Side-channel attacks in the wild: recent advances and countermeasures

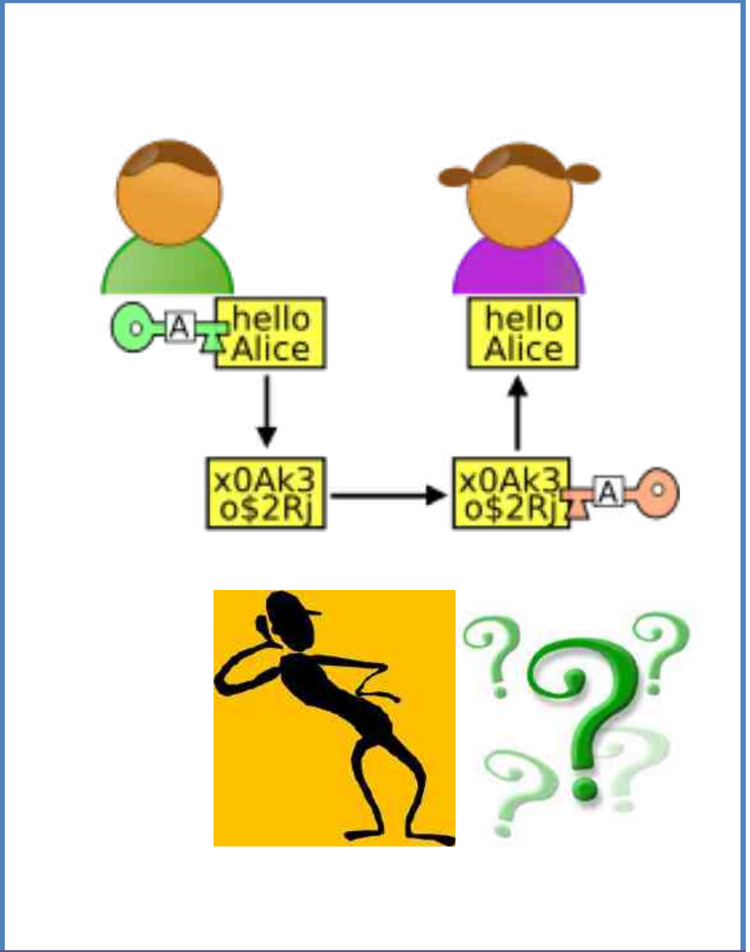
Lejla Batina

Digital Security Group
Institute for Computing and Information Sciences (ICIS)
Radboud University Nijmegen

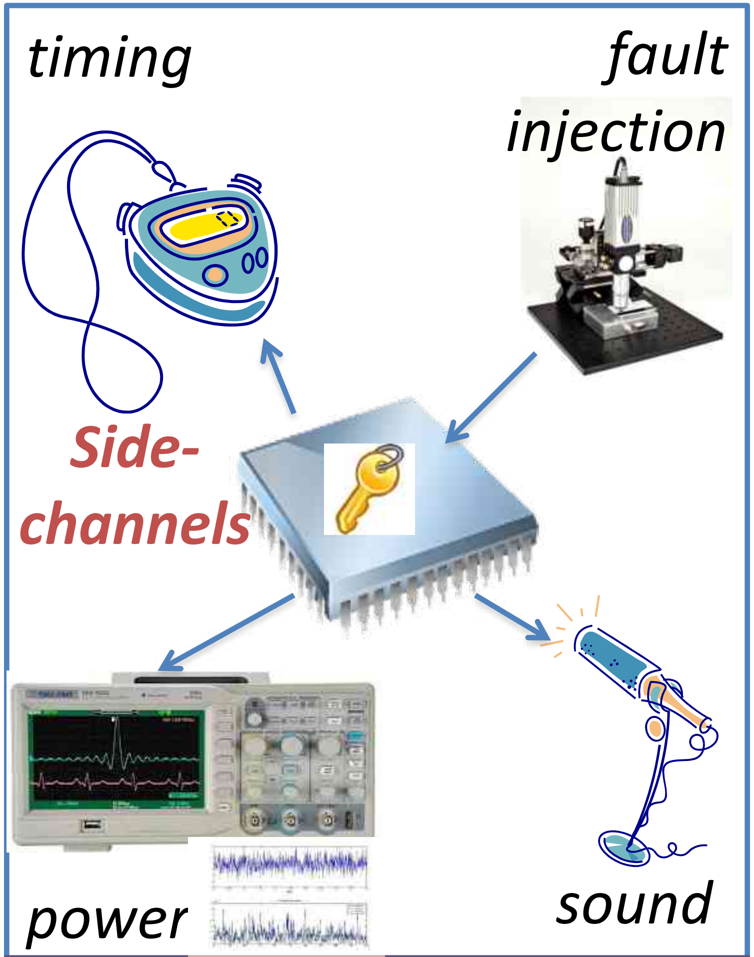
CROSSING SUMMER SCHOOL

Darmstadt, September 12, 2019

Crypto: theory vs physical reality



Algorithms are (supposed to be) theoretically secure



timing

fault injection

Side-channels

power

sound

Implementations leak in physical world

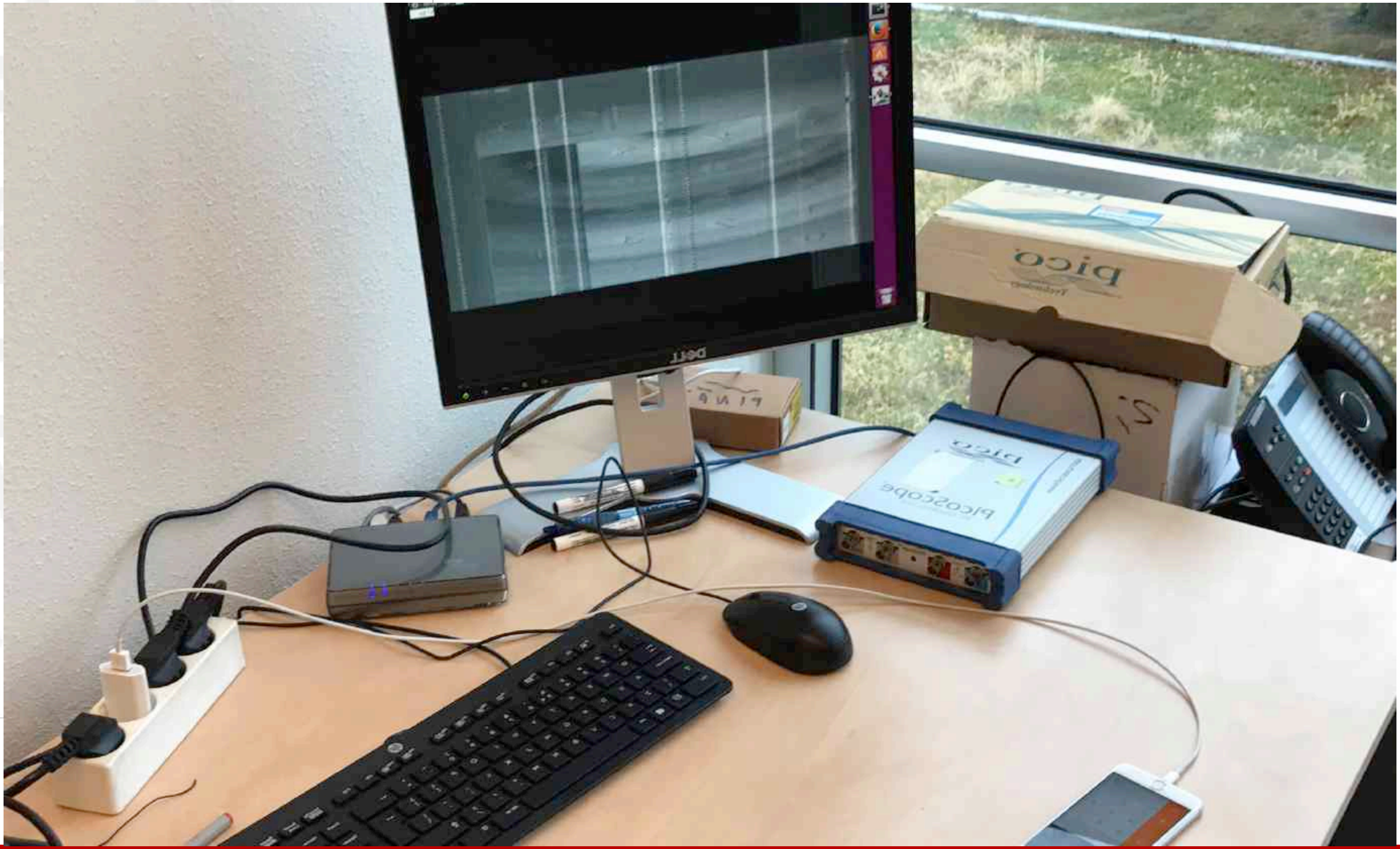
R. Anderson and M. Kuhn, P. Kocher, 1996

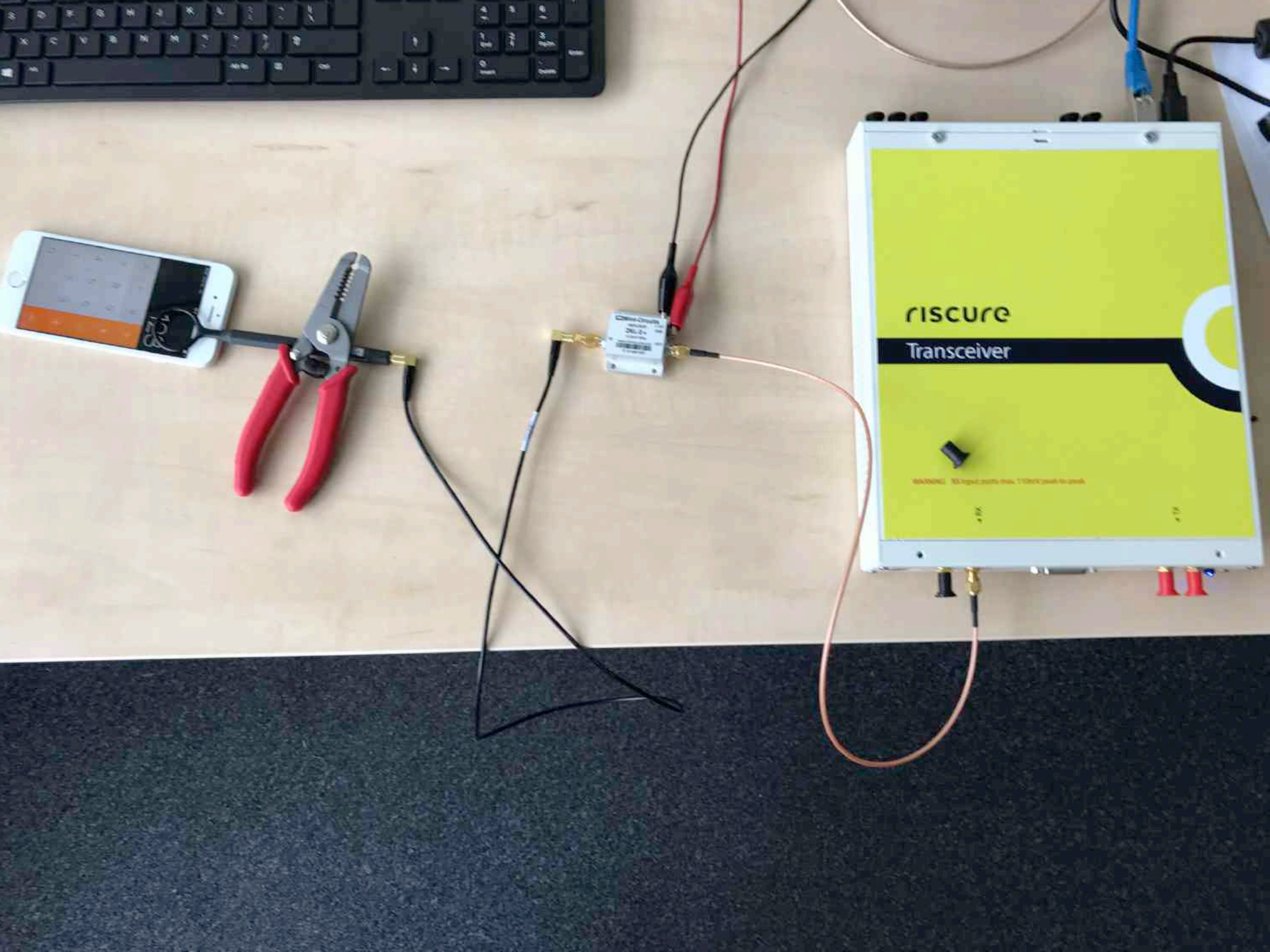
Side-channel security before

- Tempest – known since early 1960s that computers generate EM radiation that leaks info about the data being processed
  - first evidence in 1943: an engineer using a Bell telephone noticed that a digital oscilloscope spiked for every encrypted letter
  - declassified in 2008
  - van Eck phreaking in 1985

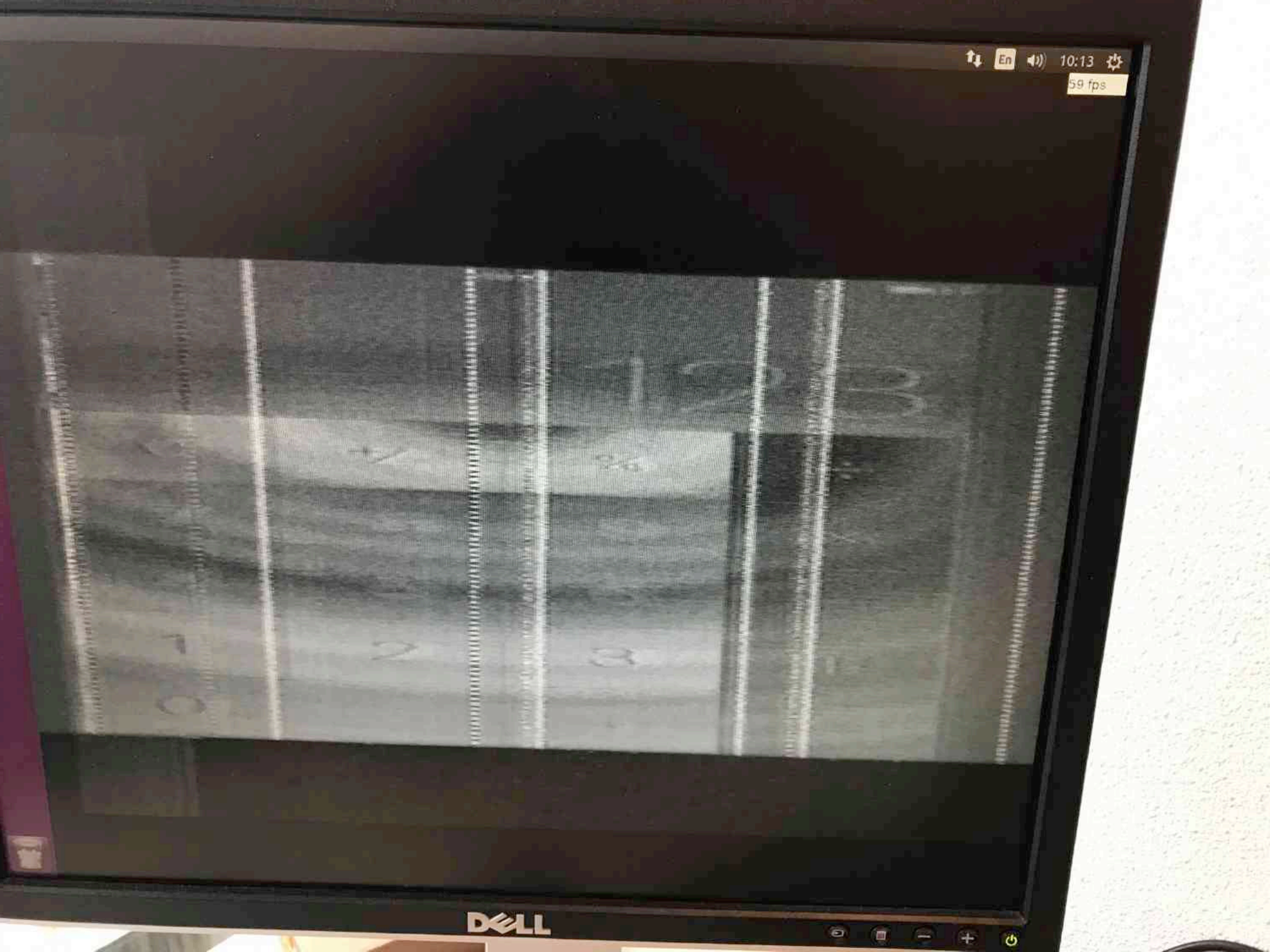
- In 1965, MI5 put a microphone near the rotor-cipher machine used by the Egyptian Embassy, the click-sound the machine produced was analyzed to deduce the core position of the machines rotors

New Tempest




riscure
Transceiver

123



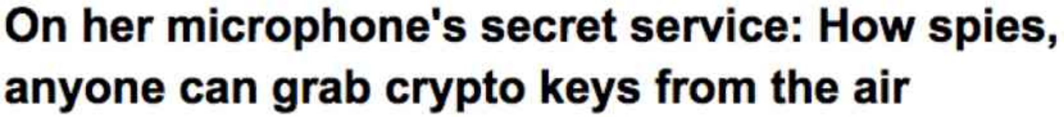
En
10:13
59 fps
1 2 3
1
2
8
0

Outline

- Implementations of security != secure implementations
- Side-channel analysis
  - Power analysis attacks
  - Other side-channels: EM
- Countermeasures
- A real-world example: hacking EdDSA in WolfSSL
- Recent developments

(In)security of Embedded Systems

"Researchers have extracted information from nothing more than the reflection of a computer monitor off an eyeball or the sounds emanating from a printer."
Scientific American, May 2009.

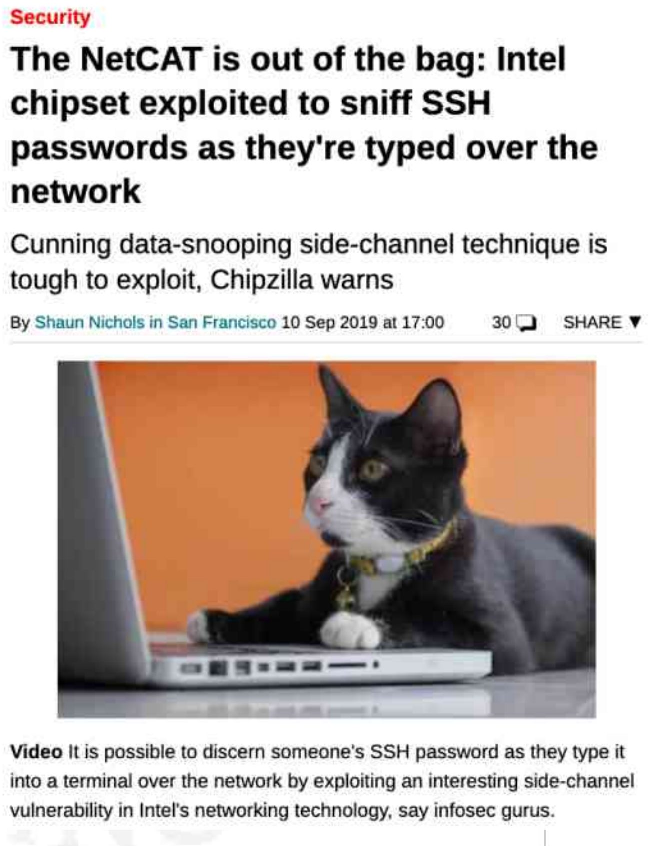


On her microphone's secret service: How spies, anyone can grab crypto keys from the air

http://www.theregister.co.uk/2016/06/04/sidechannel_encryption_theft/

"Using EM measurements, we were able to fully extract secret signing keys from OpenSSL and CoreBitcoin running on iOS devices. We also showed partial key leakage from OpenSSL running on Android…, March 2016.
https://www.cs.tau.ac.il/~tromer/mobilesc/

SCA in the news - recent



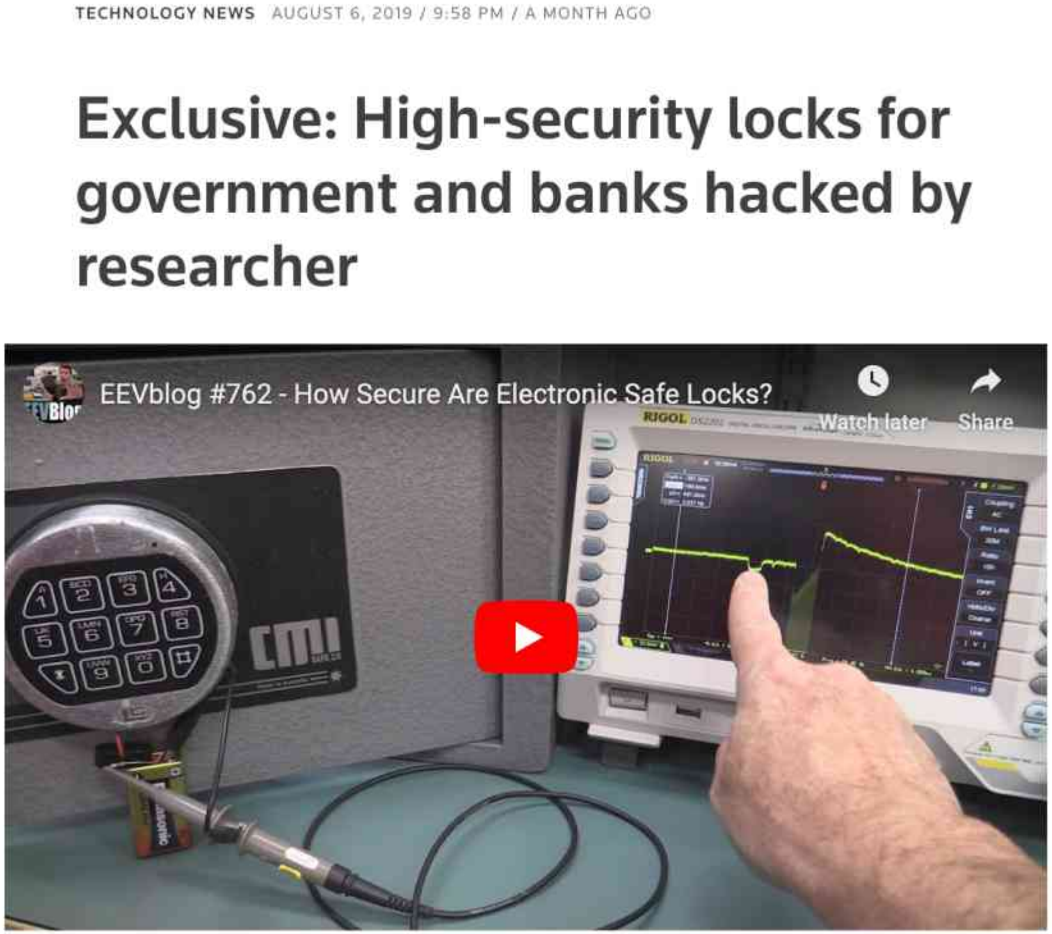
Security

The NetCAT is out of the bag: Intel chipset exploited to sniff SSH passwords as they're typed over the network

Cunning data-snooping side-channel technique is tough to exploit, Chipzilla warns

By Shaun Nichols in San Francisco 10 Sep 2019 at 17:00 30 SHARE ▼

Video It is possible to discern someone's SSH password as they type it into a terminal over the network by exploiting an interesting side-channel vulnerability in Intel's networking technology, say infosec gurus.



TECHNOLOGY NEWS AUGUST 6, 2019 / 9:58 PM / A MONTH AGO

Exclusive: High-security locks for government and banks hacked by researcher

EEVblog #762 - How Secure Are Electronic Safe Locks?

Embedded cryptographic devices

Embedded security:

- resource limitation
- physical accessibility

The goals of attackers

- Secret keys/data
- Unauthorized access
- IP/piracy
- (Location) privacy
- (Theoretical) cryptanalysis
- Reverse engineering
- Finding backdoors in chips
- …

Some real-world attacks

- Remote keyless entry system for cars KeeLoq and buildings was hacked in 2008
  - KeeLoq: eavesdropping from up to 100 m
  - remote can be cloned from only 10 power traces
  - practical key recovery in few minutes

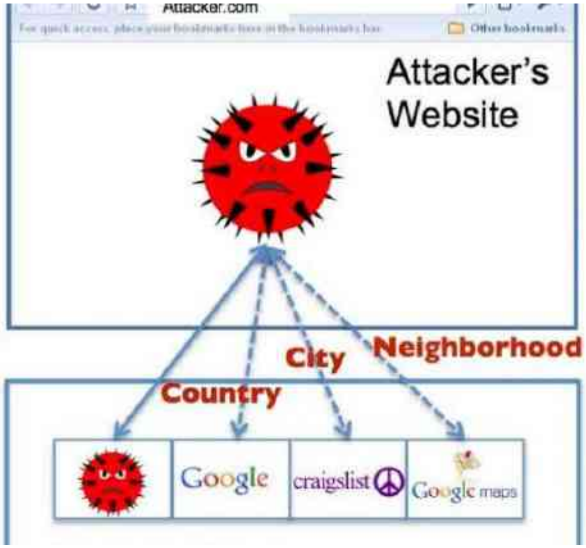
- Mifare DESFire MF3ICD40 cracked in 2011
  - contactless card used in transit in San Francisco, Australia, and the Czech Republic, also adopted by NASA in 2004
- Acoustic cryptanalysis
  - Attacking a computer by listening to the high-pitched (10 to 150 KHz) sounds produced as it decrypts data
  - Extracted 4096-bit RSA keys
  - Using low- and high-pass filters to ensure to get only the sounds that emanate from the PC while the CPU is decrypting data

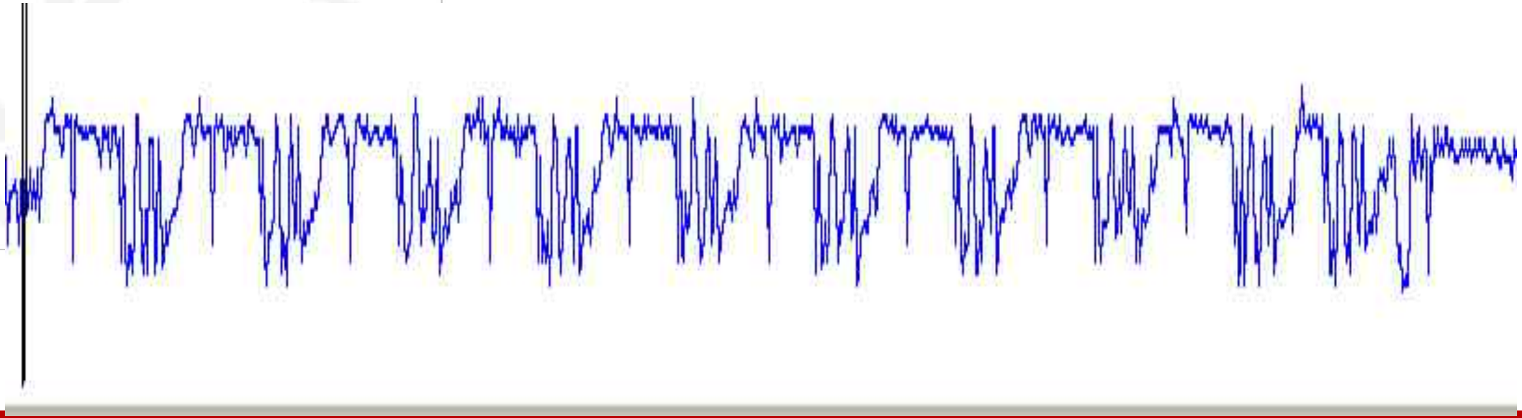
Side-channel security today

- As a research area took off in the 90’s
- Many successful attacks published on various platforms and real products e.g. KeeLoq [EK+08], CryptoMemory [BG+12], (numerous) contactless cards
- A good business model for security evaluation labs e.g. Riscure and Brightsight

Concepts of side-channel leakage

- Based on (non-intentional) physical information
- Often, optimizations enable leakages
    - Cache: faster memory access
    - Fixed computation patterns (rounds)
    - Square vs multiply (for RSA)



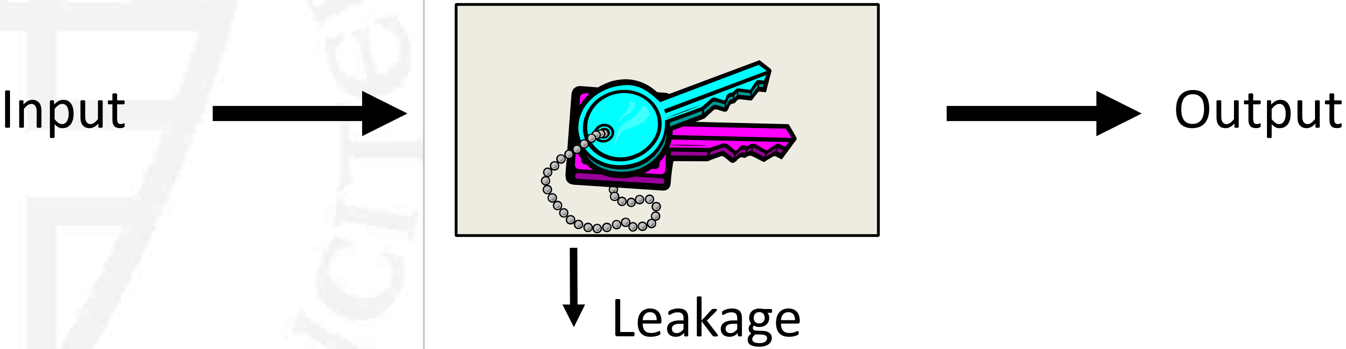


Side-Channel Leakage

- Physical attacks ≠ Cryptanalysis

(gray box, physics) vs (black box, math)

- Does not tackle the algorithm's mathematical security



Input

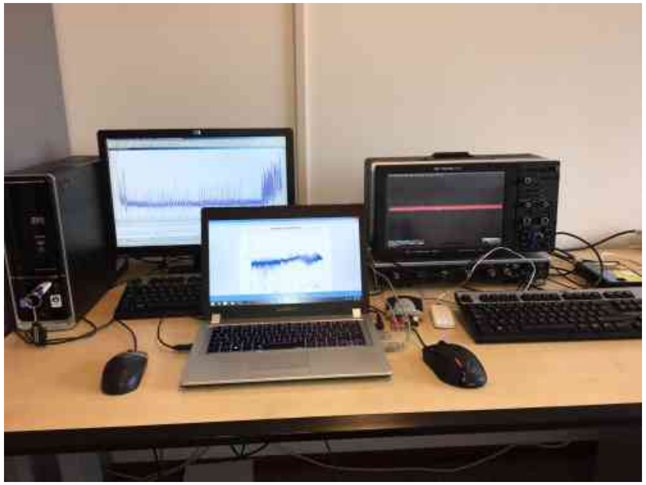
Output

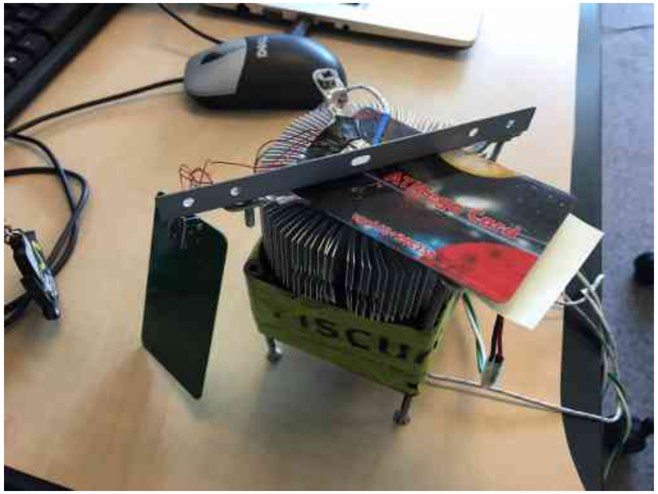
Leakage

- Leakages: Timing, Power, EM, Light, Sound, Temperature
- Observe physical observances in the device's vicinity and use additional information to perform the attack
- Unintentional signals are used to reconstruct data

Attack categories

- Side-channel attacks
  - use some physical (analog) characteristic and assume access to it
- Faults
  - use abnormal conditions causing malfunctions in the system e.g. voltage, clock, temperature, light
- Micro-probing
  - accessing the chip surface directly in order to observe, learn and manipulate the device
- Reverse engineering
  - using side-channel analysis to understand inner workings of a system (used on 3060 locking system of Simons Voss)





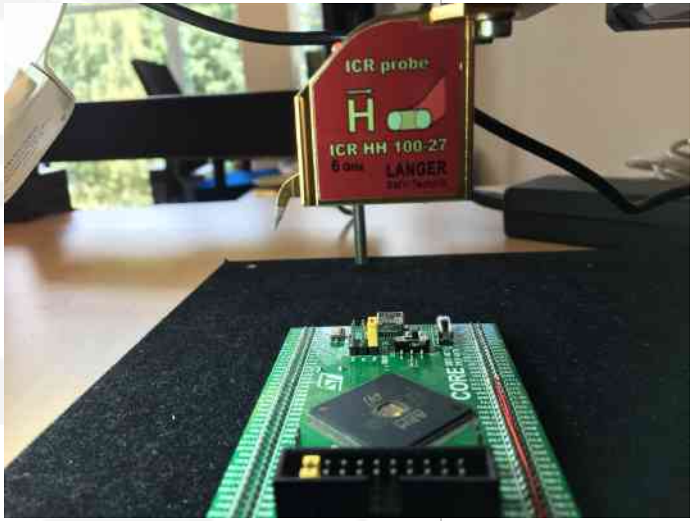
Taxonomy of Implementation Attacks

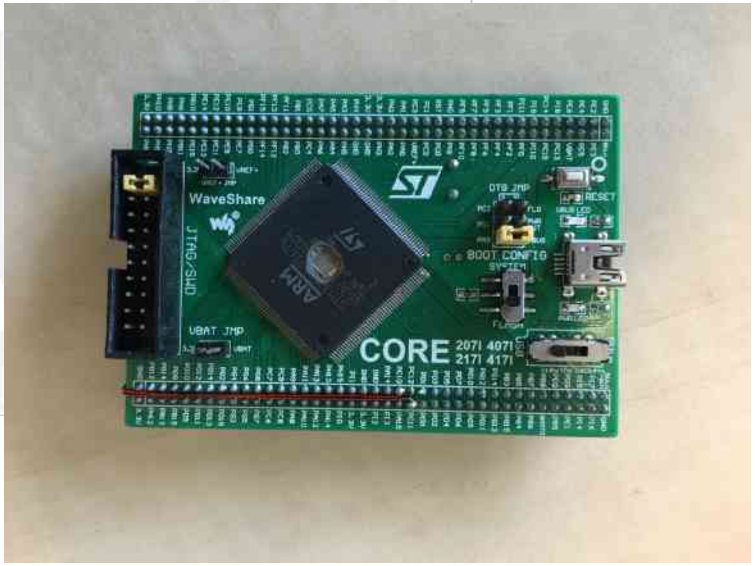
- Invasive versus non-invasive
  - Invasive aka expensive: the strongest type e.g. bus probing
  - Semi-invasive: the device is de-packaged but no contact to the chip e.g. optical attacks that read out memory cells (or faults/glitches by voltage, power supply, clock, EM, etc.)
  - Non-invasive aka low-cost: power/EM measurements
  - Non-invasive: data remanence in memories – cooling down is increasing the retention time
- Side-channel attacks: passive and non-invasive

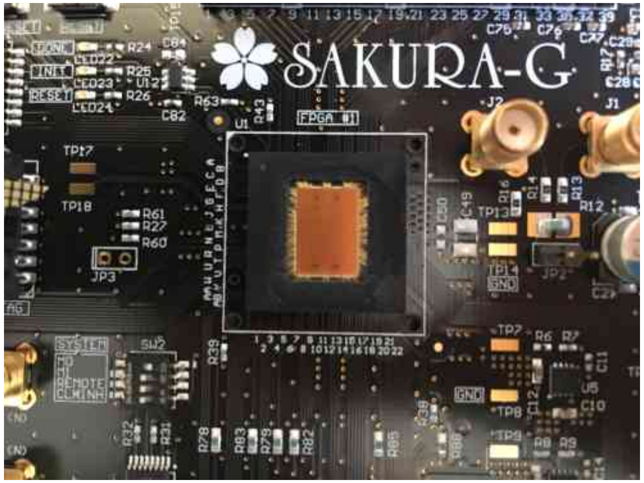
Attackers models

- “Simple” attacks: one or a few measurements - visual inspection
- Differential attacks: multiple measurements
  - – Use of statistics, signal processing, etc.
- Univariate vs multivariate
- Combining two or more side-channels
- Combining side-channel attack with theoretical cryptanalysis
- Template attacks – strongest in

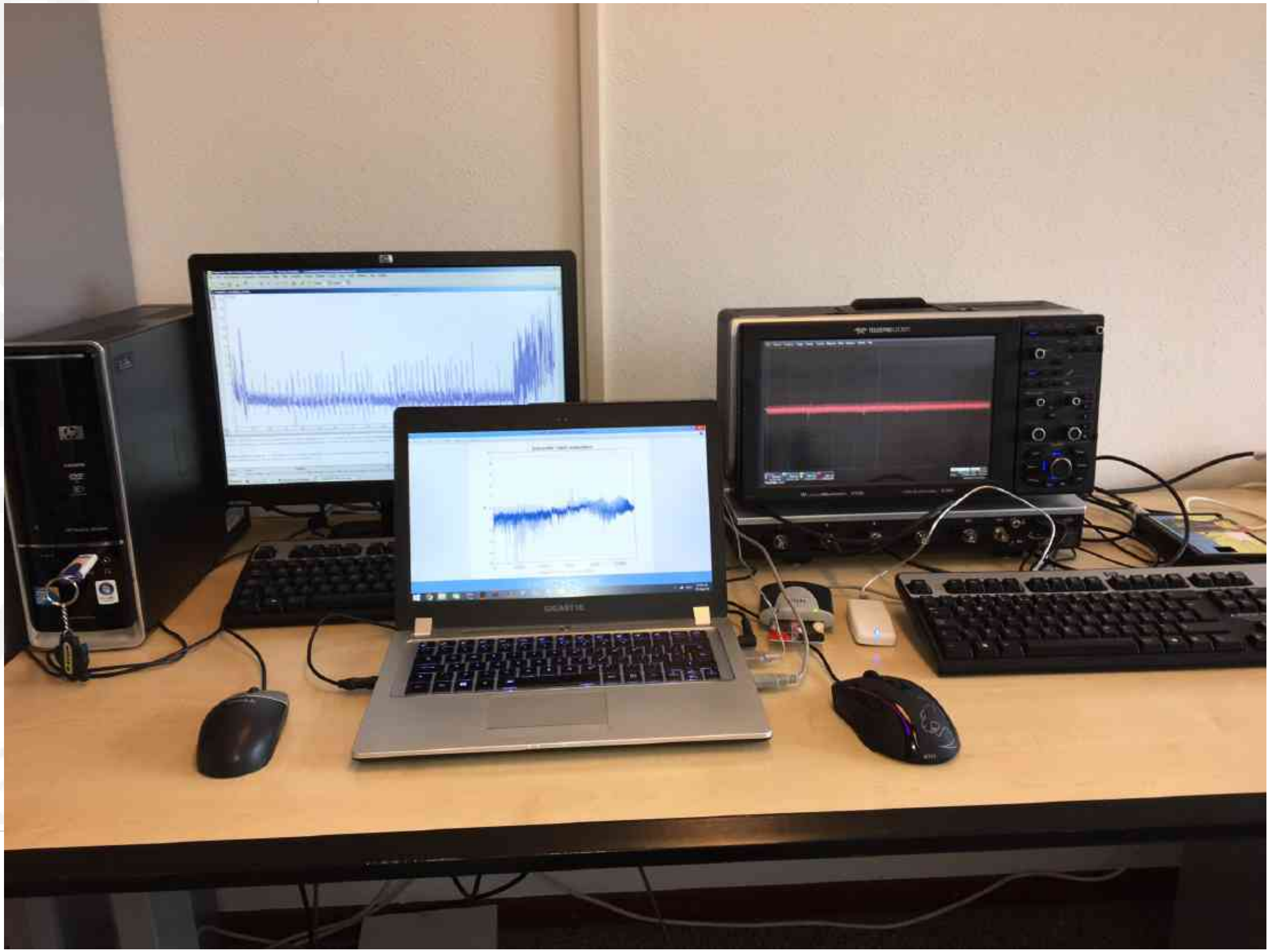
Devices under attack







Measurement setup for power analysis



Simple Power Analysis (SPA)

Simple Power Analysis (SPA)

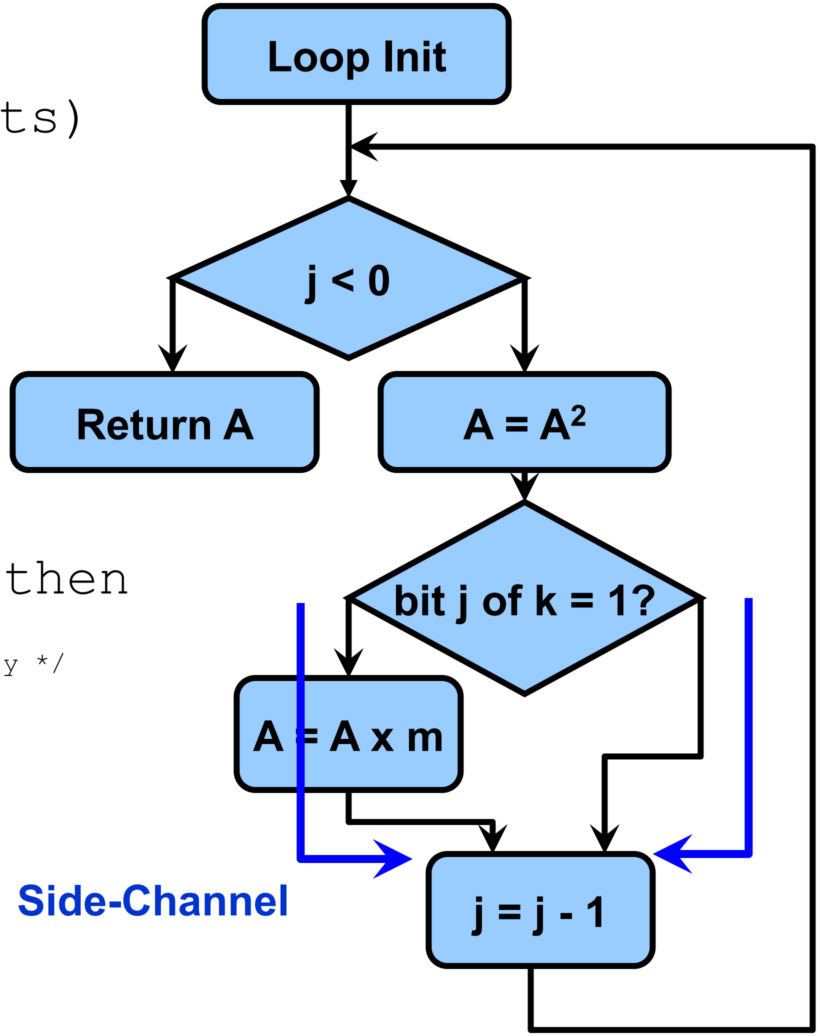
- Based on one or a few measurements
- Mostly discovery of data-(in)dependent but instruction-dependent properties e.g.
  - Symmetric:
    - Number of rounds (resp. key length)
    - Memory accesses (usually higher power consumption)
  - Asymmetric:
    - The key (if badly implemented, e.g. RSA / ECC)
    - Key length
    - Implementation details: for example RSA w/wo CRT
- Search for repetitive patterns

Insecure RSA implementation

RSA modular exponentiation

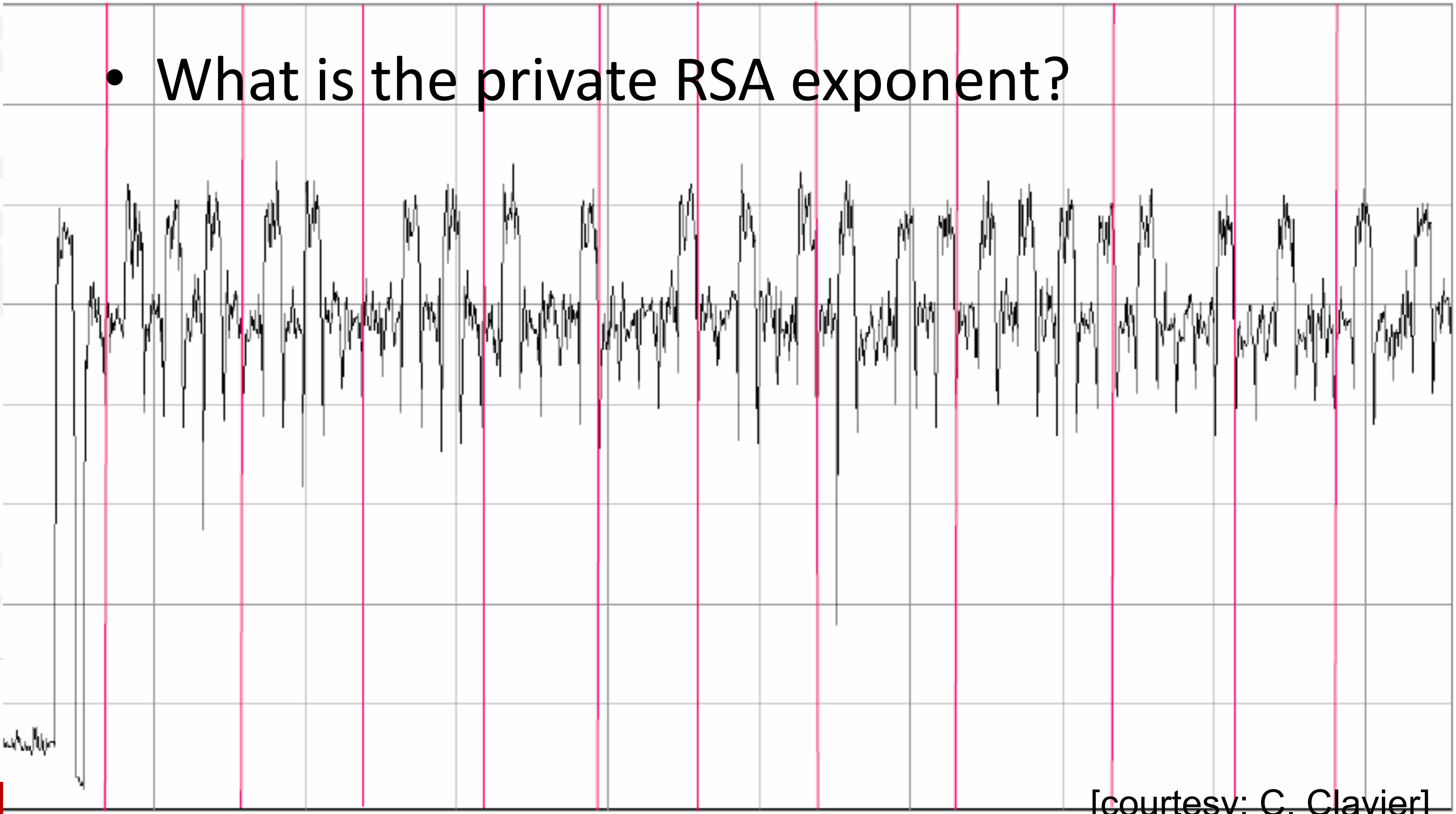
```
In: message m,key e(l bits)
Output: m^e mod n

A = 1
for j = l - 1 to 0
    A = A^2 mod n /* square */
    if (bit j of k) is 1 then
    A = A x m mod n /* multiply */
Return A
```



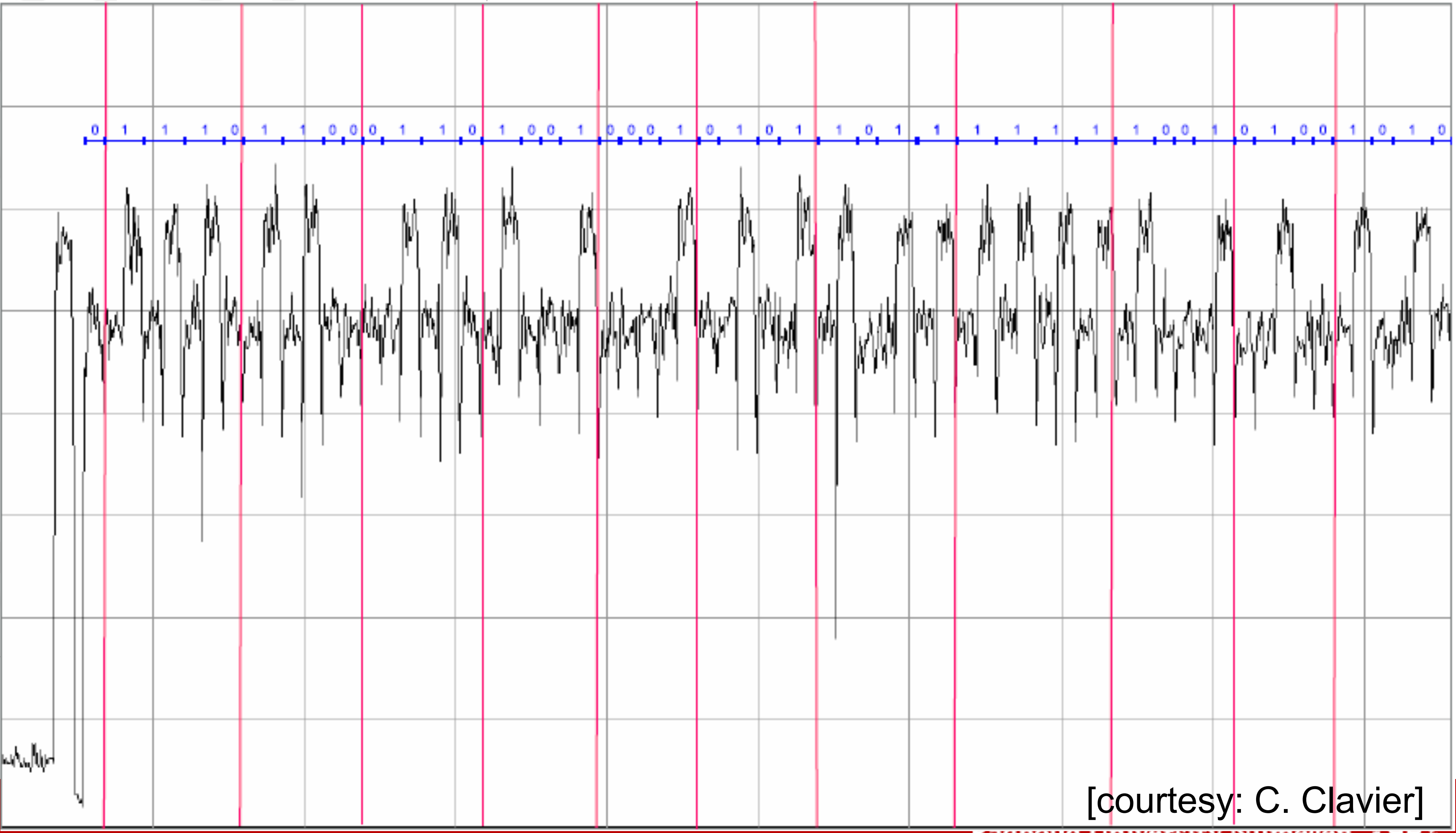
Simple Power Analysis (RSA)

- What is the private RSA exponent?



[courtesy: C. Clavier]

Simple Power Analysis (RSA)

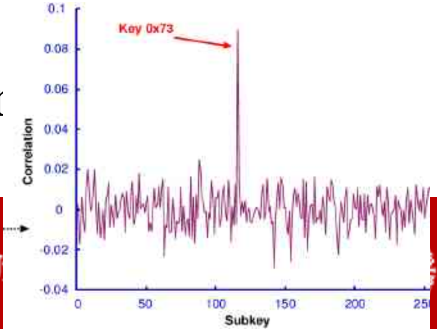


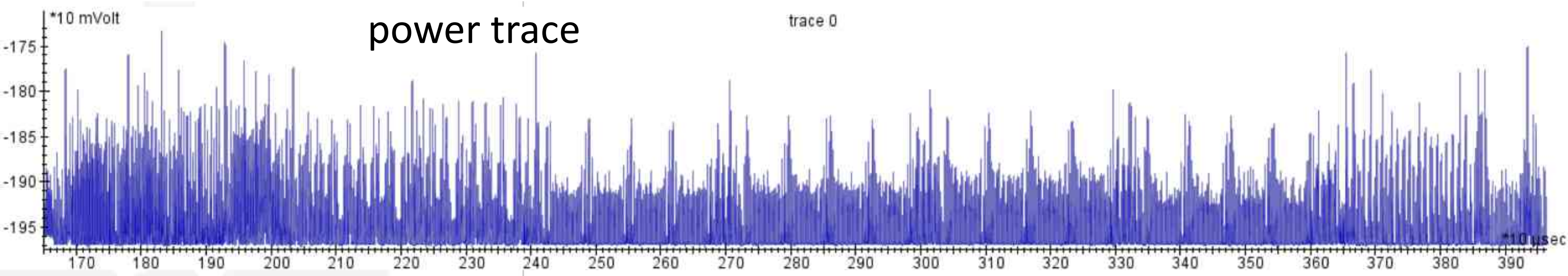
[courtesy: C. Clavier]

Differential Power Analysis (DPA)

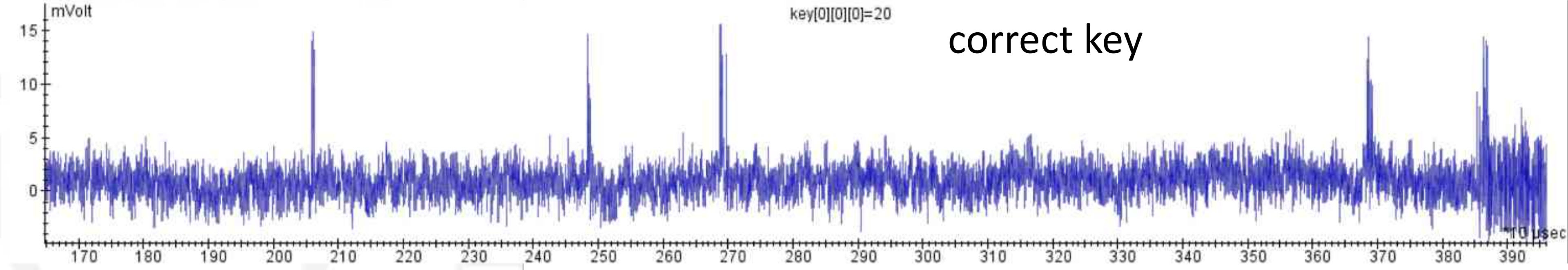
DPA summary

- Attack has 2 parts:
  - 'Cryptanalysis': target a sensitive intermediate result for which exhaustive key search is feasible
  - Engineering, statistics: provide access to an oracle that verifies sub-key hypotheses using power traces
- Working principle:
  - Acquisition part: collect a set of traces with varying inputs
  - Select sensitive intermediate variable
  - For each key hypothesis:
    - Compute hypothetical values of the sensitive variable, sort curves into subset
    - Compute difference between the subsets
- Intuition:
  - wrong key guesses -> no correlation P vs model,
  - correct key guess -> good correlation P vs model

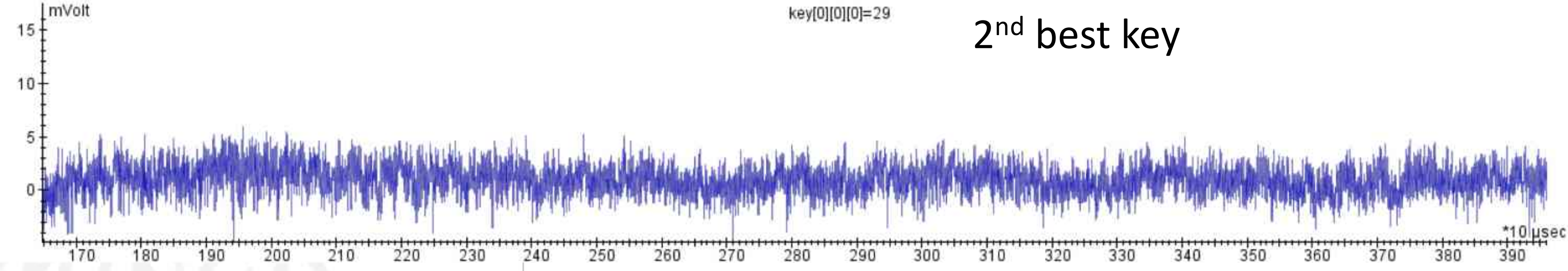




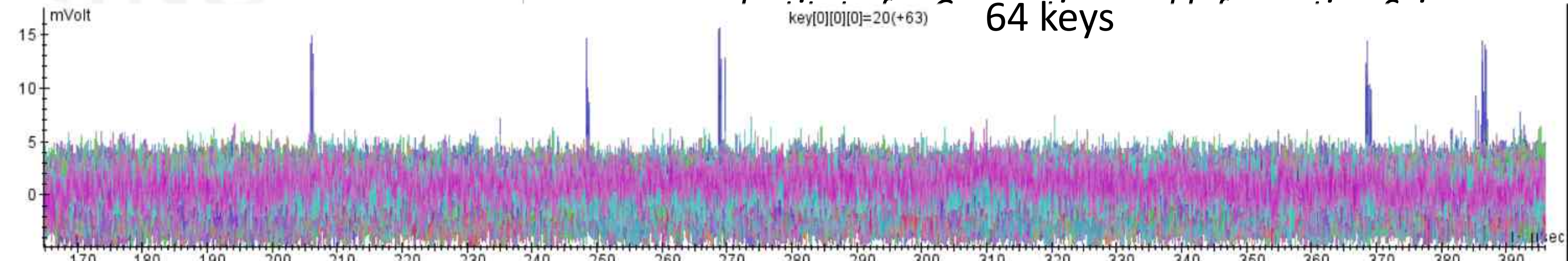
power trace



correct key



2nd best key



64 keys

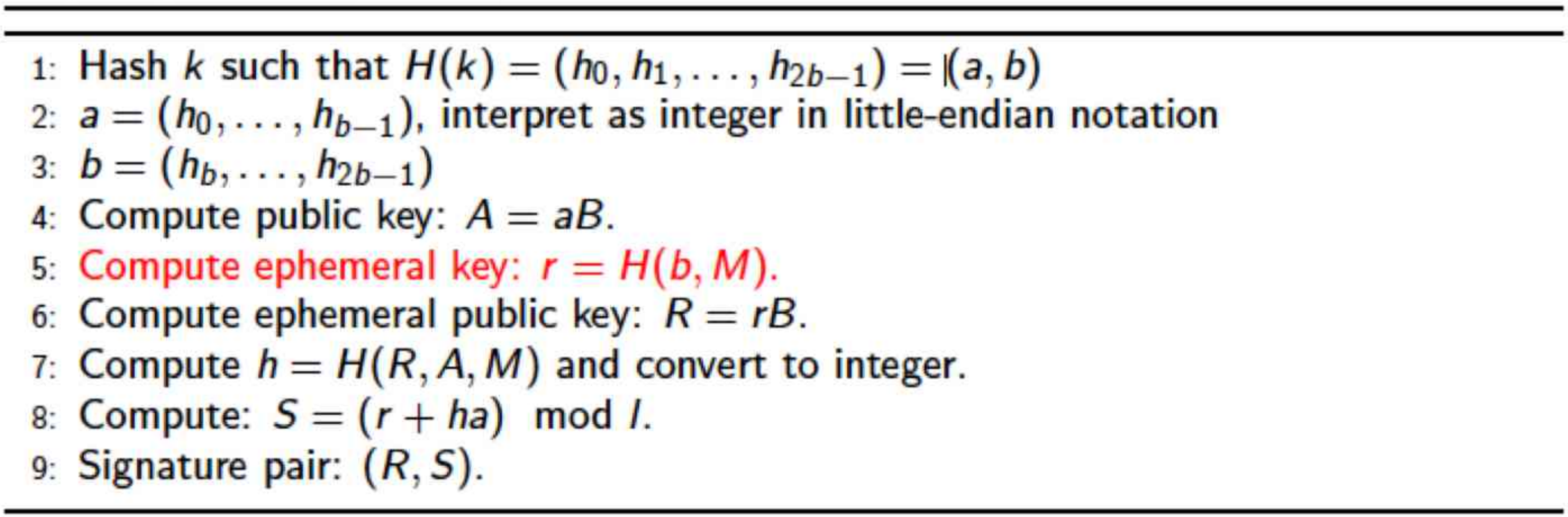
Breaking Ed25519 in WolfSSL

with N. Samwel et al.

Ed25519 facts

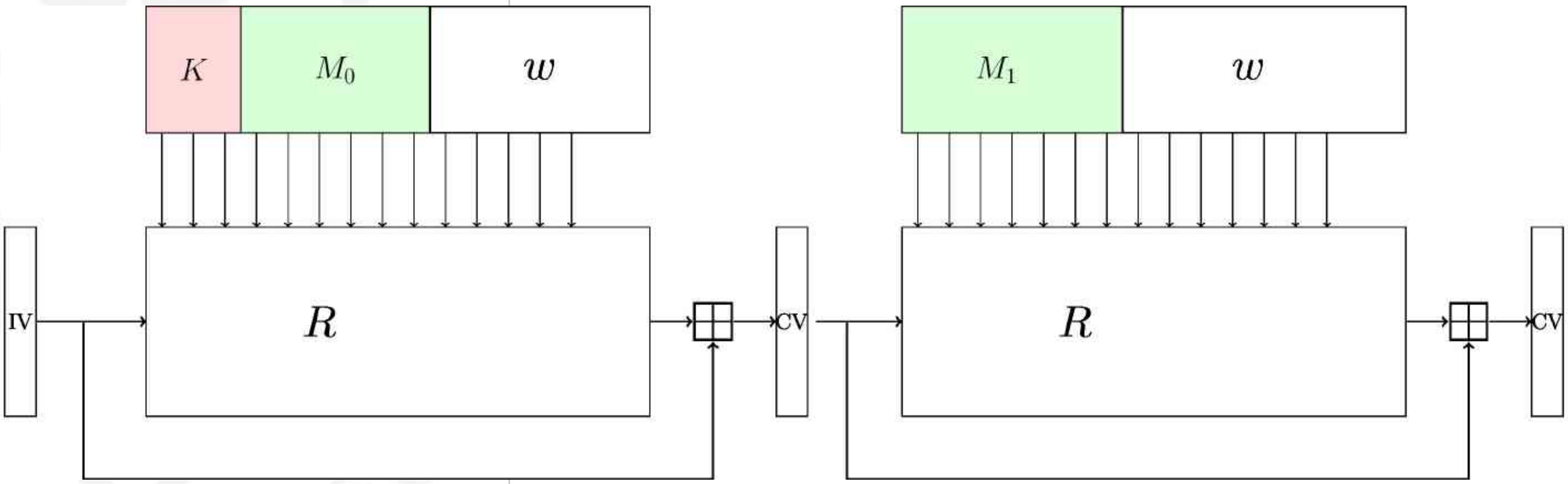
- Instance of EdDSA, which was proposed to “fix the unnecessary requirements on randomness" in ECDSA
- Does not depend on a “good" source of randomness, but instead derives a secret deterministically (hashing the msg and a long-term auxiliary key)
- Widely adopted by OpenSSH, Tor, Signal, WolfSSL etc.

EdDSA signature generation

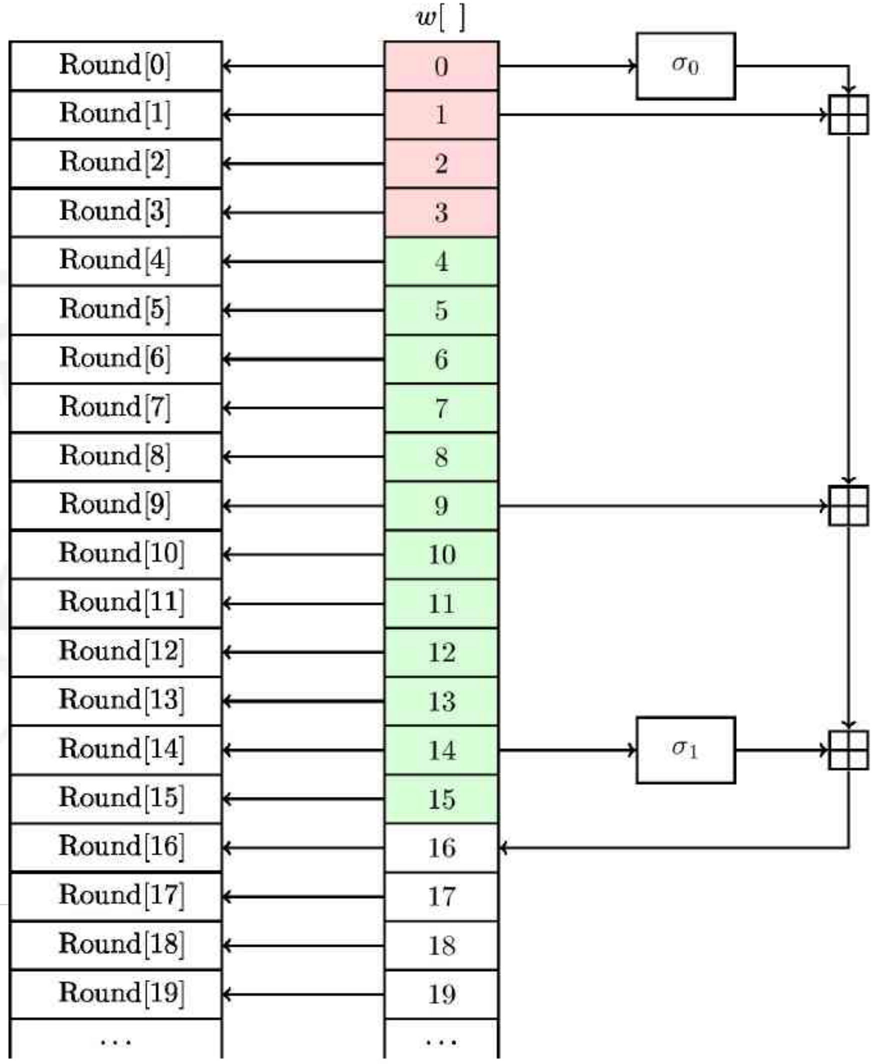


```
Hash $k$ such that $H(k) = (h_0, h_1, \ldots, h_{2b-1}) = (a, b)$
$a = (h_0, \ldots, h_{b-1})$, interpret as integer in little-endian notation
$b = (h_b, \ldots, h_{2b-1})$
Compute public key: $A = aB$.
Compute ephemeral key: $r = H(b, M)$.
Compute ephemeral public key: $R = rB$.
Compute $h = H(R, A, M)$ and convert to integer.
Compute: $S = (r + ha) \mod l$.
Signature pair: $(R, S)$.
```

SHA-512 construction



SHA-512 message schedule



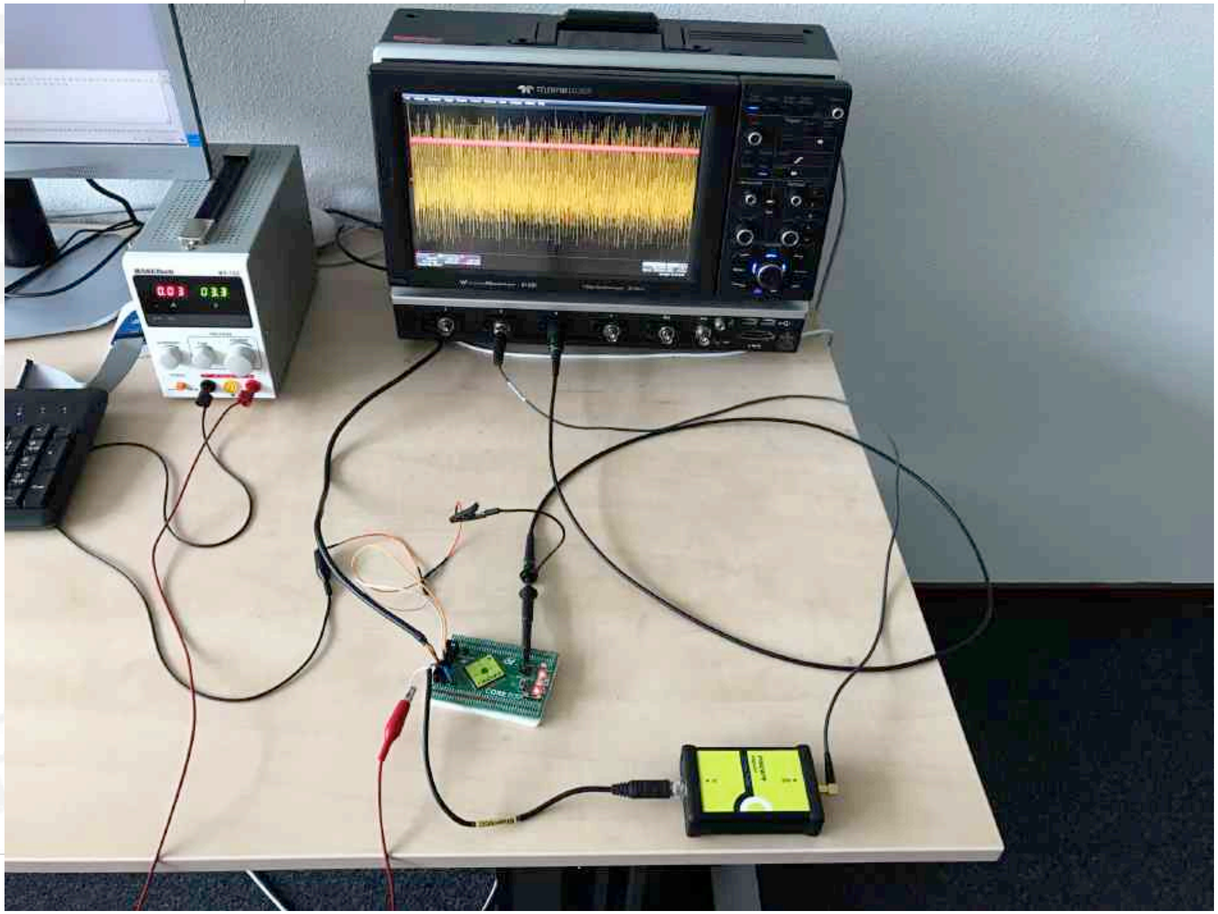
The attack

The attack point is the following computation:

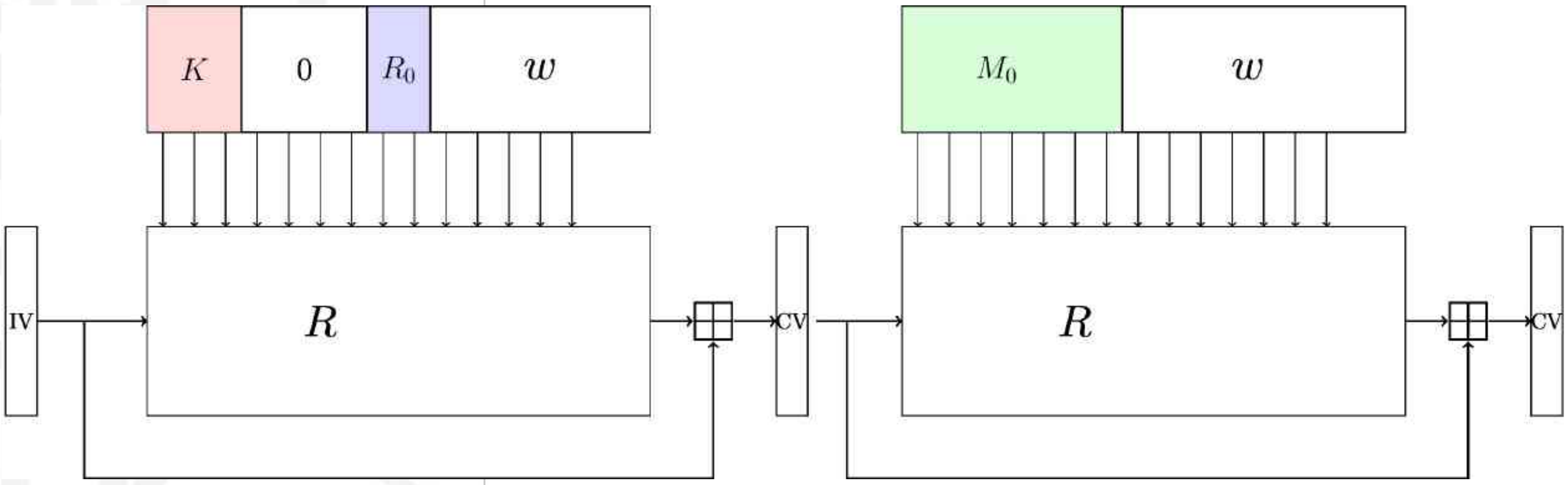
$$w[16] \leftarrow \sigma_1(w[14]) + w[9] + \sigma_0(w[1]) + w[0] \qquad (1)$$

- $w[14]$ and $w[9]$ are part of the message therefore known (green)
- $w[1]$ and $w[0]$ are part of the auxiliary key value so constant and unknown (red)
- the attack recovers $\sigma_0(w[1]) + w[0]$
- recursively and using $w[16], \ldots, w[19]$ we compute $w[0], \ldots, w[3]$, hence auxiliary key b

Setup



A countermeasure



Template Attacks

- Combination of statistical modeling and power-analysis attacks
- Similar ideas are used in detection and estimation theory
- Template attacks consist of two stages:
  - Template-Building Phase (profiling the unprotected device to create the templates)
  - Template-Matching Phase (use the templates for secret data recovery)

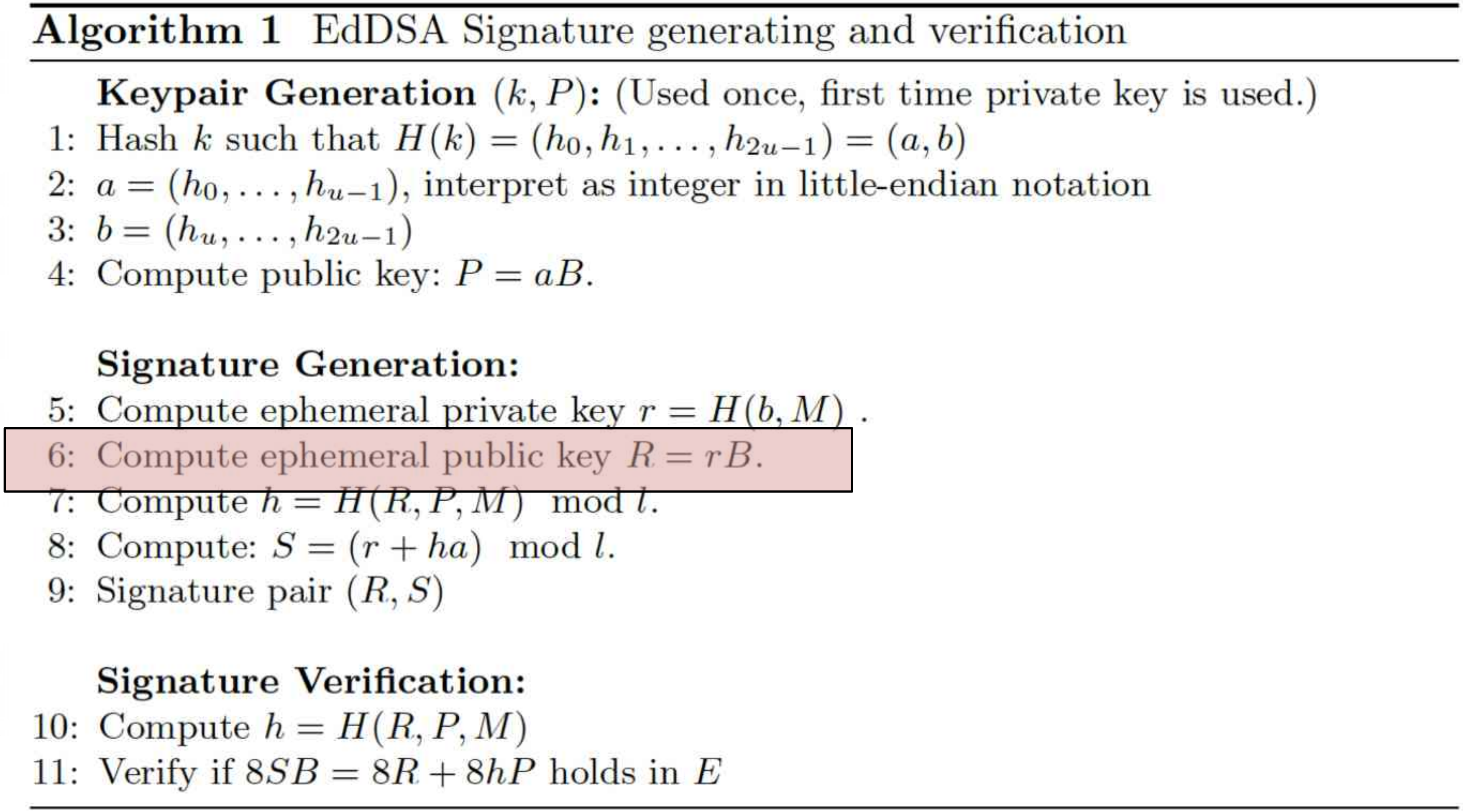
Recent ideas: Deep learning in SCA

- Machine learning for profiling introduced a while ago
- Recent ideas use deep learning to:
  - build a profiling model for each possible value of the targeted sensitive variable during the training phase and, during the attack phase these models are used to output the most likely key
  - deal with misalignment countermeasures using CNNs together with Data Augmentation techniques

Attacking ECC signatures through Deep learning

with L. Weissbart and S. Picek

EdDSA signature generation



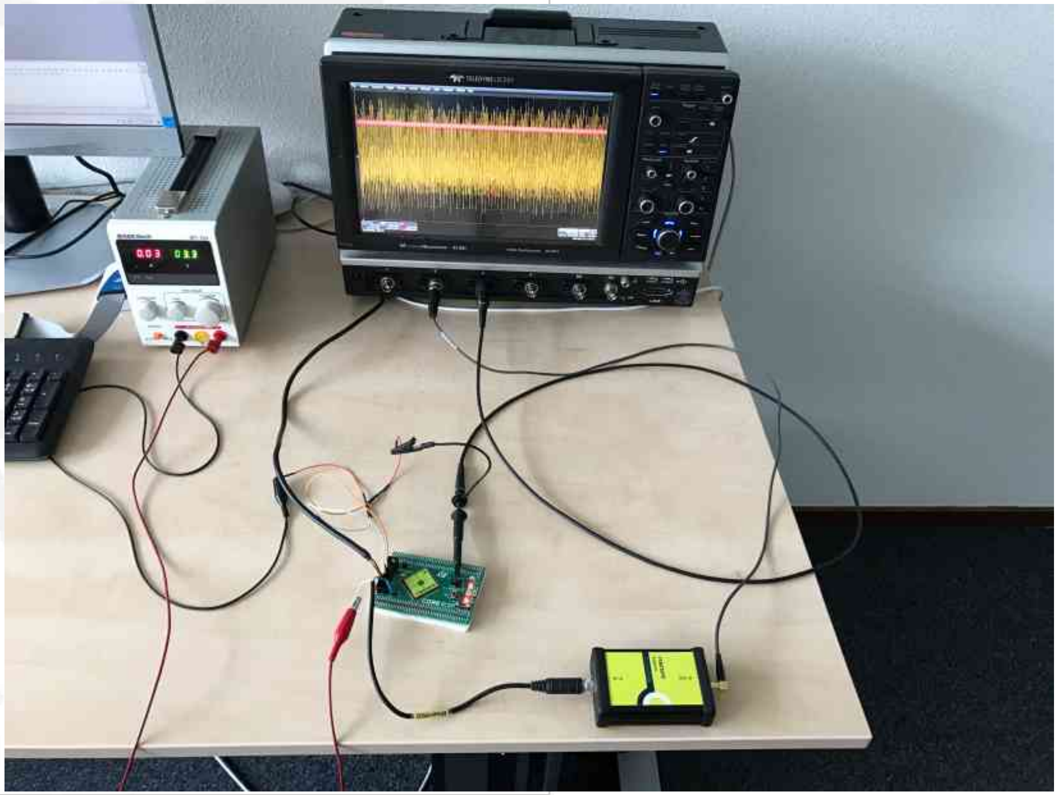
Algorithm 1 EdDSA Signature generating and verification

```
    Keypair Generation $(k, P)$: (Used once, first time private key is used.)
 1: Hash $k$ such that $H(k) = (h_0, h_1, \ldots, h_{2u-1}) = (a, b)$
 2: $a = (h_0, \ldots, h_{u-1})$, interpret as integer in little-endian notation
 3: $b = (h_u, \ldots, h_{2u-1})$
 4: Compute public key: $P = aB$.

    Signature Generation:
 5: Compute ephemeral private key $r = H(b, M)$ .
 6: Compute ephemeral public key $R = rB$.
 7: Compute $h = H(R, P, M) \mod l$.
 8: Compute: $S = (r + ha) \mod l$.
 9: Signature pair $(R, S)$

    Signature Verification:
10: Compute $h = H(R, P, M)$
11: Verify if $8SB = 8R + 8hP$ holds in $E$
```

Setup



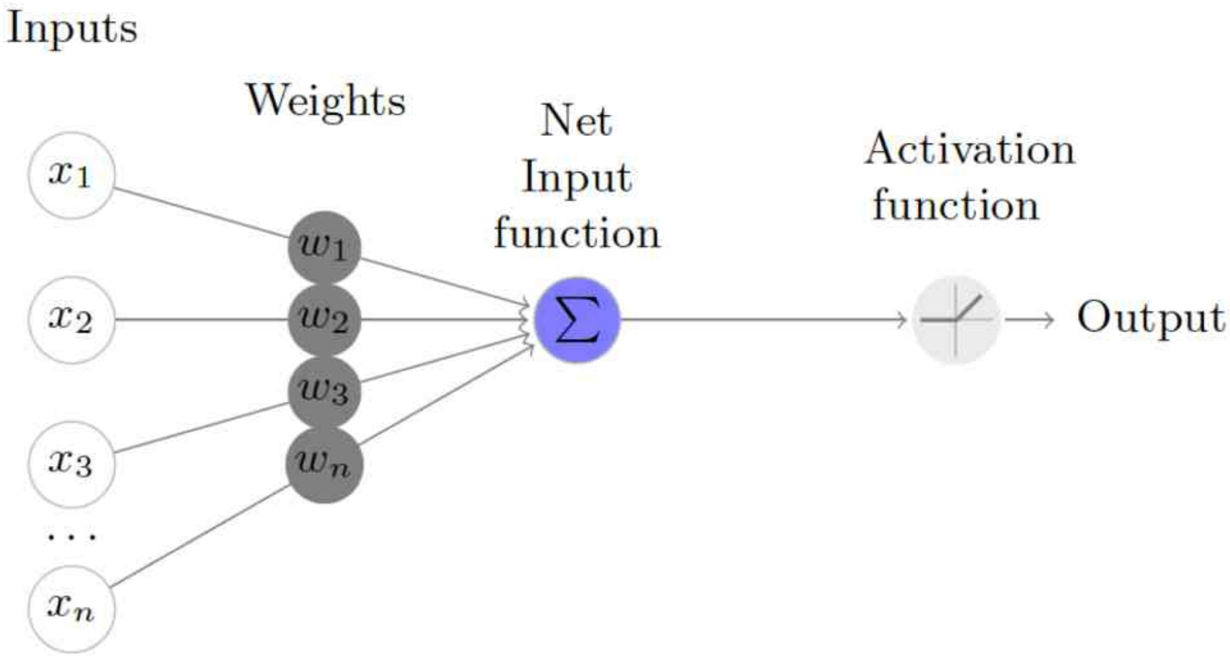
- Pinata board: ARM Cortex-M4F core running at 168 MHz
- power side-channel
- Ed25519 implement. from WolfSSL 3.10.2.
- sampling frequency of 1.025 GHz

DL part

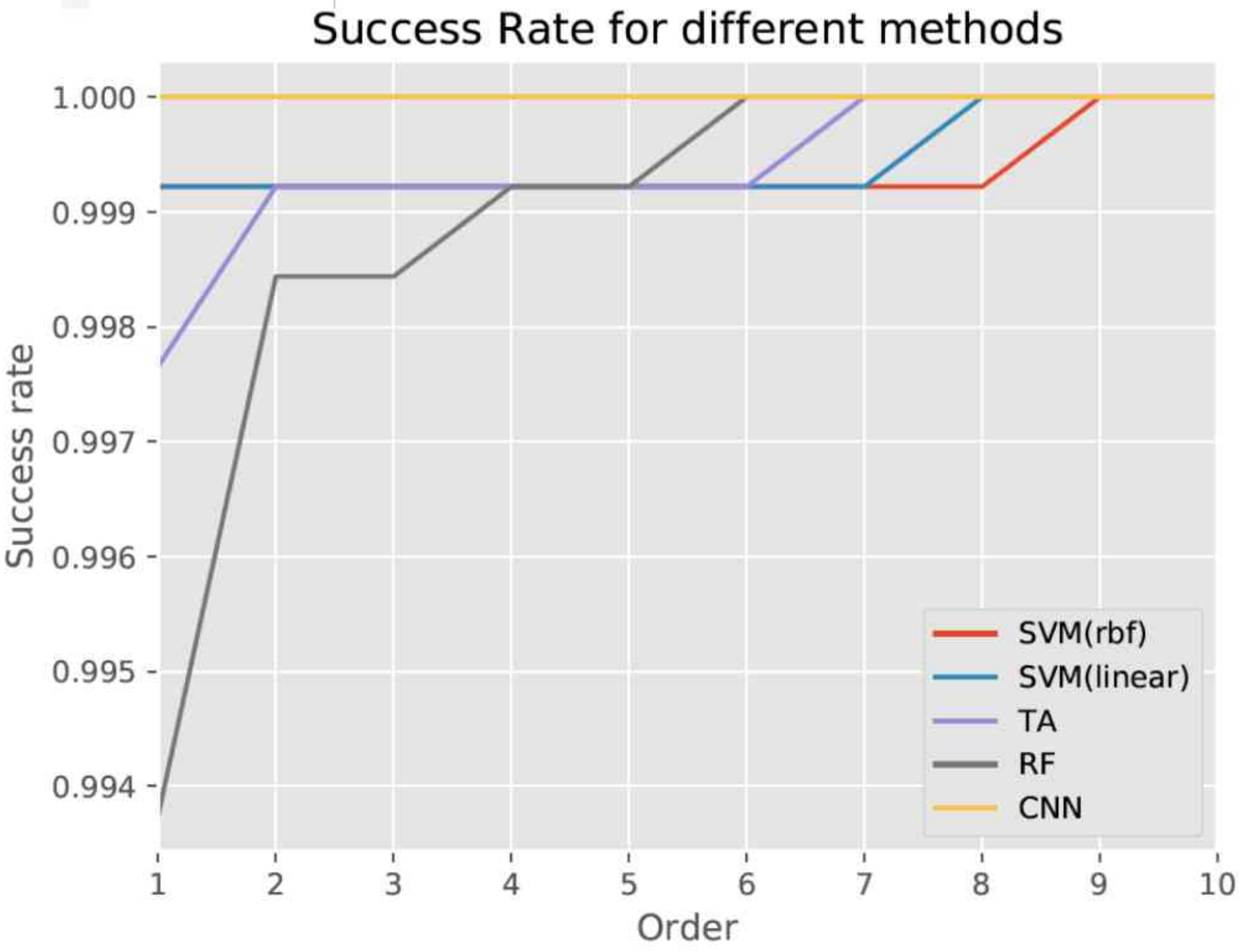
- ECC scalar multiplication is using a window-based method with radix-16
- Dataset: 6400 traces divided in 80/20 ratio for profiling/attacking groups
- 1000 samples (features) recorded for each trace
- 16 labels (value-based model)

CNN

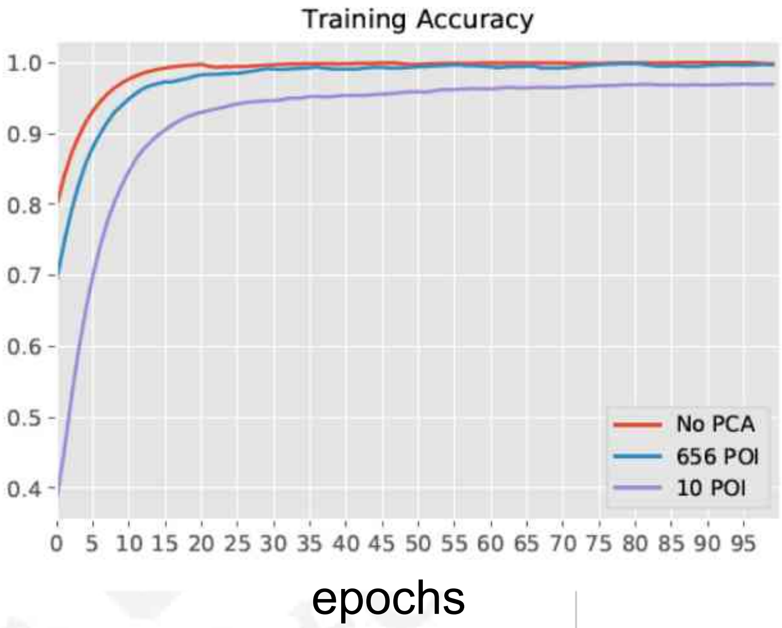
- VGG-16 architecture was used and ReLU

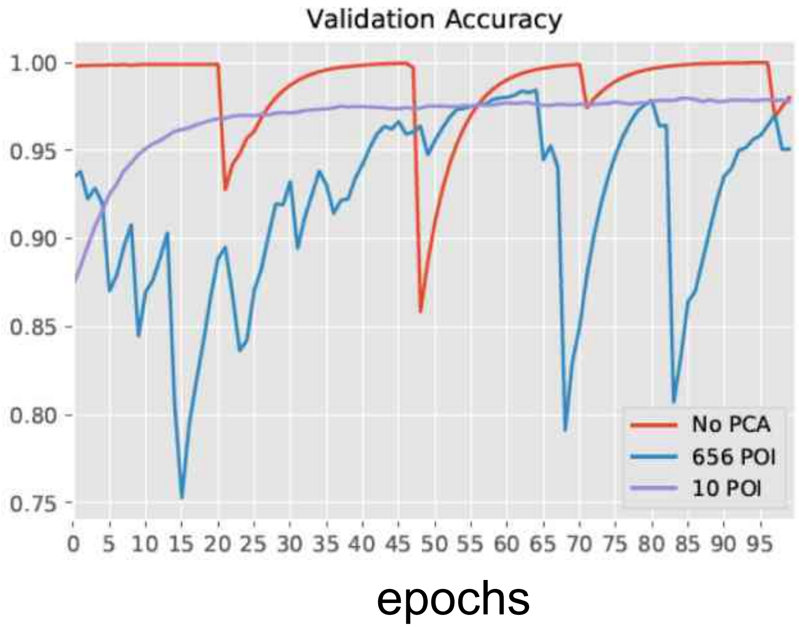


Results


Success Rate for different methods
Success rate
1.000
0.999
0.998
0.997
0.996
0.995
0.994
1
2
3
4
5
6
7
8
9
10
Order
SVM(rbf)
SVM(linear)
TA
RF
CNN

Results CNN





L. Weissbart, S. Picek and L. Batina. ***One trace is all it takes: Machine Learning-based Side-channel Attack on EdDSA***, to appear at SPACE 2019.

Results summary

- All techniques have very good performance with all accuracy scores above 95%
- CNN performs the best and (accuracy 100%)
- ML techniques outperform TA
- Applying PCA to the dataset lowers accuracy scores, except for TA
- For training CNN 30 traces per class for is enough for this dataset

Conclusions

- Physical access allows many attack paths
- Requires knowledge in many different areas
- Many crypto devices are still vulnerable to SCA
- Protocols provide a context for SCA attacks and there are many points of attack
- Attacking PK signatures requires non-standard approaches

References and further reading 1/2

- [AK96] R. Anderson and M. Kuhn. “Tamper resistance – a cautionary note”. USENIX 1996, http://www.cl.cam.ac.uk/~rja14/tamper.html
- [Koc96] P. Kocher. “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems”. CRYPTO 1996
- [RS01] T. Romer and J.-P. Seifert. “Information Leakage Attacks against Smart Card Implementations of the Elliptic Curve Digital Signature Algorithm”. E=Smart 2001
- [SW12] Skorobogatov and Woods. “Breakthrough silicon scanning discovers backdoor in military chip” http://www.cl.cam.ac.uk/~sps32/ches2012-backdoor.pdf CHES 2012.
- [EK+08] T. Eisenbarth et al. “On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoqCode Hopping Scheme”. CRYPTO 2008.
- [KK+09] M. Kasper et al. “Breaking KeeLoq in a Flash: On Extracting Keys at Lightning Speed.” AFRICACRYPT 2009.

References and further reading 2/2

- [KS+10] T. Kasper et al. "All You Can Eat or Breaking a Real-World Contactless Payment System." Financial Cryptography 2010.
- [BG+12] J. Balasch et al. "Power Analysis of Atmel CryptoMemory - Recovering Keys from Secure EEPROMs." CT-RSA 2012.
- [KJJ99] P. Kocher, J. Jaffe, B. Jun. "Differential Power Analysis". CRYPTO 1999.
- [GMO01] K. Gandolfi et al. "Electromagnetic Analysis: Concrete Results". CHES 2001.
- [BK+09] J. Brouchier et al. "Temperature Attacks". IEEE Security & Privacy 7(2): 79-82 (2009)
- [SN+13] A. Schlösser et al. "Simple photonic emission analysis of AES. J. Cryptographic Engineering 3(1): 3-15 (2013)
- [SB+16] Niels Samwel et al. "Breaking Ed25519 in WolfSSL. CT-RSA 2018: 1-20.
- [WPB19] L. Weissbart et al. "One trace is all it takes: Machine Learning-based Side-channel Attack on EdDSA", SPACE 2019, to appear.

Questions?