depends primarily on “S-boxes”

DES Round Operation



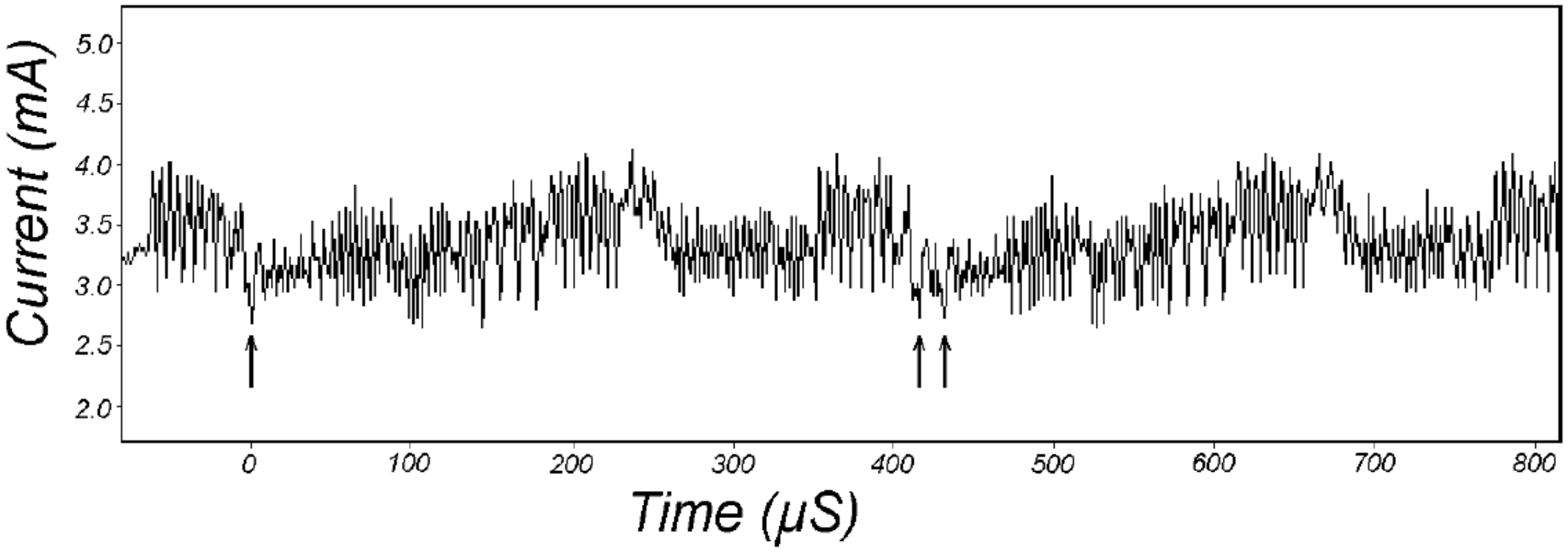
NANYANG TECHNOLOGICAL UNIVERSITY

Power Traces of DES



NANYANG TECHNOLOGICAL UNIVERSITY

Power Traces for DES



The 28 bit key registers C and D are rotated once in round 2, while twice in round 3. These conditional branches depending on the key bits leak critical information.

Contents

- Side Channel Attacks
- Timing Attack
- Power Attack
- *Attacks on ‘Secure’ Processor*
- Discussion

NANYANG TECHNOLOGICAL UNIVERSITY

1 Go to wooclap.com

2 Enter the event code in the top banner

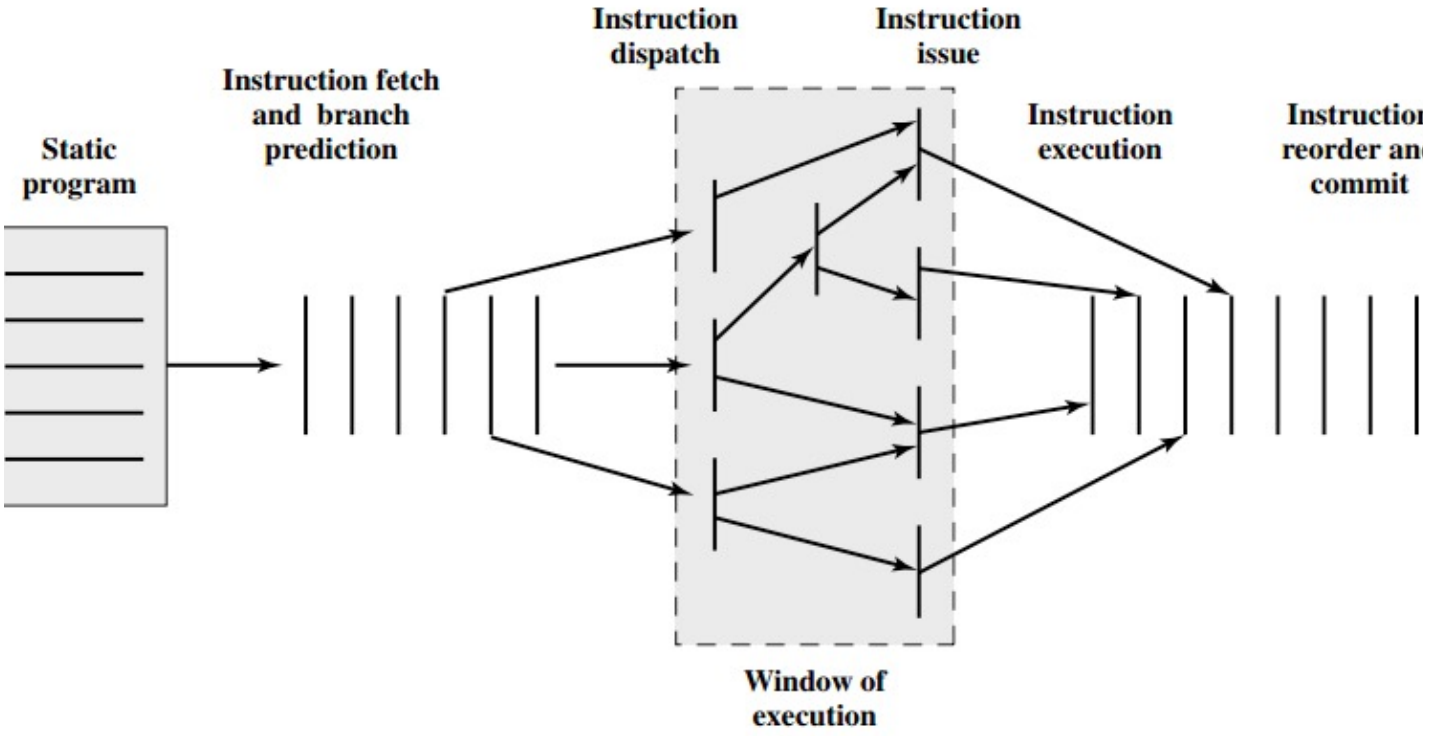
Event code
CPSSECURITY

Review: Pipeline Hazards

- Data hazards – read after write
  - Use data forwarding inside the pipeline
  - Do out-of-order execution for no dependency

- Control hazards – `beq`, `bne`, `j`, `jr`, `jal`
  - Stall – hurts performance
  - Predict – with even more hardware, can reduce the impact of control hazard stalls even further if the branch prediction (BHT) is correct and if the branched-to instruction is cached (BTB)

Superscalar Processor



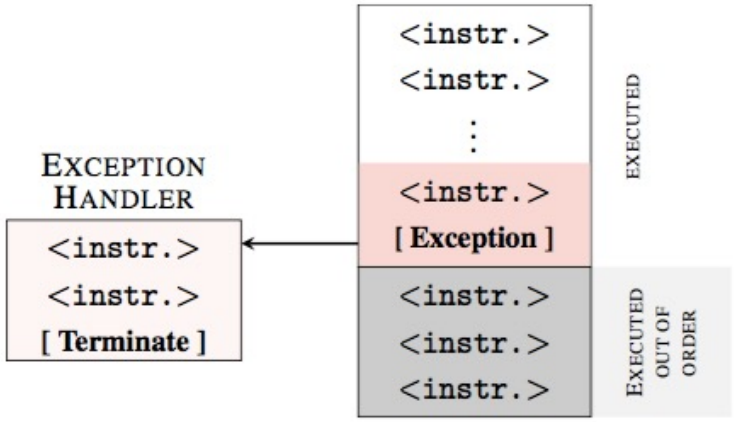
Meltdown Attack

- Out-of-order execution is an indispensable performance feature and present in a wide range of modern processors.
- The attack is independent of the operating system, and it does not rely on any software vulnerabilities.
- Meltdown exploits side-channel information available on most modern processors,
  - e.g., modern Intel microarchitectures since 2010 and potentially on other CPUs of other vendors.

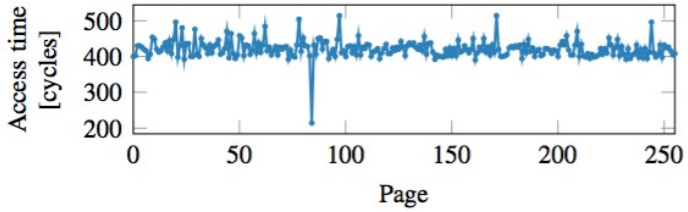
https://meltdownattack.com/

Meltdown Attack *(contd.)*

```
1 raise_exception();
2 // the line below is never reached
3 access(probe_array[data * 4096]);
```



OOO Execution



Data loaded into cache

NANYANG TECHNOLOGICAL UNIVERSITY

Plundervolt Attack

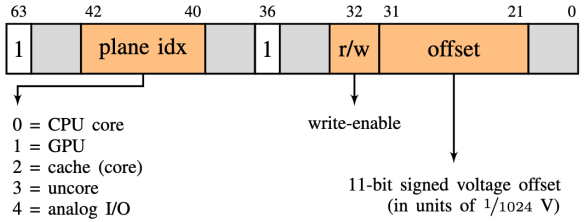
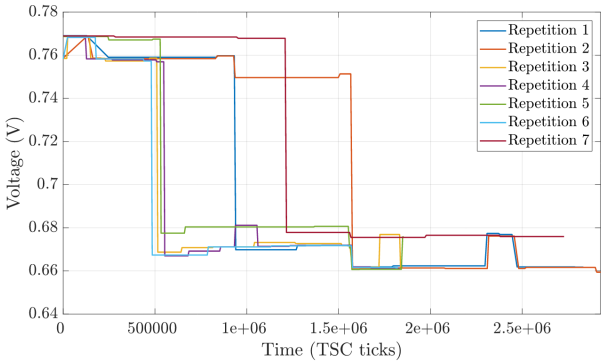


Fig. 1. Layout of the undocumented undervolting MSR with address `0x150`.

- Software-based fault injection flow
  - Undocumented Model-specific Register used for controlling voltage scaling
  - Voltage modification leads to slower execution and unfinished computations



- Can be controlled to mount attacks
  - OpenSSL signature corruption
  - RSA key recovery
  - Redirecting outside secure enclave

Follow-up

- Speculative Execution can be disabled
  - Up to 45% performance drop reported
- Can also be vulnerable for other speculative executions, e.g., branch prediction
- Intel SGX discontinued, new product line Trust Domain Extensions (TDX) introduced
- Fundamental trade-off between Security and Efficiency

Contents

- Side Channel Attacks
- Timing Attack
- Power Attack
- Attacks on ‘Secure’ Processor
- *Discussion*

NANYANG TECHNOLOGICAL UNIVERSITY

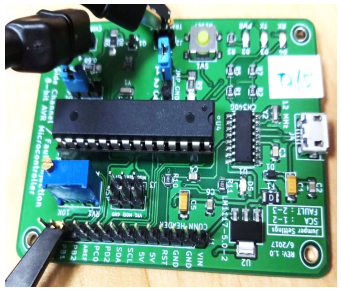
1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
CPSSECURITY

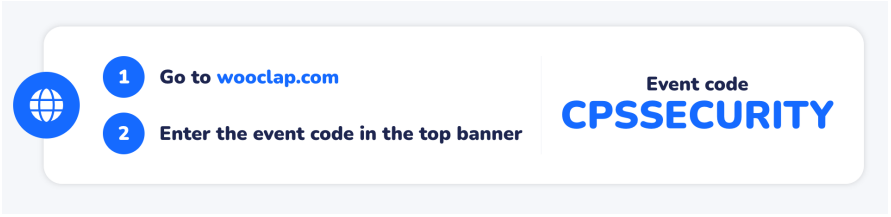
What did we learn?

- **What are typical micro-architectural attacks?**
  - *Active*
  - *Passive*



- **Timing Attack**
  - *Cache access*
- **Power Attack**
  - *Correlation of Power and Data*
- **Recent Attacks**
  - *Discontinued Product Line*

The End



NANYANG TECHNOLOGICAL UNIVERSITY