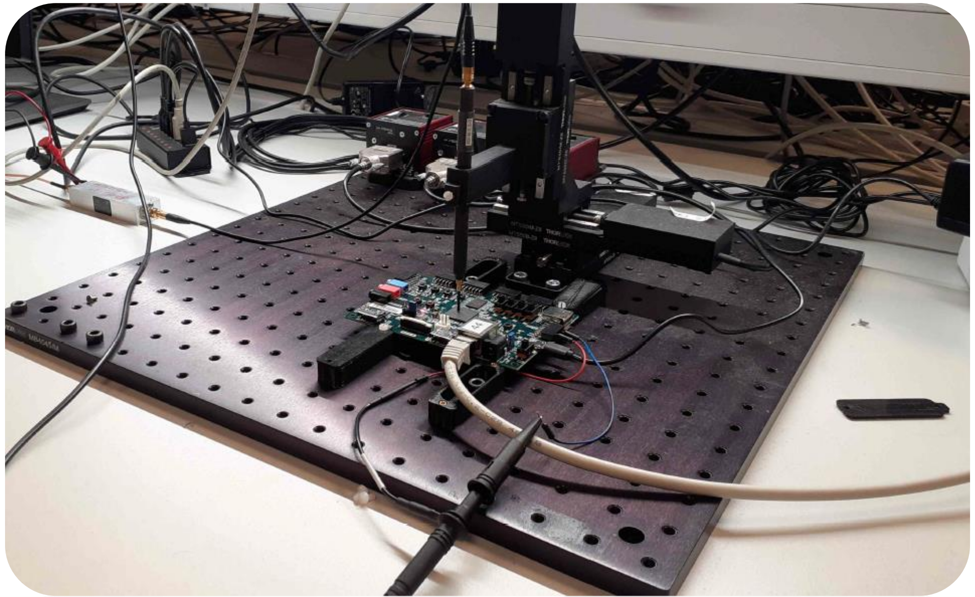
Side-channel Analysis



Thomas Hiscock (thomas.hiscock@cea.fr)

LTSO Laboratory (CEA/LETI)

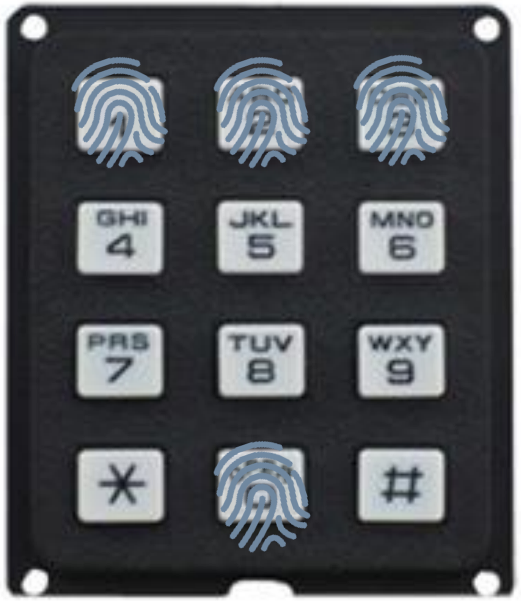
Outline

1. Introduction
2. Basic side-channel analysis techniques
3. Side-channel analysis on smartphones

Specification vs. Reality

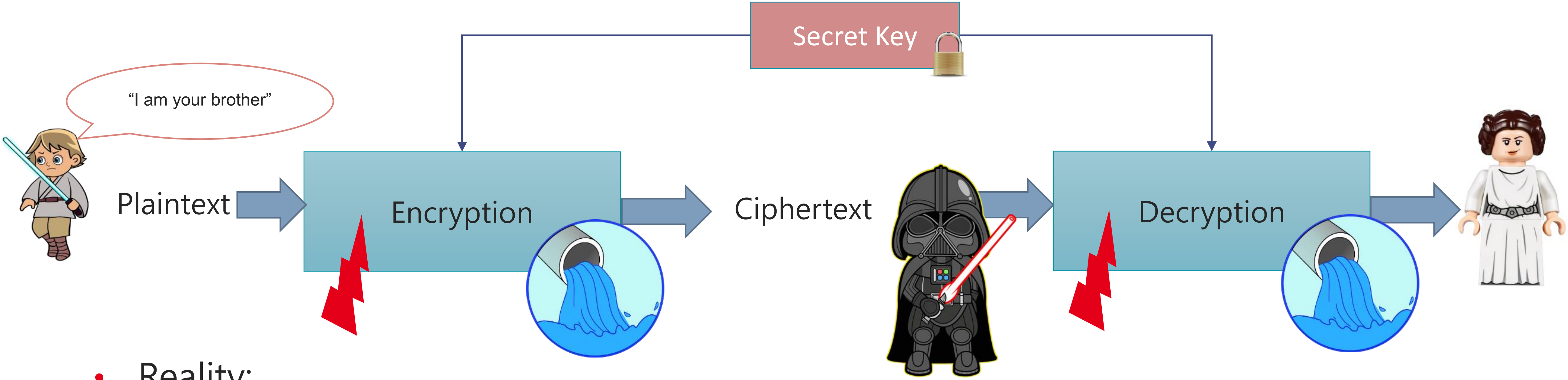
- Specification:
  - 4 character password
  - 12^4 = 20 736 possibilities

- Reality:
  - 4! = 24 possibilities



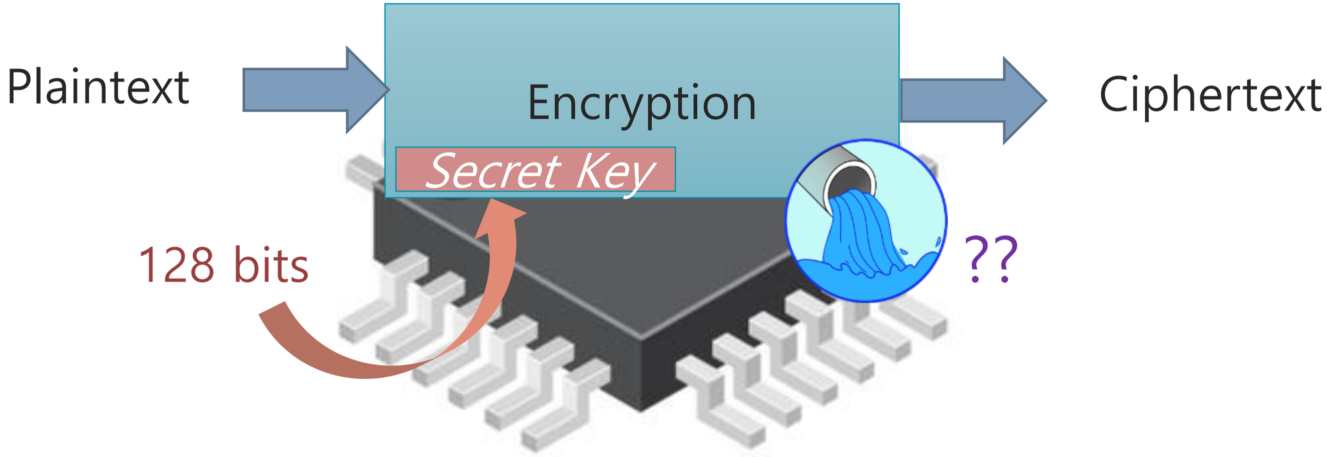
Cryptographic primitives

- Designer’s view: “Black box” model



- Reality:
  - Bugs in implementation (sometimes)
  - Encryption / Decryption run on real hardware
    - Observability
    - Perturbation

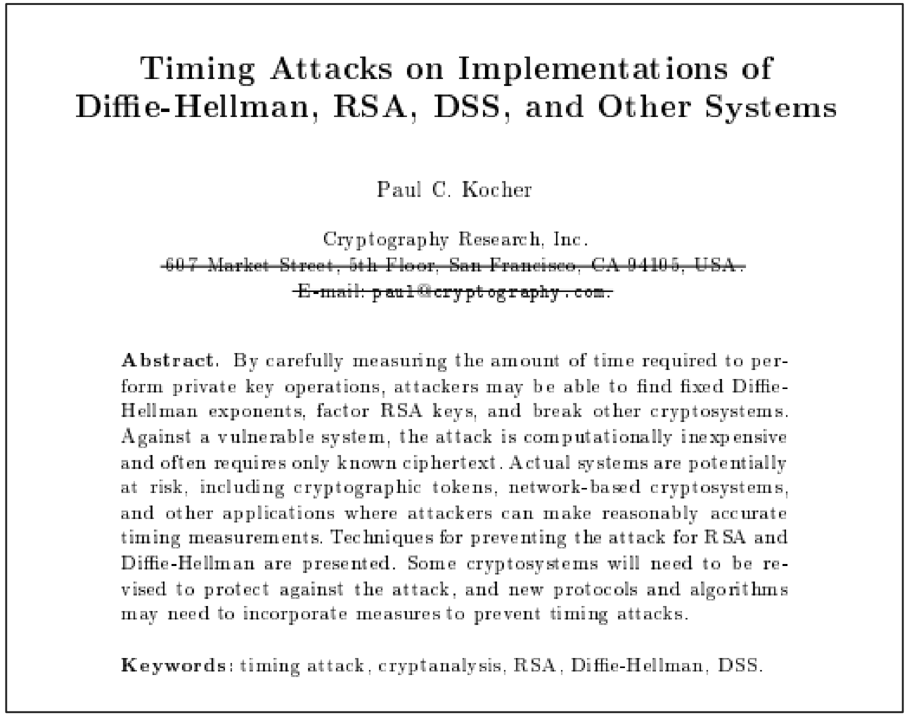
Focus on "observability"



- Without knowledge of the *Secret Key*, ciphertexts leak no information on plaintexts
  - Best key recovery strategy: bruteforce $\approx 2^{128}$ operations
- With side-channel information: bruteforce $\ll 2^{128}$

Timing Attacks

- Variability on execution time
  - Influenced by some secret information
- First reported in 1999 by Kocher et. al (RSA)
- Still found in recent implementations:
  - https://tpm.fail/
  - Found on certified products (EAL4+, FIPS 140-2 level 2)
- Achieving constant-time is hard on complex micro-architectures



Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems

Paul C. Kocher

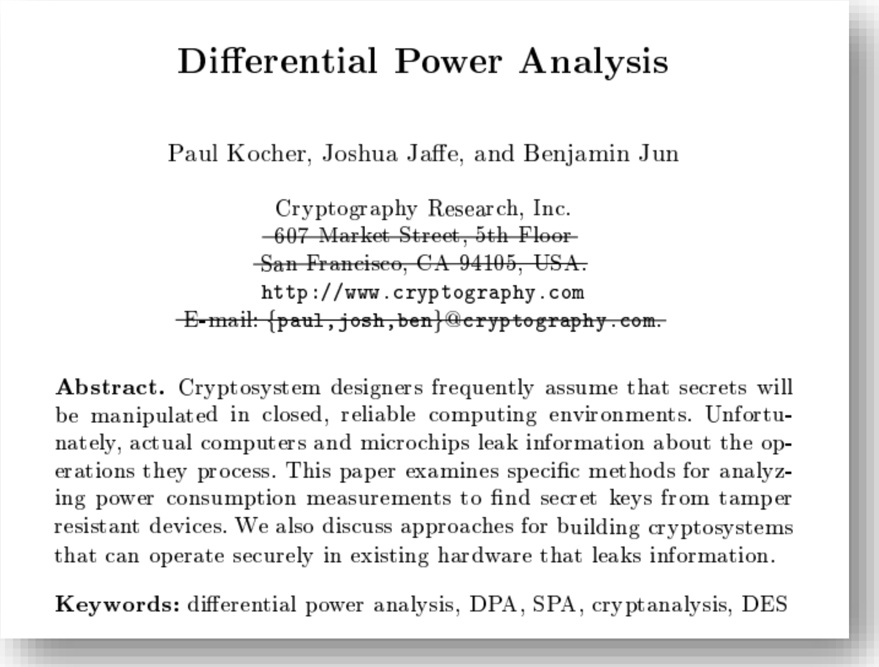
Cryptography Research, Inc.
~~607 Market Street, 5th Floor, San Francisco, CA 94105, USA.~~
~~E-mail: paul@cryptography.com.~~

Abstract. By carefully measuring the amount of time required to perform private key operations, attackers may be able to find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems. Against a vulnerable system, the attack is computationally inexpensive and often requires only known ciphertext. Actual systems are potentially at risk, including cryptographic tokens, network-based cryptosystems, and other applications where attackers can make reasonably accurate timing measurements. Techniques for preventing the attack for RSA and Diffie-Hellman are presented. Some cryptosystems will need to be revised to protect against the attack, and new protocols and algorithms may need to incorporate measures to prevent timing attacks.

Keywords: timing attack, cryptanalysis, RSA, Diffie-Hellman, DSS.

Power Measurements

- Inexpensive, simple and effective
- Invasive
- Noisy on complex systems



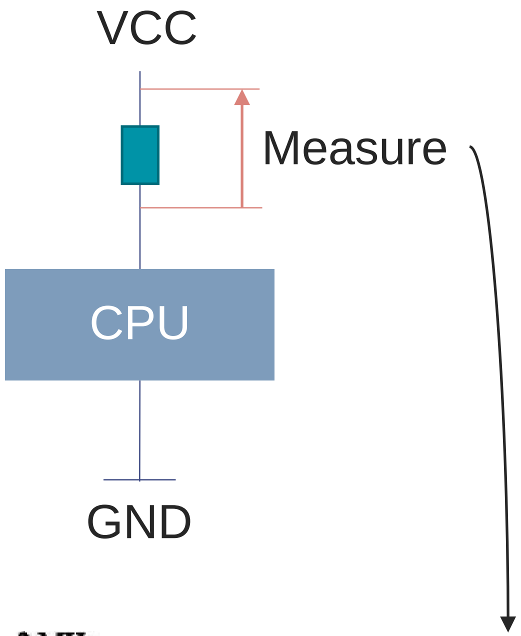
Differential Power Analysis

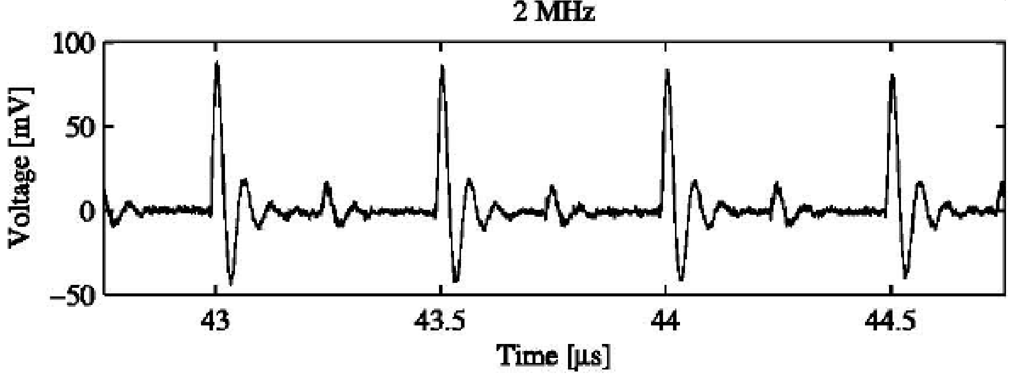
Paul Kocher, Joshua Jaffe, and Benjamin Jun

Cryptography Research, Inc.
~~607 Market Street, 5th Floor~~
~~San Francisco, CA 94105, USA.~~
http://www.cryptography.com
~~E-mail: {paul,josh,ben}@cryptography.com.~~

Abstract. Cryptosystem designers frequently assume that secrets will be manipulated in closed, reliable computing environments. Unfortunately, actual computers and microchips leak information about the operations they process. This paper examines specific methods for analyzing power consumption measurements to find secret keys from tamper resistant devices. We also discuss approaches for building cryptosystems that can operate securely in existing hardware that leaks information.

Keywords: differential power analysis, DPA, SPA, cryptanalysis, DES

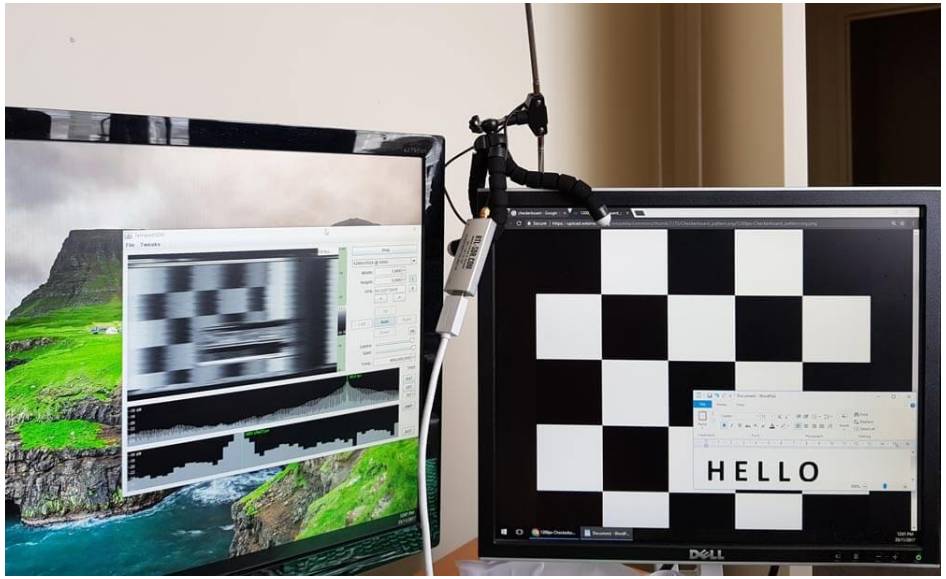


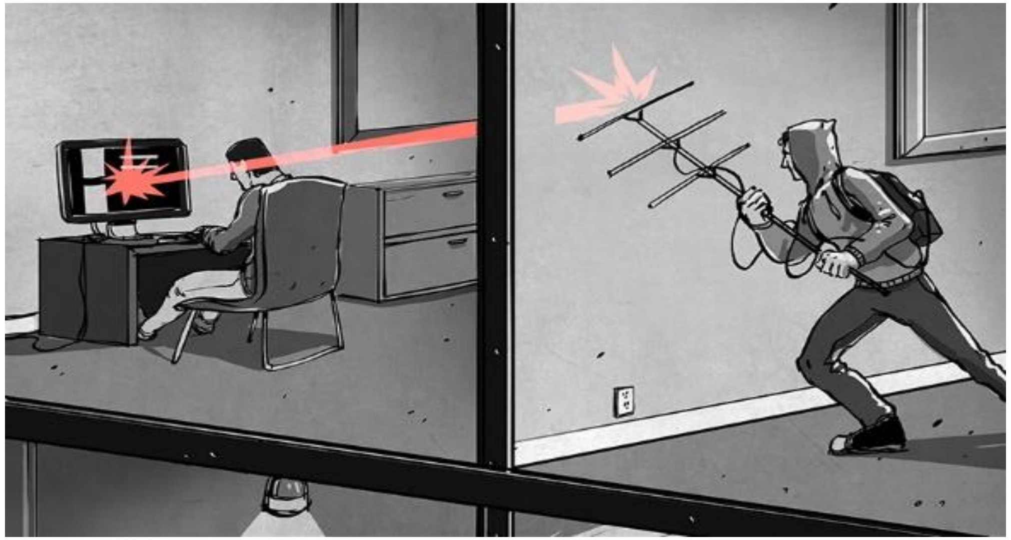


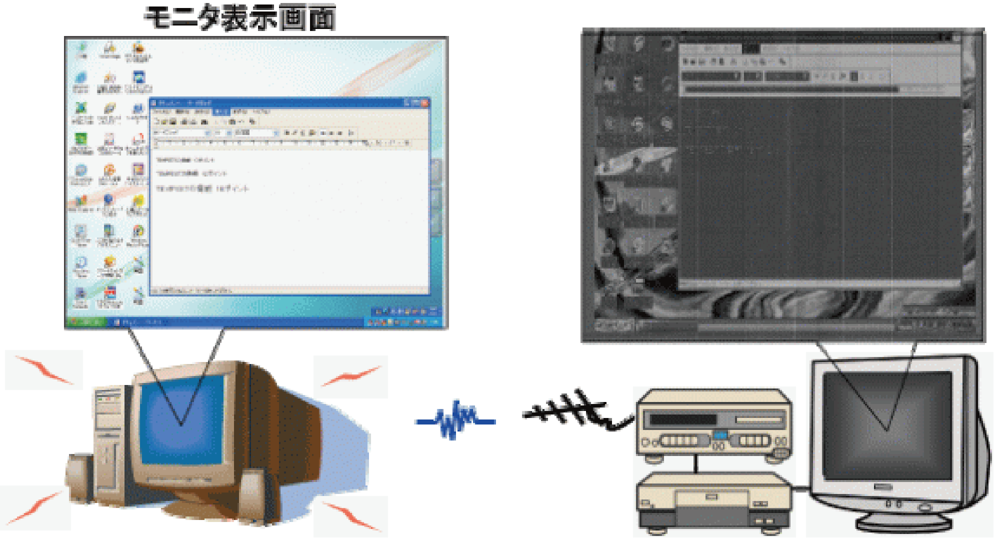
Source: Mangard, Stefan, Elisabeth Oswald, and Thomas Popp. Power analysis attacks: Revealing the secrets of smart cards. Vol. 31. Springer Science & Business Media, 2008.

Electromagnetic measurements

- Wim van Eck (1985)
  - Eavesdropping from CRT display
- TEMPEST

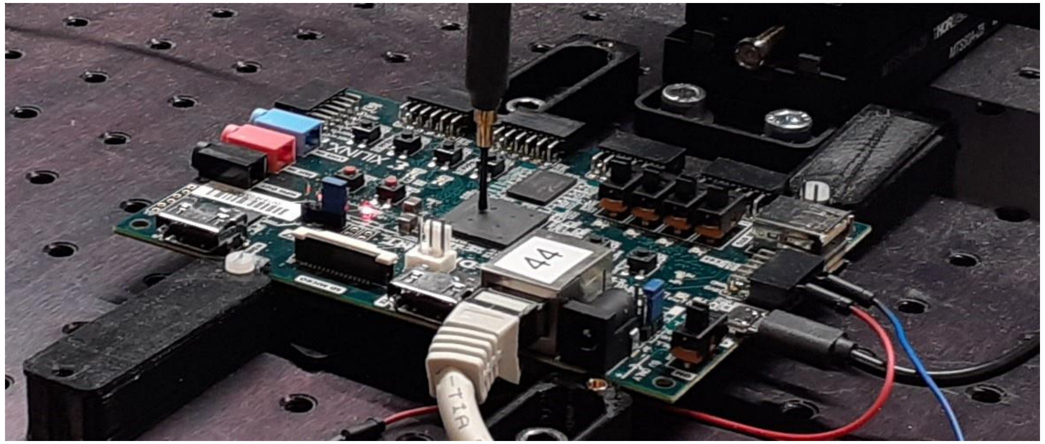


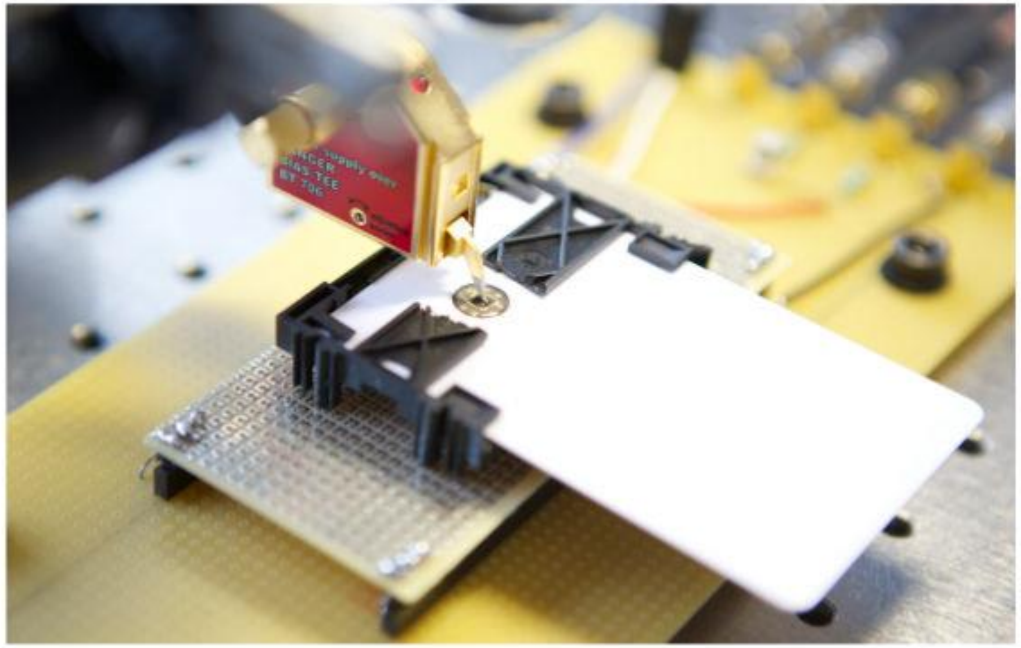


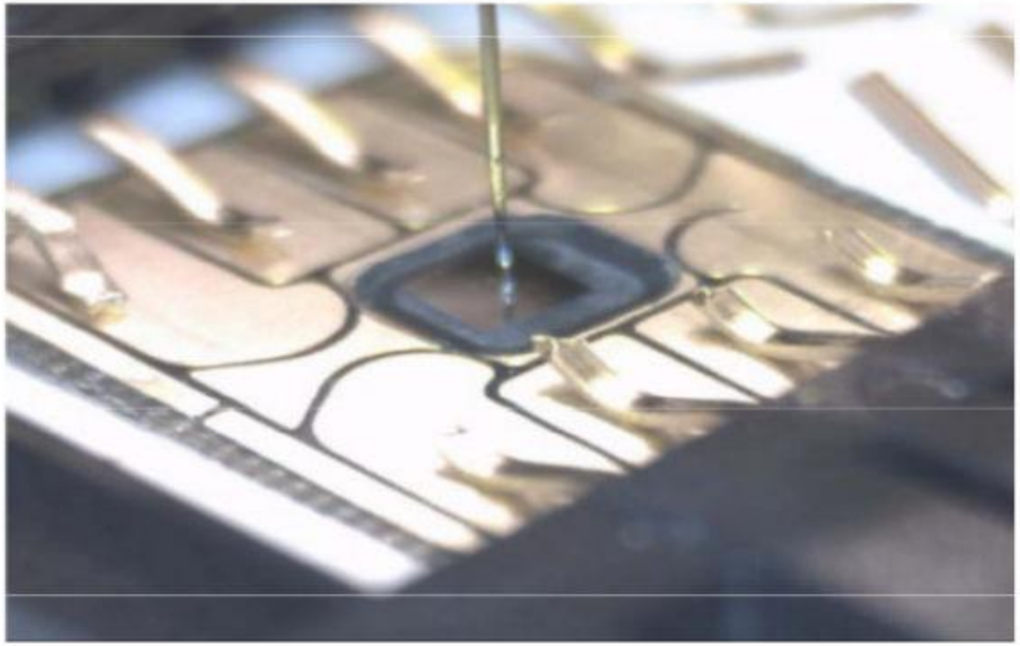


Electromagnetic measurements

- Non invasive
  - Decapping (invasive) can provide better signal
- Local measurements (better signal-to-noise ratio)
- Spatial dimension to explore

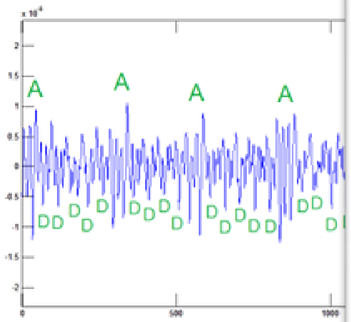




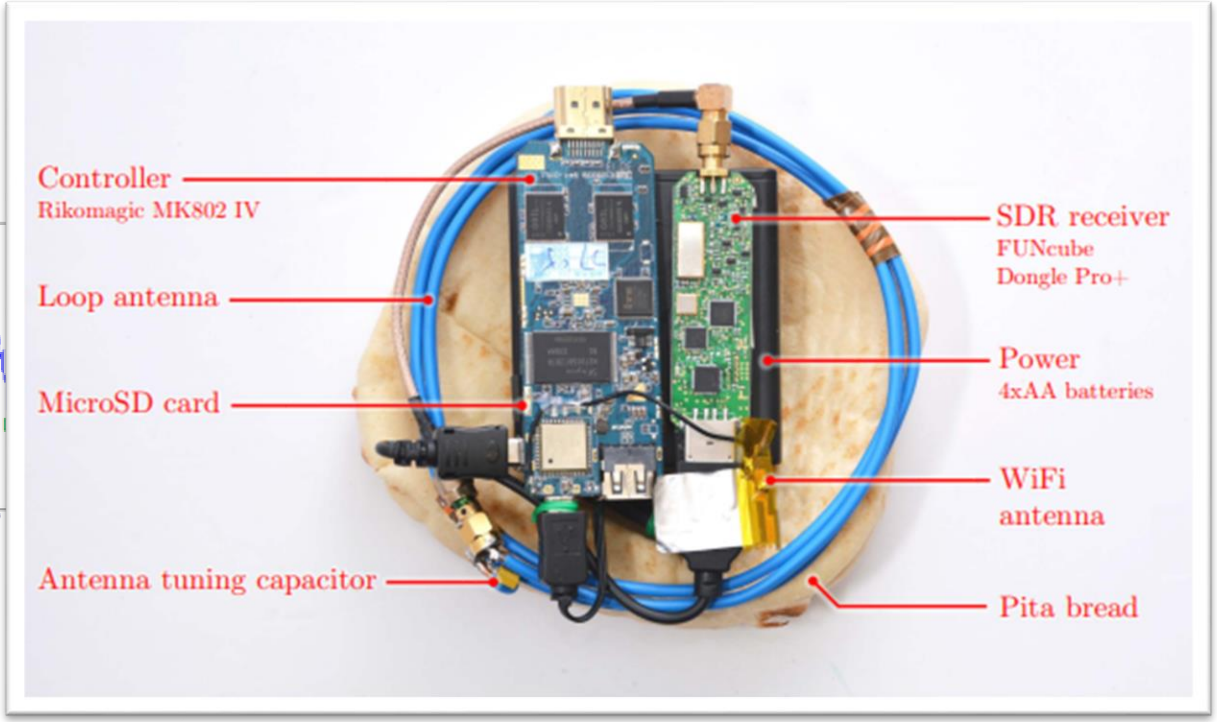


Electromagnetic measurements

- You do not need expensive hardware!
- Genkin et. al: cheap EM probe + soundcard
  - Successful attack on ECDSA double-and-add



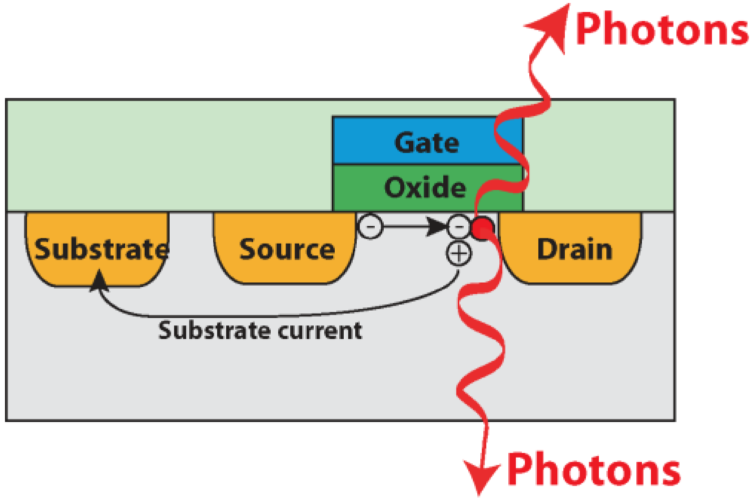
PITA Attack !



- Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Tromer, Yuval Yarom, ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels, IACR Cryptology ePrint Archive, https://eprint.iacr.org/2016/230
- Genkin, Daniel, et al. "Stealing keys from PCs using a radio: Cheap electromagnetic attacks on windowed exponentiation." *Cryptographic Hardware and Embedded Systems--CHES 2015: 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings 17*. Springer Berlin Heidelberg, 2015.

Other physical channels

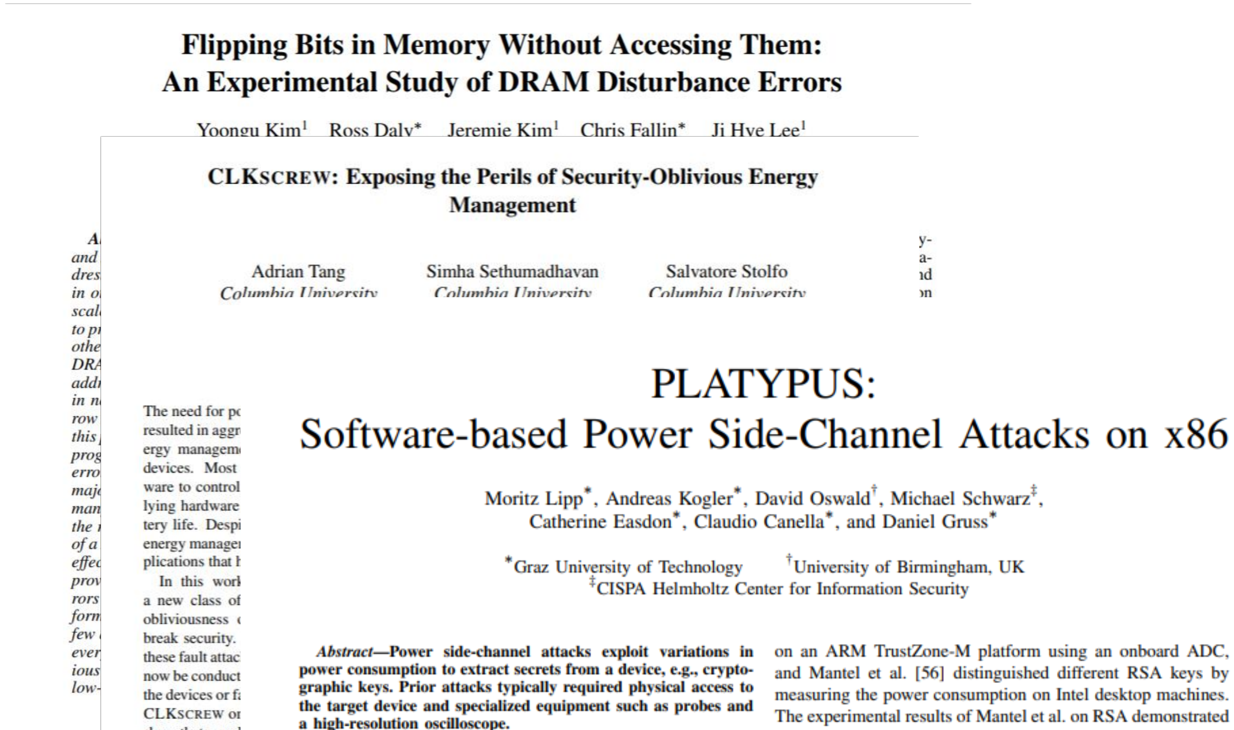
- Screaming channels
- Photon-emission in transistors
  - Very good spatial resolution
  - Long capture time
  - Useful for reverse-engineering
- Heat
- Sound



Sources:
Tosi, Alberto, et al. "Hot-carrier photoemission in scaled CMOS technologies: a challenge for emission based testing and diagnostics." *2006 IEEE International Reliability Physics Symposium Proceedings*. IEEE, 2006.
Daniel Genkin, Adi Shamir, Eran Tromer, “RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis”, http://www.cs.tau.ac.il/~tromer/acoustic/

Microarchitectural attacks

- Hardware state observable/modifiable from software
- No physical access needed (remote attack)
  - Code execution is required
- Not covered in this talk



Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors

Yoongu Kim[1] Ross Daly* Jeremie Kim[1] Chris Fallin* Ji Hye Lee[1]

CLKSCREW: Exposing the Perils of Security-Oblivious Energy Management

Adrian Tang, Columbia University · Simha Sethumadhavan, Columbia University · Salvatore Stolfo, Columbia University

The need for po… resulted in aggr… ergy managem… devices. Most … ware to control … lying hardware … tery life. Despi… energy manage… plications that … In this work … a new class of … obliviousness … break security. … these fault attac… now be conduct… the devices or f… CLKSCREW or…

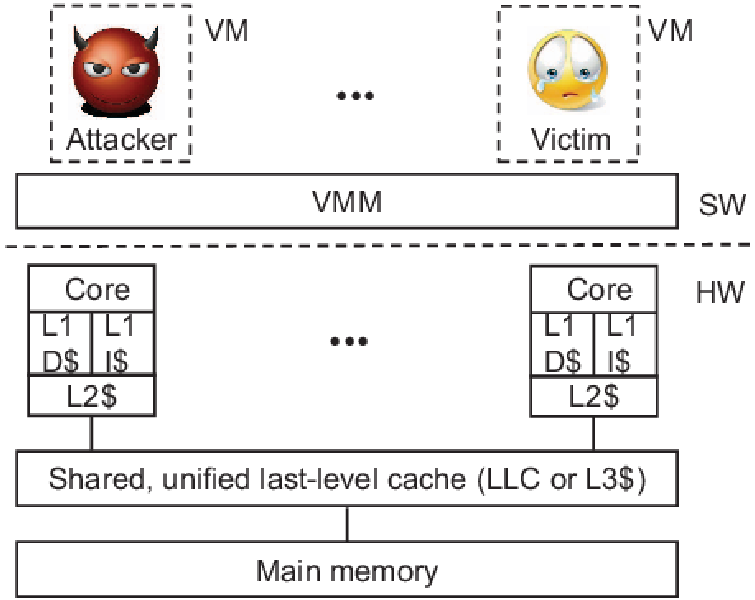
PLATYPUS: Software-based Power Side-Channel Attacks on x86

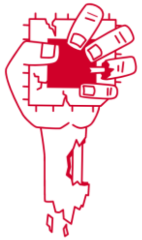
Moritz Lipp*, Andreas Kogler*, David Oswald†, Michael Schwarz‡, Catherine Easdon*, Claudio Canella*, and Daniel Gruss*

*Graz University of Technology †University of Birmingham, UK ‡CISPA Helmholtz Center for Information Security

***Abstract*—Power side-channel attacks exploit variations in power consumption to extract secrets from a device, e.g., cryptographic keys. Prior attacks typically required physical access to the target device and specialized equipment such as probes and a high-resolution oscilloscope.**

on an ARM TrustZone-M platform using an onboard ADC, and Mantel et al. [56] distinguished different RSA keys by measuring the power consumption on Intel desktop machines. The experimental results of Mantel et al. on RSA demonstrated





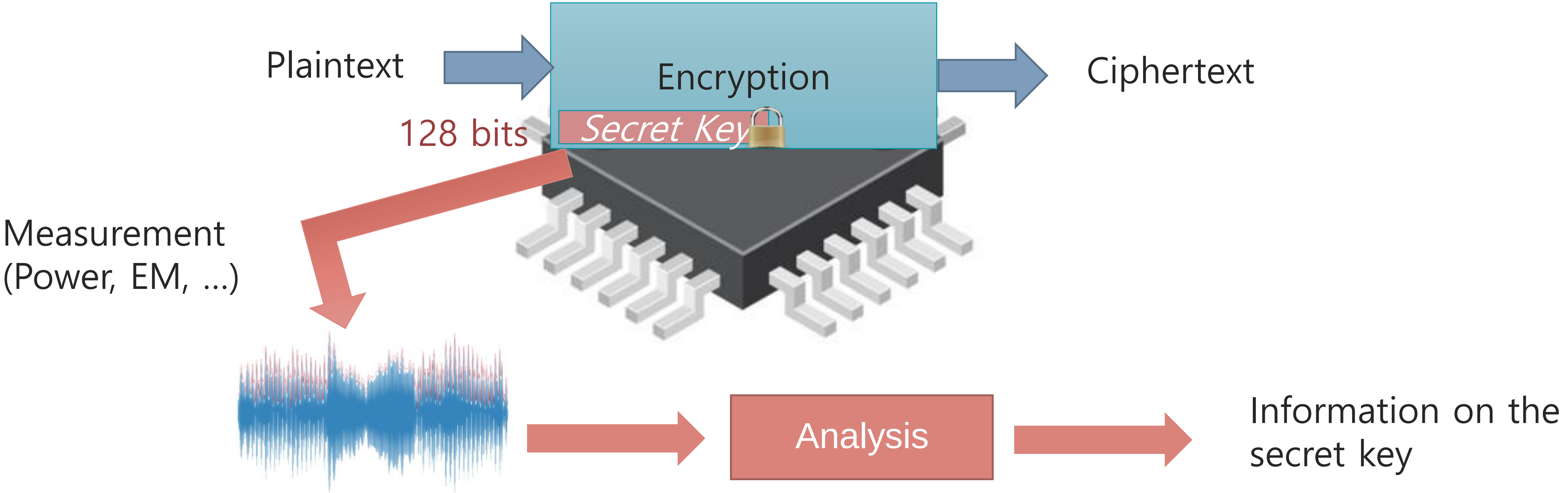
Wrap-up

- Security functions are built from “ideal” primitives

- Assumptions not always maintained after implementation
  - Implementation bugs
  - Unexpected leakage channels
  - External perturbations

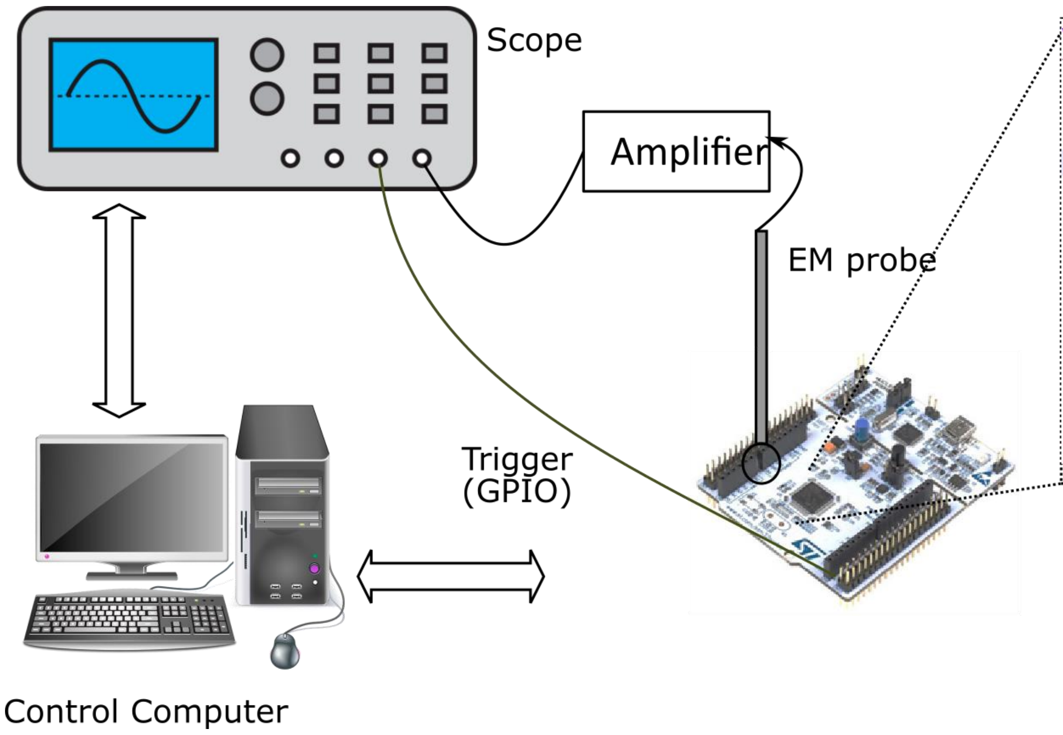
- Different types of leakages
  - Physical
  - Remote (microarchitectural attacks)

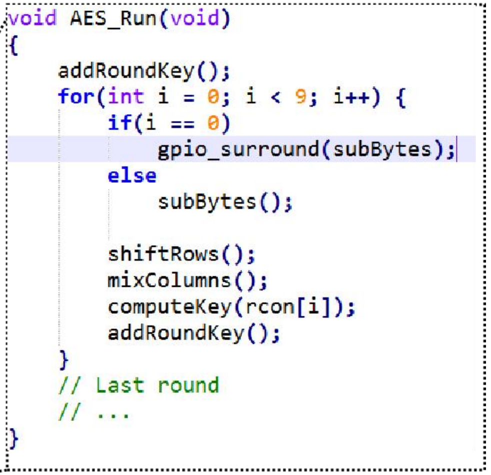
Side-channel analysis against symmetric cryptography



- Best key recovery strategy: bruteforce ≈ 2^{128} operations
- For AES: the key is processed byte by byte
  - Information may leak on individual key bytes

Demo time

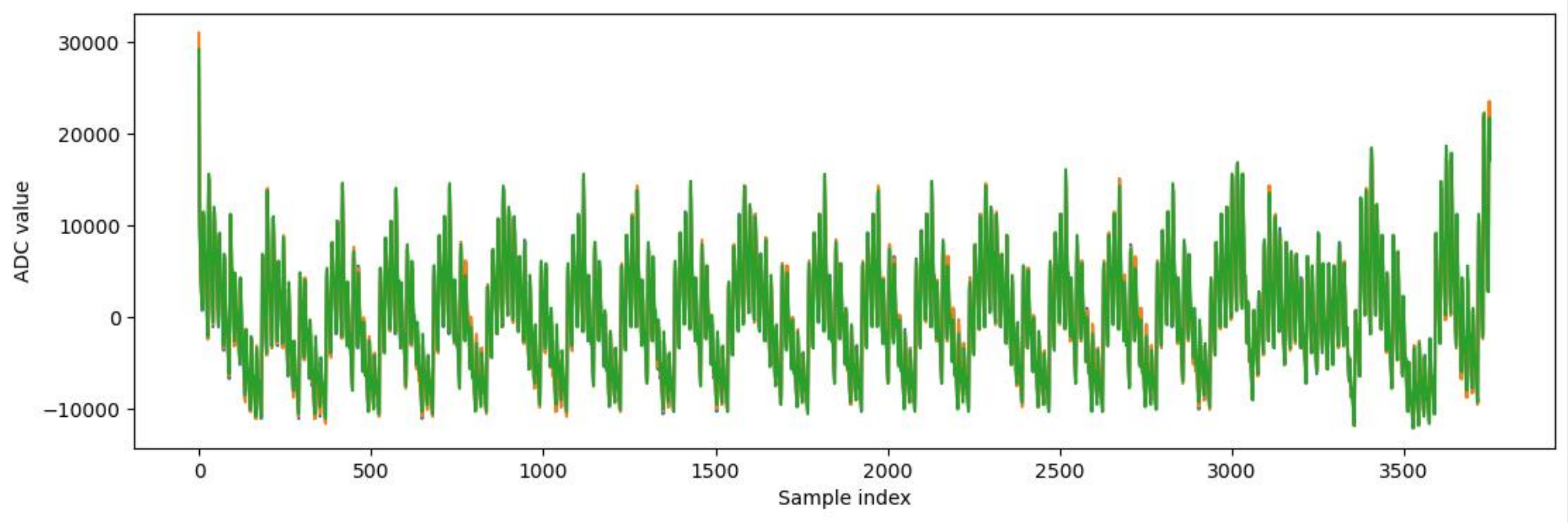




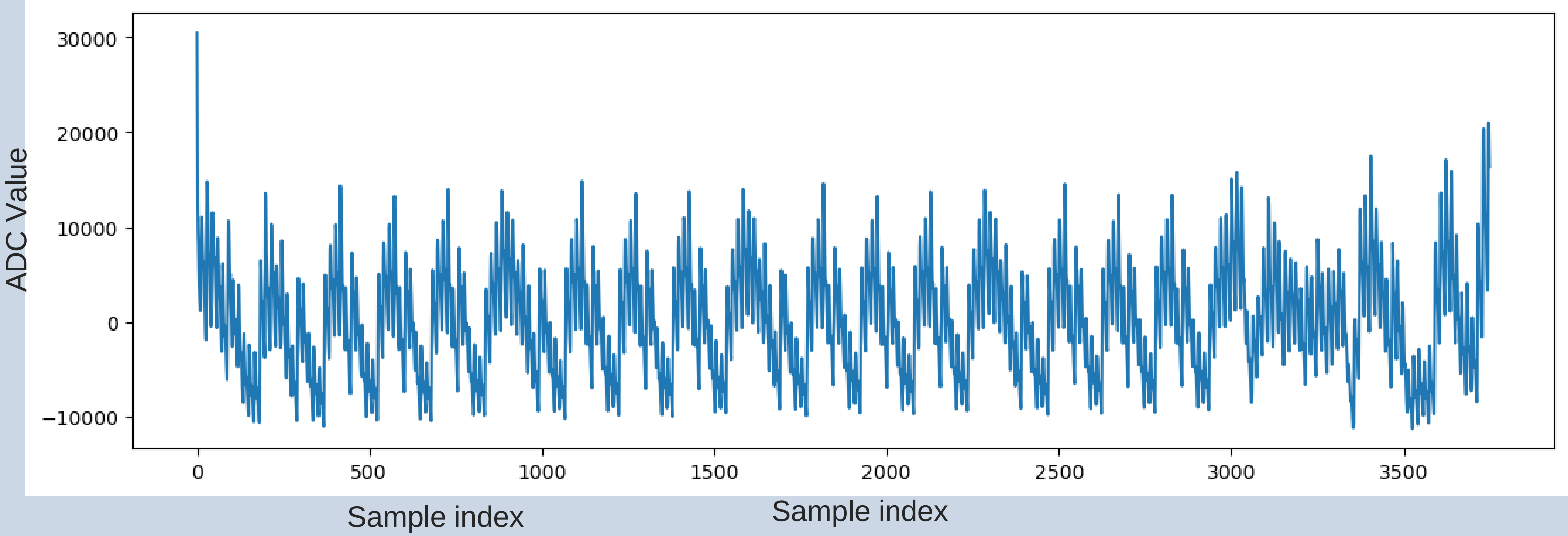
```
void AES_Run(void)
{
    addRoundKey();
    for(int i = 0; i < 9; i++) {
        if(i == 0)
            gpio_surround(subBytes);
        else
            subBytes();

        shiftRows();
        mixColumns();
        computeKey(rcon[i]);
        addRoundKey();
    }
    // Last round
    // ...
}
```

Demo (Example traces)

Multiple traces with different plaintexts

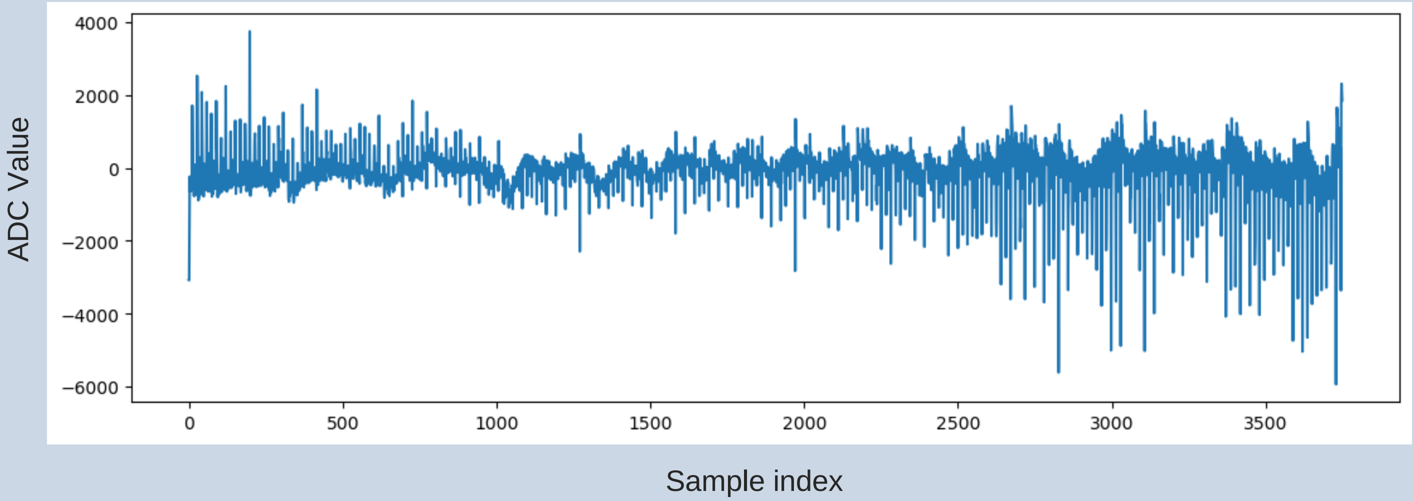


Average trace (5000 acquisitions)

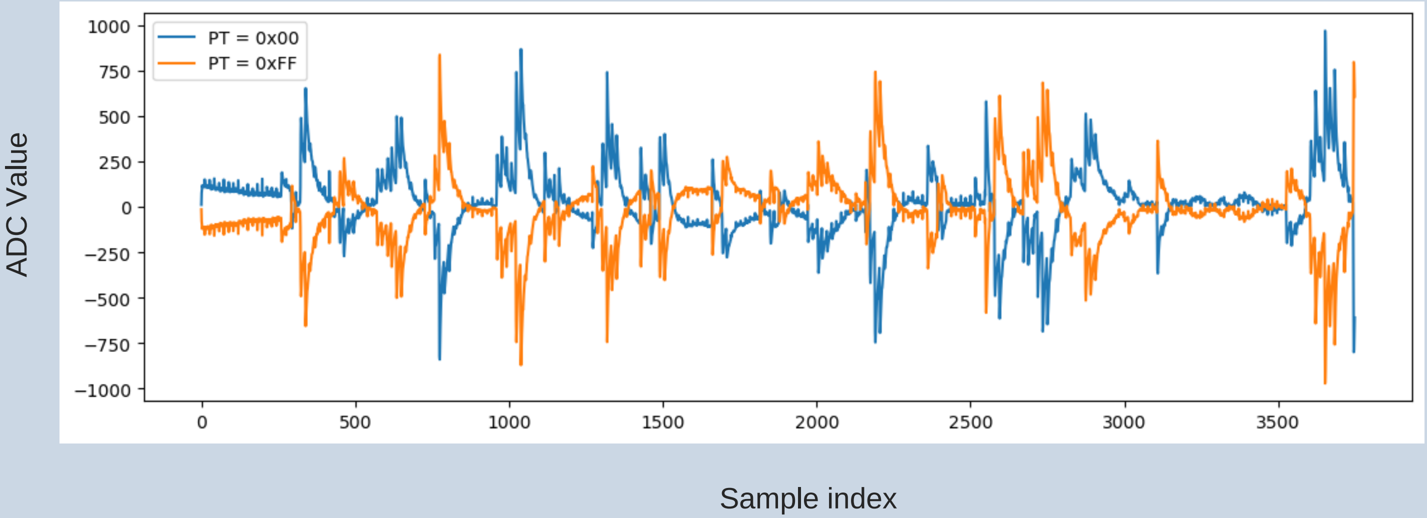


Demo (Example traces)

Trace with mean removed

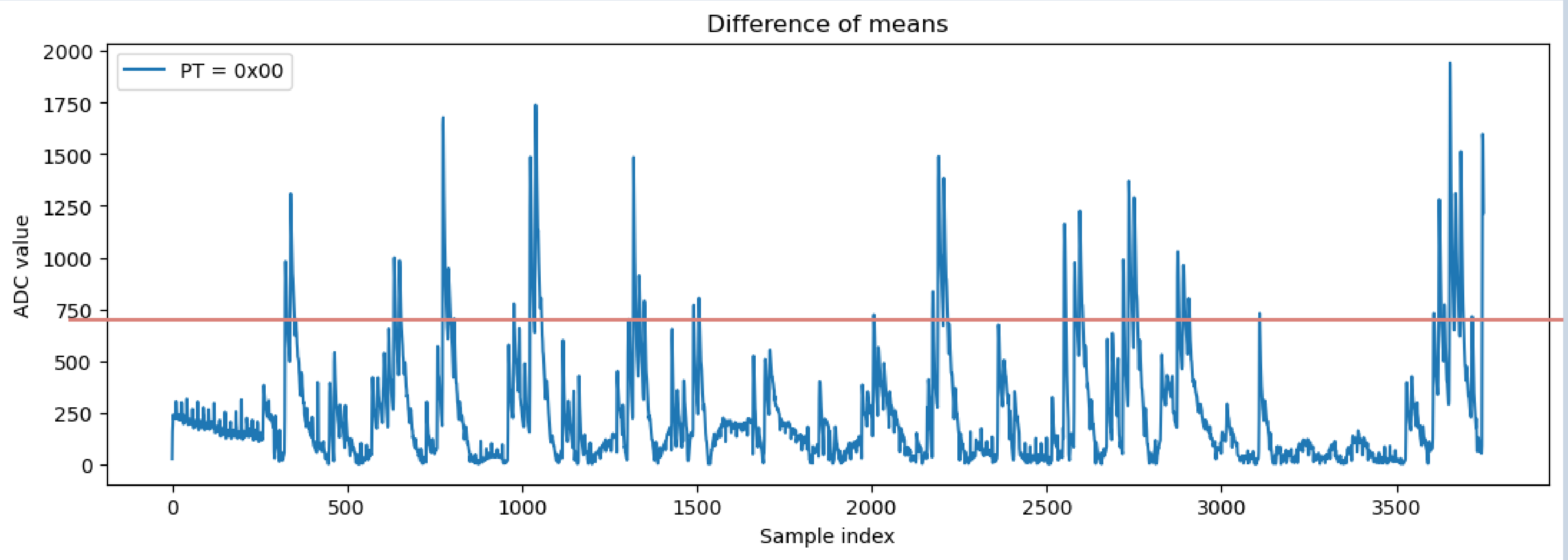


Average trace per plaintext value



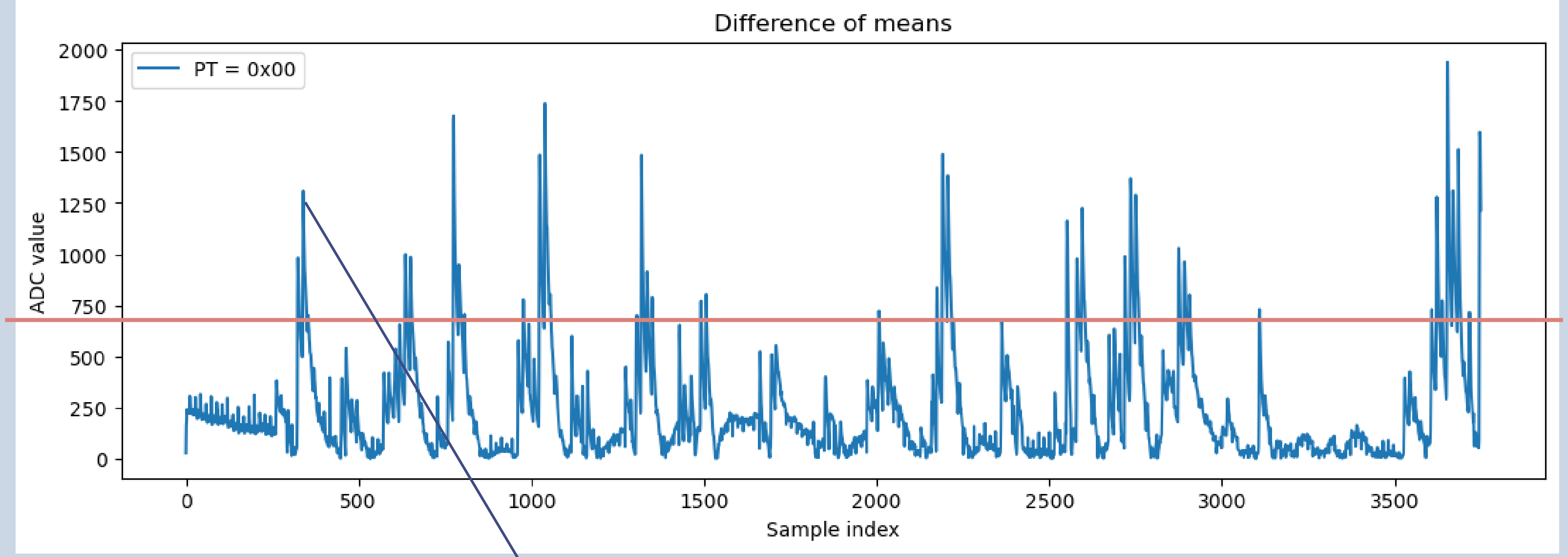
Demo (Example traces)

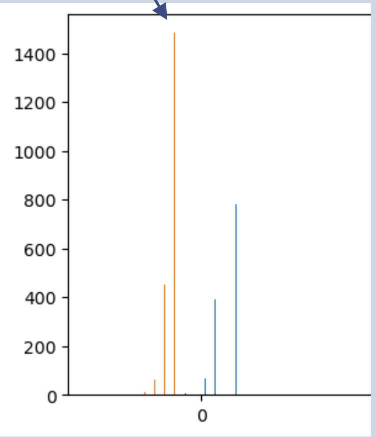
Difference of means per class. The highest samples indicate where (in time) means are the most distinguishable. We can use this simple test to reduce the number of samples used in analysis/attack phases.



Kocher, Paul, Joshua Jaffe, and Benjamin Jun. "Differential power analysis." Advances in Cryptology—CRYPTO’99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19. Springer Berlin Heidelberg, 1999.

Demo (Example traces)

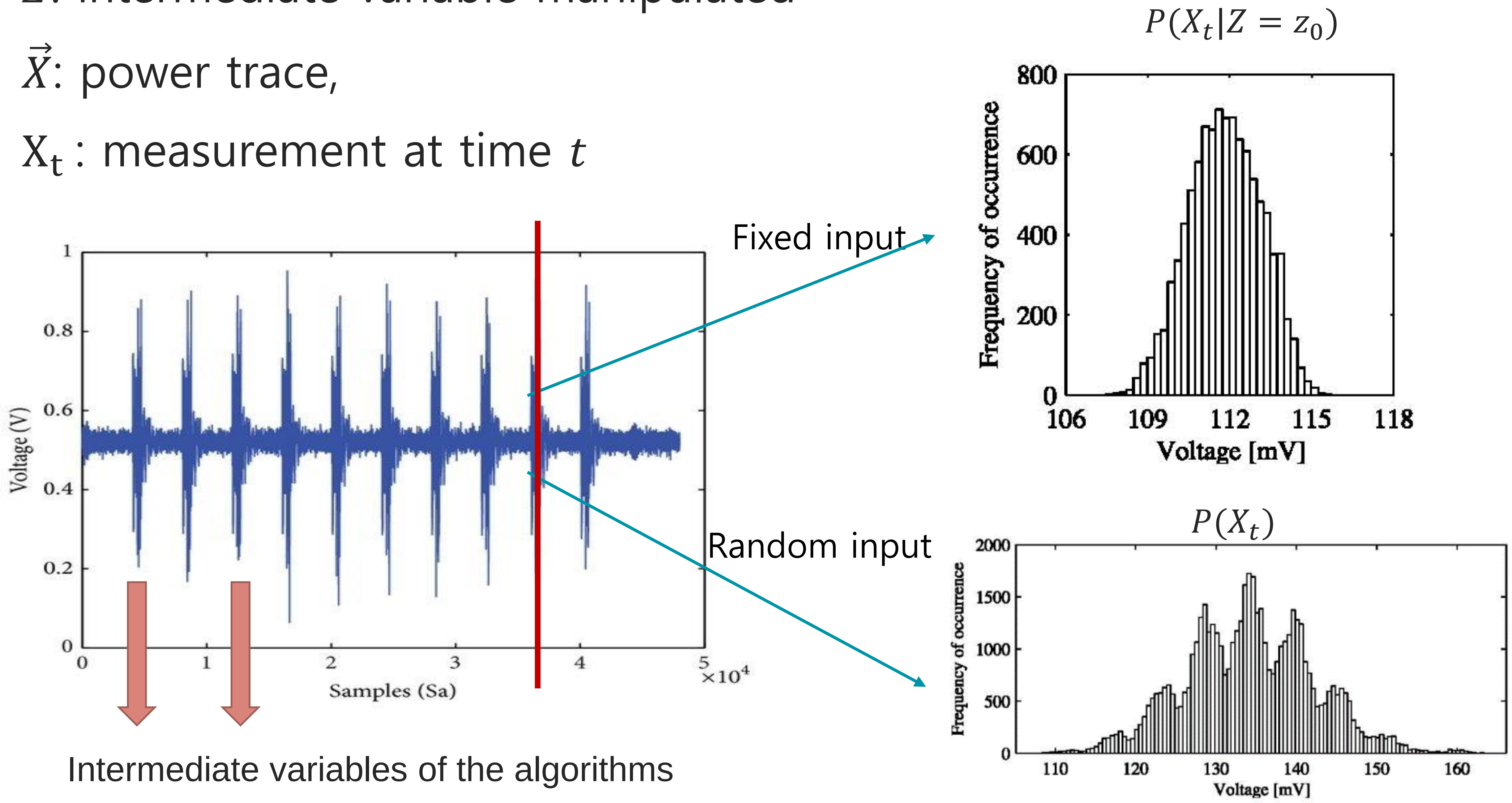




Histogram of ADC values at sample 339: two clusters appear (one for each plaintext value)

Anatomy of a trace

- Z: intermediate variable manipulated
- $\vec{X}$: power trace,
- X_{t} : measurement at time t



$P(X_t|Z = z_0)$

Fixed input

Random input

$P(X_t)$

Intermediate variables of the algorithms

Source: Mangard, Stefan, Elisabeth Oswald, and Thomas Popp. Power analysis attacks: Revealing the secrets of smart cards. Vol. 31. Springer Science & Business Media, 2008

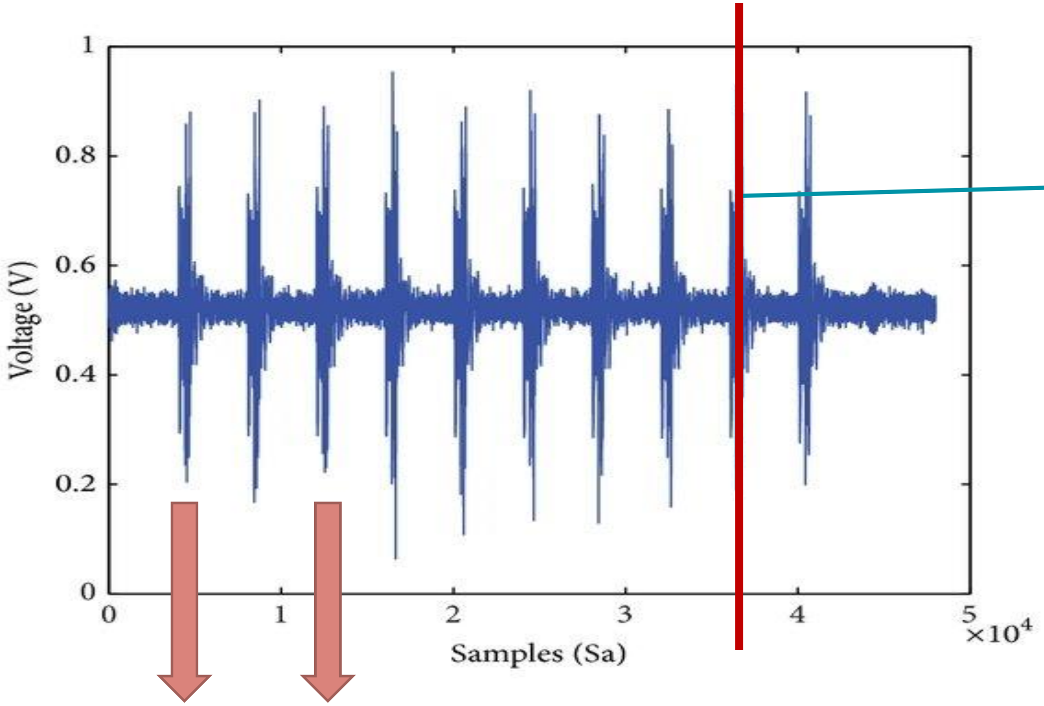
Anatomy of a trace

- Z: intermediate variable manipulated
- $\vec{X}$: power trace,
- $\mathrm{X_t}$: measurement at time t

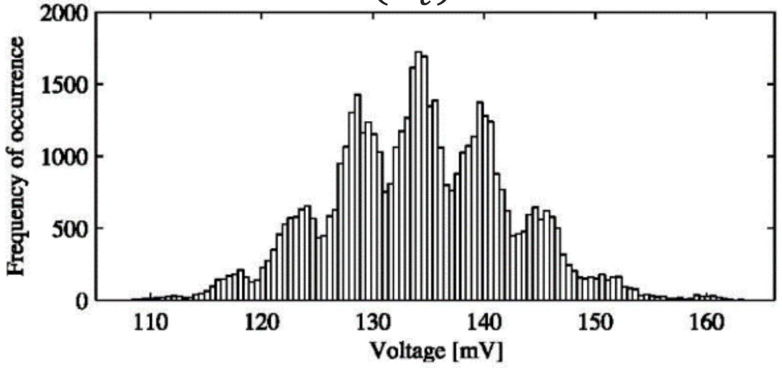
Leakage model

Noise term, idealy $N(0,\sigma)$

$$\mathrm{X_t} = \varphi(Z) + \mathrm{E}$$



$P(X_t)$



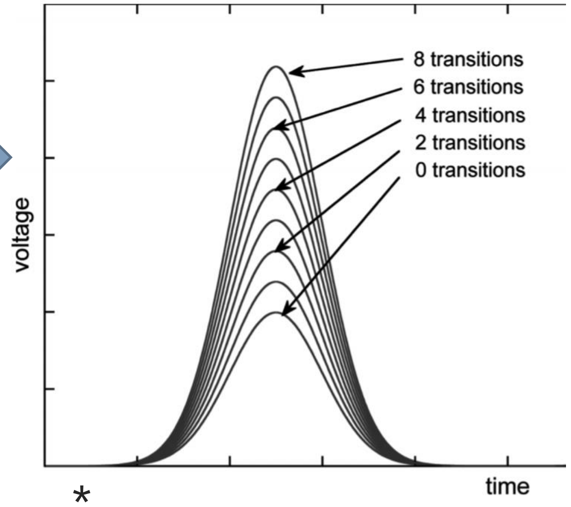
Intermediate variables of the algorithms

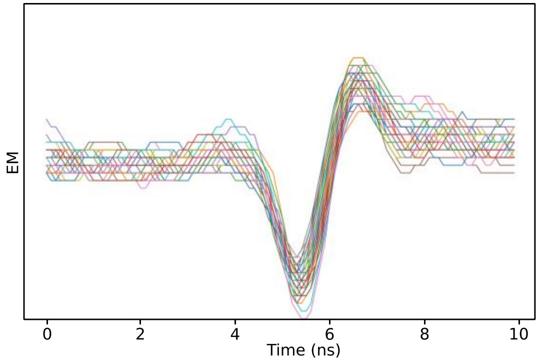
Source: Mangard, Stefan, Elisabeth Oswald, and Thomas Popp. Power analysis attacks: Revealing the secrets of smart cards. Vol. 31. Springer Science & Business Media, 2008.

Common leakage models

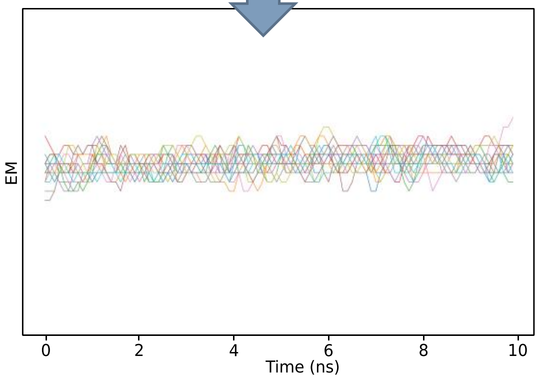
Special case of a linear bit model

- Hamming weight: number of bits to 1 in Z
- Linear bit combination => see lab ☺
- Hamming distance: number of bit transition in Z
- Signed hamming distance



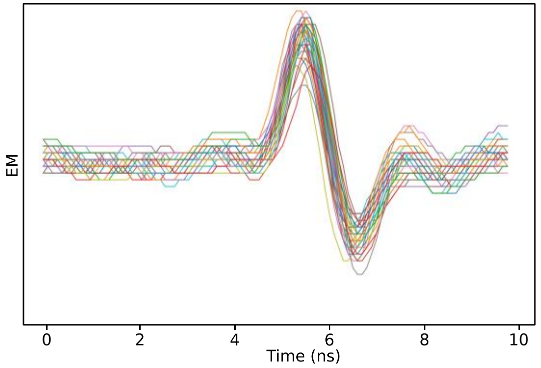


0 ⟶ 1



0 ⟶ 0

1 ⟶ 1

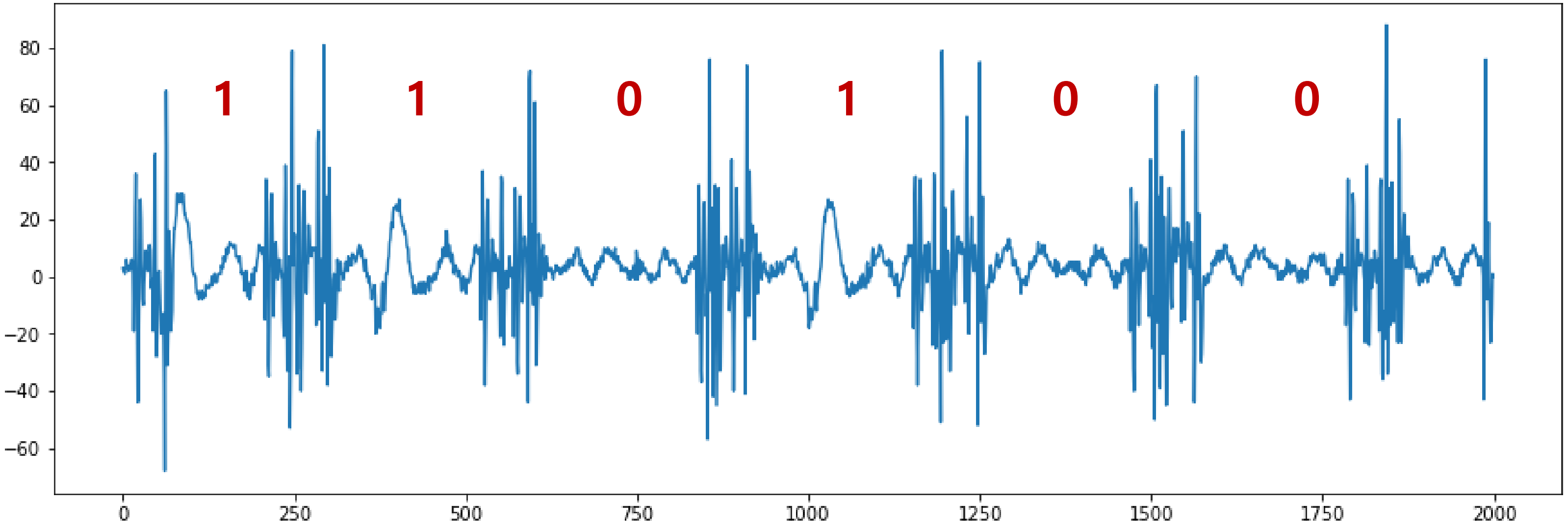


1 ⟶ 0

* Source : Standaert, F. X. (2010). Introduction to side-channel attacks. In *Secure Integrated Circuits and Systems* (pp. 27-42). Springer.

Side-channel Attacks against cryptography

- Simplest approach: visual inspection
- Known as “simple power analysis” (SPA), still works in 2023!*
- Unsupervised approach, traces have no labels

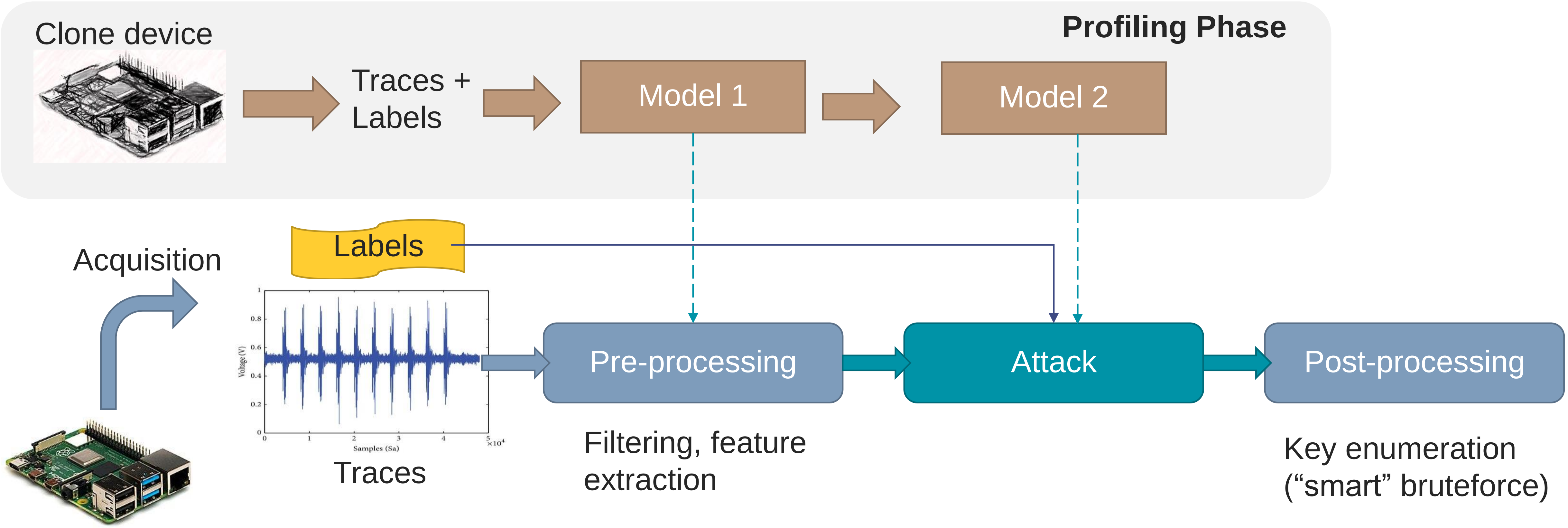


Kyber 512 Key encapsulation (Compression/Decompression)

[* https://github.com/mupq/pqm4](https://github.com/mupq/pqm4)

Side-channel attack strategies

- Supervised attacks: labels are available (e.g., plaintexts)
  - Unprofiled: no preliminary profiling
  - Profiled: use of a clone device



Clone device

Profiling Phase

Traces + Labels

Model 1

Model 2

Acquisition

Labels

Traces

Pre-processing

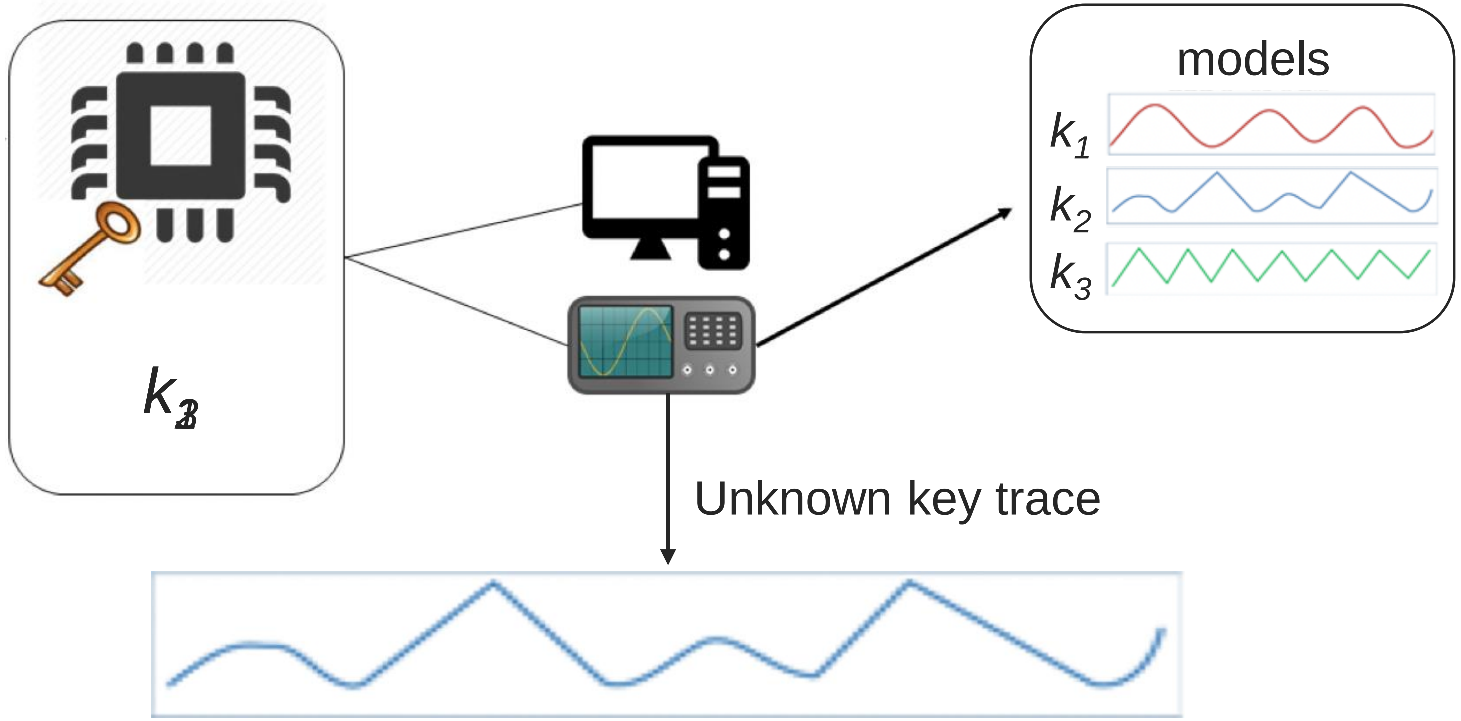
Attack

Post-processing

Filtering, feature extraction

Key enumeration (“smart” bruteforce)

Example profiled attack



Correct key is k2

- Typical models:
  - Multivariate Gaussian (“template attacks”)
  - Neural networks

Chari, Suresh, Josyula R. Rao, and Pankaj Rohatgi. "Template attacks." *Cryptographic Hardware and Embedded Systems-CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Papers 4*. Springer Berlin Heidelberg, 2003.

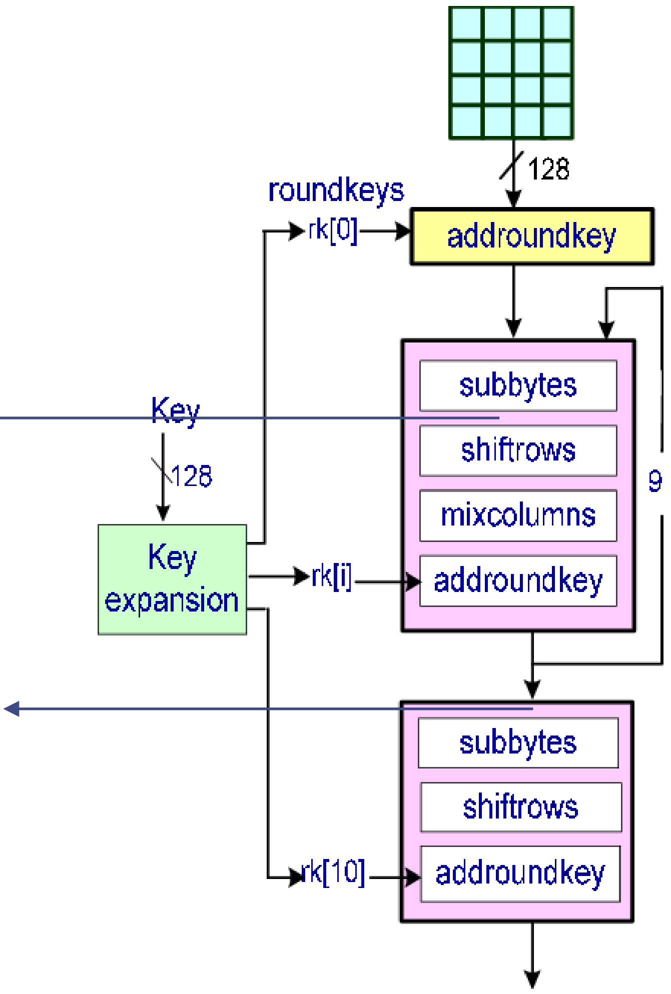
Cagli, Eleonora, Cécile Dumas, and Emmanuel Prouff. "Convolutional neural networks with data augmentation against jitter-based countermeasures: Profiling attacks without pre-processing." *Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*. Springer International Publishing, 2017.

Unprofiled attack on AES

- Advanced Encryption Standard

- Interesting intermediate variables
  - Round 0 (first round)
  - Round 9 (last round)

- Why ?
  - Key manipulated by bytes
  - Mixed with the plaintext



Round 0: no key diffusion (bytes)

Round 9: no key diffusion (bytes) if ciphertext is know

Unprofiled AES Attack

- Target operation: output of the first subbytes operation

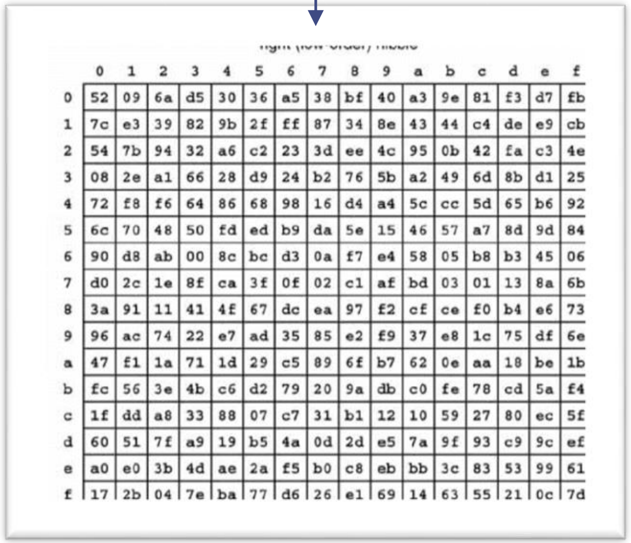
i-th key byte

i-th plaintext byte

8-bit
One per key byte

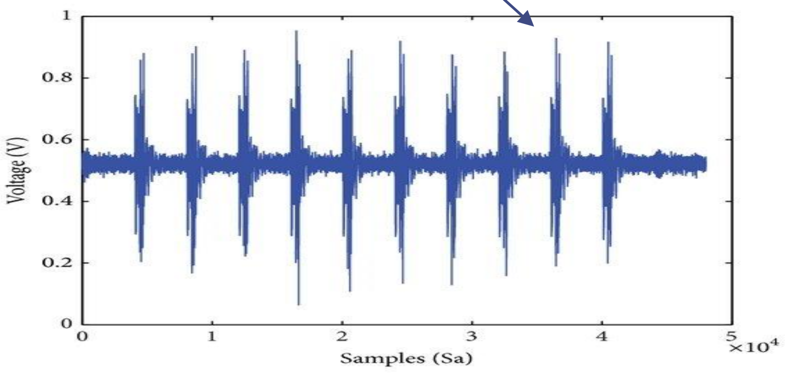
$$Z = SBOX(K, P)$$

φ
(Leakage model)



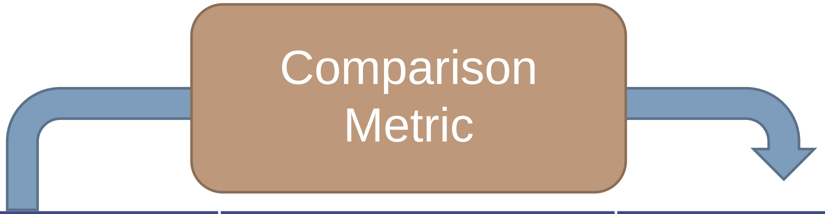
right (low-order) nibble

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

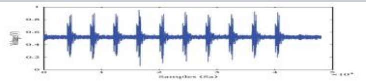
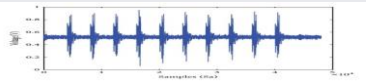
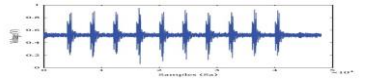
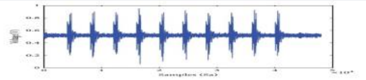
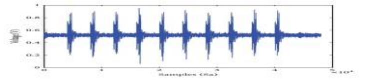


Correlation-based attack

- Principle:
  - Good key hypothesis => Z labels are correct
  - Bad key hypothesis => Z labels are invalid
    - Behavior is somewhat similar to a random labeling

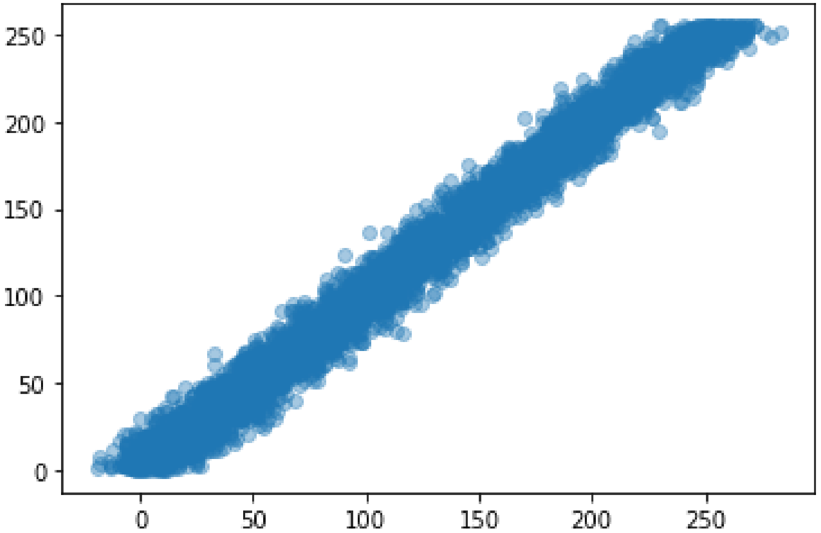


Comparison Metric

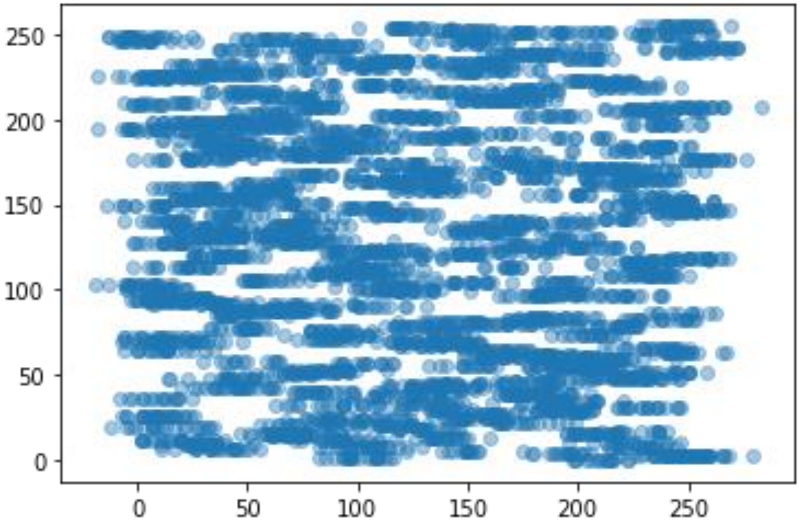
Trace	Z when k = 0	Z when k = 1	…	Z when k = 0xFF
	0xAA	**0x14**		0xDE
	0xBC	**0xFA**		0xAD
	0xDE	**0xCA**		0xBE
	0xFF	**0xFF**		0xEF
	0x12	**0xAB**		0xC0

Correlation-based attack

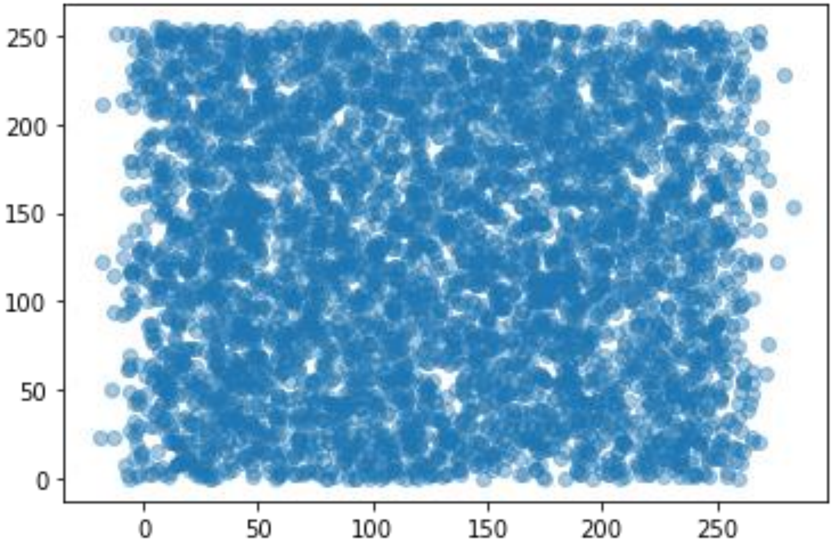
Pearson correlation between traces and predicted power $\varphi(Z)$



Good labels

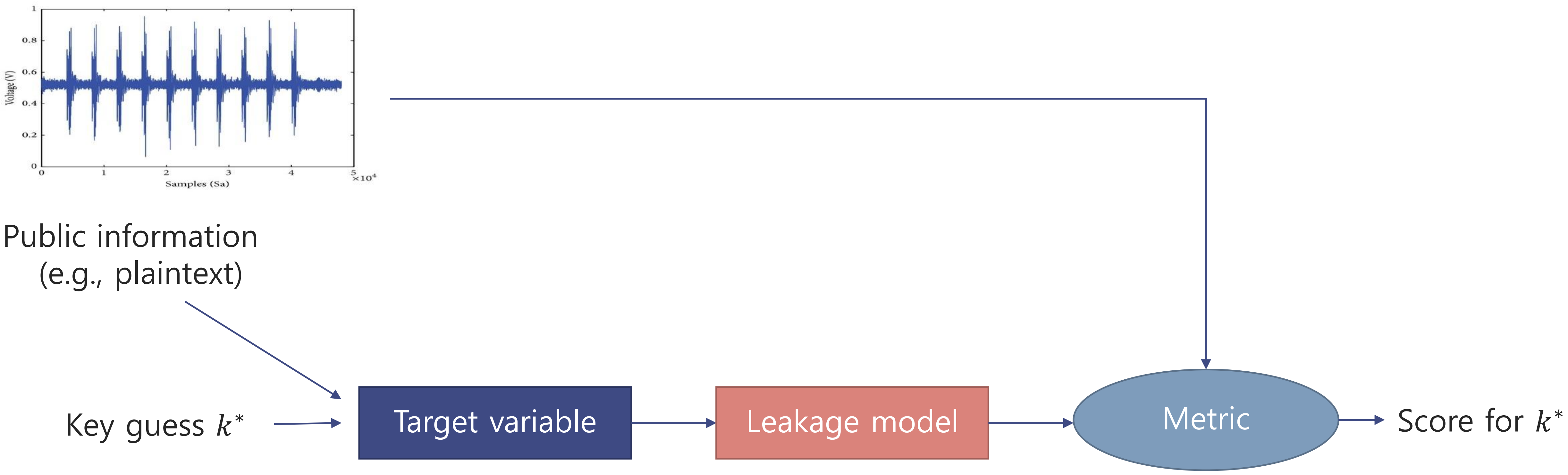


Bad labels



Random labels

Correlation-based attack



Public information (e.g., plaintext)

Key guess k^*

Target variable

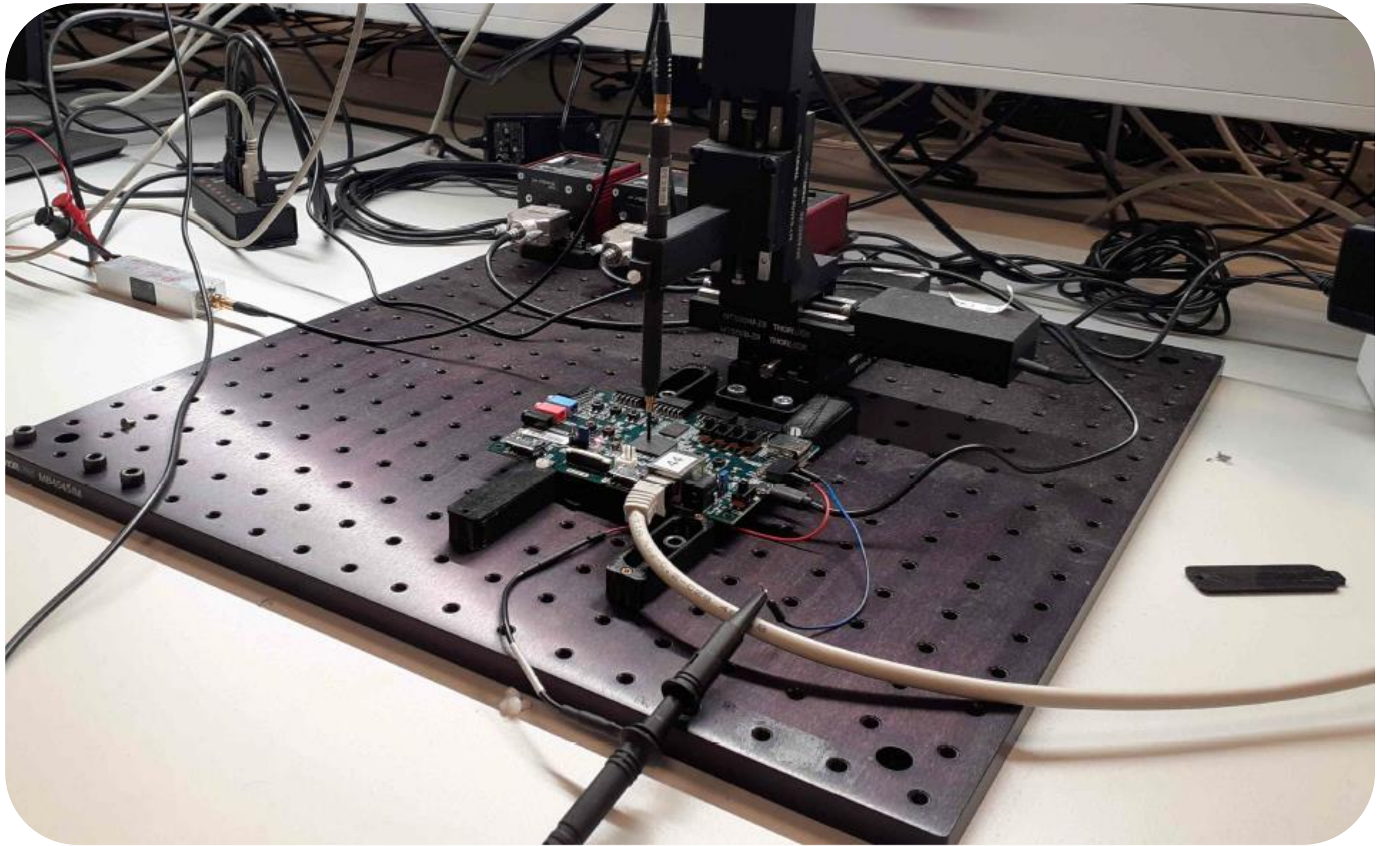
Leakage model

Metric

Score for k^*

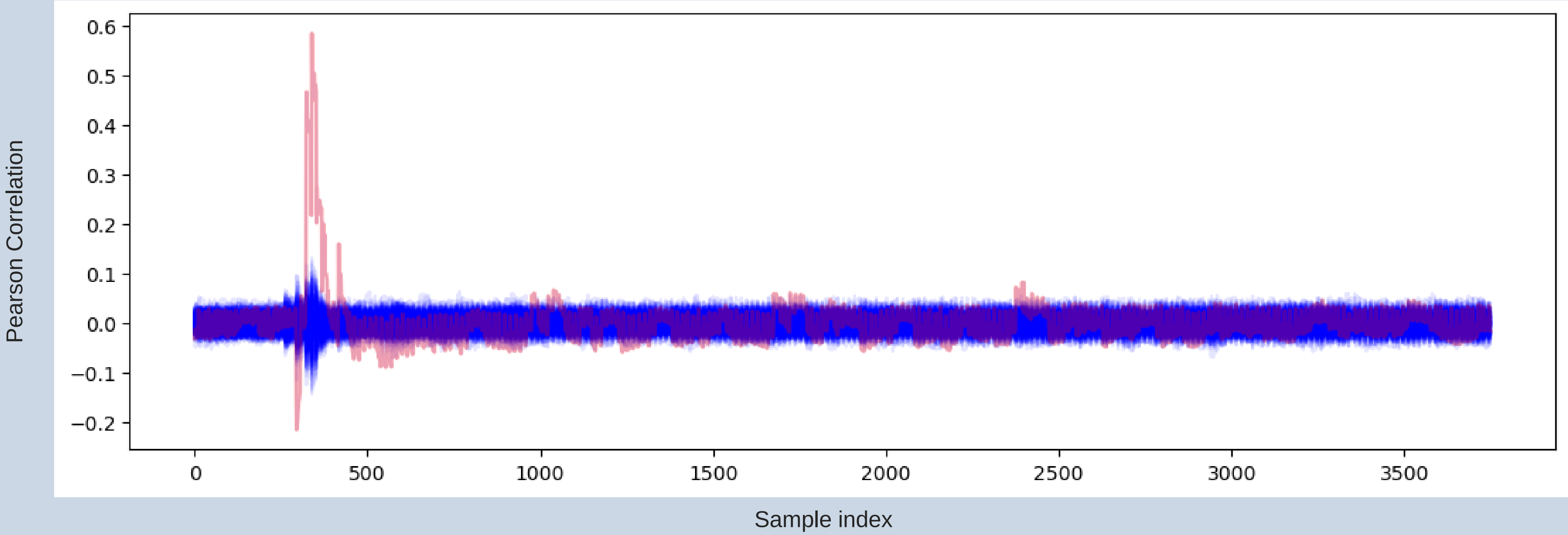
- Select the key with the best score, or use scores for enumeration

Demo time



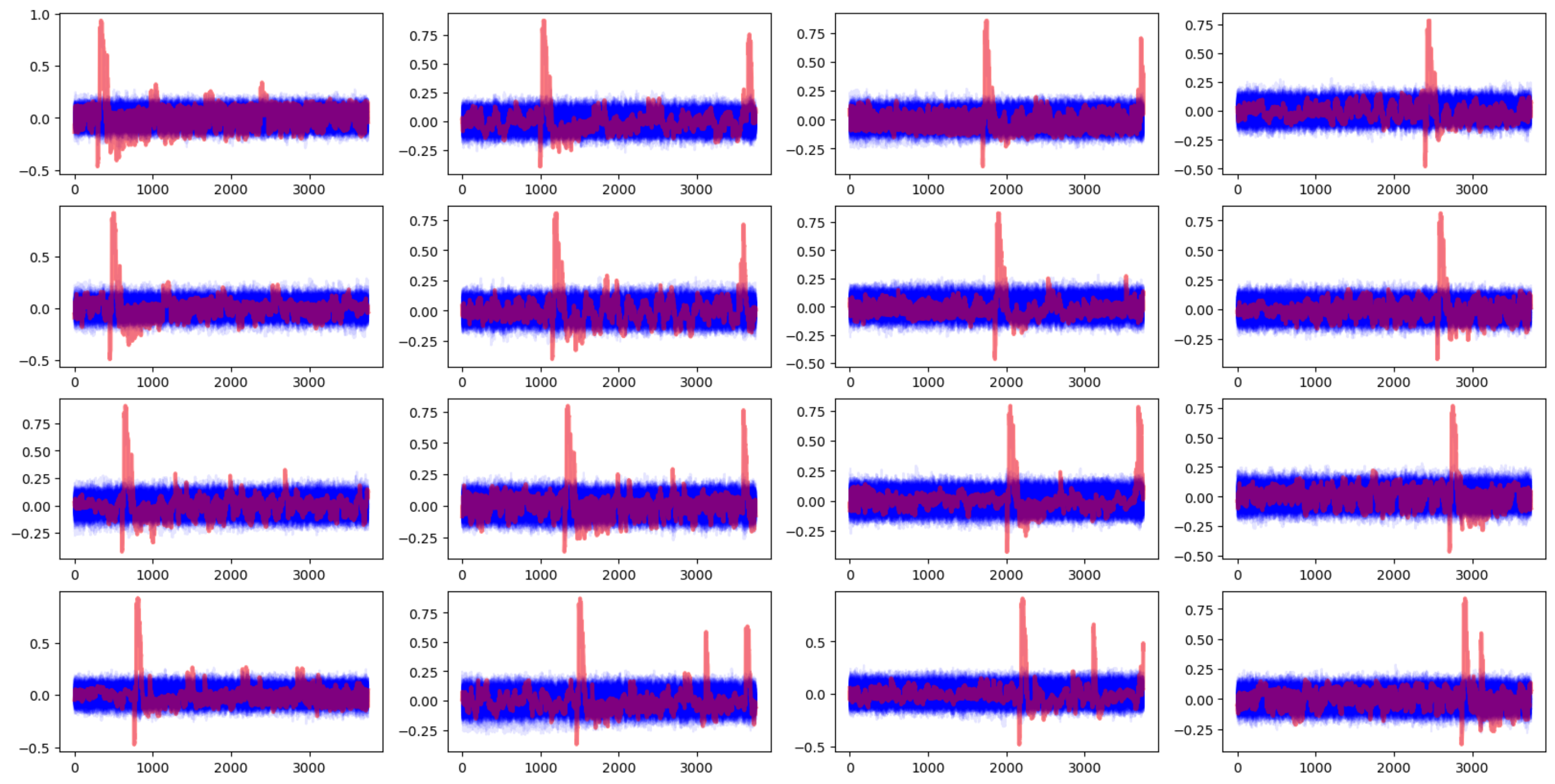
Demo (Correlation Power Analysis)

Correlations obtained for key byte 0. There are 256 curves overlaid (one for each key hypothesis). The red curve corresponds to the correct key hypothesis. It shows a very high correlation peak at the beginning (where the intermediate value is manipulated).



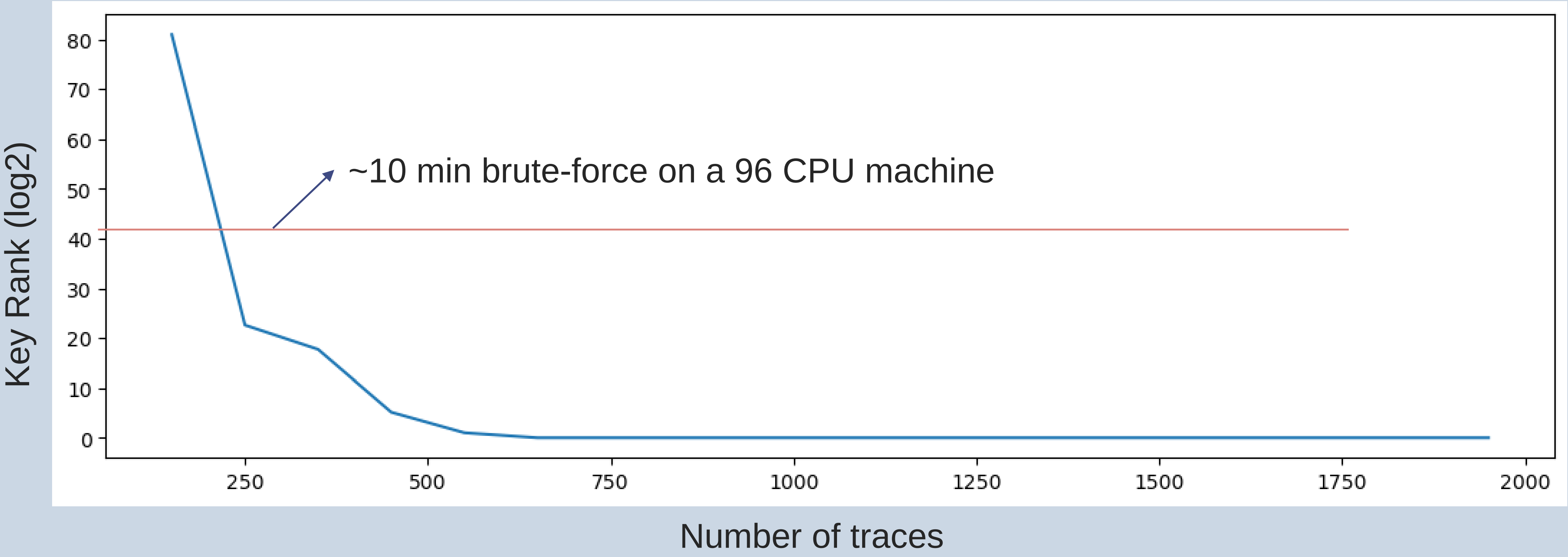
Demo (Correlation Power Analysis)

Correlation curves for all 16 key bytes.



Demo (Correlation Power Analysis)

Key rank evolution with the number of traces.



~10 min brute-force on a 96 CPU machine

On this software implementation around 500 traces are needed for a fast attack.
1000 traces for a reliable attack. End to end attack : ~5 seconds.

Side-channel analysis on smartphones

- Forensic application: break memory encryption (FBE or FDE)
  - iPhone4 UID key extraction [1]
  - A10 CoreCrypto attack [2]
  - AES key extraction (unknown model) [3]
  - https://exfiles.eu/

- SCA techniques employed are the same as on MCUs.
  - Profiling is hard ⇔ jailbreaking the phone
  - Unprofiled attacks
    - Less effective that profiled attacks
    - How to leverages multiple samples (multivariate attacks)? [4]

[1] Lisovets, Oleksiy, et al. "Let's take it offline: Boosting brute-force attacks on iPhone's user authentication through SCA." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2021): 496-519.

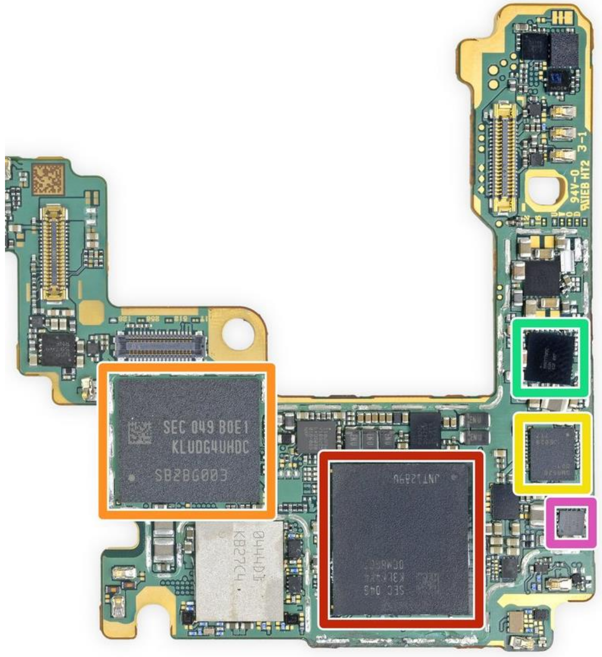
[2] Haas, Gregor, and Aydin Aysu. "Apple vs. EMA: electromagnetic side channel attacks on apple CoreCrypto." *Proceedings of the 59th ACM/IEEE Design Automation Conference*. 2022.

[3] Vasselle, Aurélien, Philippe Maurine, and Maxime Cozzi. "Breaking mobile firmware encryption through near-field side-channel analysis." *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop*. 2019.

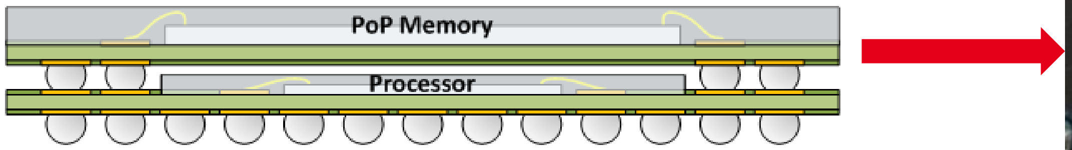
[4] Cristiani, Valence, Maxime Lecomte, and Philippe Maurine. "The EVIL Machine: Encode, Visualize and Interpret the Leakage." Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. 2023.

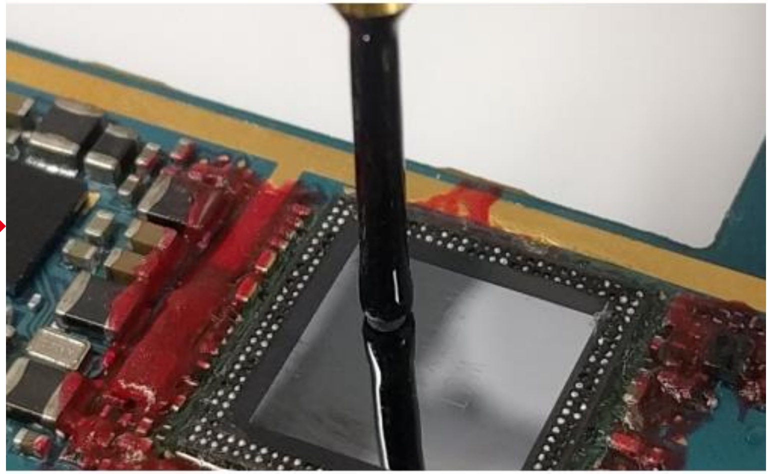
Side-channel analysis on smartphones

- Difficulties
  - Complex PCB, good luck finding the power line.
  - Stacked RAM: cannot place an EM probe close to the chip
    - Can be removed, but risky and expensive
  - Hardware cryptographic accelerators



Galaxy S21 PCB





Source: [1]

[1] Vasselle, Aurélien, Philippe Maurine, and Maxime Cozzi. "Breaking mobile firmware encryption through near-field side-channel analysis." *Proceedings of the 3rd ACM Workshop on Attacks and Solutions in Hardware Security Workshop*. 2019.

Side-channel analysis on smartphones

- Other difficulties:
  - Huge amount of noise
  - Important jitter
  - (Sometimes) countermeasures

- Important number of traces required:
  - iPhone4 Attack: 300M traces ~2 weeks acquisition
  - CoreCrypto attack: 5-30M traces

Countermeasures

Non-exhaustive list of countermeasures:

- Leakage assessment to evaluate the best attacker
- Rekeying, protocol : to prevent reuse of keys
- Reduce signal quality:
  - Hardware implementations (cryptographic accelerators)
  - Extra noise
  - Shielding
  - Jitter (clock)
- Non-deterministic execution: shuffling, dummy instructions
- Masking, alternative data representations (e.g., FFT, RNS)
- Delegate critical operations to certified products!

Conclusion

- Implementation != Specification => Security properties not always preserved

- Power, EM side-channel analysis: require physical access
  - Highly effective against software implementations of cryptography
  - Publicly available implementations are rarely secure against those attacks

- Some techniques translate remotely (micro-architectural attacks)

- SCA techniques developed on MCUs work on smartphones
  - Unprofiled, but important noise requiring large number of traces

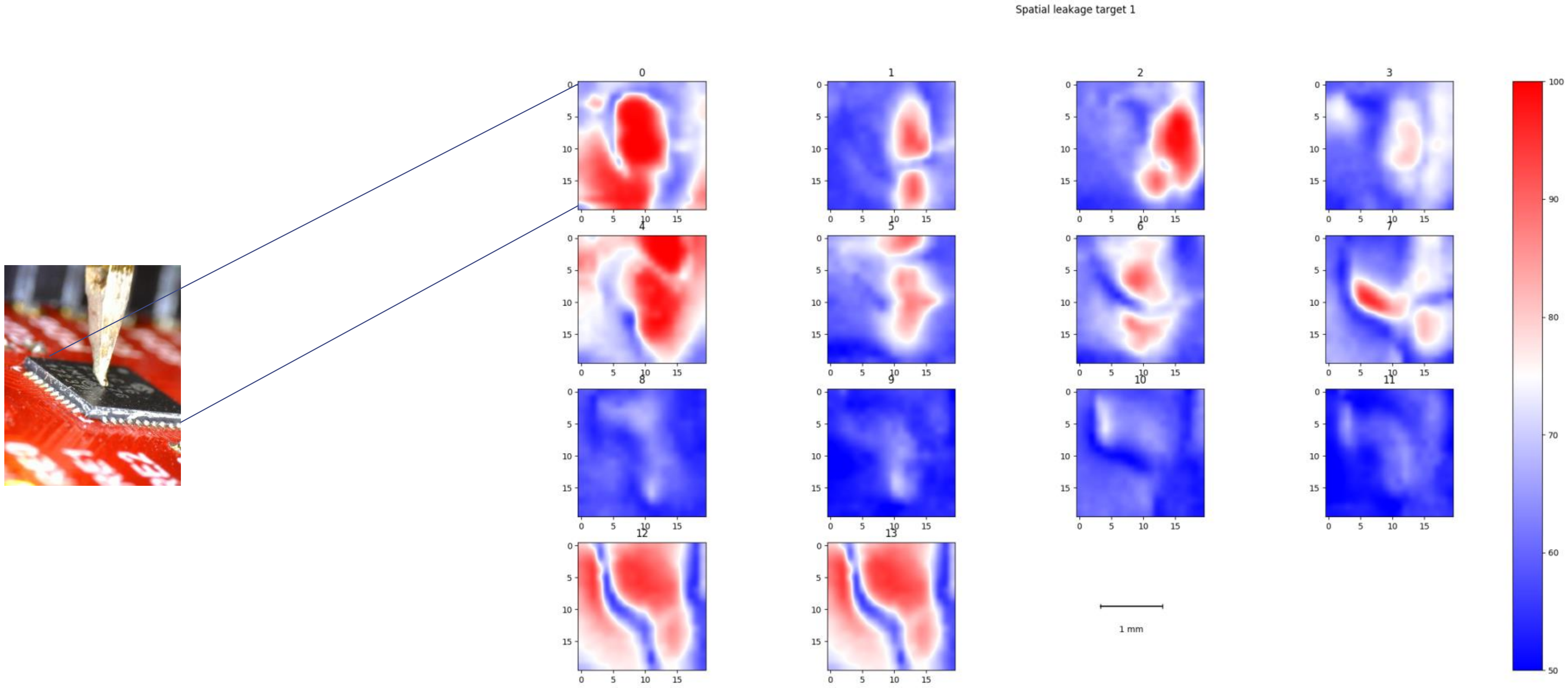
- Side-channel analysis is only a small class of physical attacks

Merci

CEA-Leti, Grenoble, France
cea-leti.com
Thomas.hiscock@cea.fr
T. + 33 (0)0 00 00 00 00
M. + 33 (0)0 00 00 00 00

About model portability

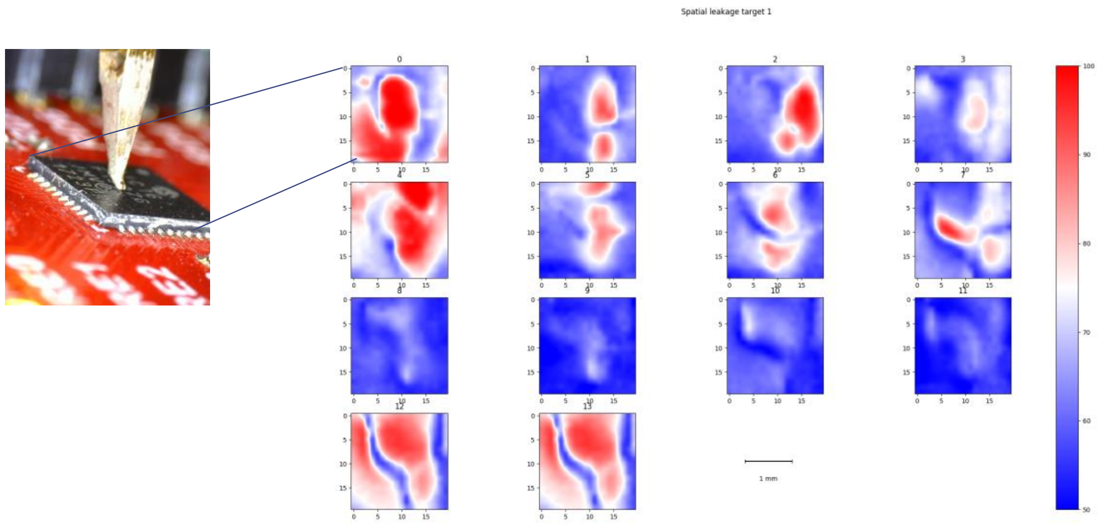
- Can we really swap boards like that?



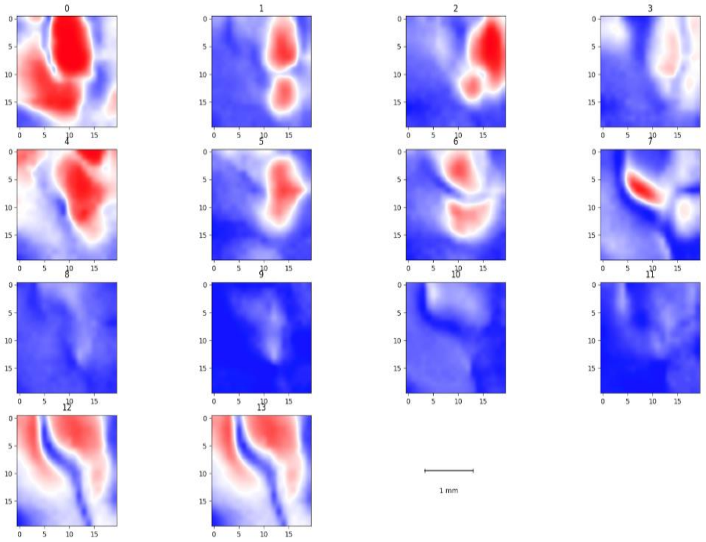
Cristiani, Valence, Maxime Lecomte, and Thomas Hiscock. "A bit-level approach to side channel based disassembling." *Smart Card Research and Advanced Applications: 18th International Conference, CARDIS 2019, Prague, Czech Republic, November 11–13, 2019, Revised Selected Papers 18*. Springer International Publishing, 2020.

About model portability

- Can we really swap boards like that? Yes ☺
- Spatial correction had to be applied



Target 1
(Profiling)



Target 2
(Attack)

Cristiani, Valence, Maxime Lecomte, and Thomas Hiscock. "A bit-level approach to side channel based disassembling." *Smart Card Research and Advanced Applications: 18th International Conference, CARDIS 2019, Prague, Czech Republic, November 11–13, 2019, Revised Selected Papers 18*. Springer International Publishing, 2020.