Power Analysis Attacks
能量分析攻擊

童御修[1] 李祐棠[2] JP[2,3] 陳君明[4,5] 鄭振牟[1,3]

1 國立臺灣大學 電機工程學系
2 國立臺灣大學 電信工程學研究所
3 中央研究院 資訊科技創新研究中心
4 國立臺灣大學 數學系
5 銓安智慧科技（股）

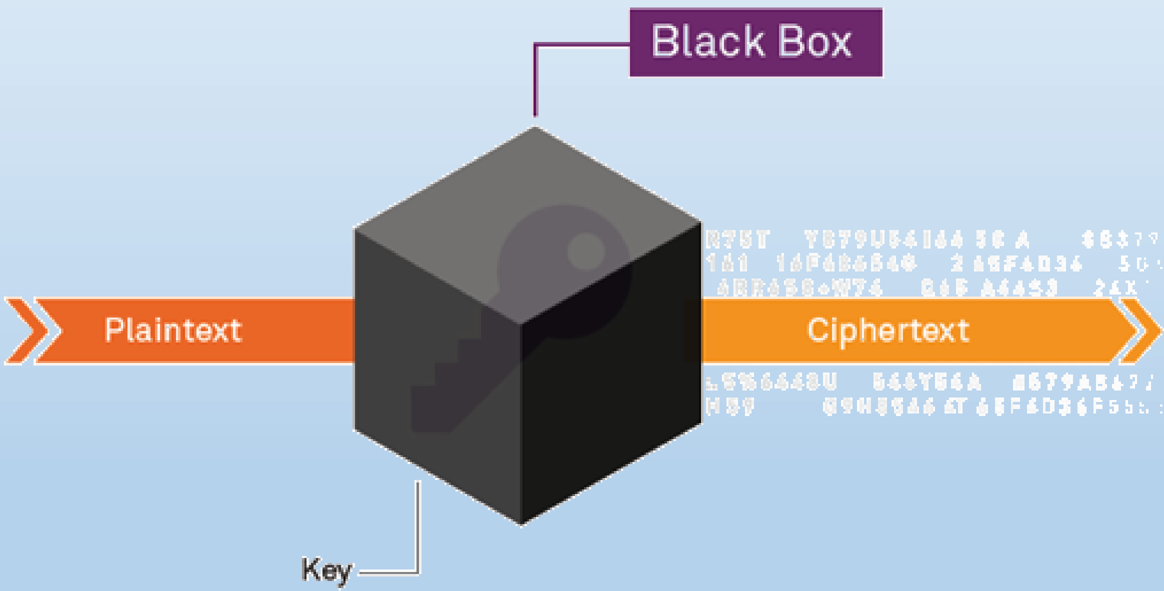
Fast Crypto Lab

Agenda

- Introduction
  - Attacks on Implementations
  - Experiment Setup
- Demo -- Break AES-128
- Power Analysis Attacks
  - Foundation
  - Example on AES-128
  - Workflows

Traditional Cryptanalysis

Attackers can only observe the external information



What if we can see insides?

Attacks on Implementations

Invasive	Semi-invasive	Non-invasive
Microprobing Reverse engineering	UV light, X-rays or lasers	Side-channel attacks

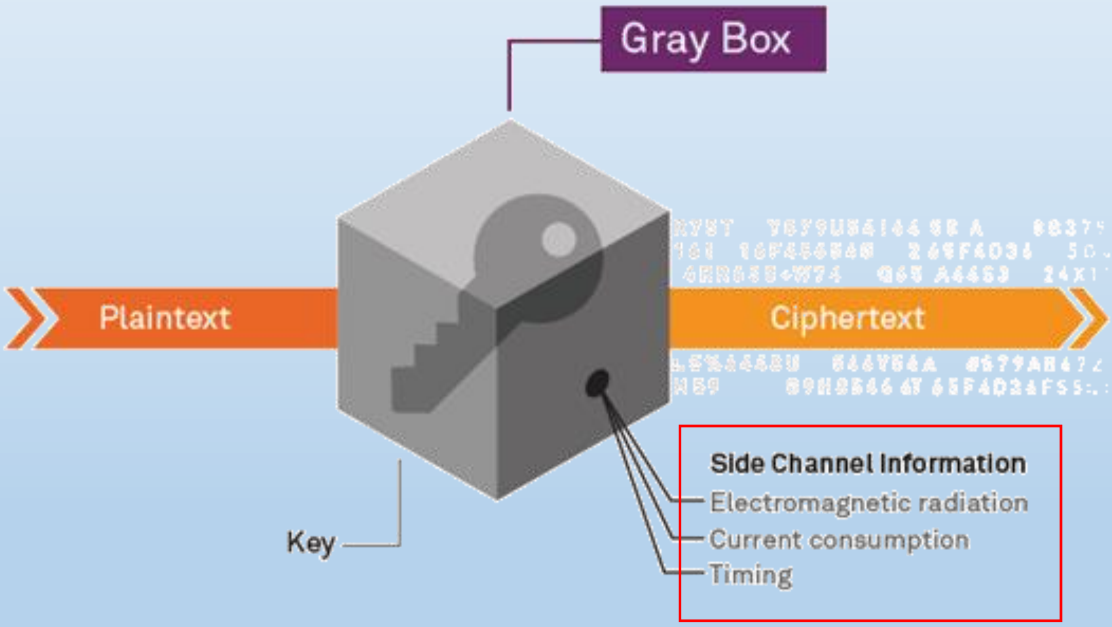
Attack scope →

← Cost

Side-channel attacks:
Cheaper & effective

Side-Channel Attacks　旁通道攻擊

Attackers analyze the “leakage” from the devices

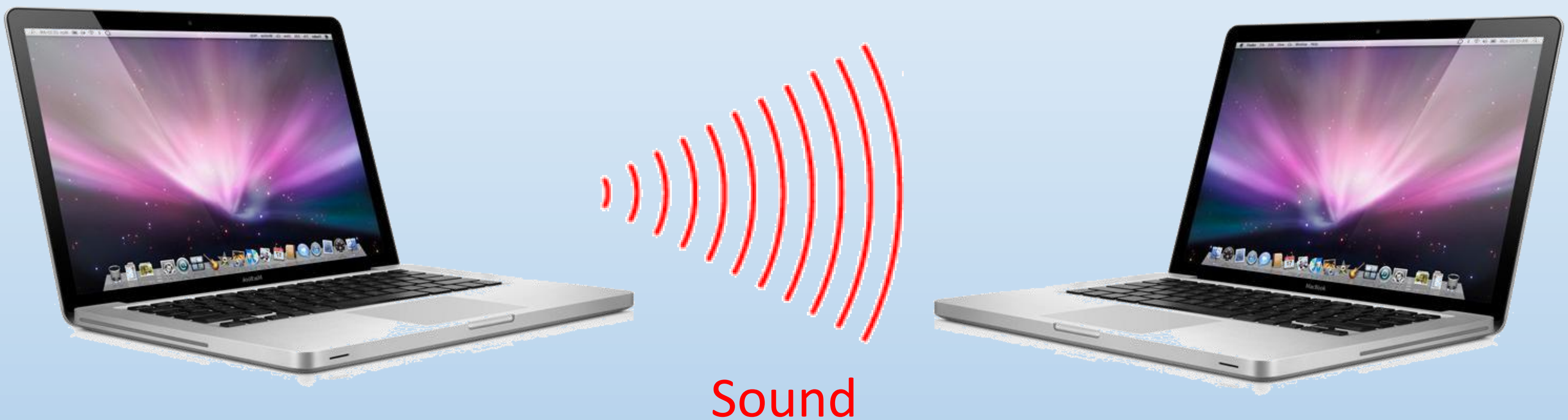


Different keys cause different leakage!


AES
Side Channel Attack
旁通道攻擊！！

Example: Acoustics Cryptanalysis

Adi Shamir (S of RSA) *et al*, 2013



Execute GnuPG's RSA-4096

Capture and analyze

Side-Channel Leakages

Timing — ex. Password comparison

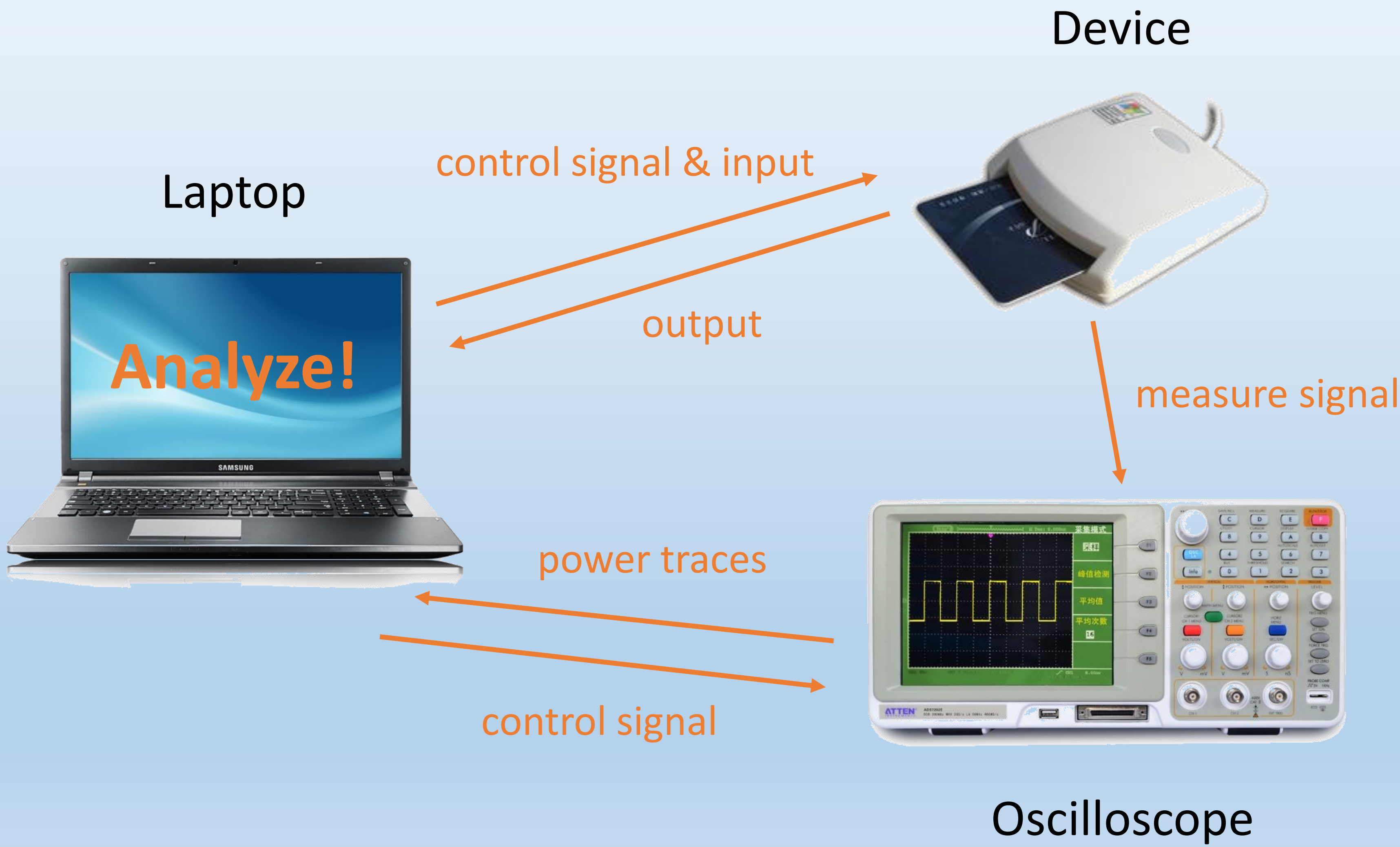
Power — Paul Kocher proposed the first attack:
DPA, Differential Power Analysis (1999)
[CRI, Cryptography Research Inc.]

EM — Similar to power consumption

Others — Sound, temperature, …

Power leakage is easier to deal with

Experiment Setup



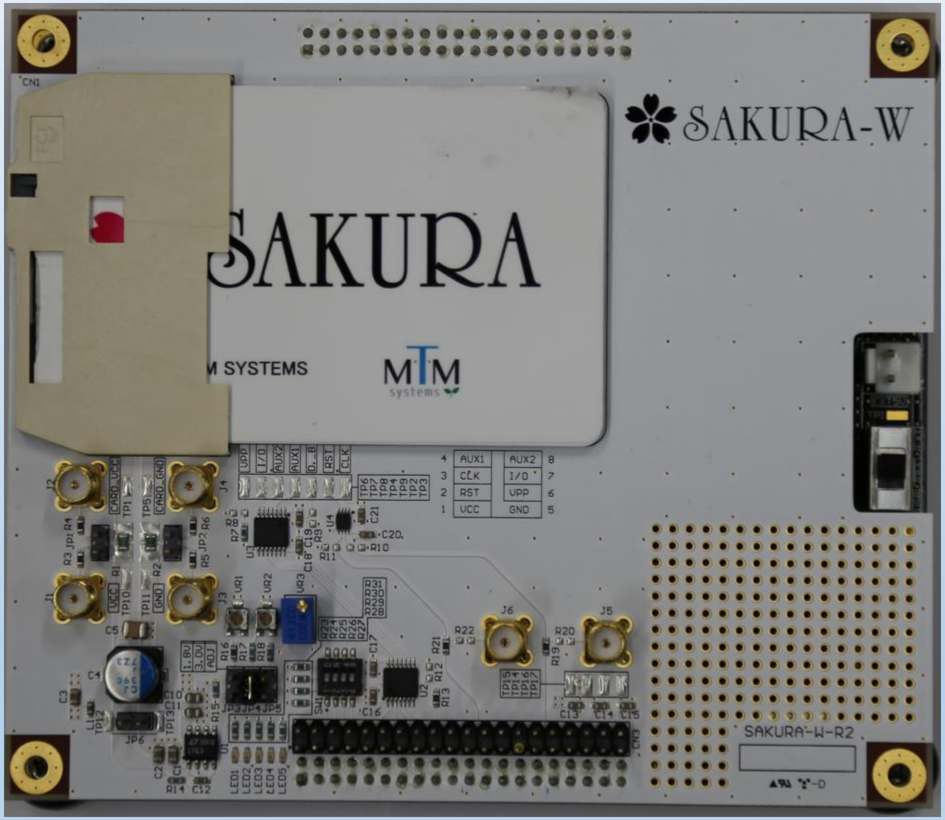
Equipment (1)

PicoScope 3206D with sampling rate 1GSa/s

≈NTD 50,000

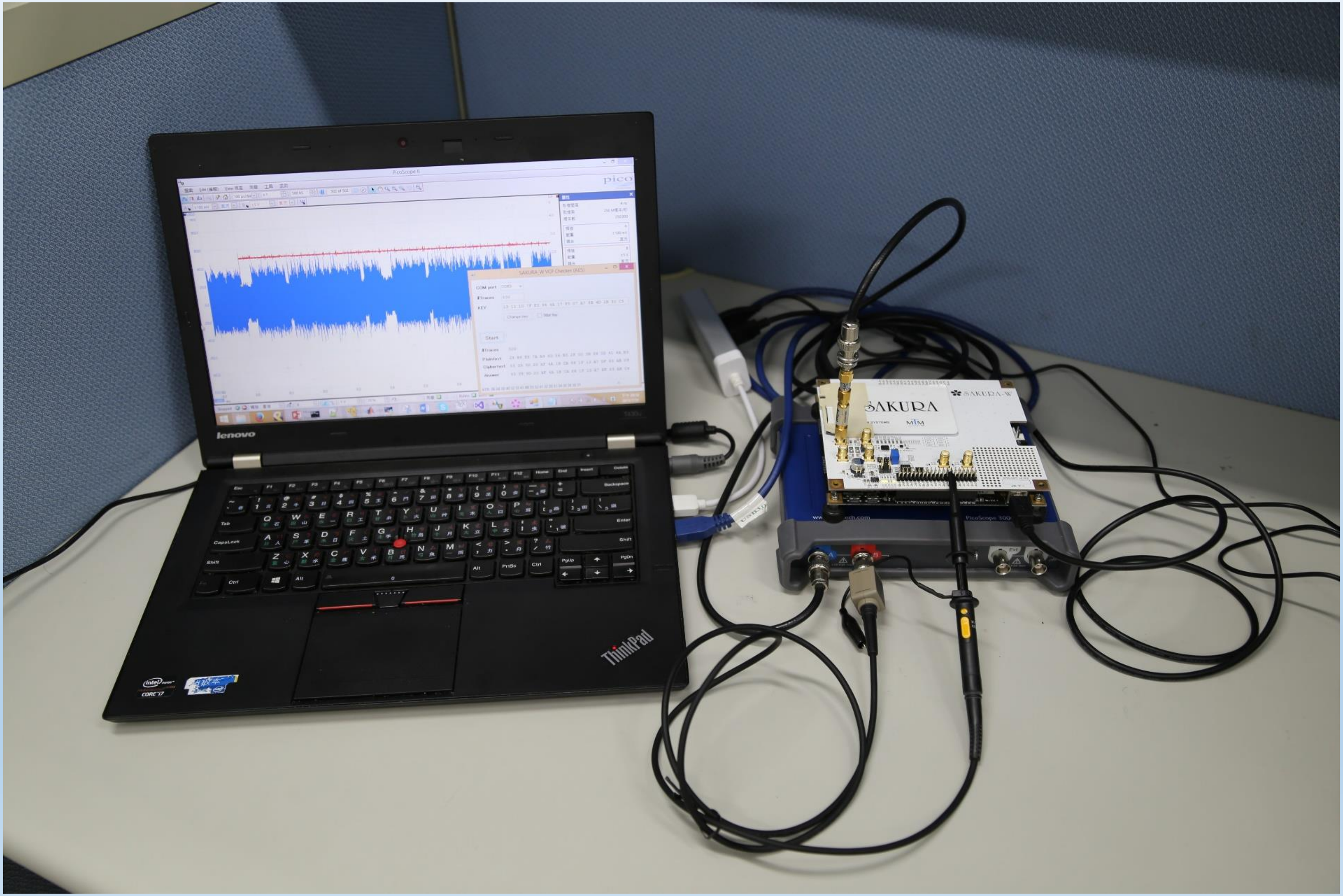
Equipment (2)

SAKURA evaluation board ***≈NTD 100,000***



UEC Satoh Laboratory

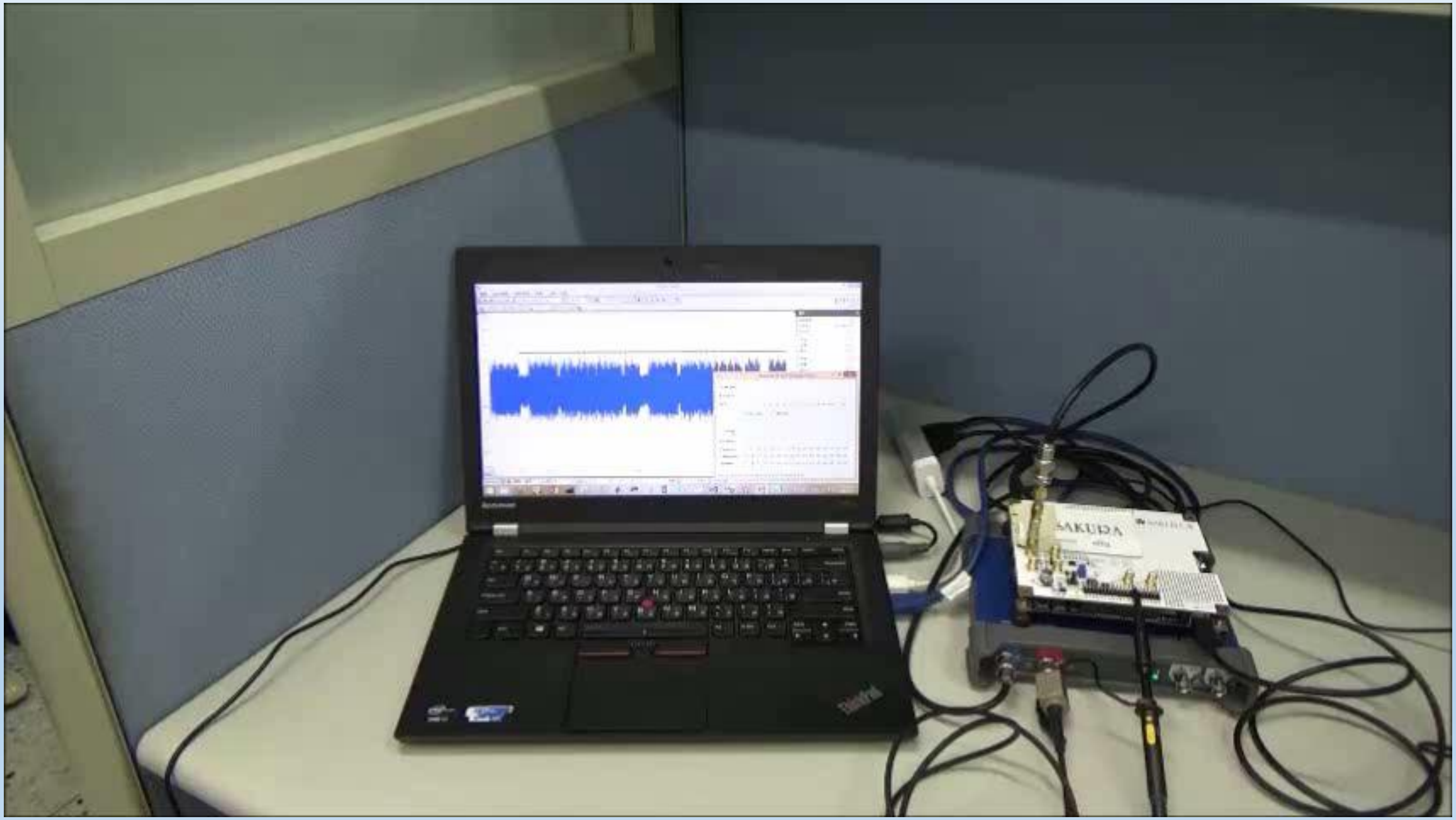
Our Environment



Demo

Extract the secret key from AES-128 on SmartCard

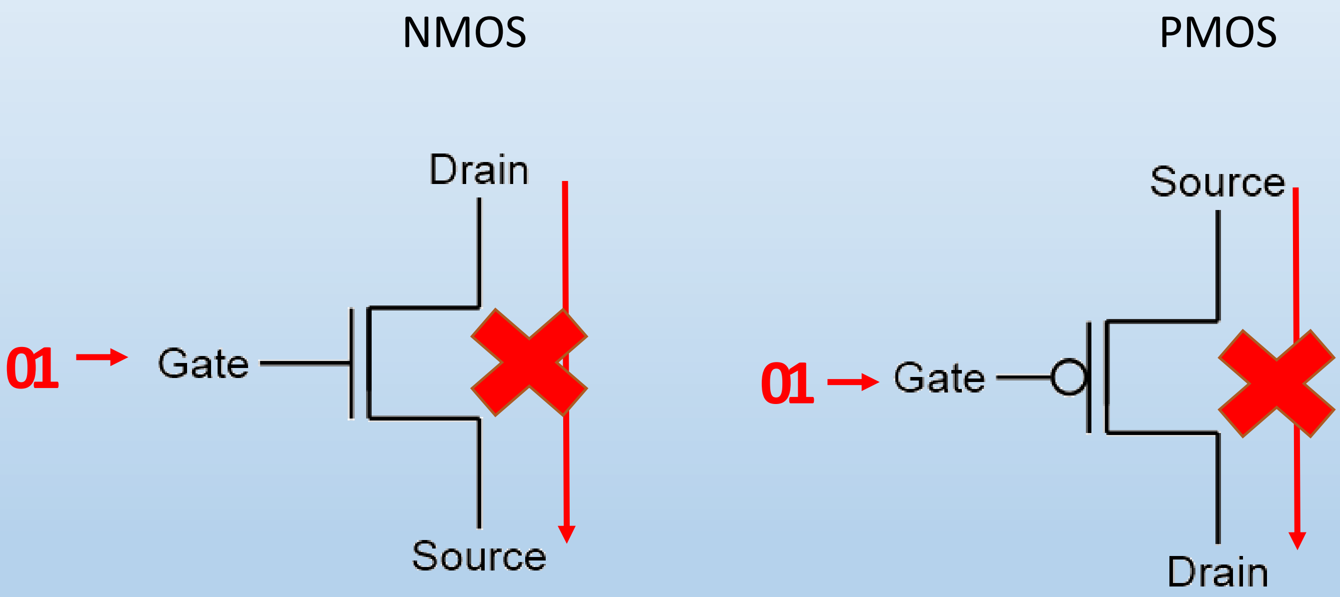
Key: 13 11 1d 7f e3 94 4a 17 f3 07 a7 8b 4d 2b 30 c5



So Why Power Analysis Succeeds?

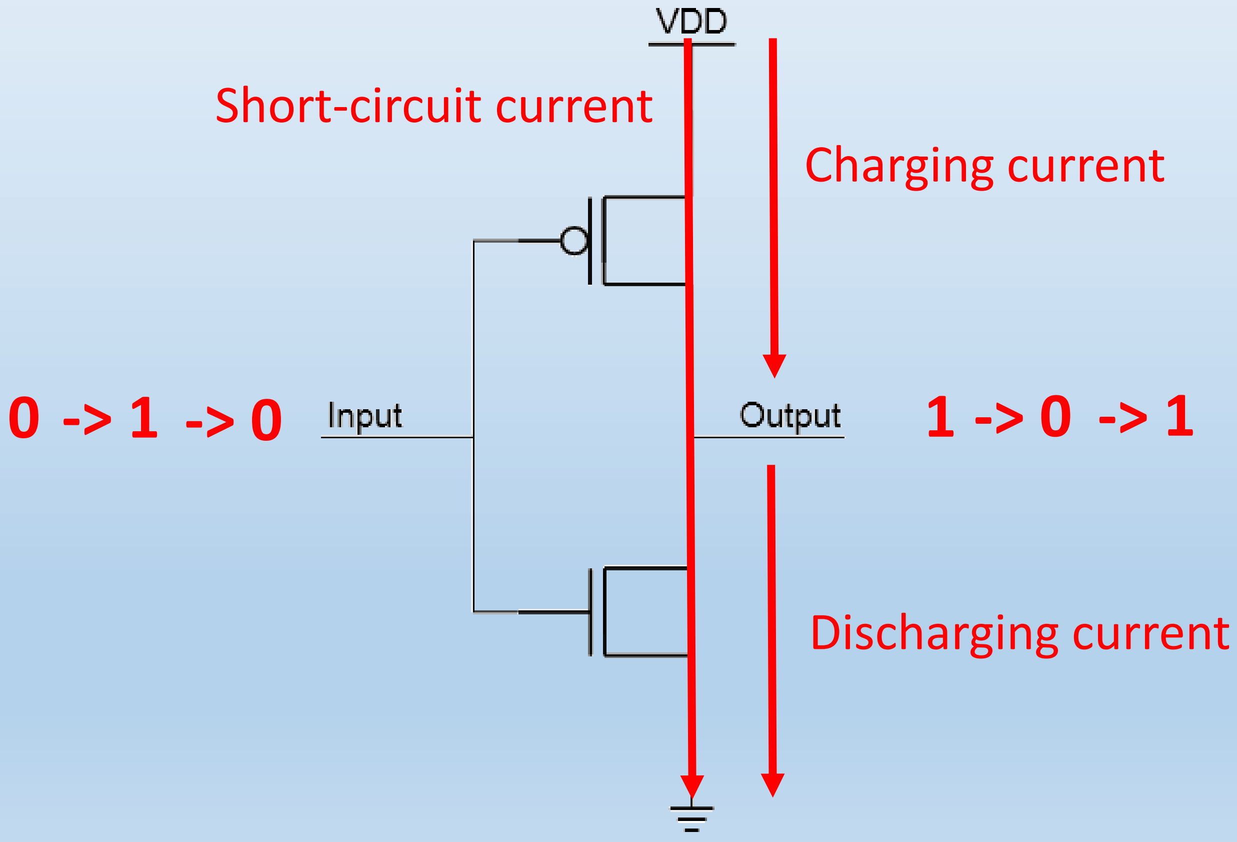
Foundation of Power Analysis (1)

CMOS technology



Foundation of Power Analysis (2)

Power consumption of CMOS inverter



Foundation of Power Analysis (3)

CMOS consumes much more power in dynamic state

Thus we use the power model

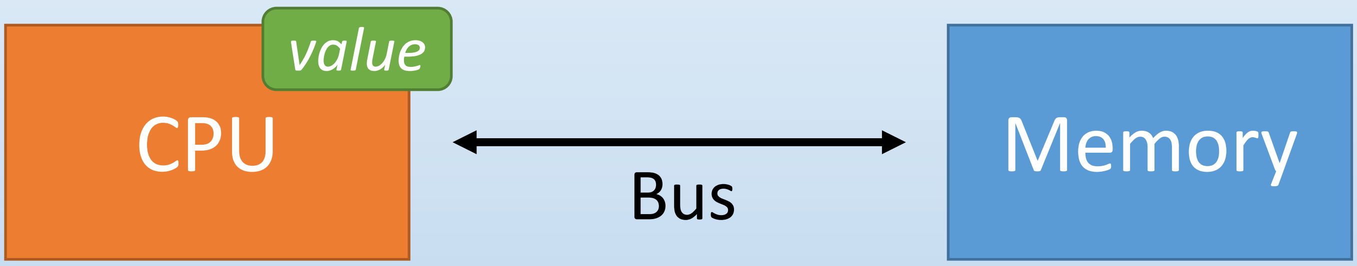
$$\text{Power} = a \cdot \#\,\textit{bitflips} + b$$

Hamming Weight: HW(101100) = 3

Hamming Distance: HD(0011, 0010) = 1

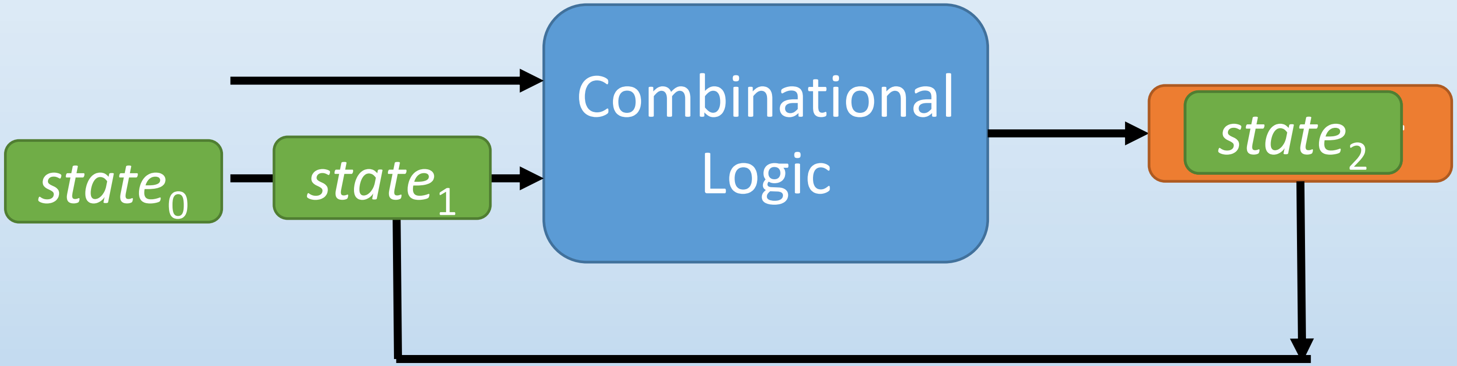
Software Example

Data transferred between memory and CPU



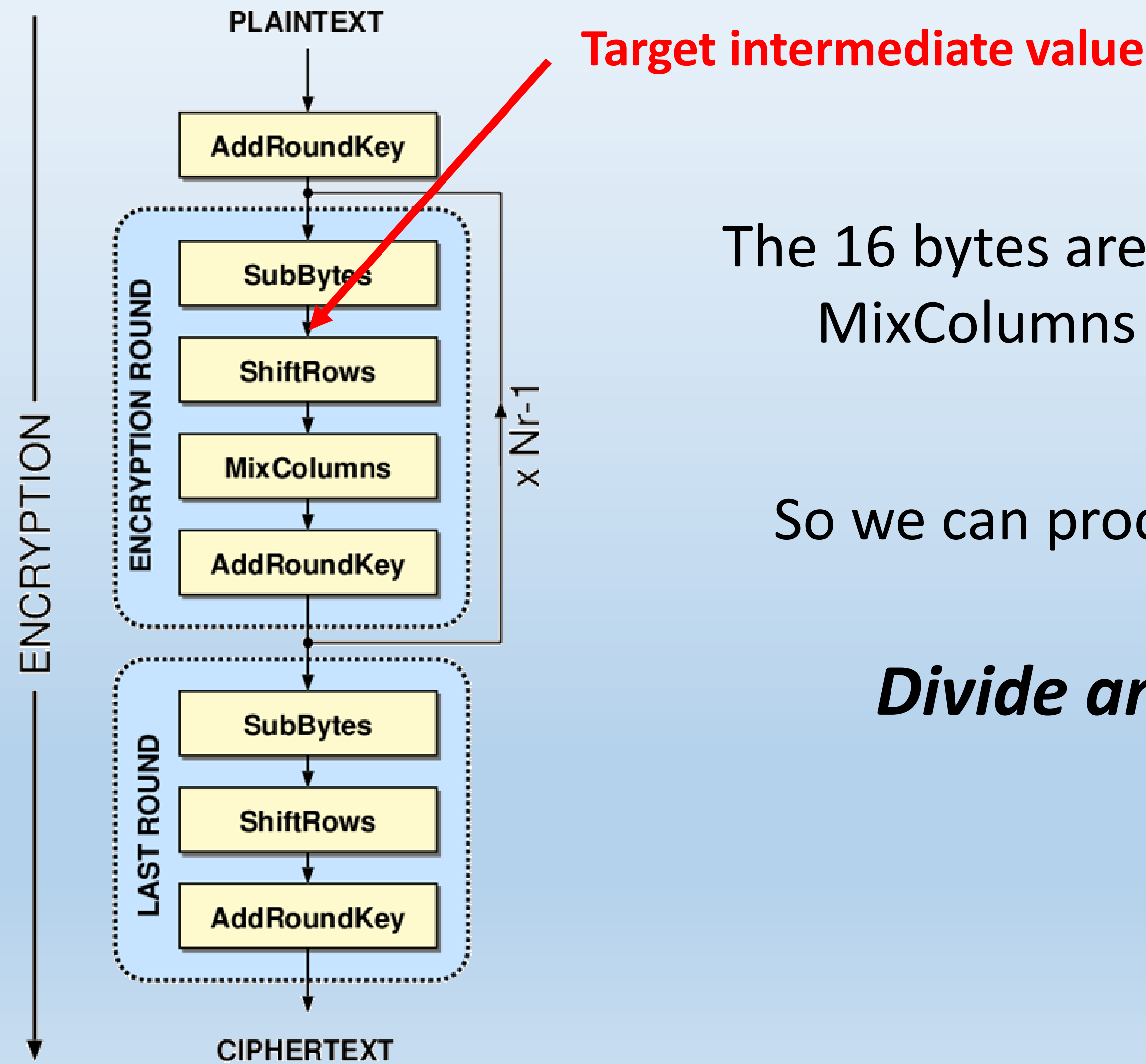
 # bitflips = HW(*value*)

Hardware Example



$$\#\ bitflips = \mathrm{HD}(state_i\,, state_{i+1})$$
$$= \mathrm{HW}(state_i \oplus state_{i+1})$$

Example: on AES-128

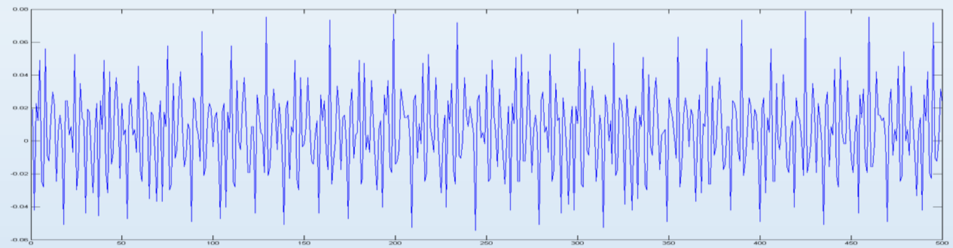


The 16 bytes are independent before MixColumns in the first round

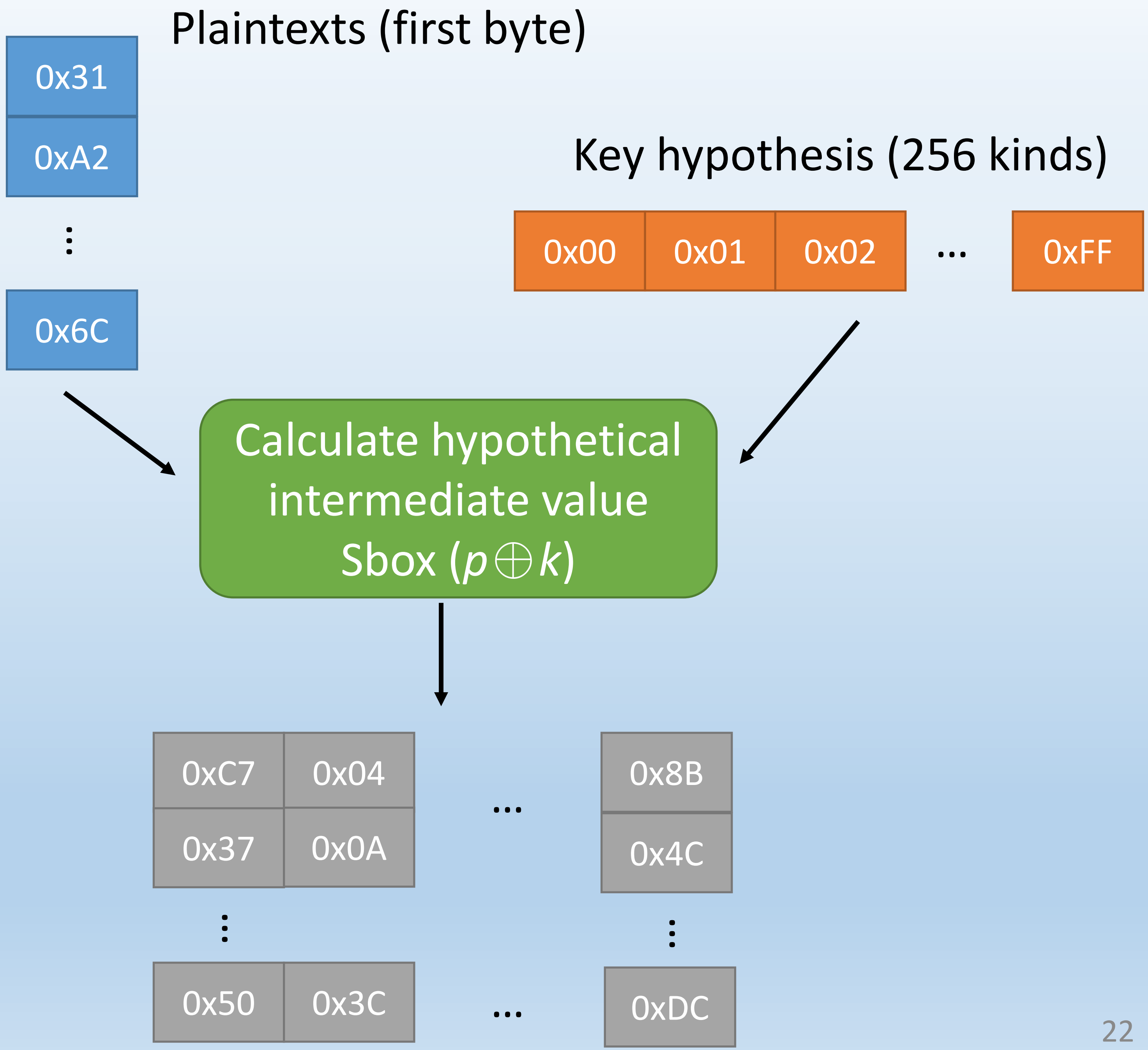
So we can process it byte by byte

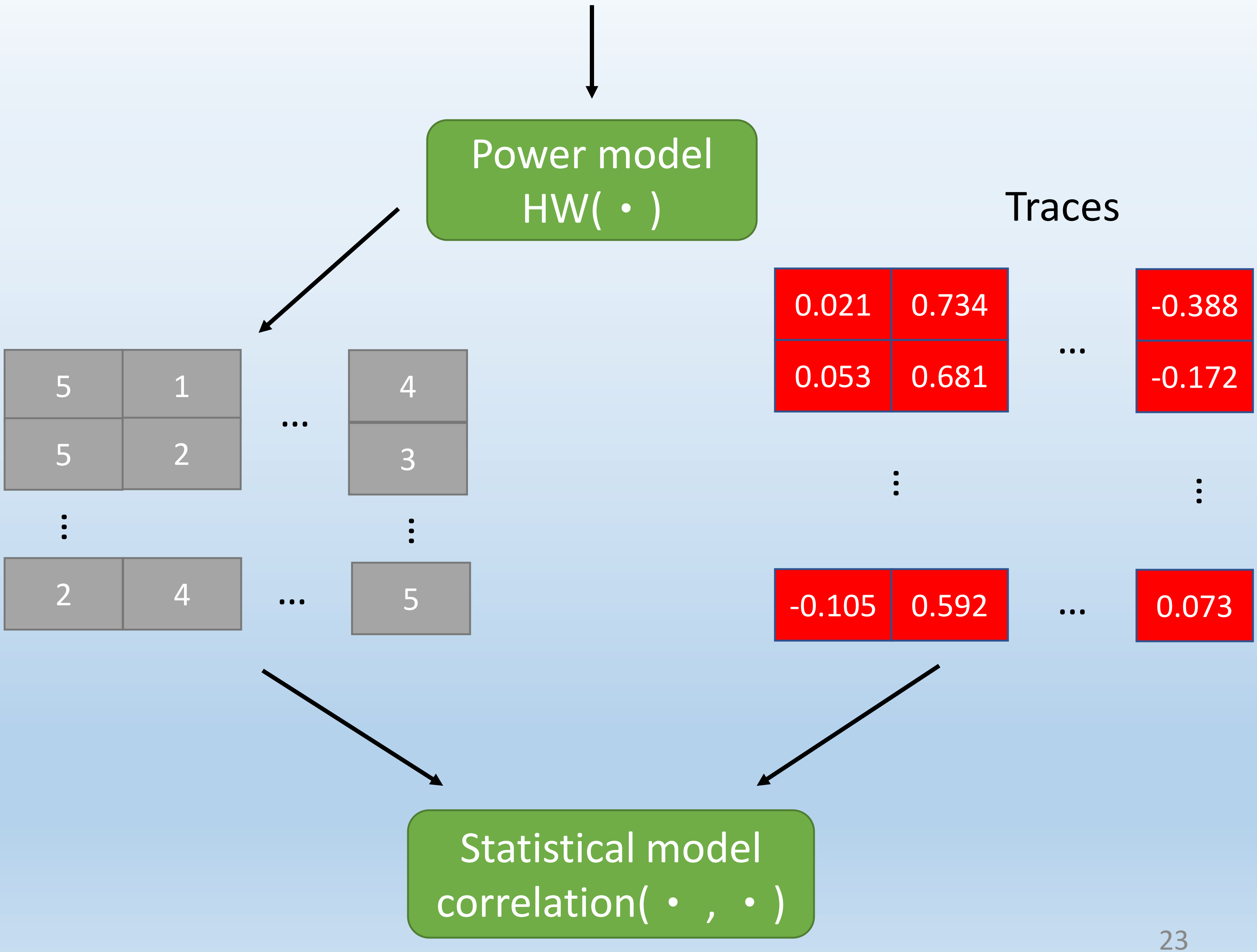
Divide and Conquer!!

Measuring Power Traces



Plaintexts		Traces			
0x3128A6DA……7C	→	0.021	0.734	…	-0.388
0xA24B6E1D……97	→	0.053	0.681	…	-0.172
⋮		⋮			⋮
0x6C7B32C……82	→	-0.105	0.592	…	0.073


Plaintexts (first byte)
0x31
0xA2
⋮
0x6C
Key hypothesis (256 kinds)
0x00
0x01
0x02
…
0xFF
Calculate hypothetical intermediate value
Sbox ($p \oplus k$)
0xC7
0x04
0x37
0x0A
⋮
0x50
0x3C
…
0x8B
0x4C
⋮
0xDC
…

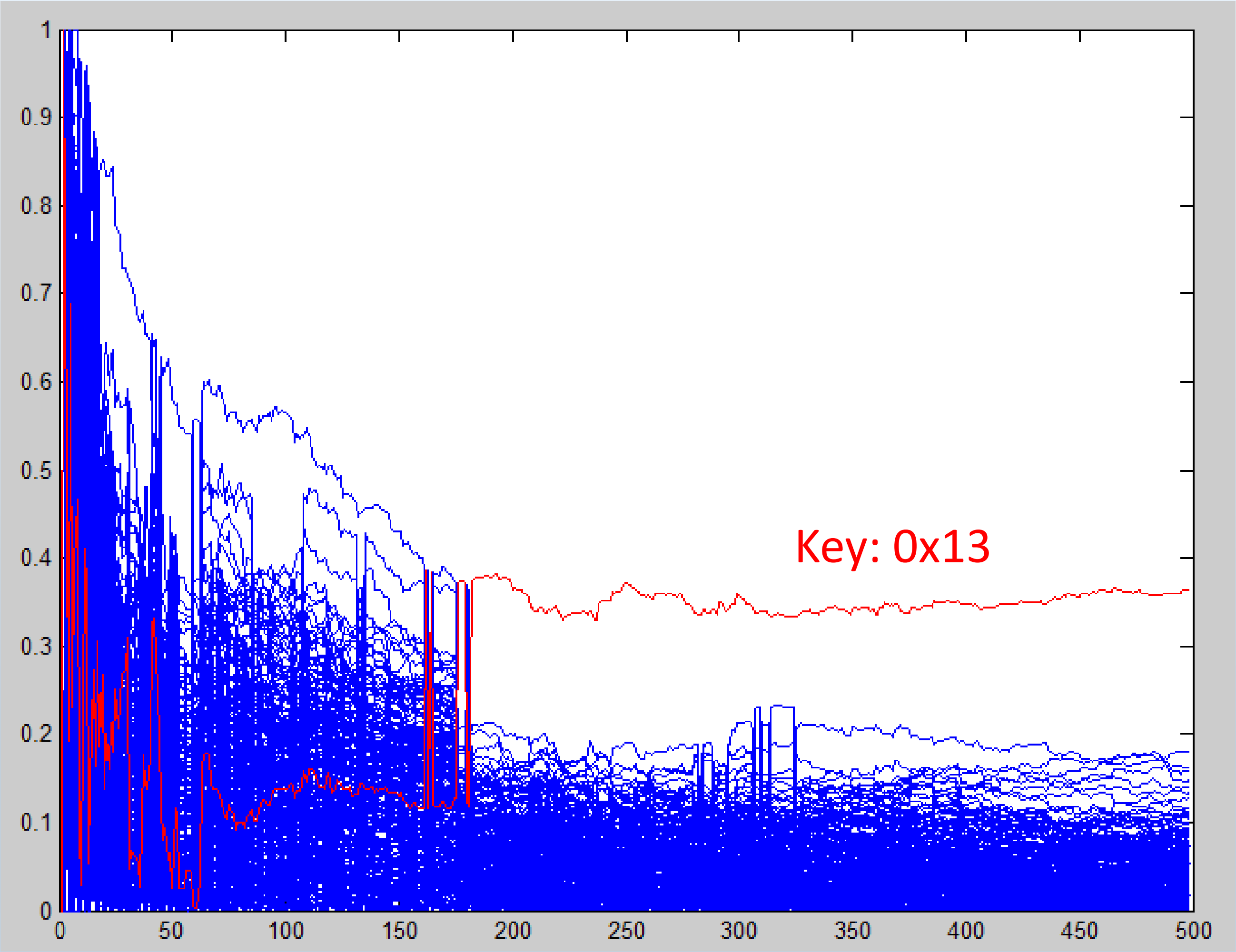

Power model
HW(•)
Traces
0.021
0.734
0.053
0.681
…
-0.388
-0.172
5
1
5
2
…
4
3
2
4
…
5
-0.105
0.592
…
0.073
Statistical model
correlation(• , •)

Correlation coeffieints matrix

Key 0x00 →	0.005	-0.124	...	0.181
Key 0x01 →	0.013	0.090		-0.103
	⋮			⋮
Key 0x13 →	0.053	0.372		-0.084
	⋮			⋮
Key 0xFF →	-0.131	0.095	...	-0.001

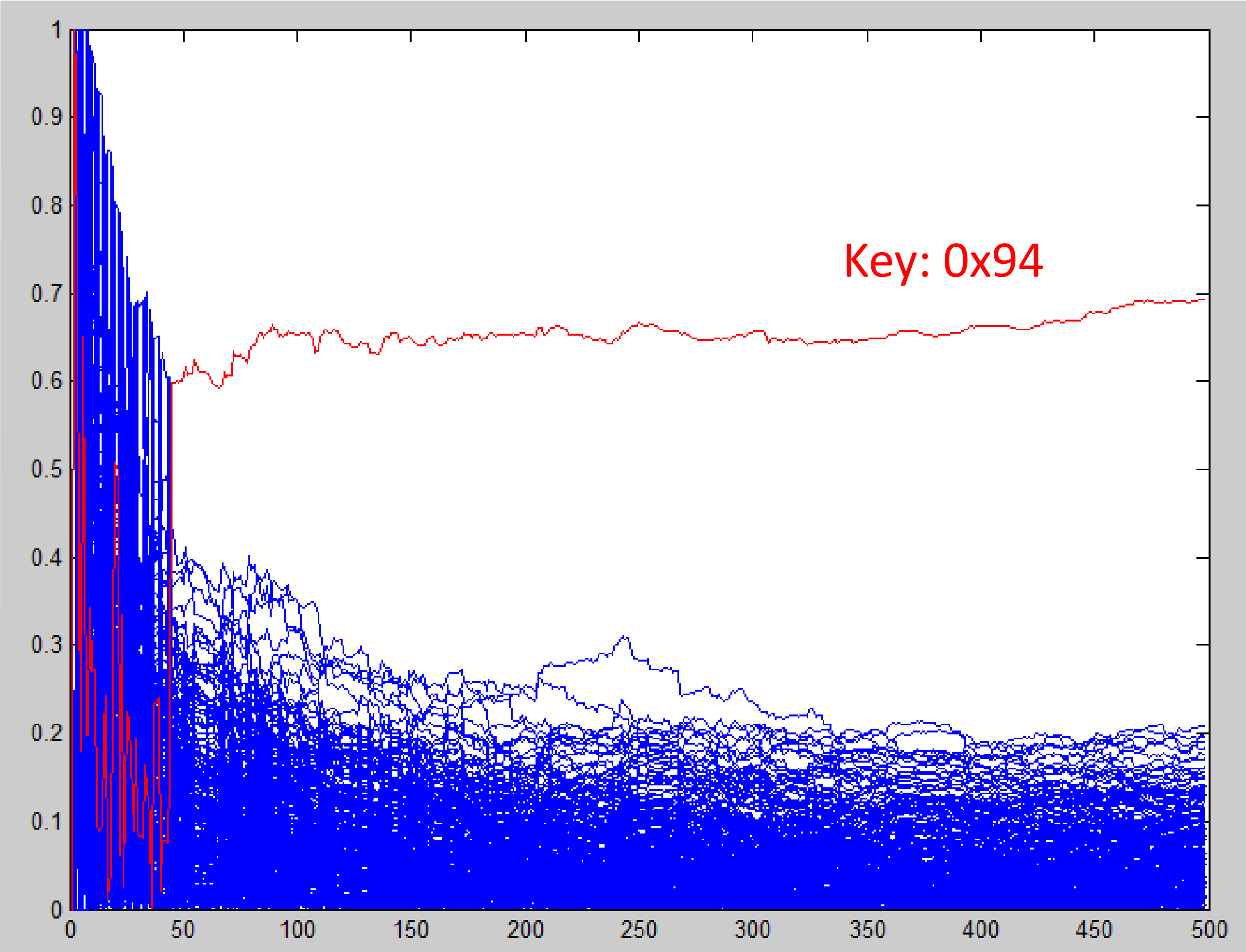
0x13 is the correct key of the first byte !

Experimental Results (1)



Byte 1

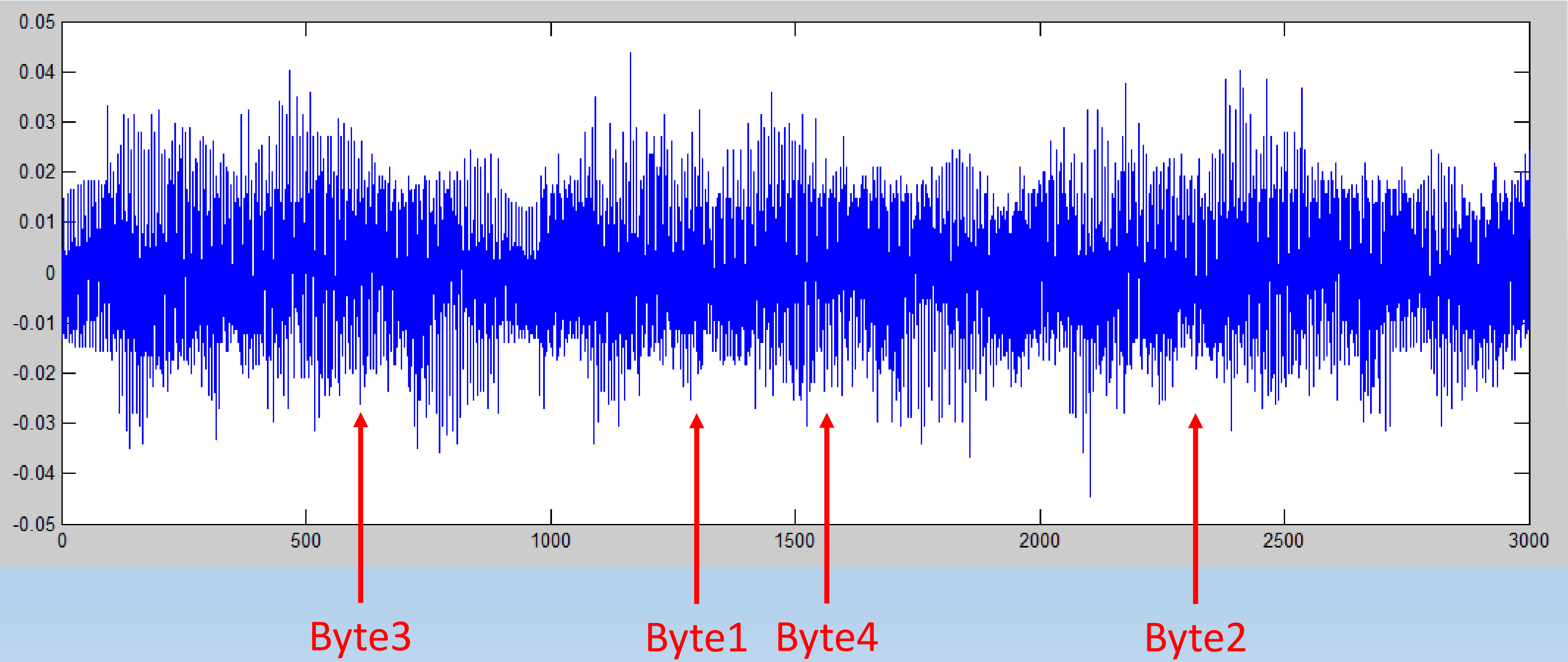
Experimental Results (2)



Byte 6

Experimental Results (3)

13	11	1D	7F	E3	94	4A	17	F3	07	A7	8B	4D	2B	30	C5
0.3632	0.4395	0.4754	0.5289	0.4127	0.6945	0.3654	0.5744	0.4273	0.5941	0.5685	0.6277	0.6100	0.3013	0.6545	0.4851
1276	2384	583	1518	1568	1072	724	1441	2015	1716	1086	2384	2447	1941	1723	1086



Power Analysis Workflow (1)

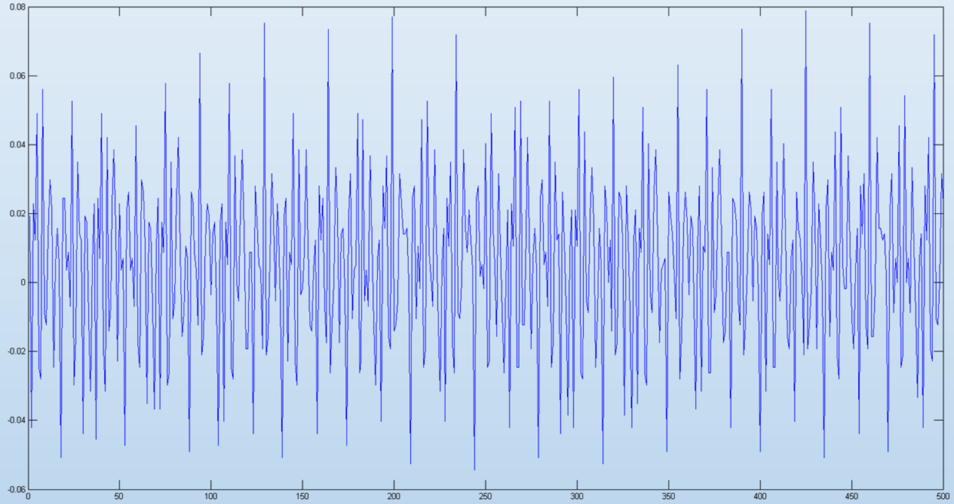
Choose the target ***intermediate value***

in the above examples

1. Both input-dependent and key-dependent
2. Better after a permutation function
3. *value* = *f* (*input*, *key*)

Power Analysis Workflow (2)

Measure the power traces



Remember to record the corresponding plaintexts

Power Analysis Workflow (3)

Choose a ***power model***

$$\#\ bitflips = \mathrm{HW}(value)$$

$$\#\ bitflips = \mathrm{HD}(state_i\ ,\ state_{i+1})$$

- Usually
  - HW model in software like SmartCard
  - HD model in hardware like ASIC and FPGA

Power Analysis Workflow (4)

hypothetical intermediate value and ***hypothetical power consumption***

For each input, calculate the intermediate value for all possible keys and apply them to the power model

$$HW(f(input_1, key_1))$$
$$HW(f(input_1, key_2))$$
$$\vdots$$
$$HW(f(input_1, key_n))$$

Power Analysis Workflow (5)

Apply the ***statistic analysis***

correlation (*measured power, hypo. power*)

1. For linear power model, Pearson's correlation coefficient is a good choice
2. Other models: difference of means, mutual information……

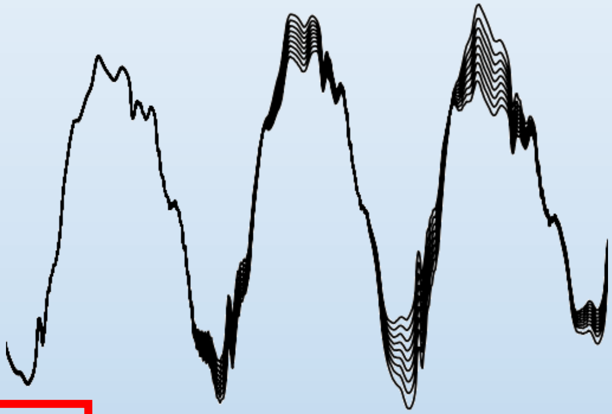
Workflow Summary

1. Choose the target ***intermediate value***
2. Measure the power traces
3. Choose a ***power model***
4. Calculate the ***hypothetical intermediate value*** and corresponding ***hypothetical power consumption***
5. Apply the ***statistic analysis*** between ***measured power consumption*** and ***hypothetical power consumption***

Remarks (1)

Many other power analysis attacks

- Simple power analysis type
  - Template attacks

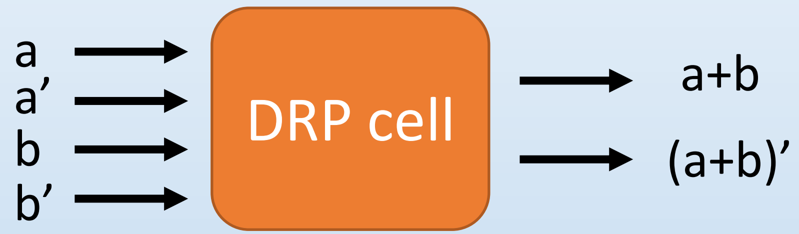


- Differential power analysis type
  - Correlation power attacks (our attack)
  - High-order side-channel attacks
  - Mutual information analysis
  - Algebraic side-channel attacks

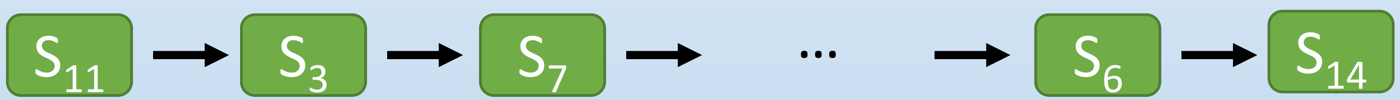
Remarks (2)

Countermeasure: Hiding

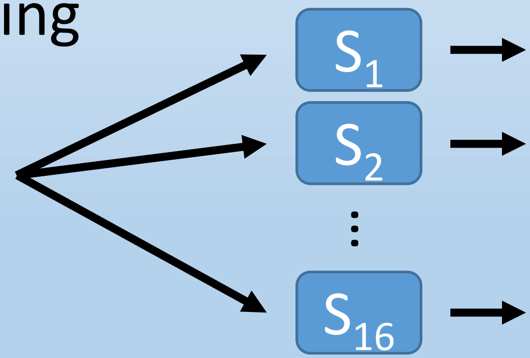
- Break the link between power and processed values
  - Dual-rail precharge logic cell



  - Shuffling



  - Parallel computing



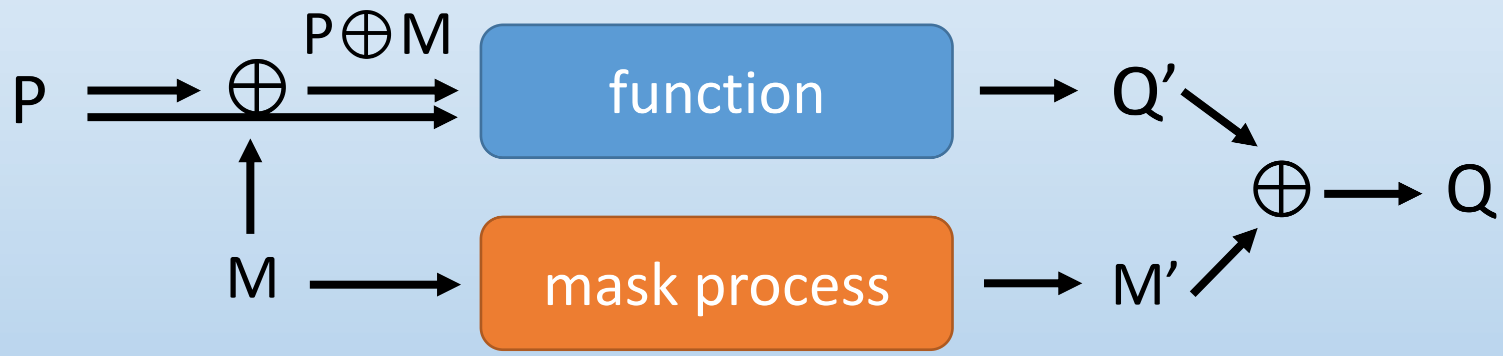
Pros: easy to implement

Cons: overhead, relationship still exists

Remarks (3)

Countermeasure: Masking

- Generate random numbers to mask the variables



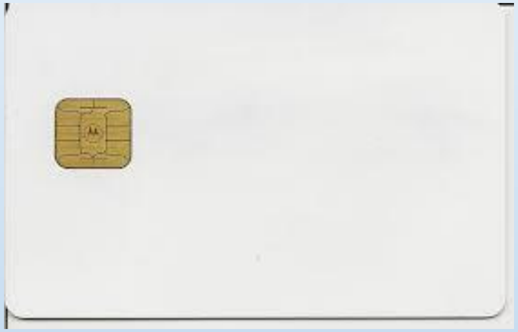
Pros: provably secure

Cons: overhead, implementation issues

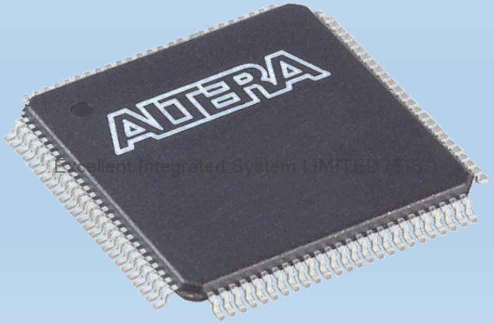
Remarks (4)

From theory to reality

- Need knowledge of the devices
  - Algorithms
  - Commands
  - Implementations



- Different attack scenario
  - Known plaintext/ciphertext
  - Known ciphertext
  - Chosen plaintext

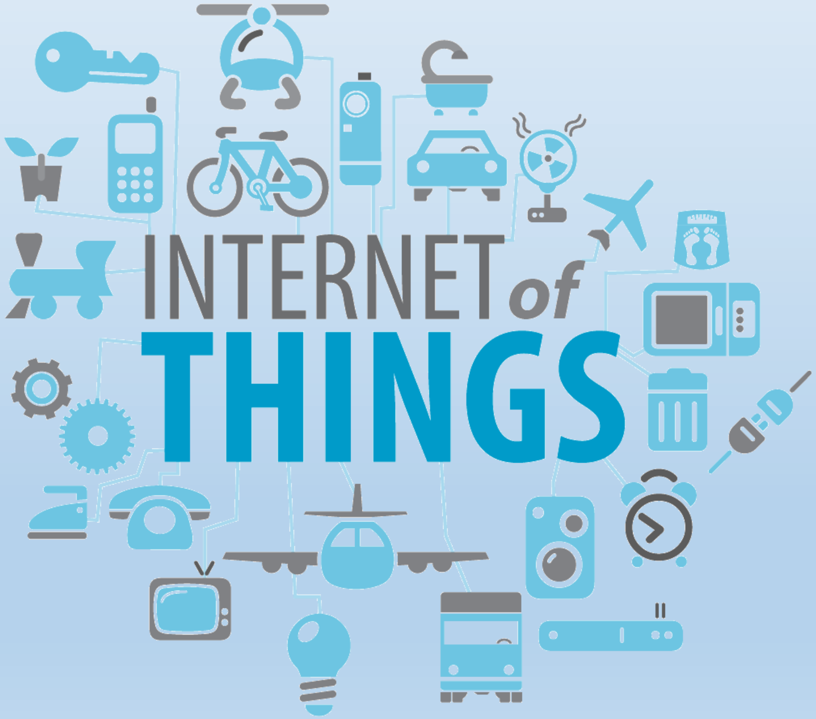


Conclusions

- A practical threat against SmartCards, embedded devices and IoT (Internet of Things) chips

- We provide a platform to evaluate/attack on those cryptographic devices

- Future study
  - different ciphers
  - different devices
  - new countermeasures



References

- S. Mangard *et al*. Power Analysis Attacks.
- SAKURA project: http://satoh.cs.uec.ac.jp/SAKURA/index.html
- DPA contest: http://www.dpacontest.org/home/
- E.Brier *et al*. Correlation Power Analysis with a Leakage Model.
- Papers from CHES, Eurocrypt, Crypto and Asiacrypt

Thank you !