Deep Learning Assisted Side-Channel Attacks

Elena Dubrova
Department of Electrical Engineering
Royal Institute of Technology (KTH), Stockholm, Sweden

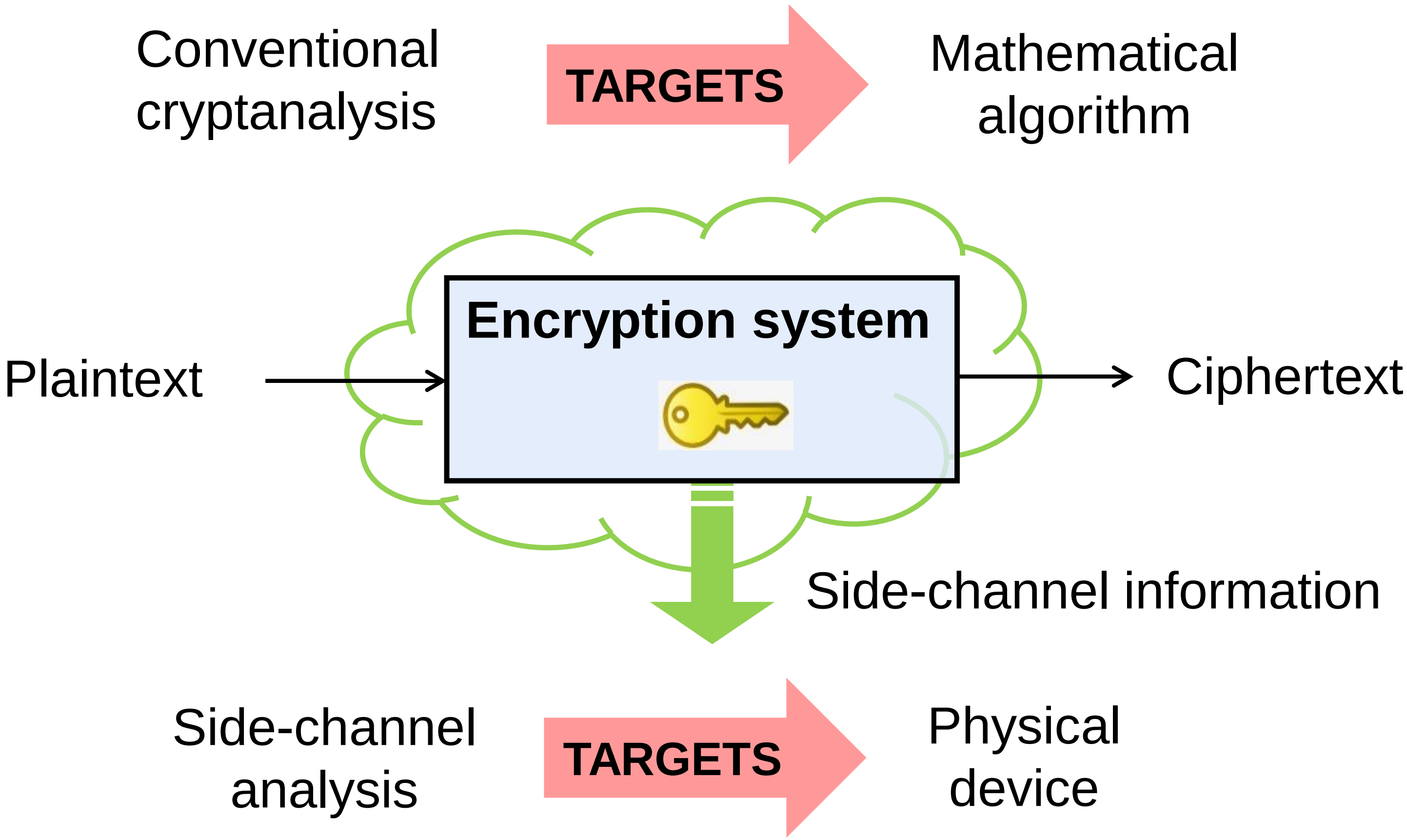
Outline

- Introduction to side-channel attacks & motivation
- Attack examples:
  - Nordic nRF52 far field EM analysis
  - USIM card power analysis
  - Masked Saber power analysis
- Summary & open probelms

Acknowledgements to:

Martin Brisfors, Sebastian Forsmark, Huanyu Wang, Ruize Wang, Kalle Ngo

What is a side-channel attack?

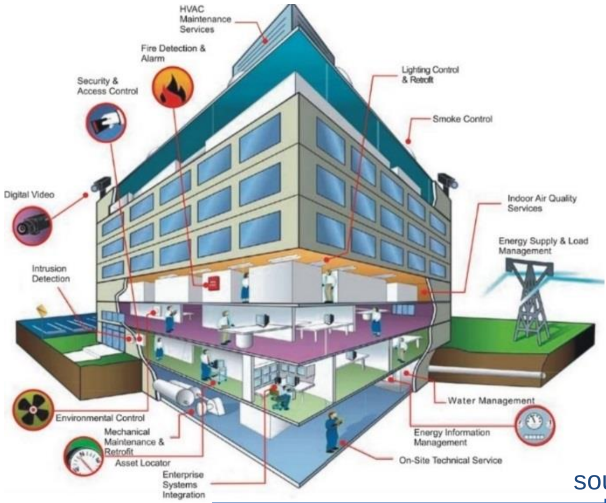


Motivation: In the near future …

- Millions not so well protected Internet-connected devices will be involved in services related to confidential data
  - Wearables
  - Connected cars
  - Smart home

source: http://www.wearables.com/5-baby-monitors-wearable-infant-tech/

source: http://www.dqindia.com/cognizant-is-betting-big-on-connected-cars/



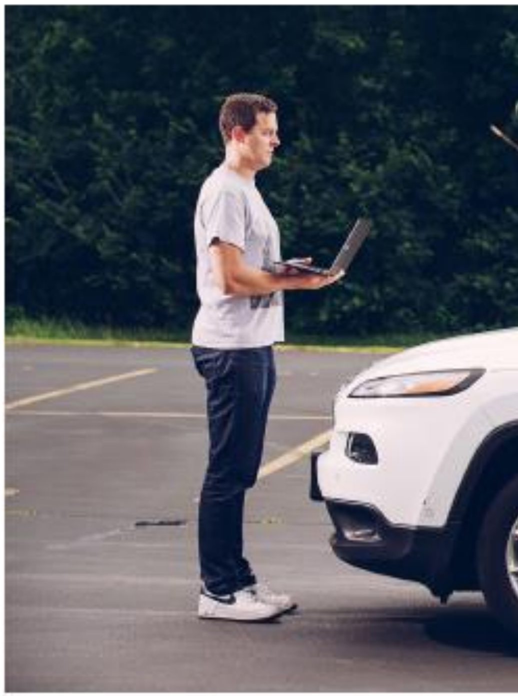
source: https://blog.econocom.com/en/blog/smartbuilding-and-bms-a-little-glossary/

ANDY GREENBERG SECURITY 03.17.16 6:59 PM

THE FBI WARNS THAT CAR HACKING IS A REAL RISK

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY —WITH ME IN IT



ANDY GREENBERG SECURITY 08.11.15 7:00 AM

HACKERS CUT A CORVETTE'S BRAKES VIA A COMMON CAR GADGET

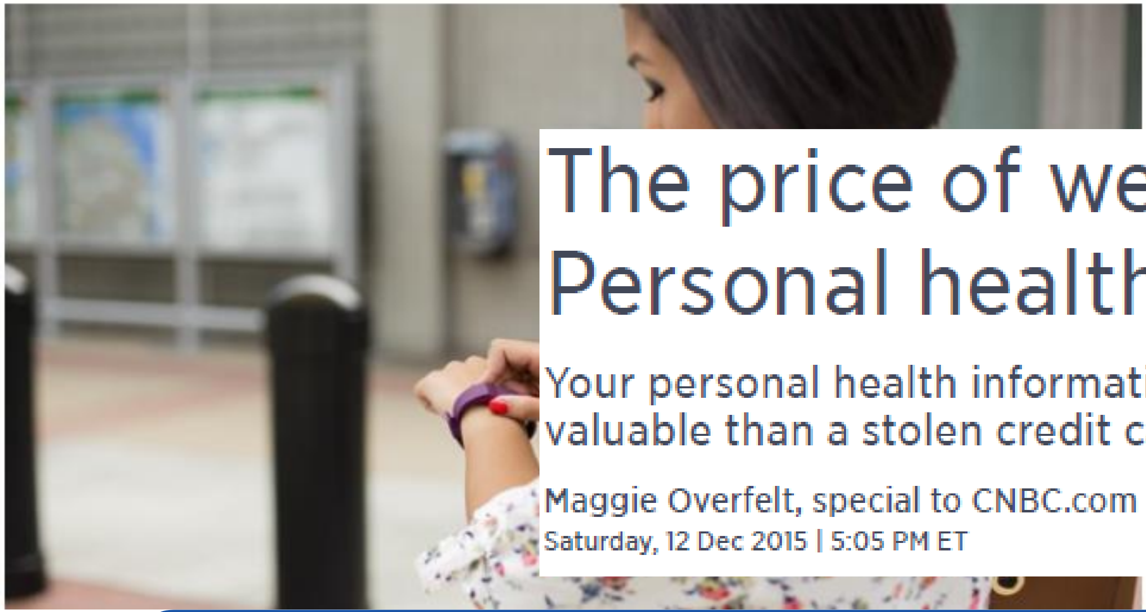
SECURITY

Hacker looks to sell 9.3 million alleged patient healthcare records on the dark web

By **James Rogers**
Published June 28, 2016

What does Fitbit hacking mean for wearables and IoT?

BY STEPHEN COBB POSTED 12 JAN 2016 - 02:49PM



The price of wearable craze: Personal health data hacks

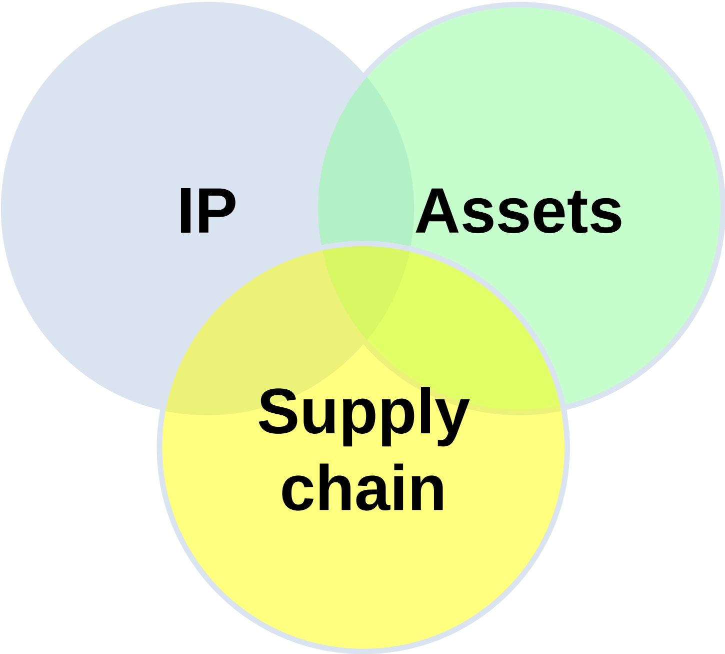
Your personal health information is about 10 times more valuable than a stolen credit card number on the black market.

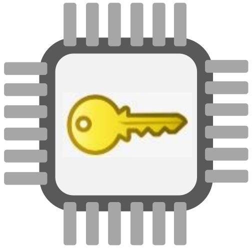
Maggie Overfelt, special to CNBC.com
Saturday, 12 Dec 2015 | 5:05 PM ET

What needs protection?

Saab@MarcusWandt

Proprietary designs
Proprietary algorithms
Proprietary bitstreams

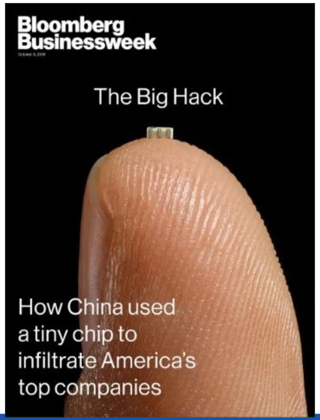




On-device data
On-device keys
TRNGs

source: http://www.publicintegrity.org/ 2011/11/07/ 7323/counte

Preventing Hardware Trojans, counterfeit, overproduction

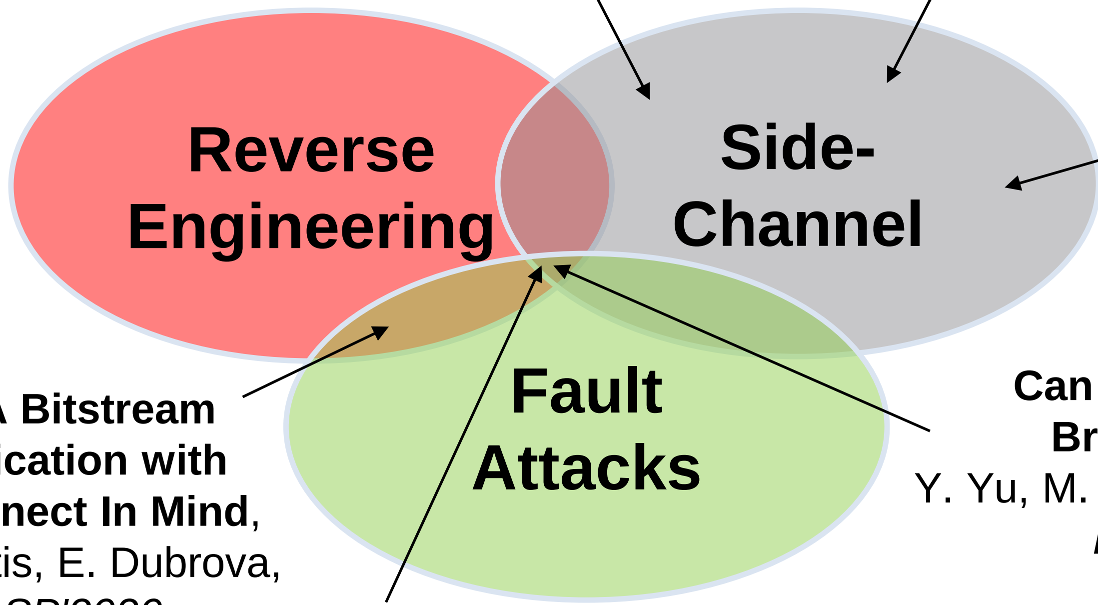


Attacks vectors

A Side-Channel Attack on a Masked IND-CCA Secure Saber KEM*,*
K. Ngo, E. Dubrova*,* Q. Guo, T. Johansson*,*
https://eprint.iacr.org/2021/079.pdf

How Deep Learning Helps Compromising USIM, M. Brisfors, S. Forsmark, E. Dubrova, CARDIS'2020

Far Field Side-Channel Attack on AES Using Deep Learning,
R. Wang, H. Wang,
E. Dubrova, *ASHES'2020*



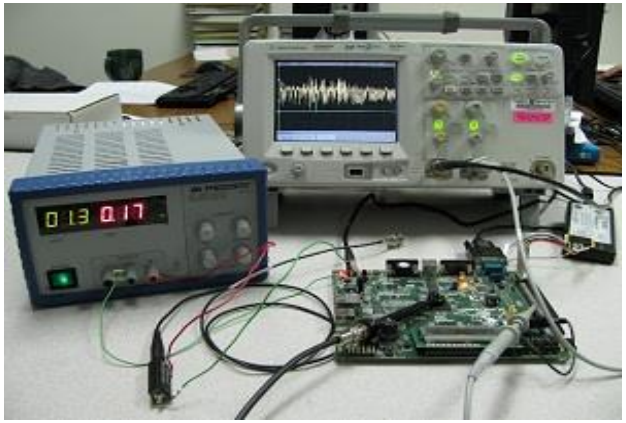
FPGA Bitstream Modification with Interconnect In Mind,
M. Moraitis, E. Dubrova,
HASP'2020

Can Deep Learning Break a TRNG?
Y. Yu, M. Moraitis, E. Dubrova,
ISCAS'2021

Why Deep Learning Makes it Difficult to Keep Secrets in FPGA-as-a-Service Setting,
Y. Yu, M. Moraitis, E. Dubrova, *DYNAMIC'2020*

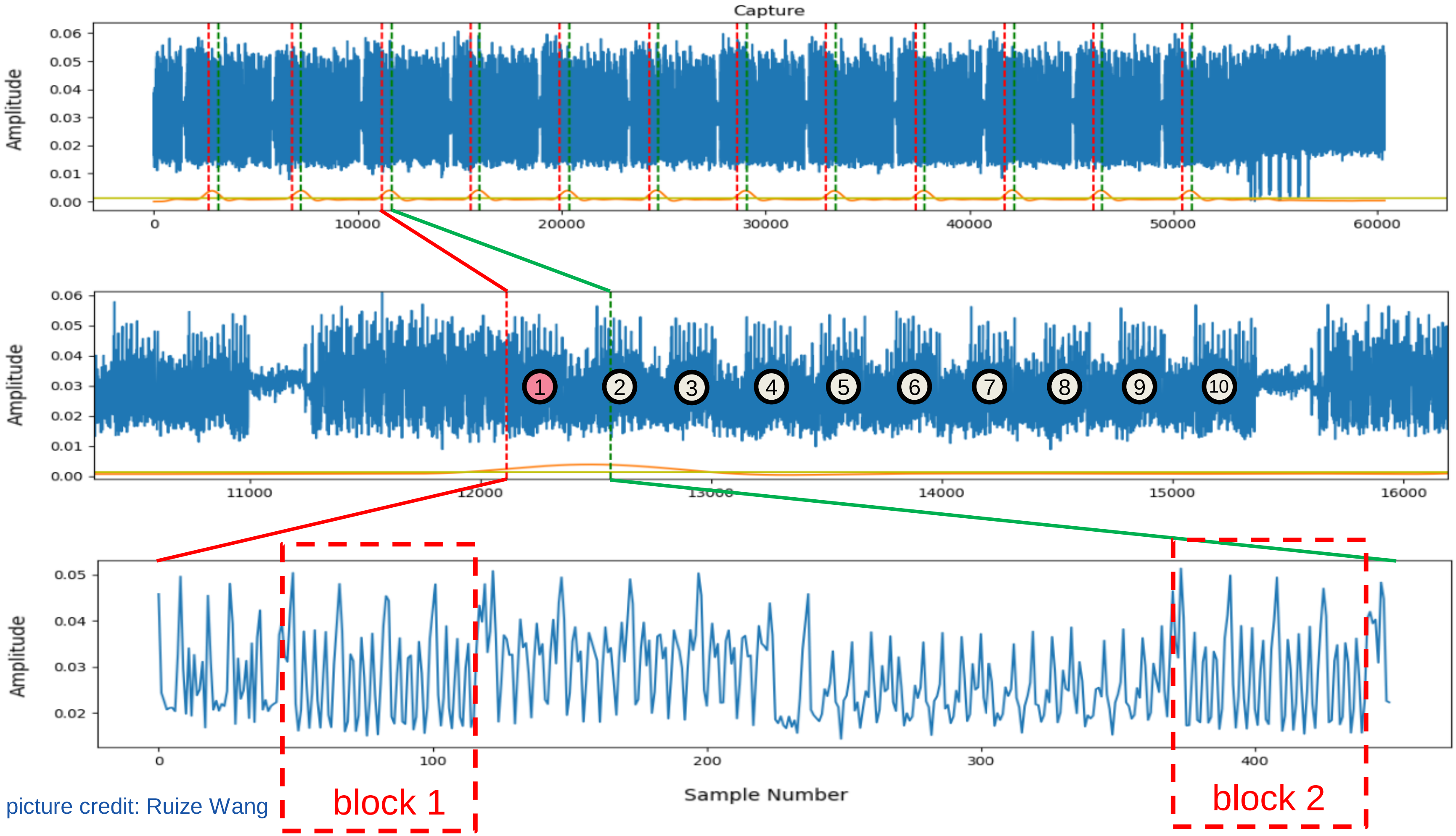
How side-channel attacks work

- Algorithms are implemented in CPUs, FPGAs, ASICs, …
- Different operations may consume different amount of power/time
- The same operation executed on different data may consume different amount of power/time
- It may be possible to recognize which operations and data are processed from power/EM traces/timing
  - if the implementation is not protected



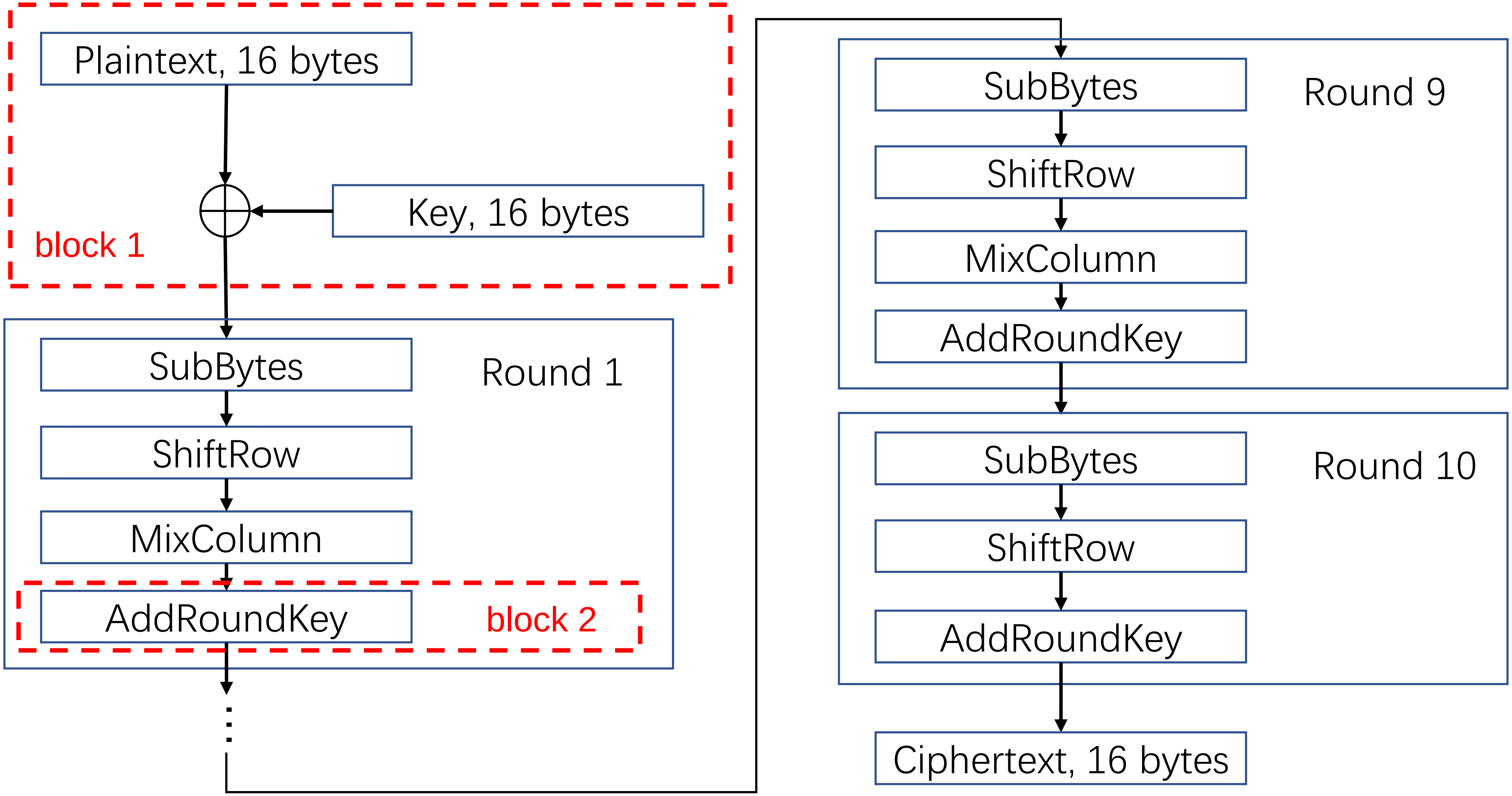
source: hackaday.com

Analsyis of AES-128 encryption algorithm



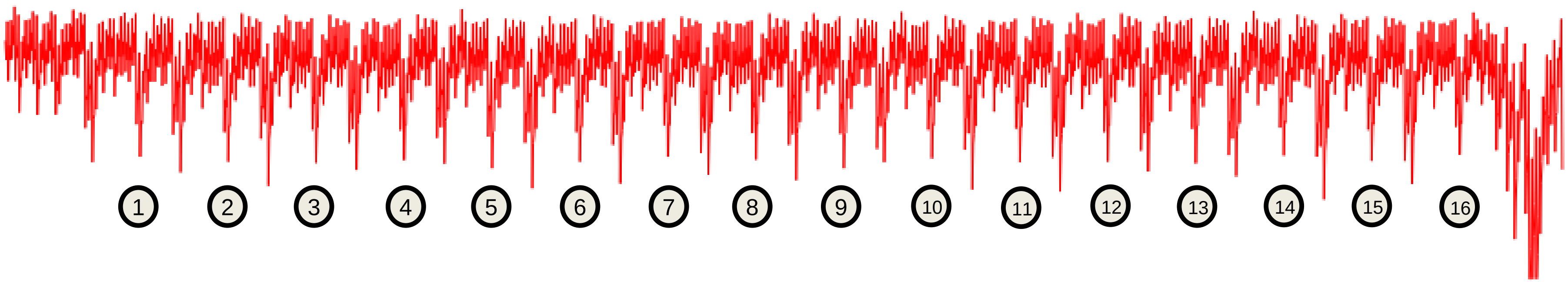
picture credit: Ruize Wang

AES-128



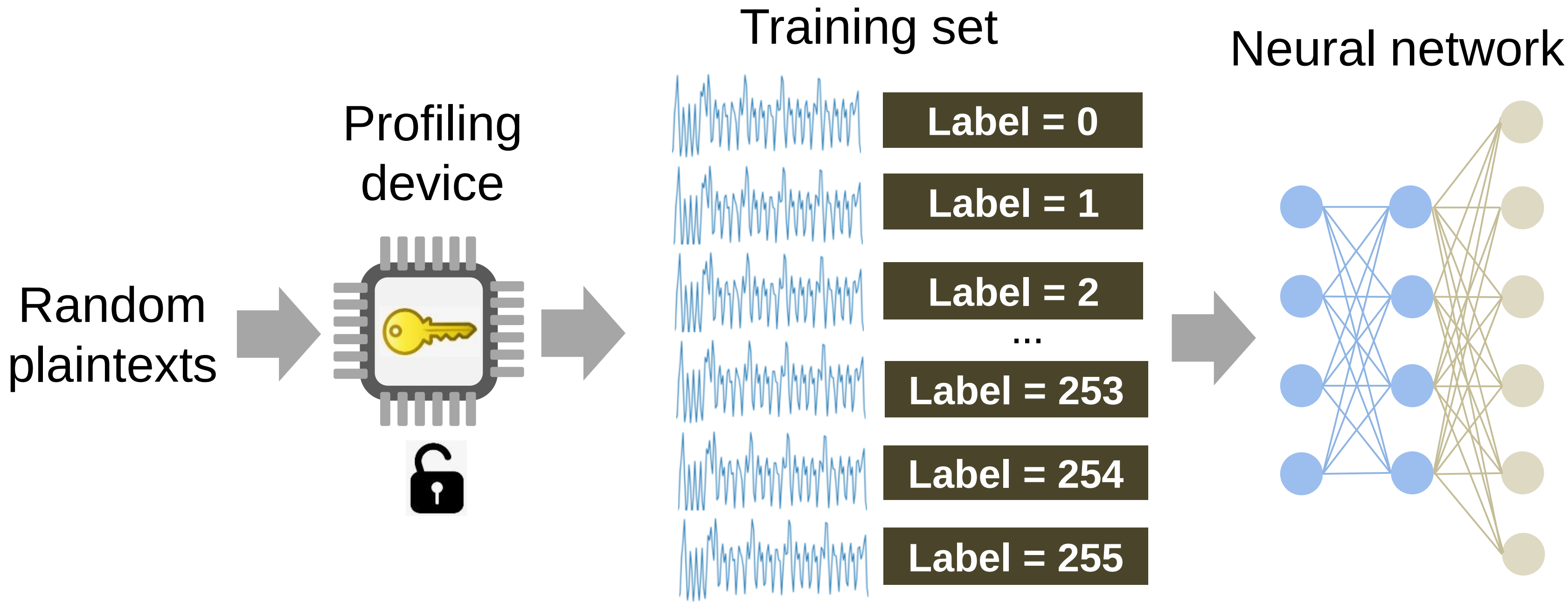
picture credit: Ruize Wang

Power trace representing 16 executions of SubBytes on 8-bit MCU (ATXmega128D4)



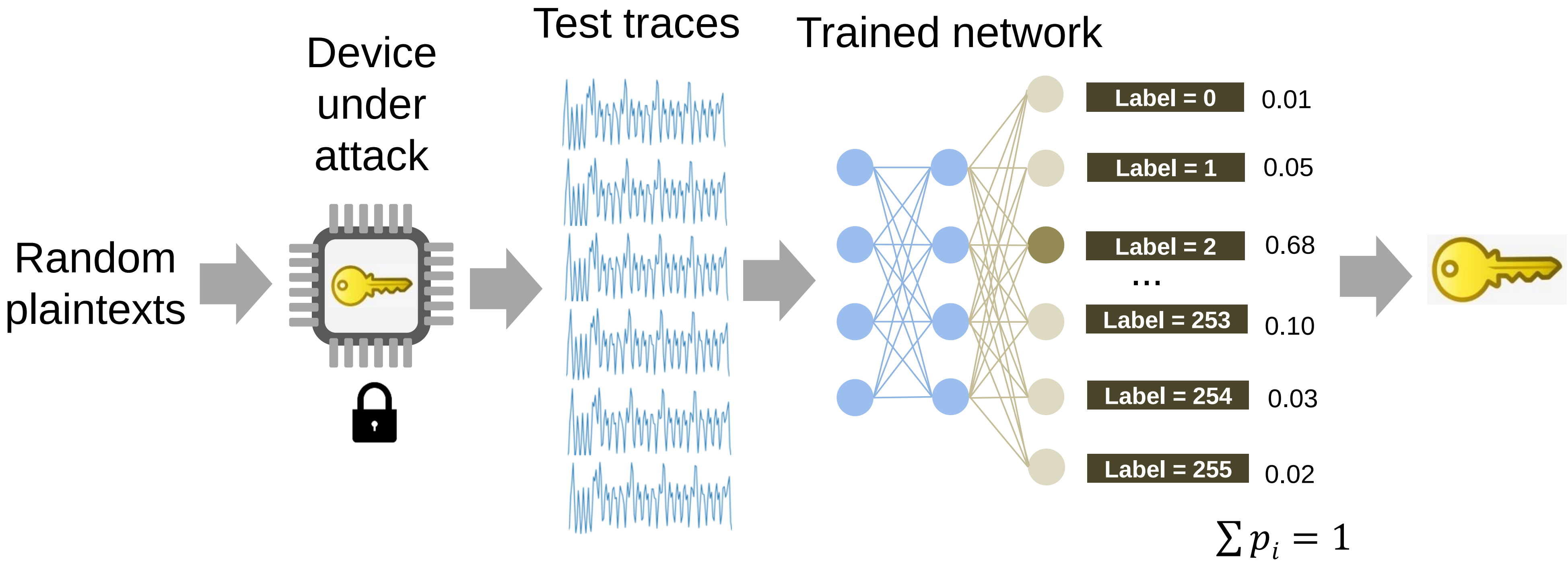
How deep learning is used in side-channel analysis

Profiling stage: Train a neural network using traces from profiling devices



How deep learning is used in side-channel analysis, cont.

Attack stage: Use the trained network to classify traces from the device under attack



Example 1: Nordic nRF52 SoC EM analysis

photo credit: Katerina Gurova

AES encryption key can be extracted from < 350 EM traces captured at 15 m distance to device

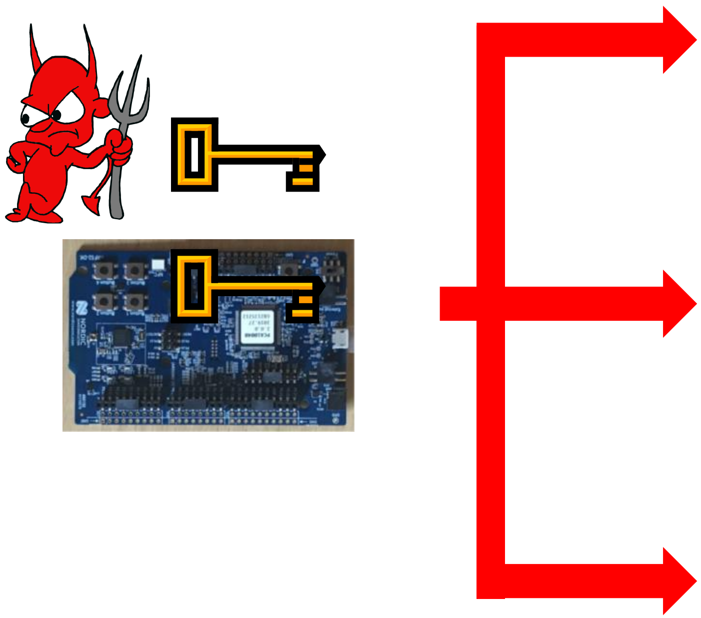
Far Field Side-Channel Attack on AES Using Deep Learning, R. Wang, H. Wang, E. Dubrova, ASHES'2020, Nov. 13, 2020

Advacned Far Field EM Side-Channel Attack on AES, R. Wang, H. Wang, E. Dubrova, CPSS'2021, June 7, 2020

Nordic Semiconductor’s nRF52832 SoC

- Powerful single-chip solutions for ultra low power wireless applications
- Dominates the IoT platforms market
  - short range communications (Bluetooth Low Energy, Zigbee,…)
- Personal area networks, interactive entertainment devices, remote control toys, computer peripherals, ...
- Contains:
  - 32-bit ARM Cortex-M4 processor
  - Multi-protocol 2.4GHz radio

Consequences of encryption key compromise

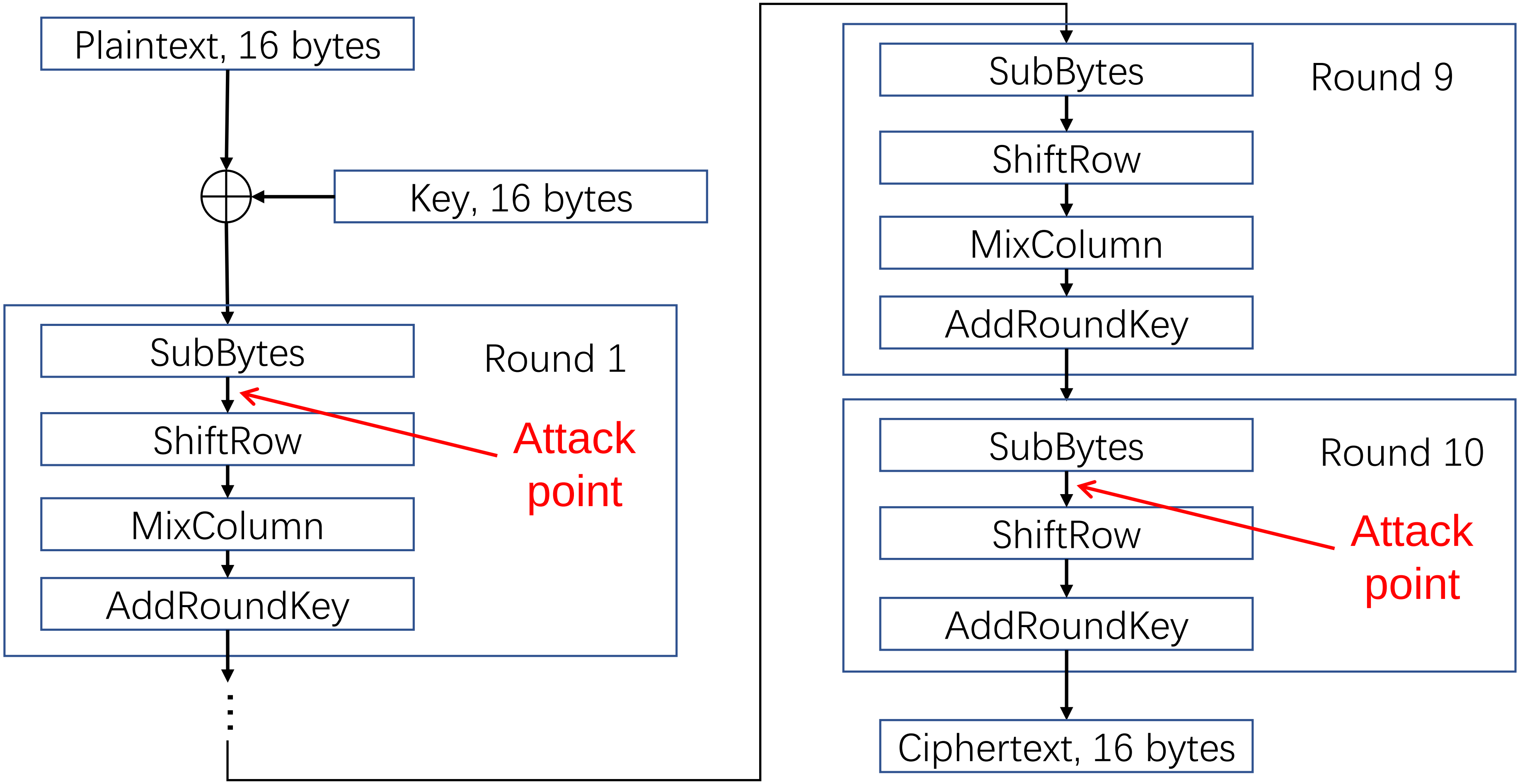


Eavesdrop & decrypt messages

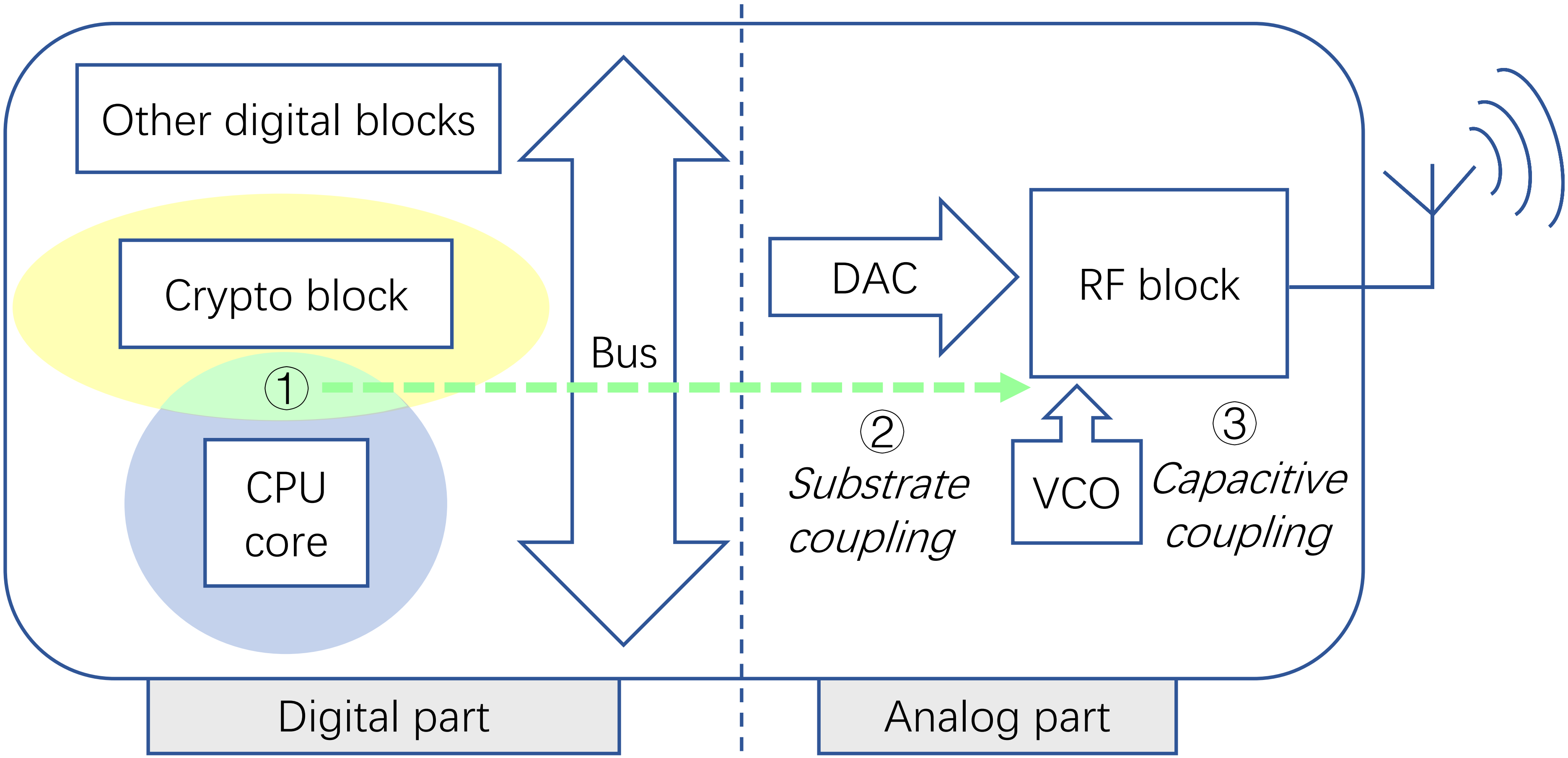
Impersonate the compromised device & send fake messages to the other party (if the message is not authenticated)

Impersonate the other party & send fake messages to the device (if the message is not authenticated)

AES-128 algorithm



Sources of EM emissions in mixed-signal circuits



Measurment setup

Grid Parabolic Antenna TL-ANT2424B

Ettus Research USRP N210 SDR

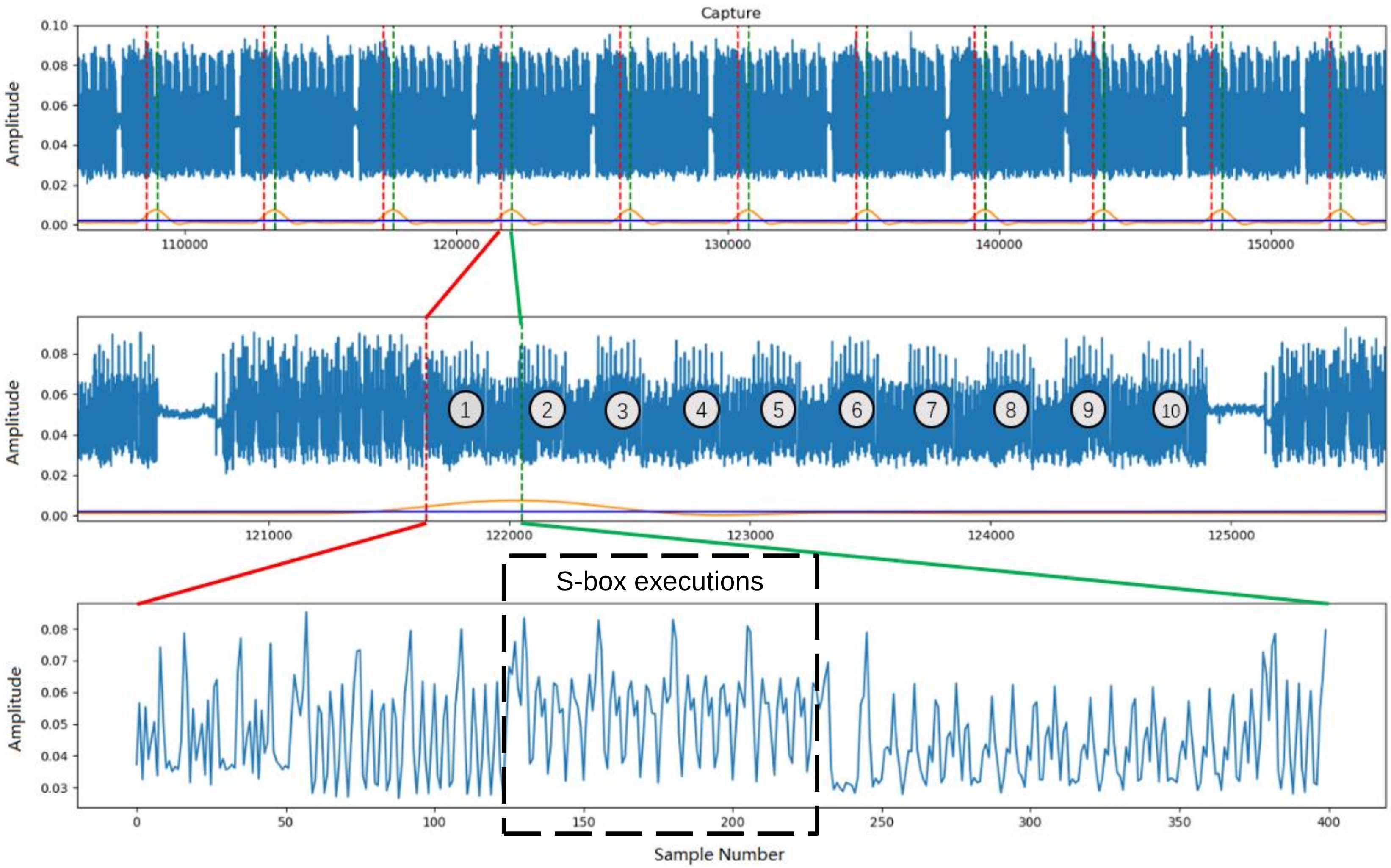
nRF52DK board

Center receiving frequency = $f_{\mathrm{BT}} + 2f_{clock}$ = 2.528 GHz

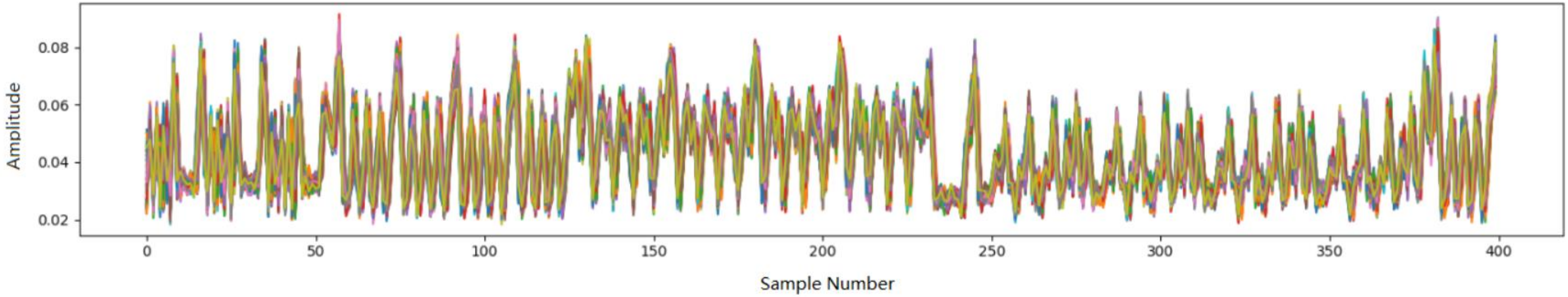
f_{BT} = 2.4 GHz (Bluetooth band frequency)

f_{clock} = 64 MHz (ARM Cortex M4 CPU clock)

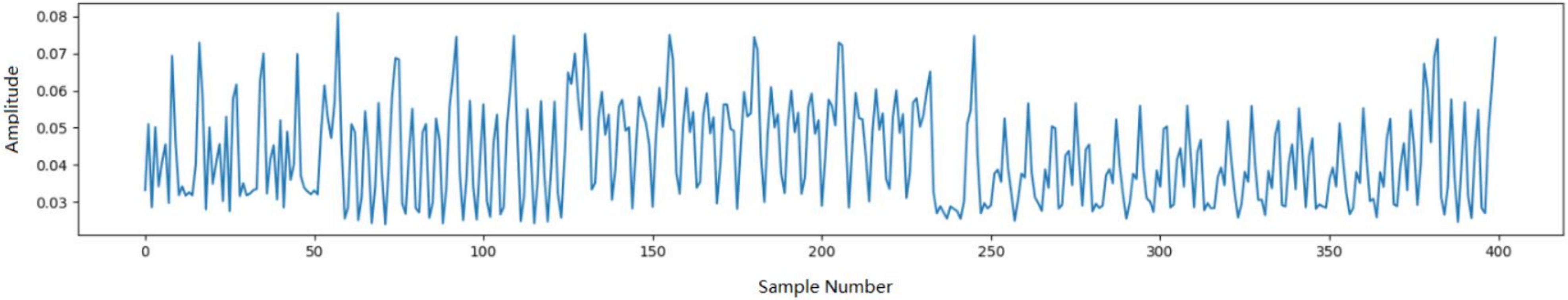
Locating the attack point in trace



Pre-processing: averaging & min-max scaling



(a) 100 single alligned traces

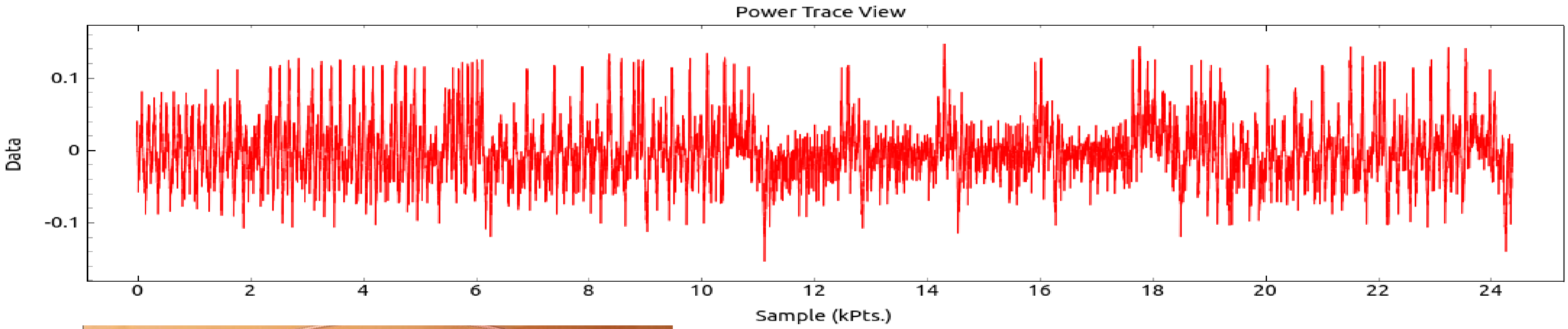


(b) One averaged traces

Experimental results & comparison with previous work

	Analysis method	Distance to device	Environment	Repetition of single trace	Key enumeration	Number of traces
CCS’2018	Template attack	10m	Anechoic chamber	500	No	1428
		1m	Office			52589
CHES’2020	Template attack	15m	Office	1000	2^{23}	5000
Our contribution	Deep learning	15m	Office	100	No	13
				10		59
				1		341

Example 2: USIM card power analysis



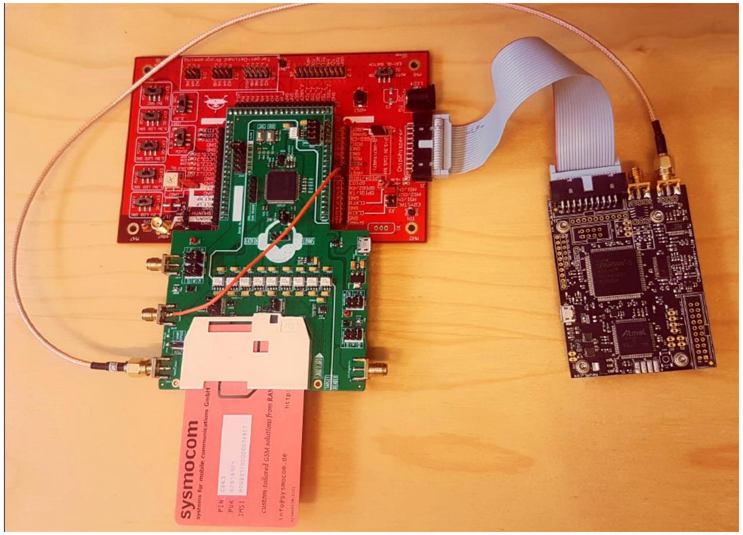
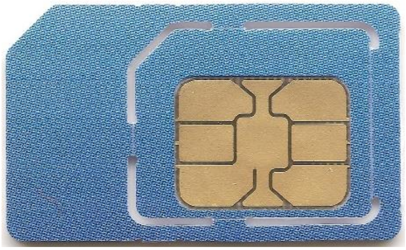


photo credit: Martin Brisfors

USIM's long-term key can be extracted from the USIM using 4 power traces on average (max 20)

How Deep Learning Helps Compromising USIM, M. Brisfors, S. Forsmark, E. Dubrova, CARDIS'2020, Nov. 18-19, 2020

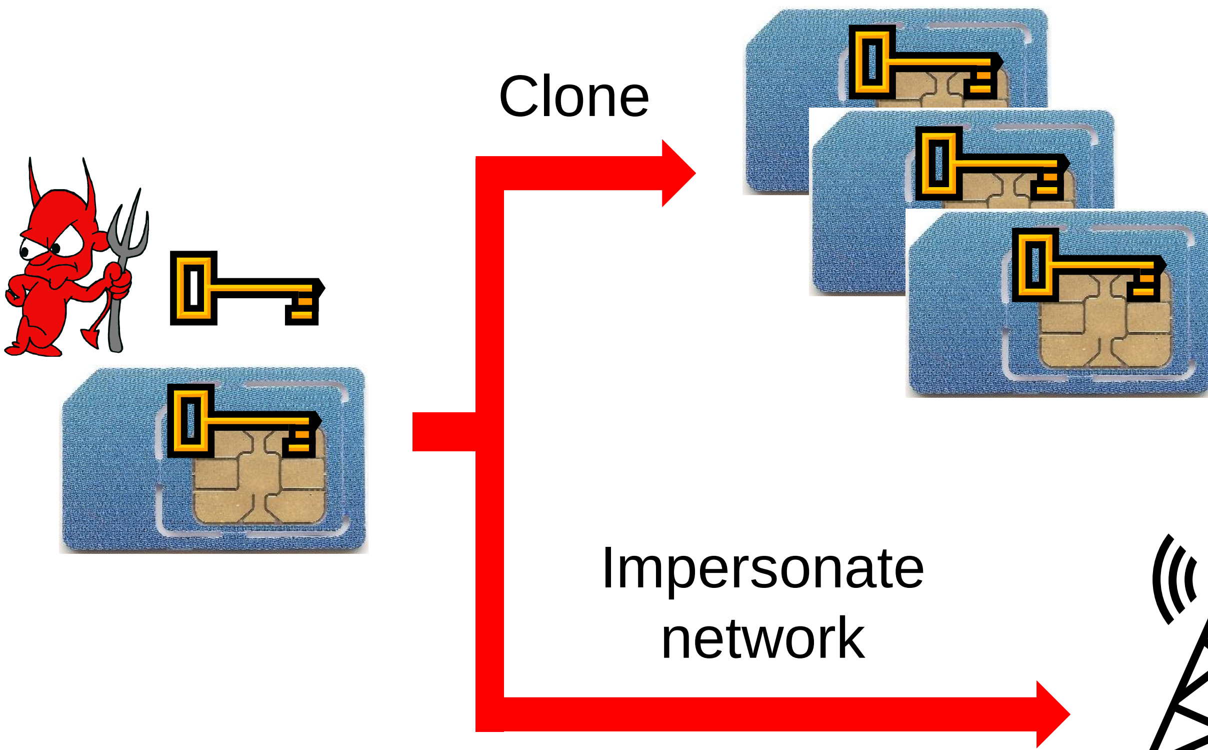
Universal Subscriber Identity Module (USIM)



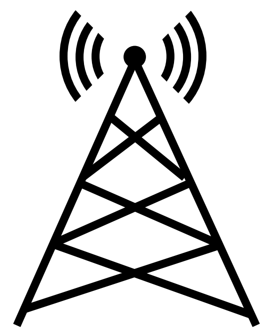
Source:Telefónica O_2 Europe

- USIM is a type of smart card
- Contains:
  - Secret key K pre-shared with home subscriber server
  - International Mobile Subscriber Identity (IMSI)
  - Operator Variant Algorithm Configuration Field (OP)
  - …
- All cryptographic operations involving K are carried out within the USIM

3G/4G/5G security relies on the USIM's key

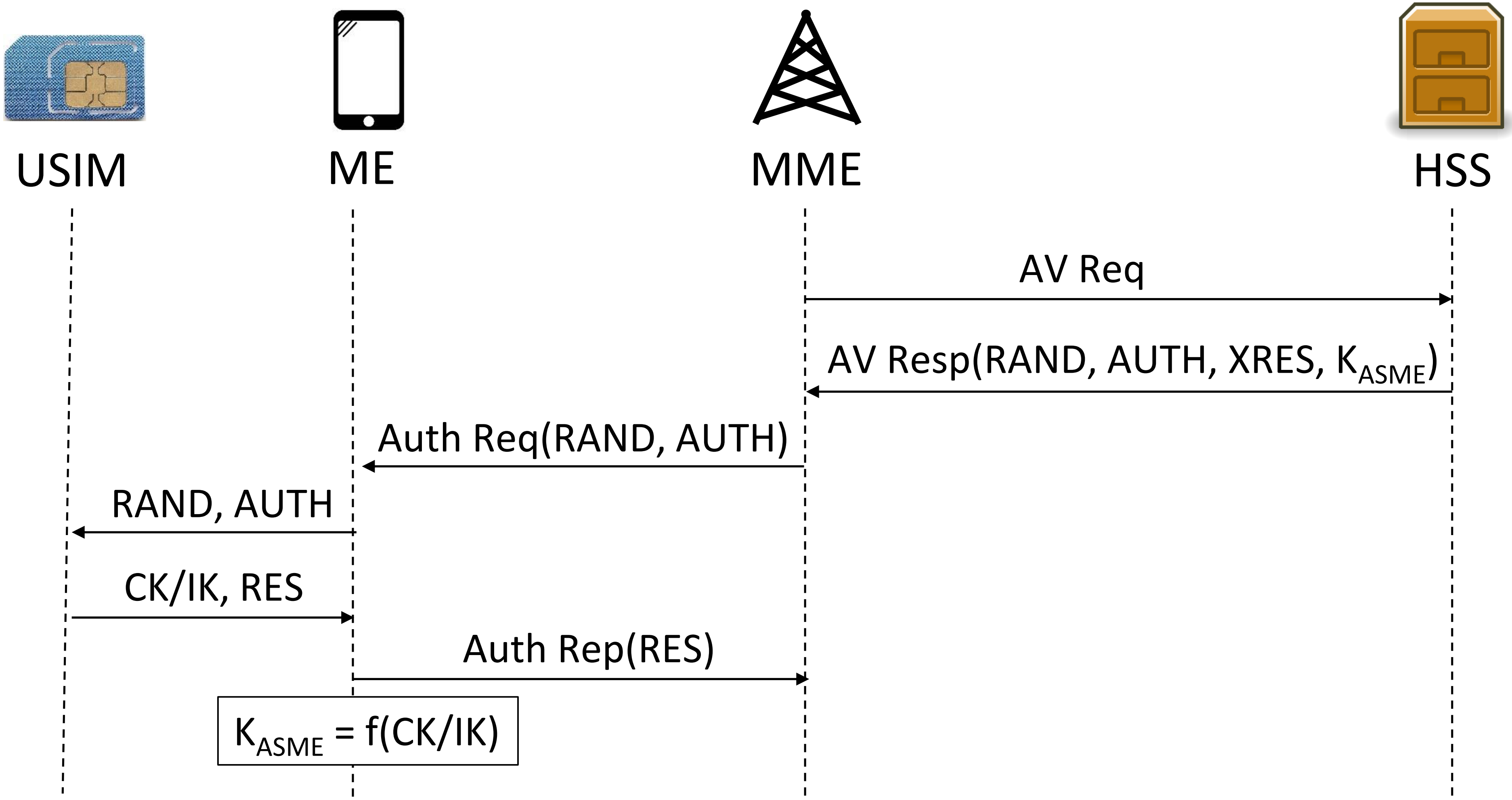


- Receive subscriber's texts and calls
- Impersonate subscriber

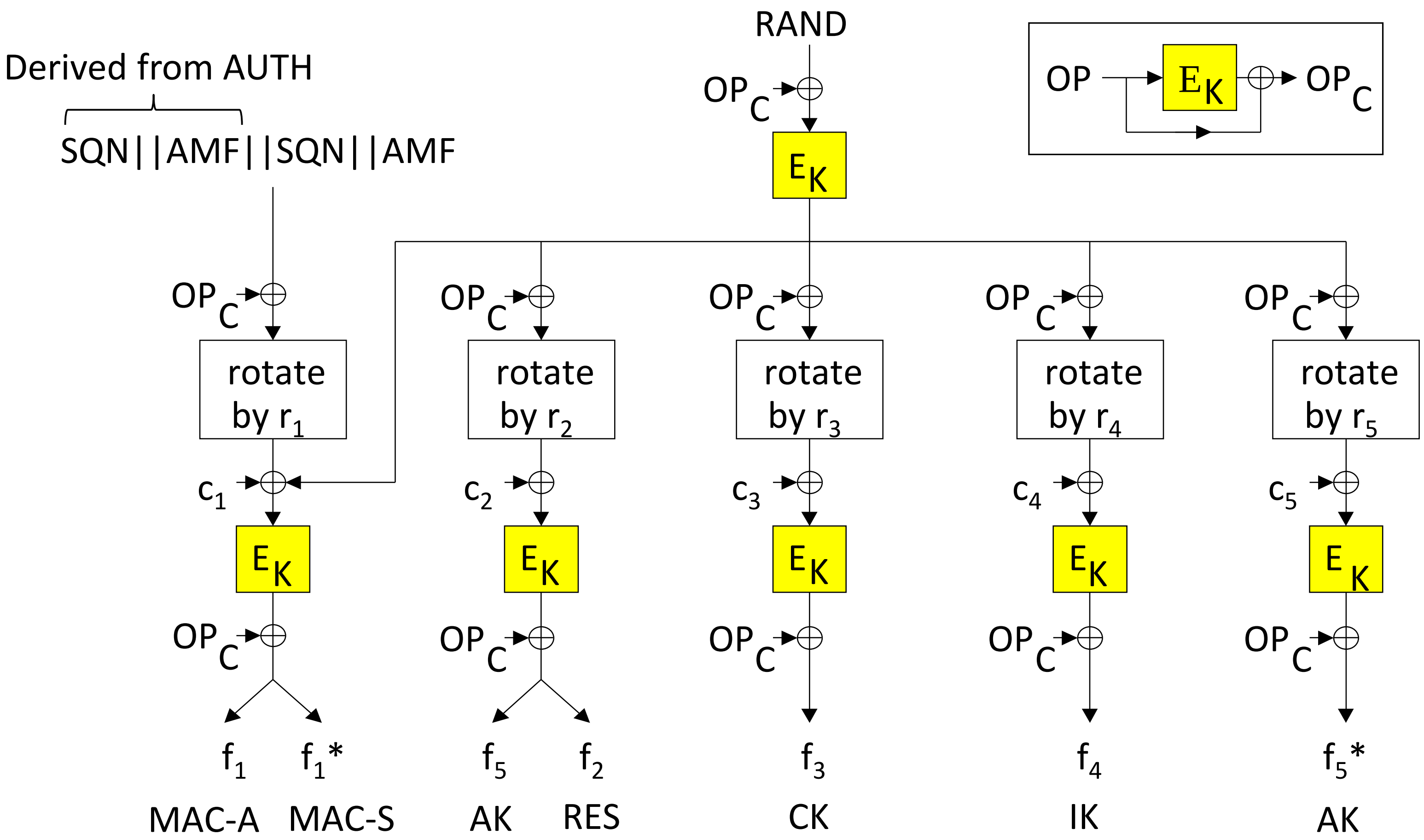


- Extract information from subscriber

Authentication and Key Agreement (AKA) in 4G



MILENAGE algorithm



Measurment setup

CW308 UFO

ChipWisperer

LEIA

USIM

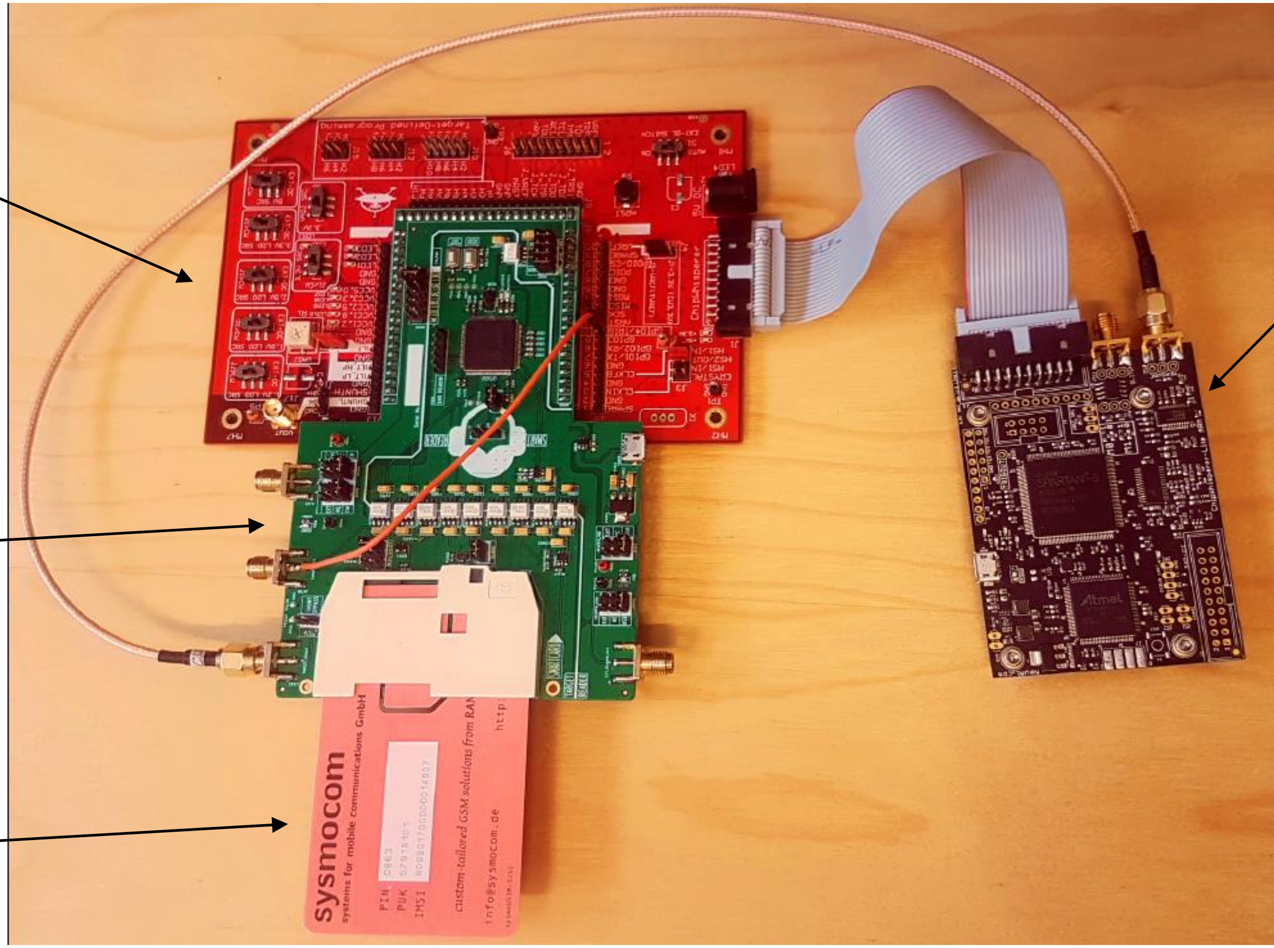
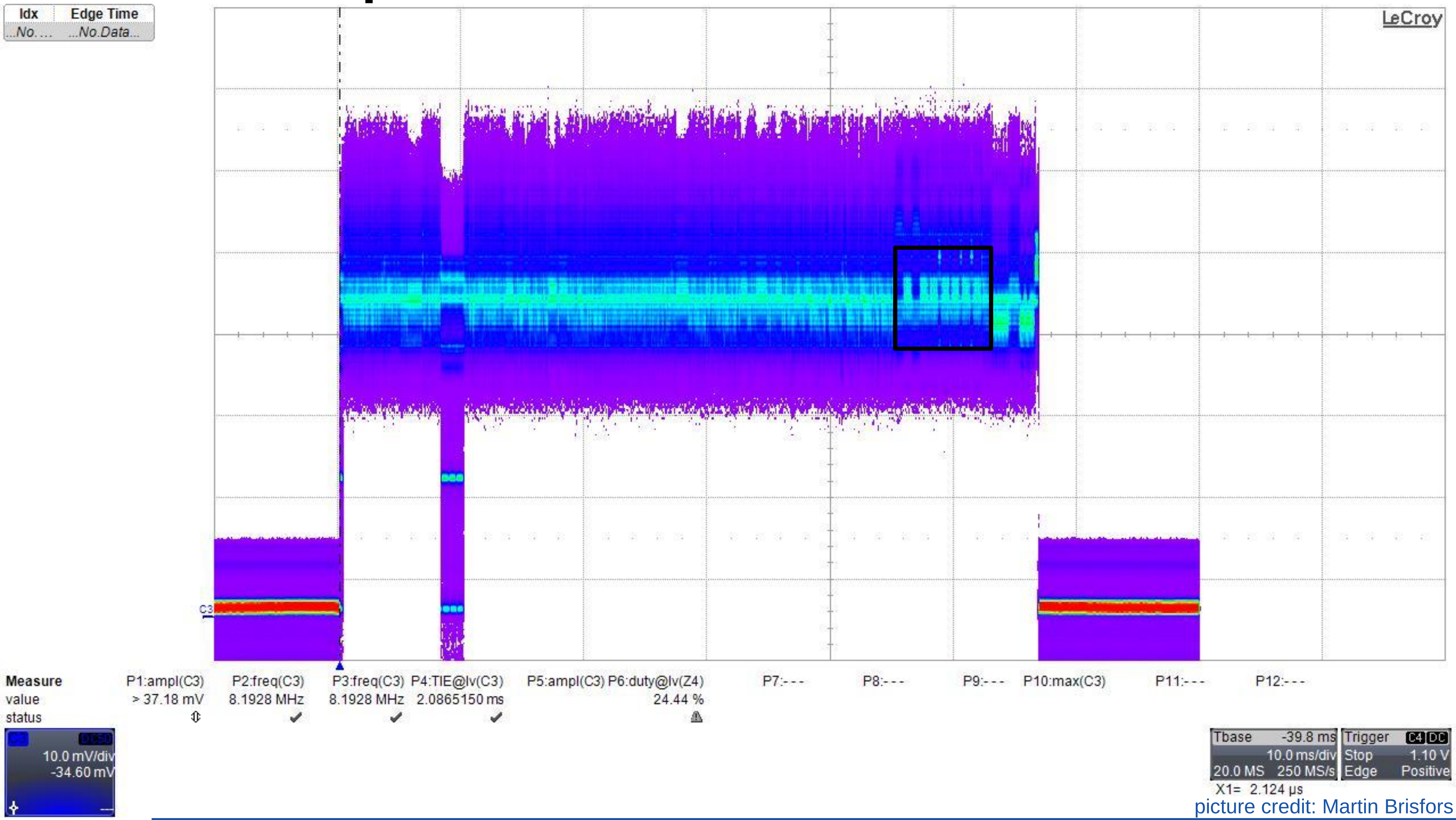


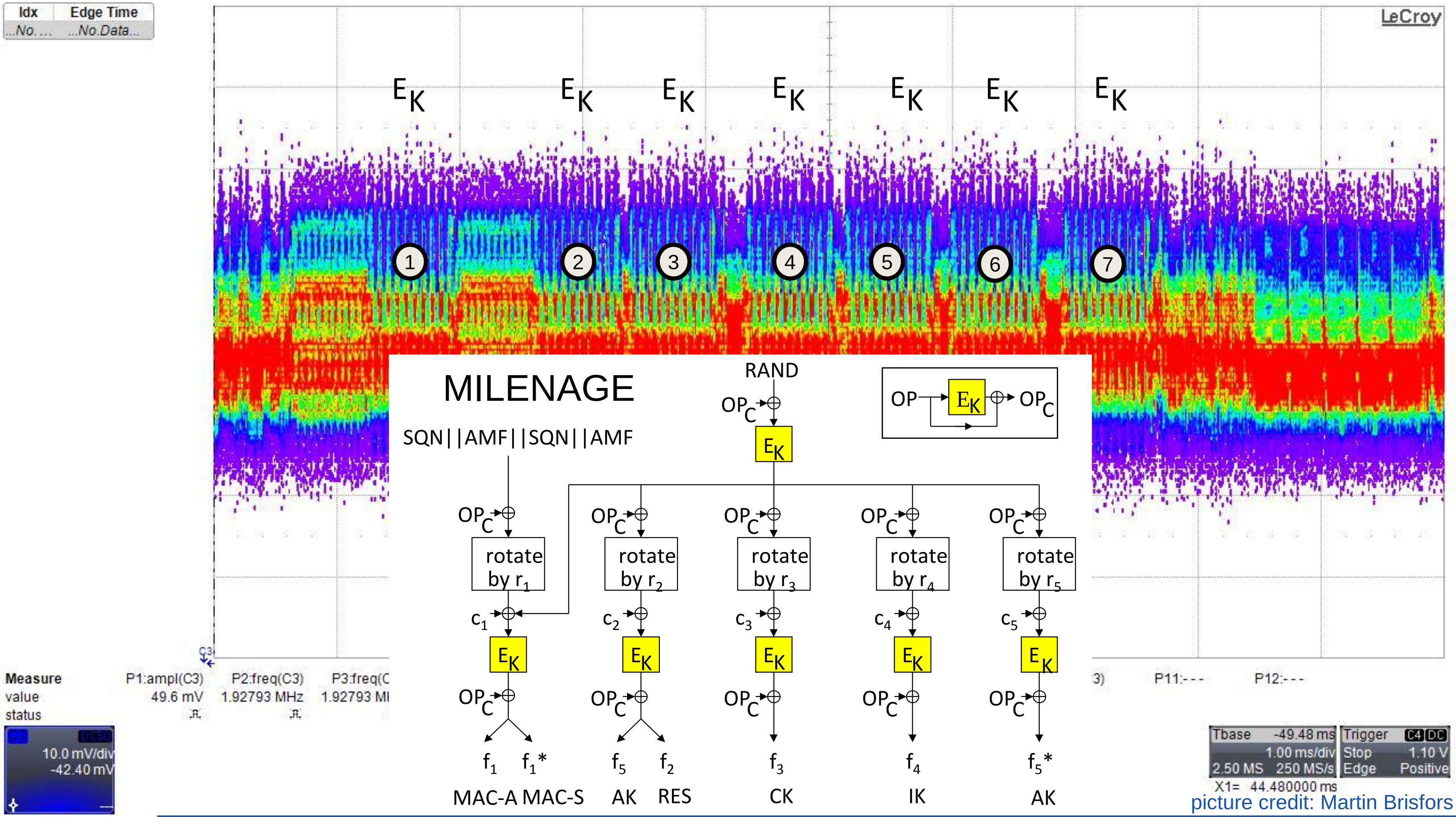
photo credit: Martin Brisfors

USIM power trace for one MILENAGE call



picture credit: Martin Brisfors

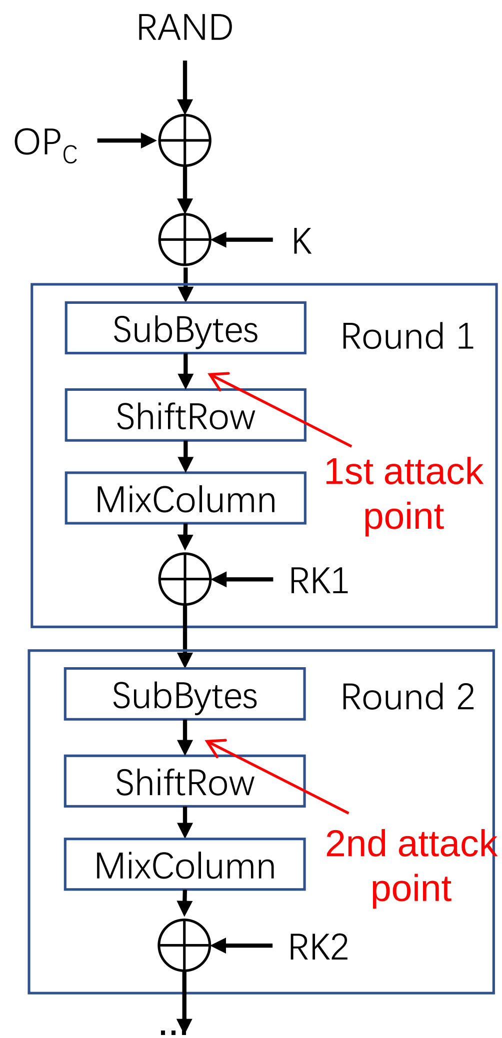
Zoomed interval of MILENAGE execution



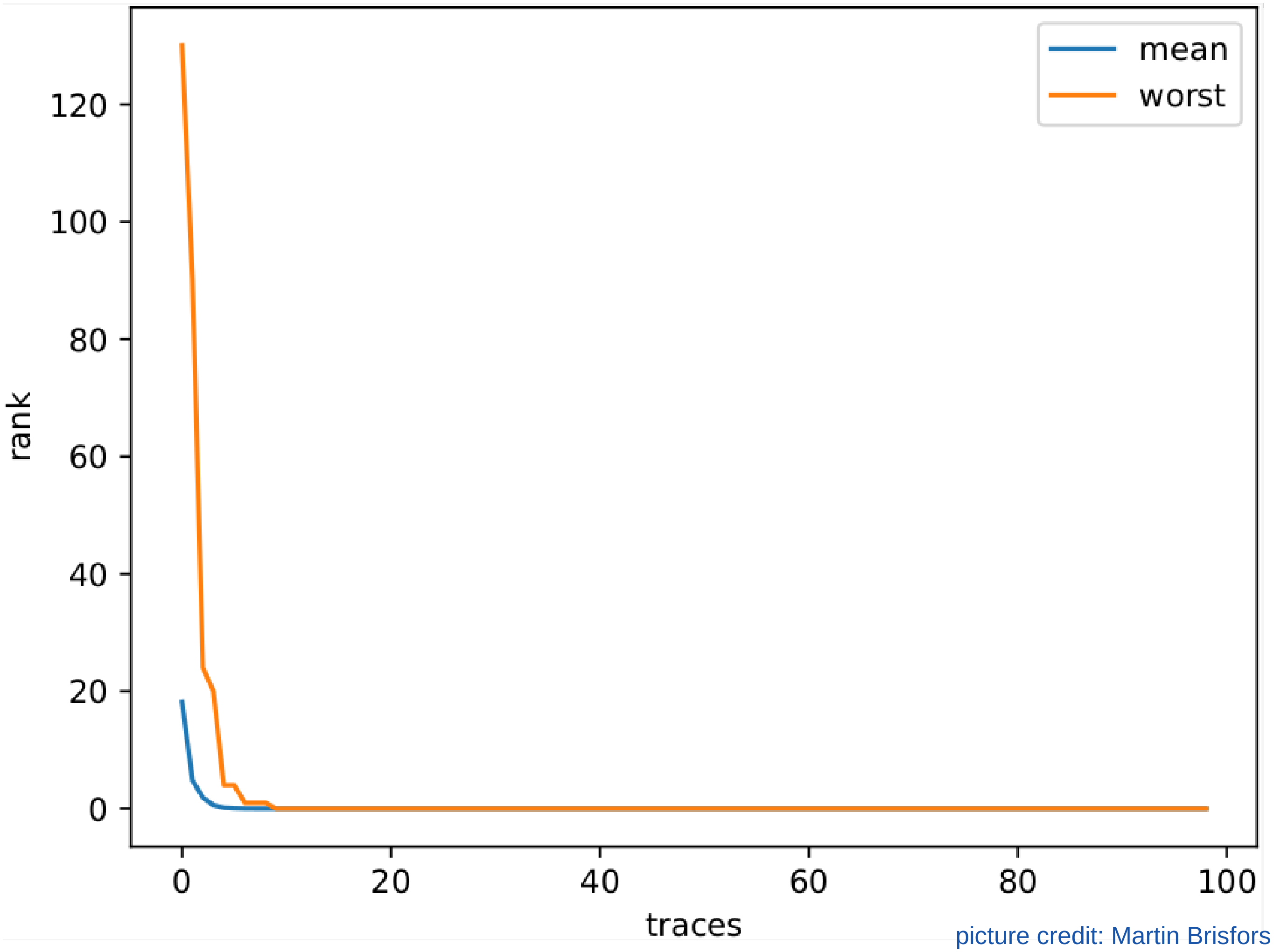
picture credit: Martin Brisfors

Attack steps

- In MILENAGE, RAND ⊕ OP_C is first computed and then the result is encrypted
- If E_k is AES-128, the key K can be recovered in two steps:
  1. Recover $OP_C \oplus K$ using S-box output in the 1st round as the attack point
  2. Recover the 1st round key, RK1, using the S-box output in the 2nd round as the attack point
  3. Compute K from RK1
  4. $OP_C = (OP_C \oplus K) \oplus K$

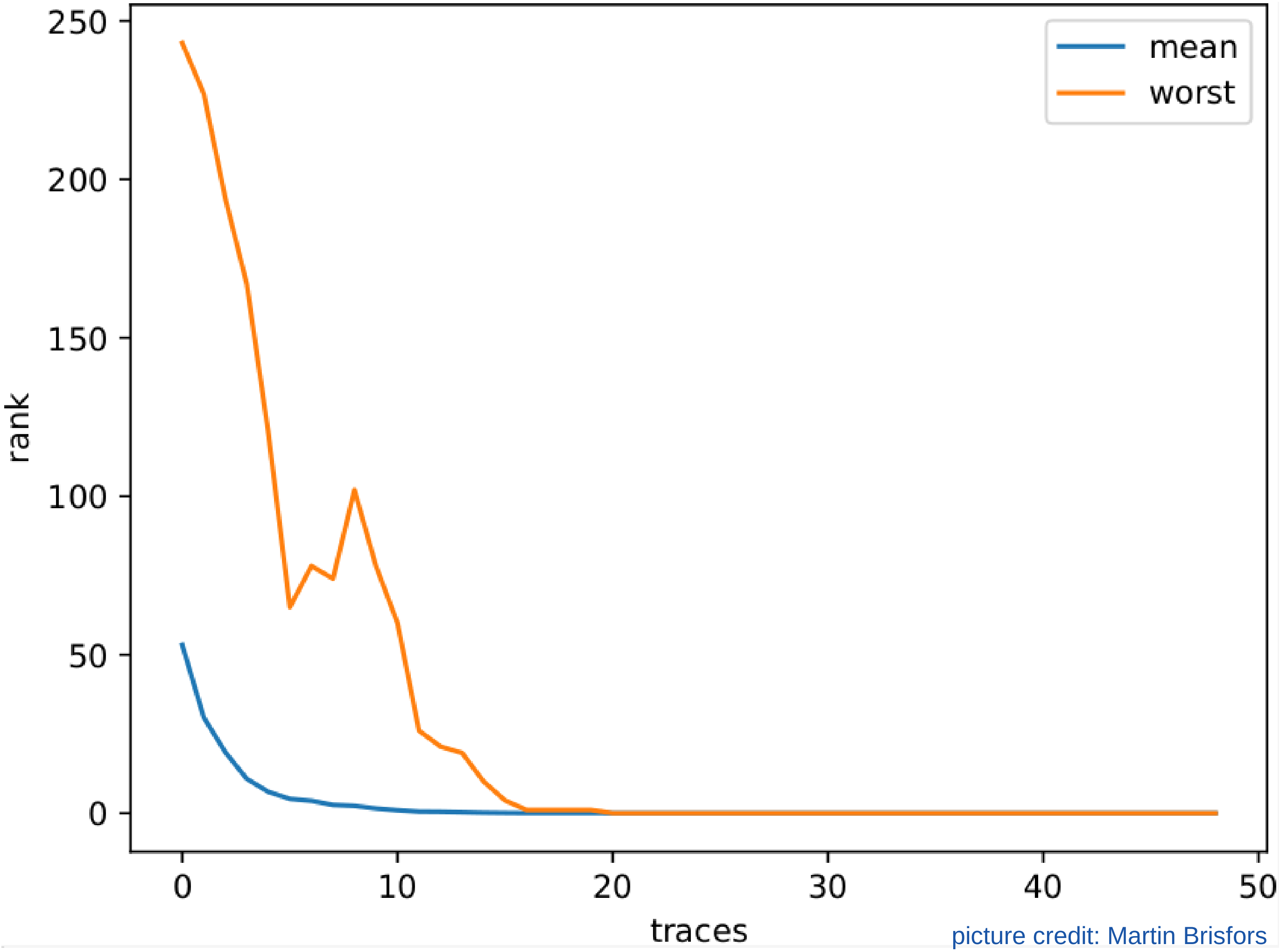


Results of 1st key byte recovery in 1st round



picture credit: Martin Brisfors

Results of 1st key byte recovery in 2nd round



picture credit: Martin Brisfors

Cost of USIM attack

- The attack can be done with a low-cost equipment

ChipWhisperer	250 USD
ChipWhisperer UFO board	240 USD
LEIA	3780 SEK
	< 1000 USD

- If trained DL models are available, the attack does not require expert-level skills in side-channel analysis

➡ Realistic threat

5 min video demo of USIM attack

Demo showing how to:

- Capture traces from a victim device
- Find attack point
- Recover the key using a trained DL model
- Estimate the number of traces required to extract the key

Example 3: Masked Saber power analysis

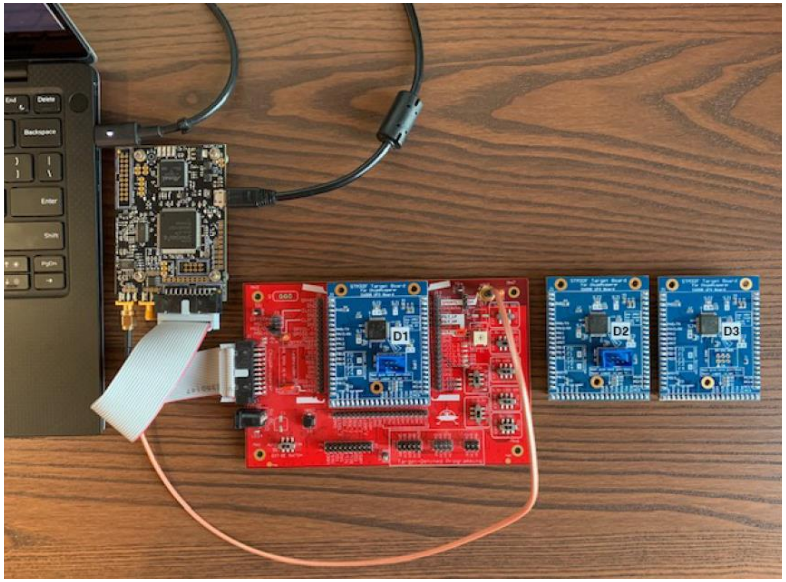


photo credit: Kalle Ngo

- Saber is one of the Round 3 candidates of NIST post-quantum cryptography standartization competition
- Key Encapsulation Mechanism (KEM)
  - security relies on the hardness of the Module Learning With Rounding problem (MLWR)

A Side-Channel Attack on a Masked IND-CCA Secure Saber KEM,
K. Ngo, E. Dubrova, Q. Guo, T. Johansson, https://eprint.iacr.org/2021/079.pdf

Saber KEM procedures

public key

long-term secret key

$\text{Saber.KEM.Encaps}((seed_{\mathbf{A}}, \mathbf{b}))$

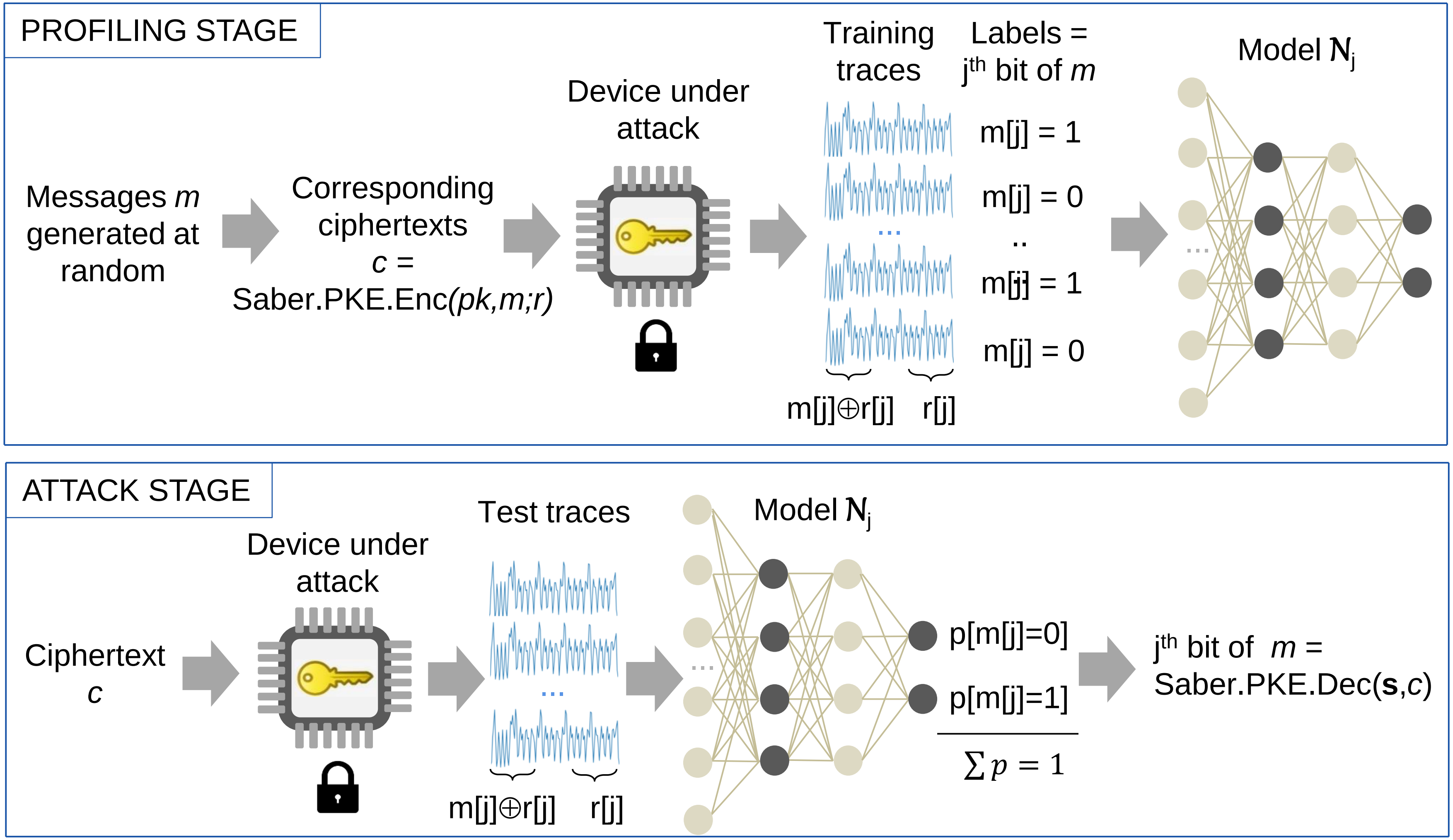
$m \leftarrow \mathcal{U}(\{0,1\}^{256})$
$(\hat{K}, r) = \mathcal{G}(\mathcal{F}(pk), m)$
$c = \text{Saber.PKE.Enc}(pk, m; r)$
$K = \mathcal{H}(\hat{K}, c)$
return (c, K)

session key

$\text{Saber.KEM.Decaps}((z, pkh, pk, \mathbf{s}),\text{c})$

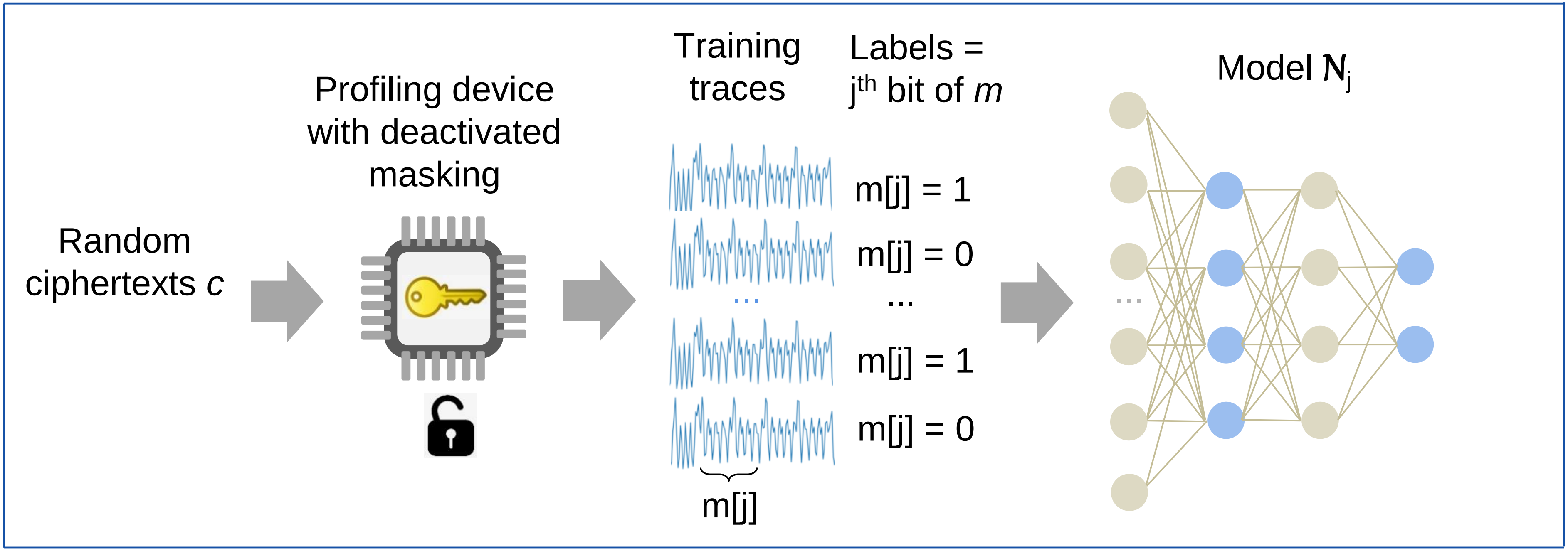
$m' = \text{Saber.PKE.Dec}(\mathbf{s}, c)$ ← attack point
$(\hat{K}', r') = \mathcal{G}(pkh, m')$
$c' = \text{Saber.PKE.Enc}(pk, m'; r')$
if $c = c'$ **then**
  return $K = \mathcal{H}(\hat{K}', c)$
else
  return $K = \mathcal{H}(z, c)$
end if

How deep learning helps break masking



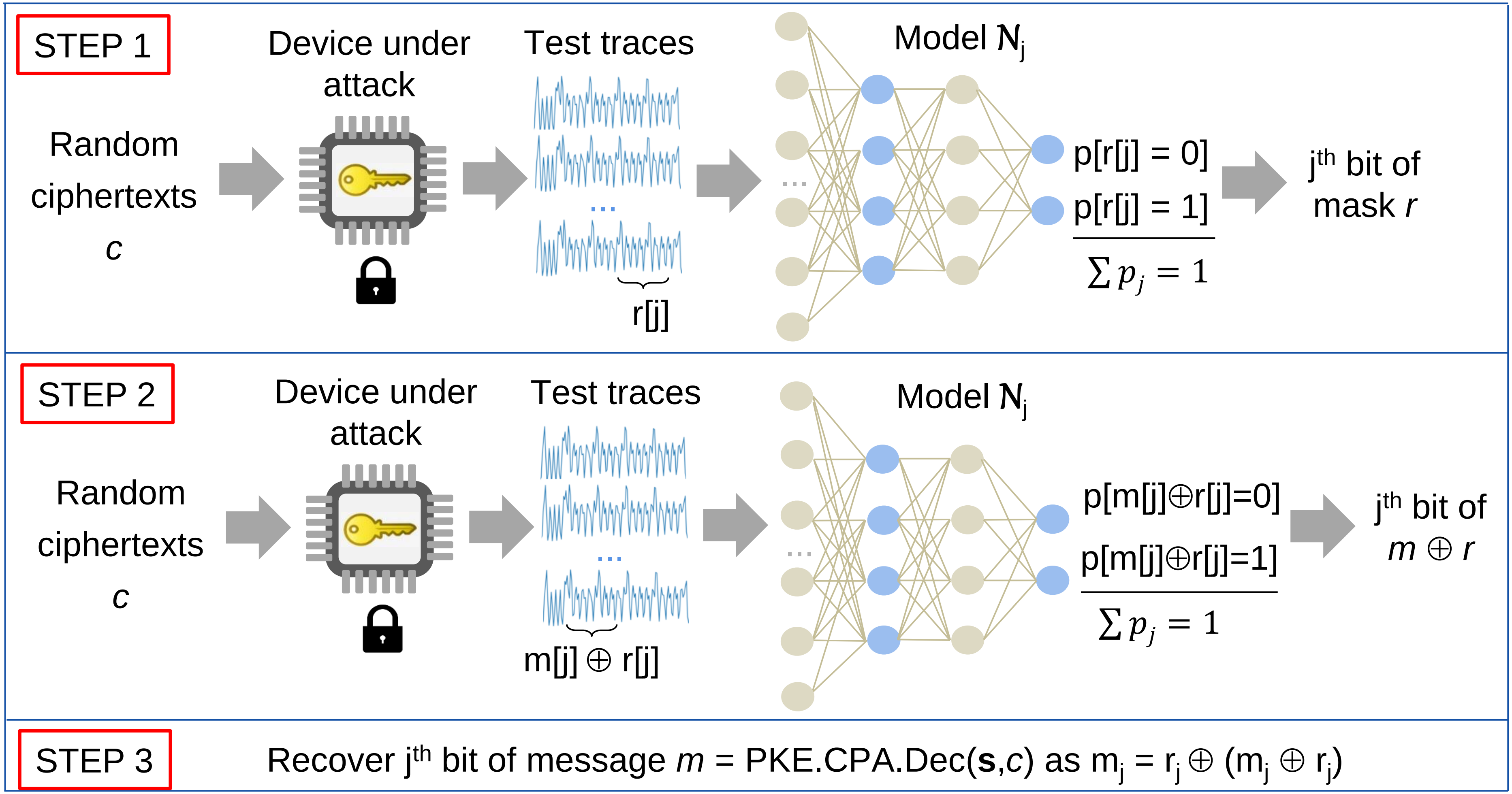
Previous attacks on masked implementations

PROFILING STAGE



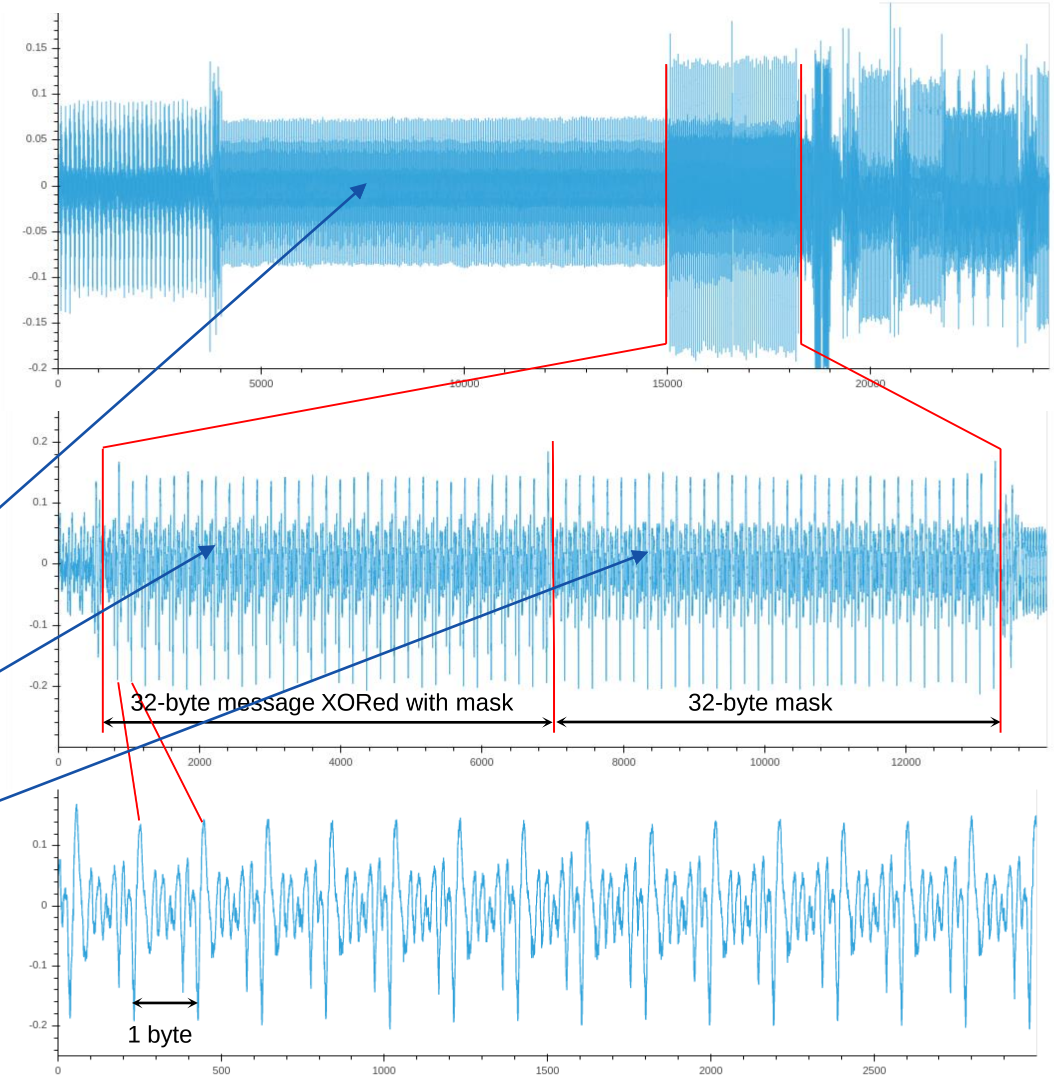
Previous attacks, cont.

ATTACK STAGE



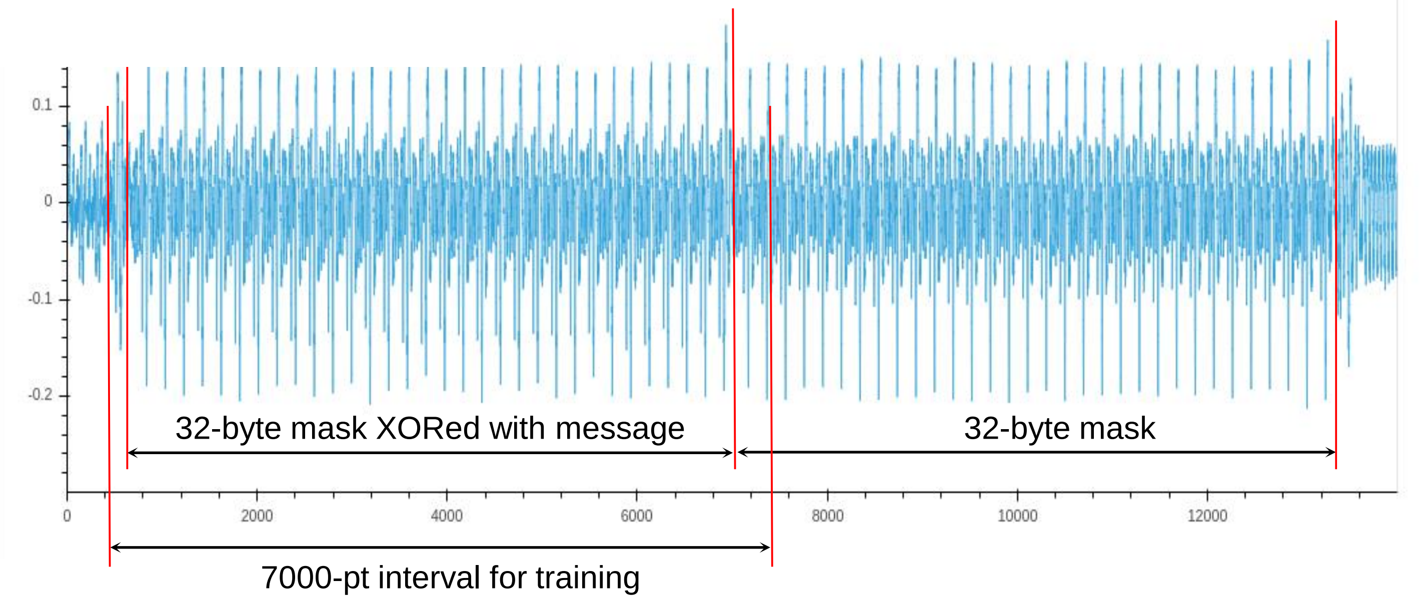
Locating attack point

```
void indcpa_kem_dec_masked(uint16_t
sksv1[], uint16_t sksv2[], char
*ct, char m1[], char m2[])
uint16_t pksv[K][N];
uint16_t v1[N]={0}, v2[N]={0};
SABER_un_pack(&ct,v1);
for (i = 0; i < N; i++) do
  v1[i] = h2-(v1[i]«(EP-ET));
end for
BS2POLVEC(ct,pksv,P);
InnerProd(pksv,sksv1,P-1,v1);
InnerProd(pksv,sksv2,P-1,v2);
poly_A2A(v1,v2);
POL2MSG(v1,m1);
POL2MSG(v2,m2);
```



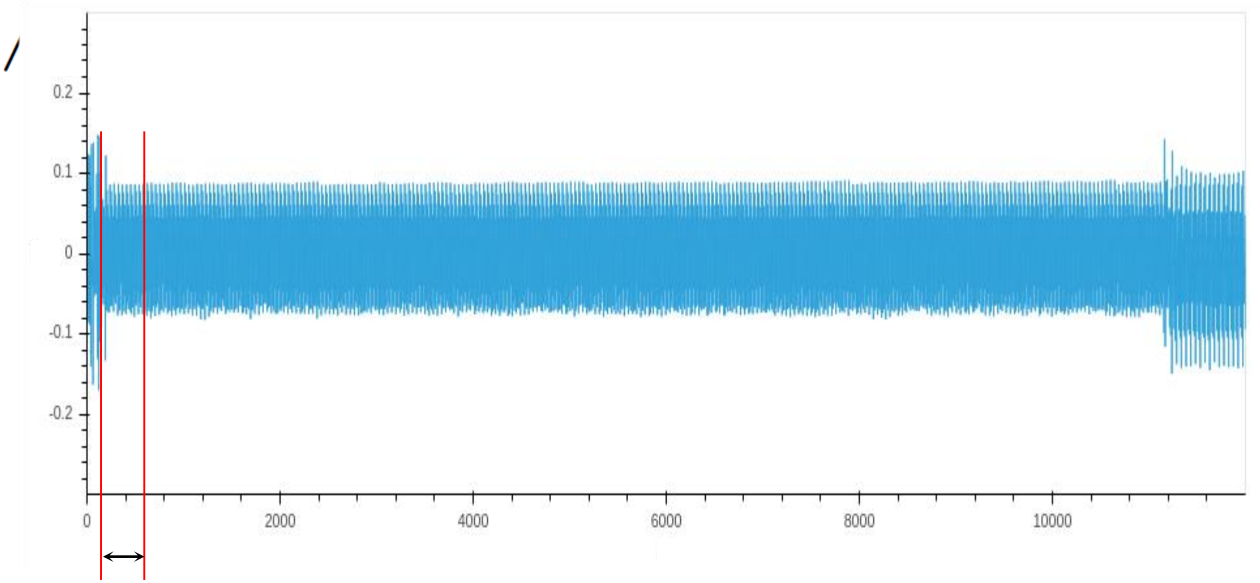
POL2MSG attack point

```
void POL2MSG(uint16_t *v, chair *m)
for (j = 0; j < BYTES; j++) do
    m[j] = 0;
    for (i = 0; i < 8; i++) do
        m[j] = m[j]|(v[8*j+i]«i);
    end for
end for
```



Poly_a2a attack point

```
void poly_A2A(uint16_t A[N],
uint16_t R[N])
uint32_t A, R;
for (i = 0; i < N; i++) do
    A = A[i]; R = R[i];
      ...   /* processing */
    A[i] = A; R[i] = R;
end for
```



600-pt interval for training

Results for POL2MSG leakage point

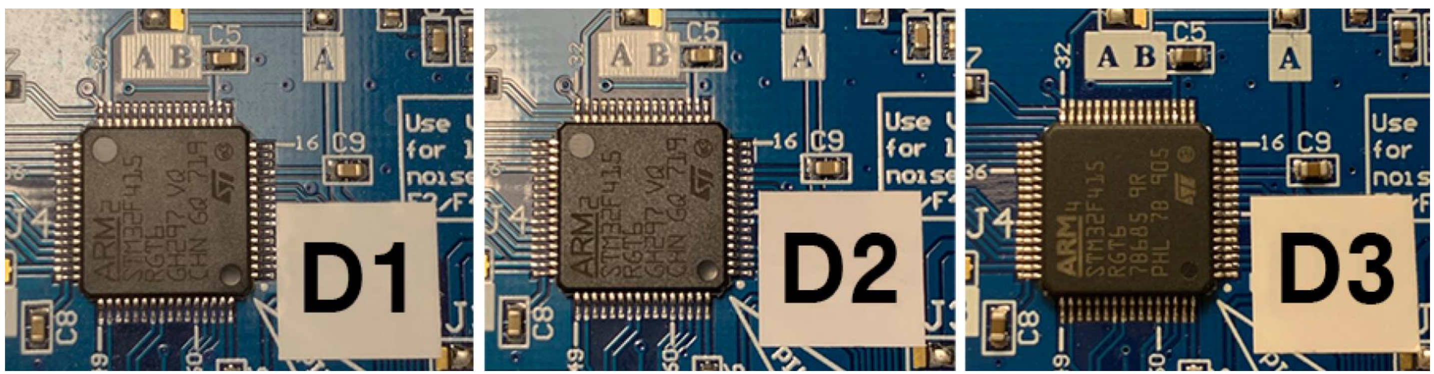
Table 3: Probability p_j to recover $m[j]$ from a single trace using `POL2MSG()` leakage point.

Device	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	**average**
D_1	0.998	0.998	0.993	0.992	0.989	0.988	0.985	0.953	0.987
D_2	0.994	0.989	0.986	0.959	0.978	0.962	0.985	0.945	0.975
D_3	0.984	0.985	0.988	0.963	0.972	0.991	0.975	0.819	0.960
average	0.992	0.990	0.989	0.971	0.979	0.980	0.982	0.906	0.974

used for training

similar to D_1

different from D_1



Messagy recovery results for poly_A2A

Table 4: Expected probability to recover a message bit from a single trace using `poly_A2A()` leakage point.

Device	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	**average**
D_1	0.845	0.970	0.959	0.905	0.948	0.960	0.953	0.972	0.939
D_2	0.828	0.962	0.942	0.945	0.920	0.919	0.950	0.950	0.927
D_3	0.848	0.900	0.941	0.884	0.949	0.905	0.914	0.947	0.911
average	0.840	0.944	0.947	0.912	0.939	0.928	0.939	0.956	0.926

Secret key recovery

- Session key can be derived directly from the recovered message
- Long-term secret key can be recovered from:
  - 16 chosen ciphertexts for LightSaber
  - 24 chosen ciphertexts for Saber
- Future work – breaking combined countermeasures

Summary

- Be aware that deep learning opens opportunities for adversaries as well
- Deep learning side-channel attacks are very powerful
  - can overcome some countermeasures
    - Noise-based
    - Masking
- We need to understand possibilities and limitations of deep learning to design stronger countermeasures

Links to videos

How Deep Learning Helps Compromising USIM:

https://www.youtube.com/watch?v=7uJq1GIfTUY&feature=youtu.be

Far Field Side-Channel Attack on AES Using Deep Learning:

https://drive.google.com/file/d/1h7RmxIEFUQSFgwrIg8DnWPzDBws49FdG/view?usp=sharing