Breaking cryptographic algorithms using power and EM side-channels

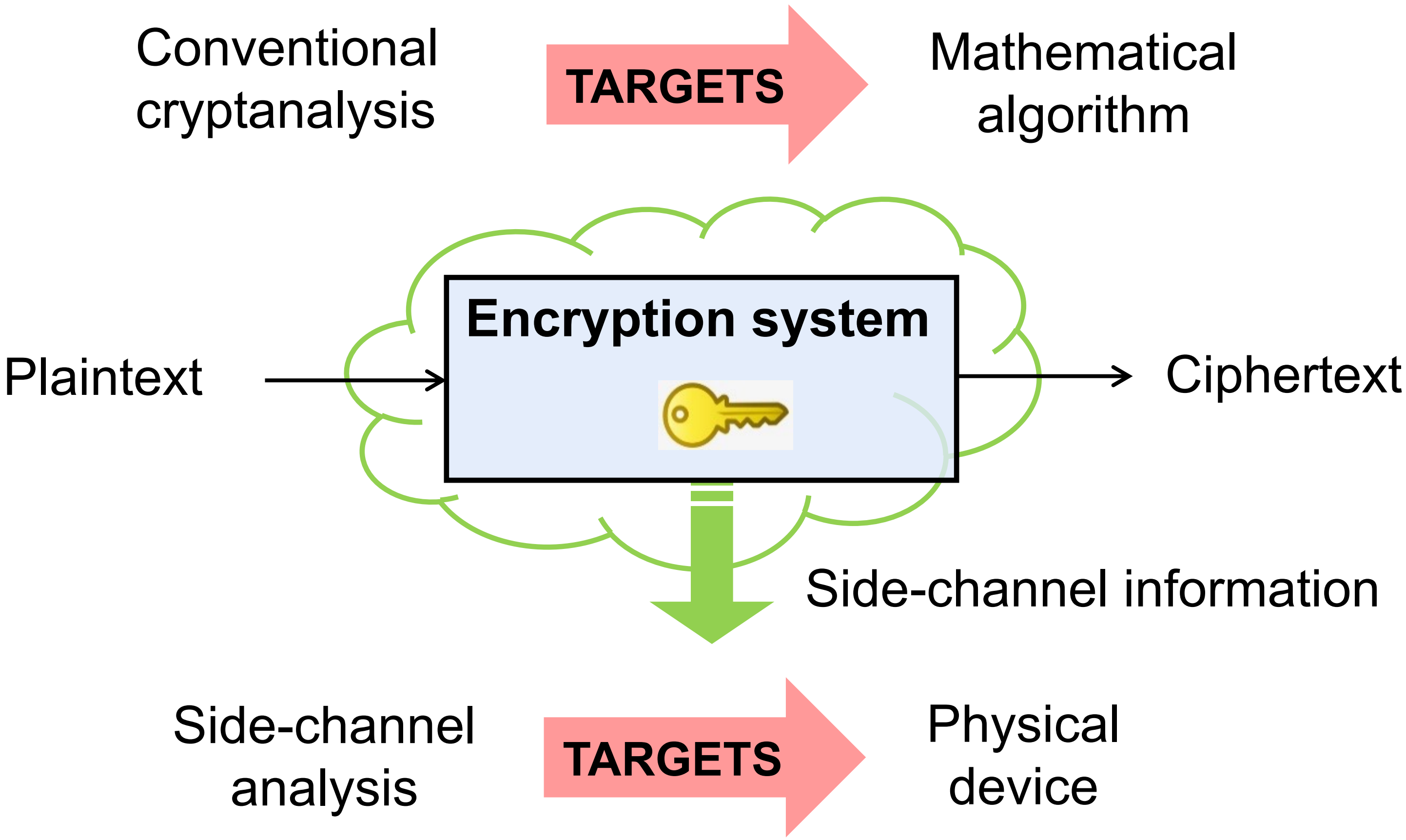
Elena Dubrova
Department of Electrical Engineering
School of Electrical Engineering and Computer Science
KTH, Stockholm, Sweden

Outline

- Introduction to side-channel attacks & motivation
- Attack examples:
  - Nordic nRF52 EM analysis
  - USIM card power analysis
  - Power/EM analysis of NIST PQC candidates
- Summary & open probelms

Acknowledgements to KTH students Kalle Ngo, Martin Brisfors, Sebastian Forsmark, Ruize Wang, Huanyu Wang, Michail Moraitis, Linus Backlund, Nils Paulsrud, Yanning Ji

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

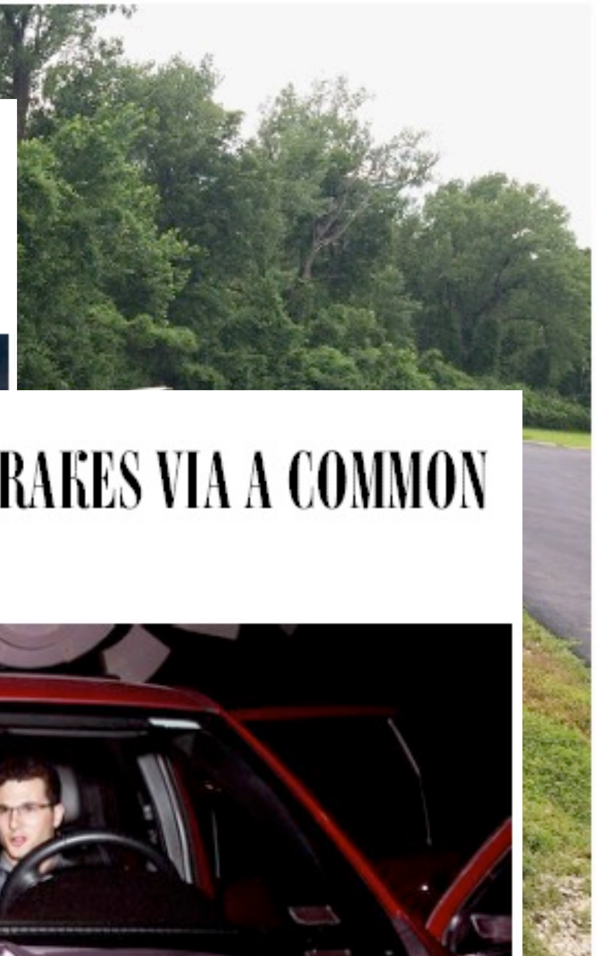
source: http://www.wearables.com/5-baby-monitors-wearable-infant-tech/

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/

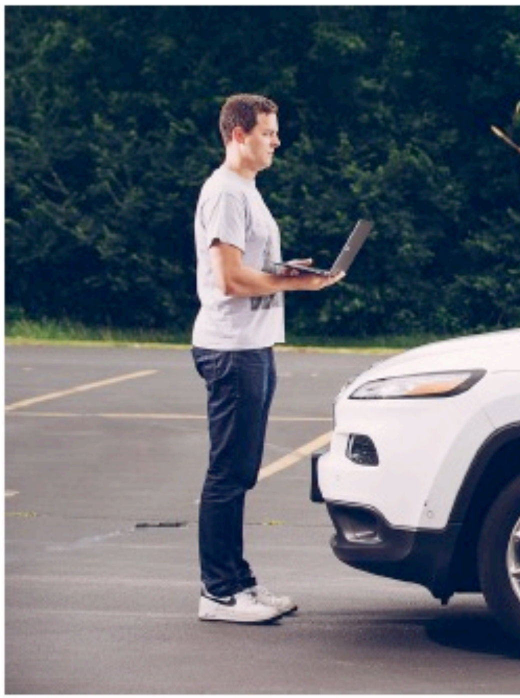
ANDY GREENBERG SECURITY 03.17.16 6:59 PM

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

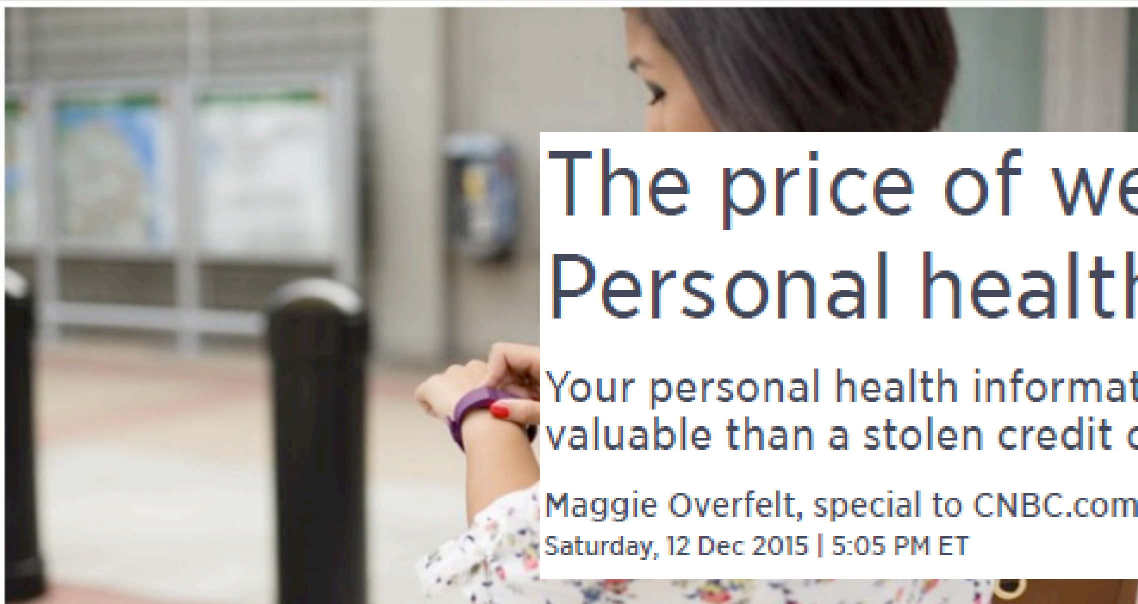
SECURITY

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

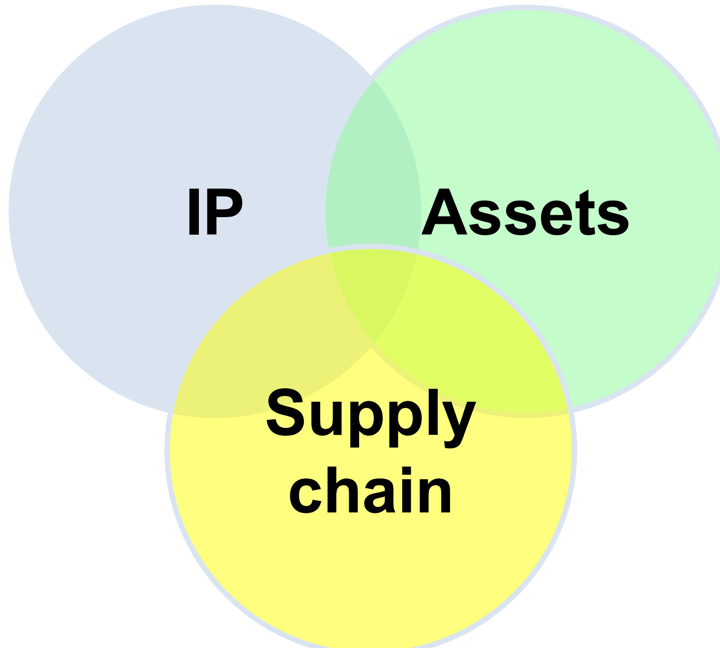
Your personal health information is about 10 times more valuable than a stolen credit card number on the black market.

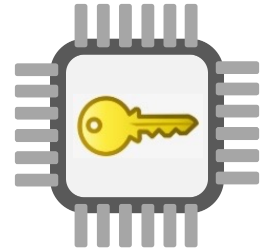
Maggie Overfelt, special to CNBC.com
Saturday, 12 Dec 2015 | 5:05 PM ET

What needs protection?

Saab@MarcusWandt

Proprietary designs
Proprietary algorithms
Proprietary bitstreams





On-device data
On-device keys
TRNGs
PUFs

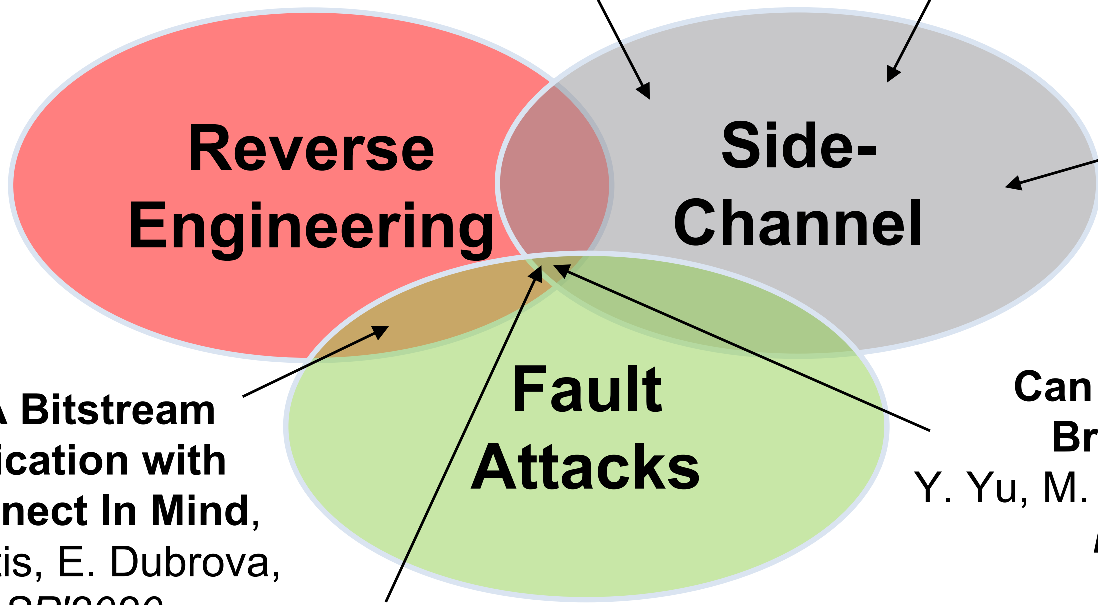
source: http://www.publicintegrity.org/ 2011/11/07/ 7323/counterfeit-chips-plague-pentagon-weapons-systems

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, *TCHES'2021*

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*

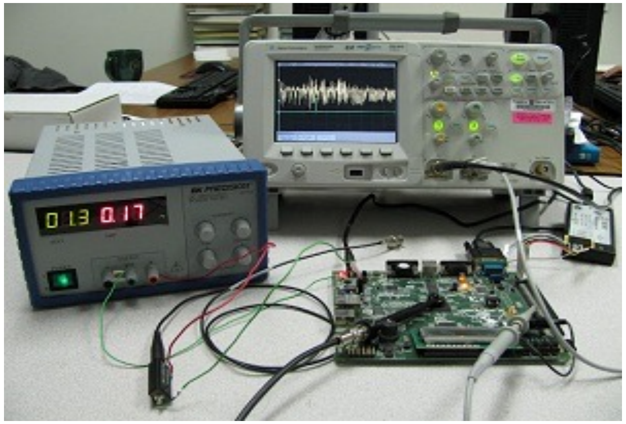
FPGA Bitstream Modification with Interconnect In Mind, M. Moraitis, E. Dubrova, *HASP'2020*

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*

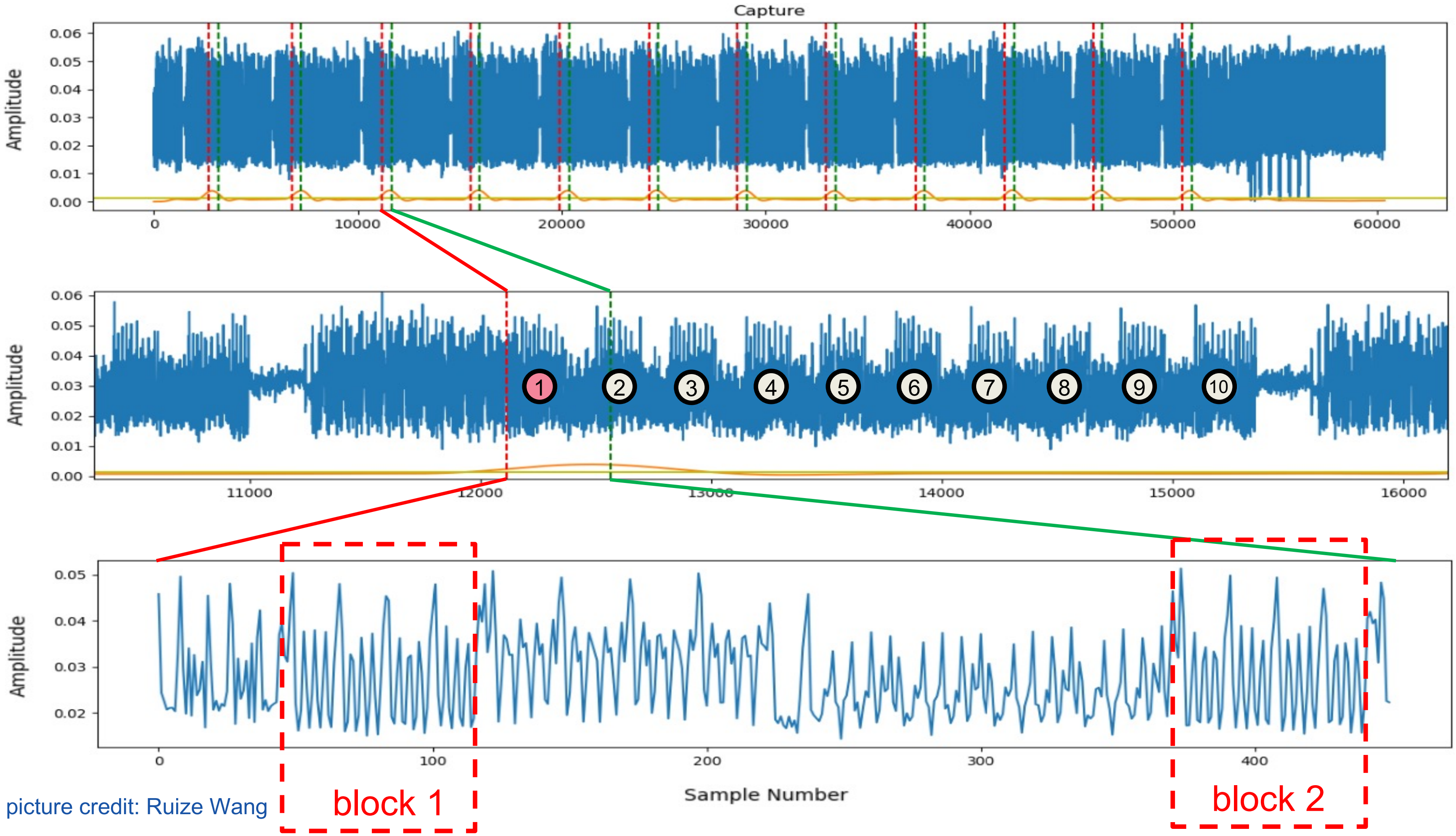
How side-channel attacks work

- 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



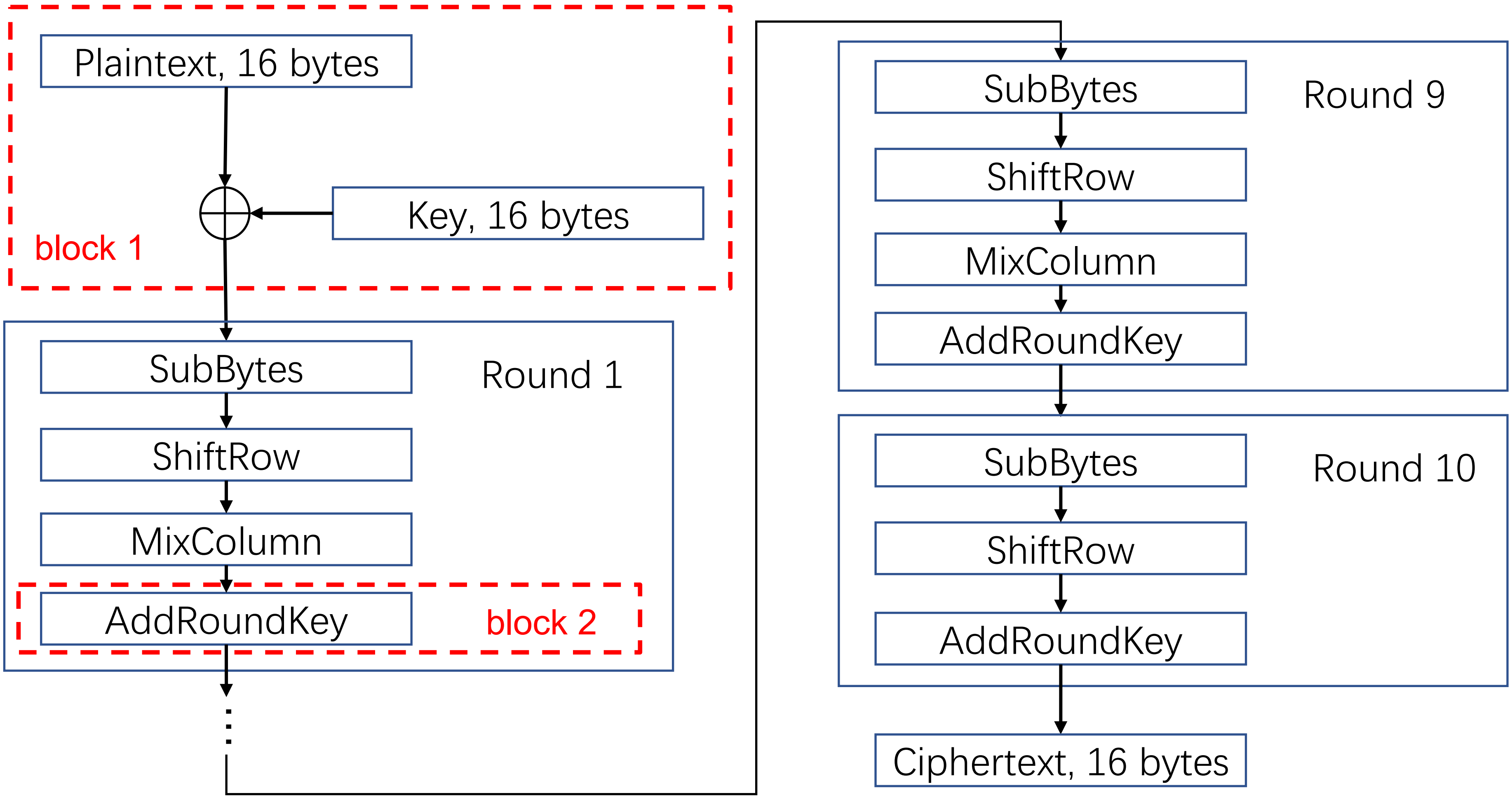
source: hackaday.com

Analsyis of AES-128 encryption algorithm



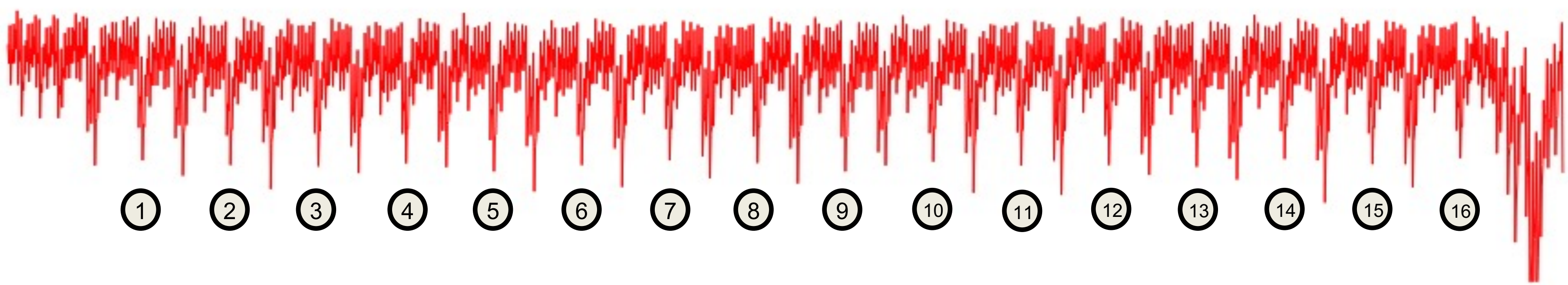
picture credit: Ruize Wang

AES-128



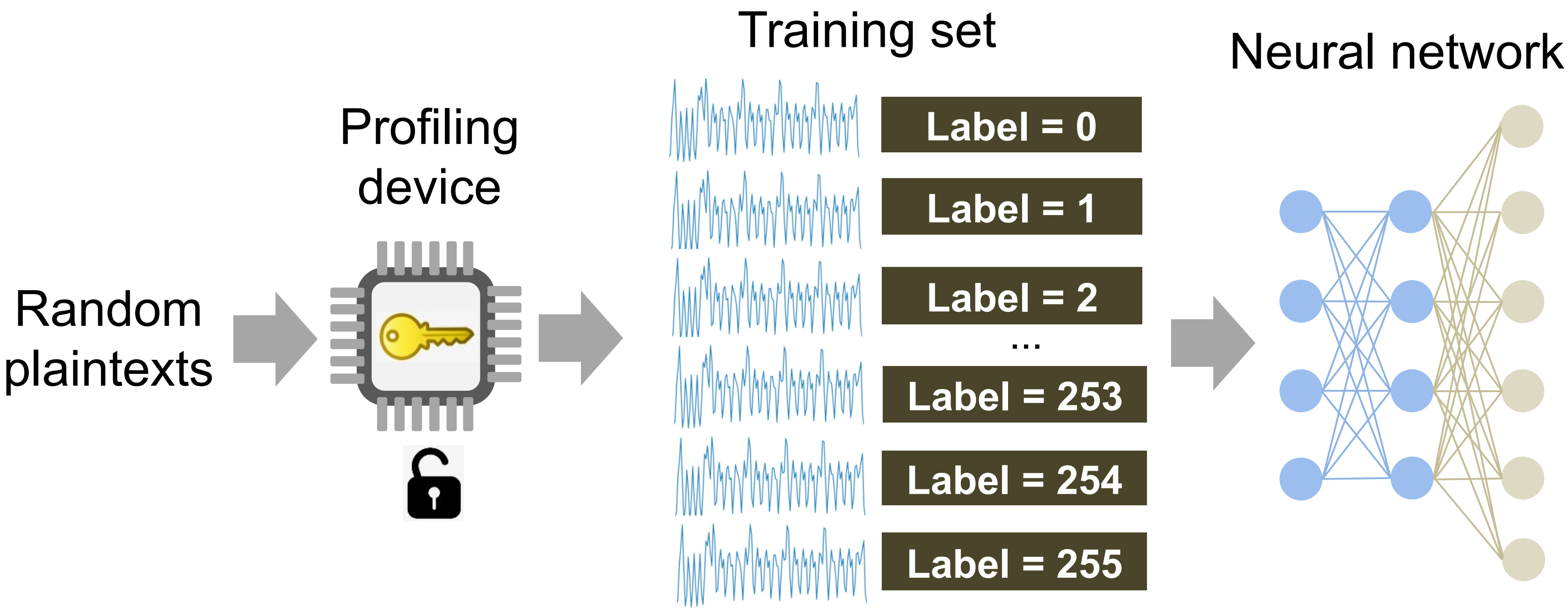
picture credit: Ruize Wang

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



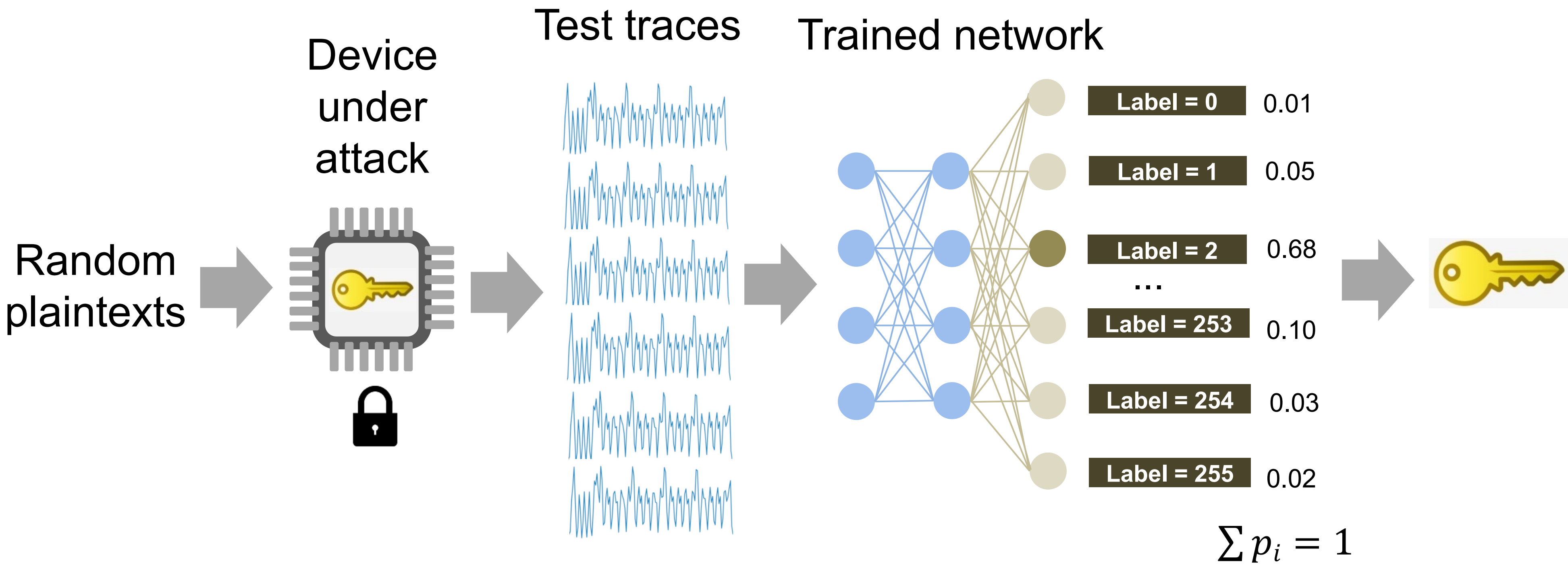
Deep learning-based side-channel analysis

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



Deep learning-based 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

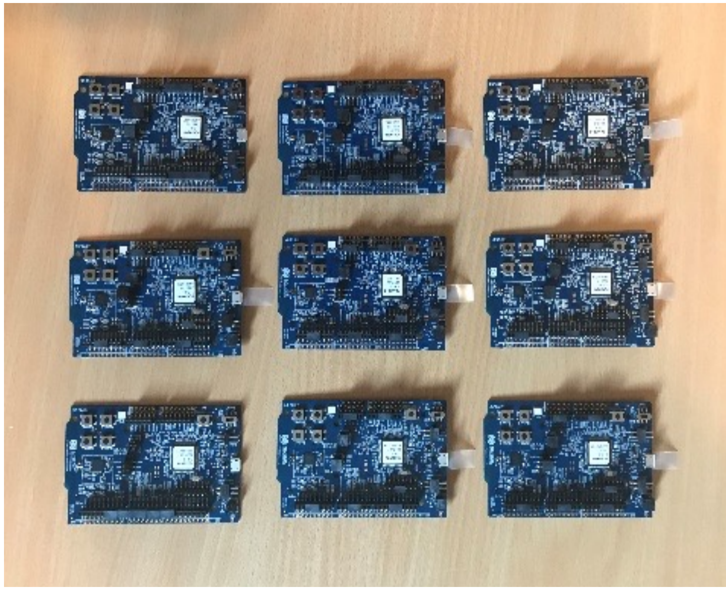


photo credit: Katerina Gurova

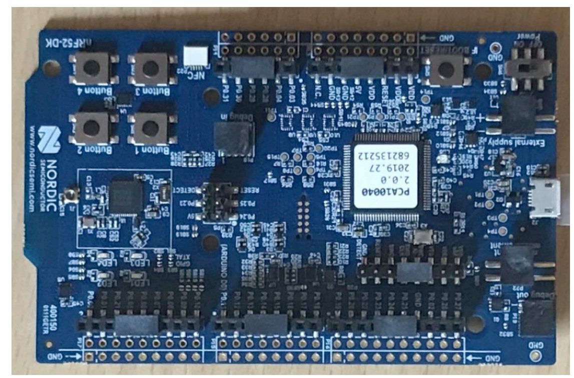
AES encryption key can be extracted from < 350 EM traces captured at 15 m distance to device

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

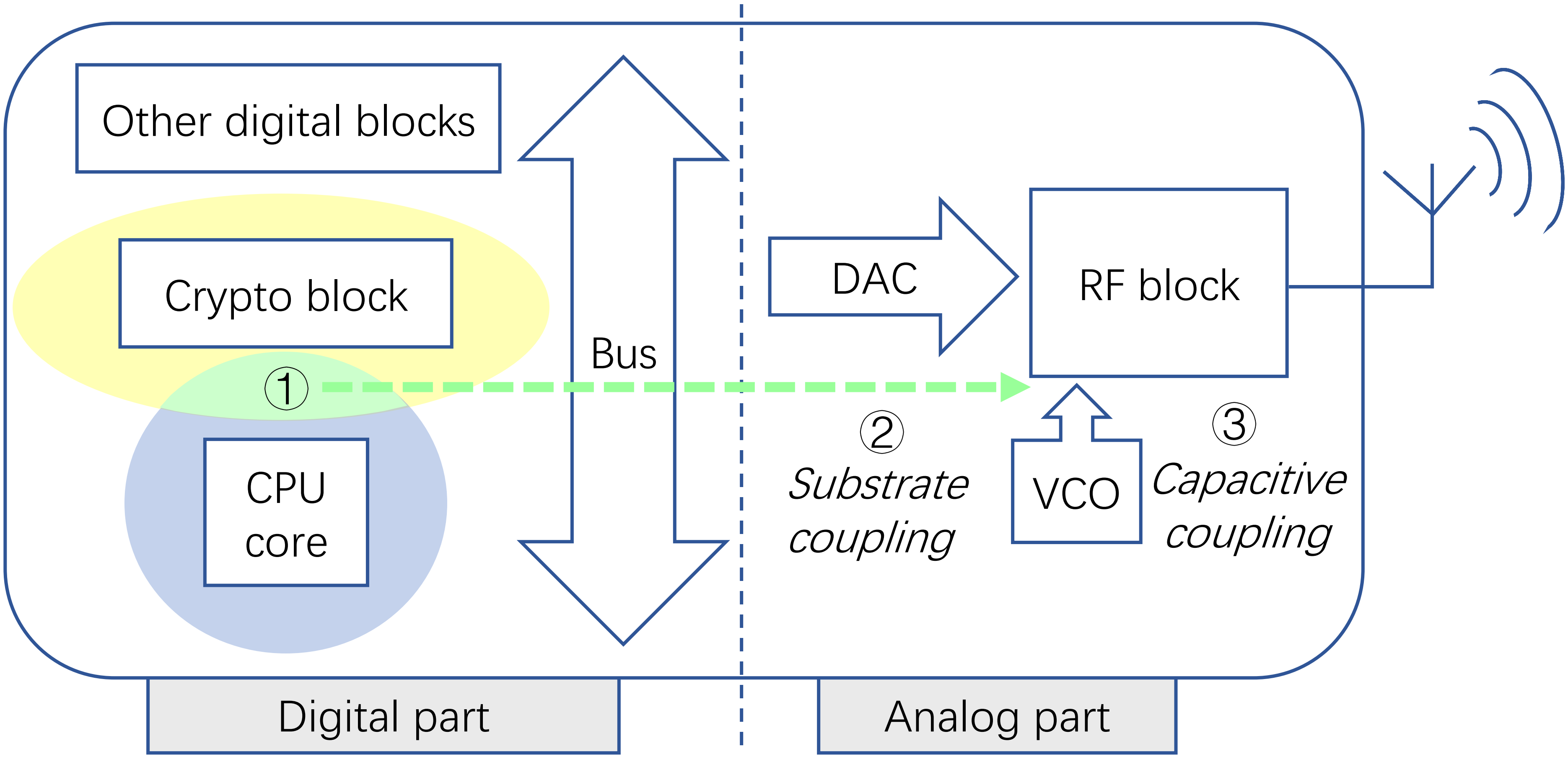
Advacned Far Field EM Side-Channel Attack on AES, R. Wang, H. Wang, E. Dubrova, CPSS’2021, June 7, 2020

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



Sources of EM emissions in a mixed-signal circuit



Measurment setup

Grid Parabolic Antenna TL-ANT2424B

Ettus Research USRP N210 SDR

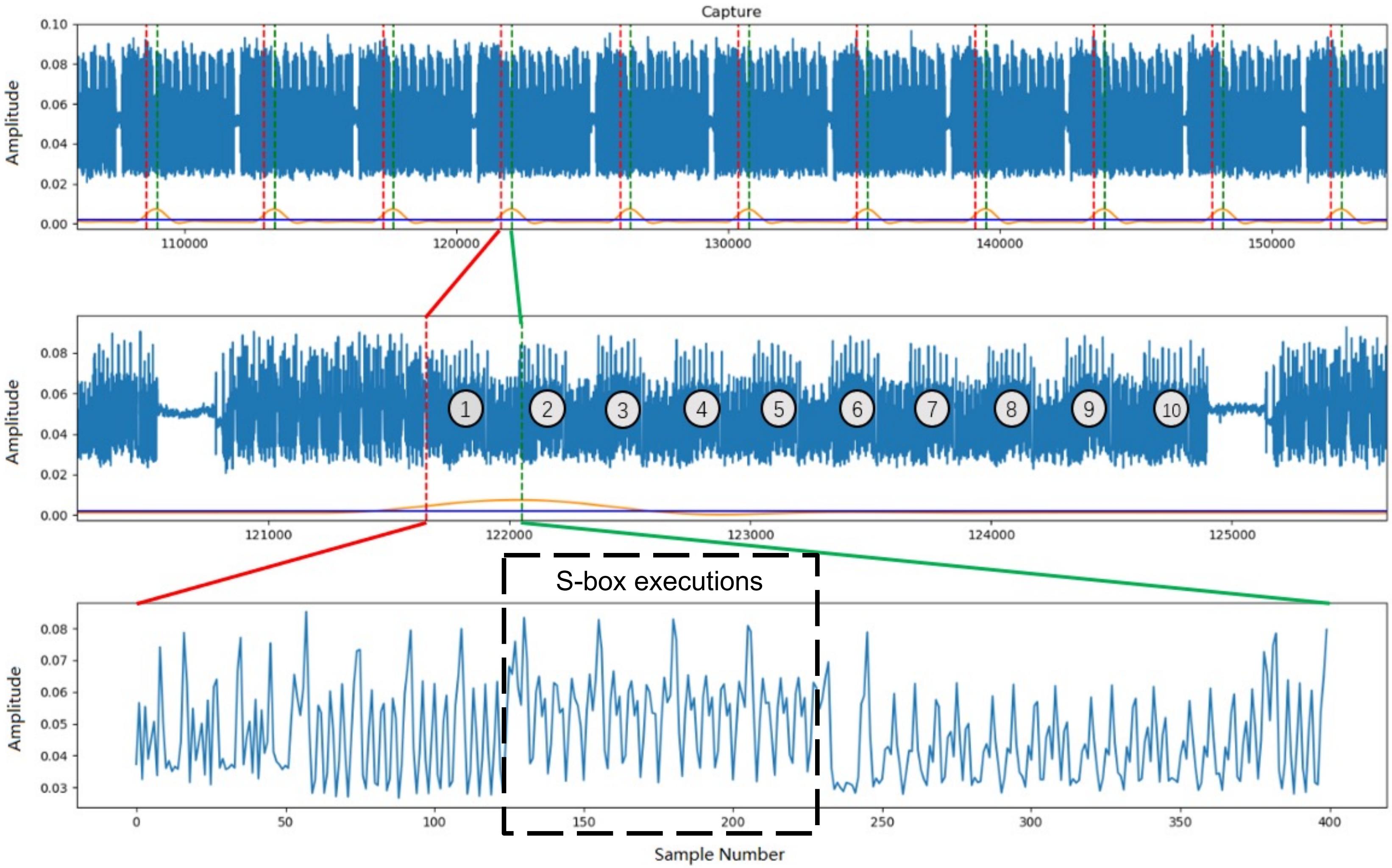
nRF52DK board

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)

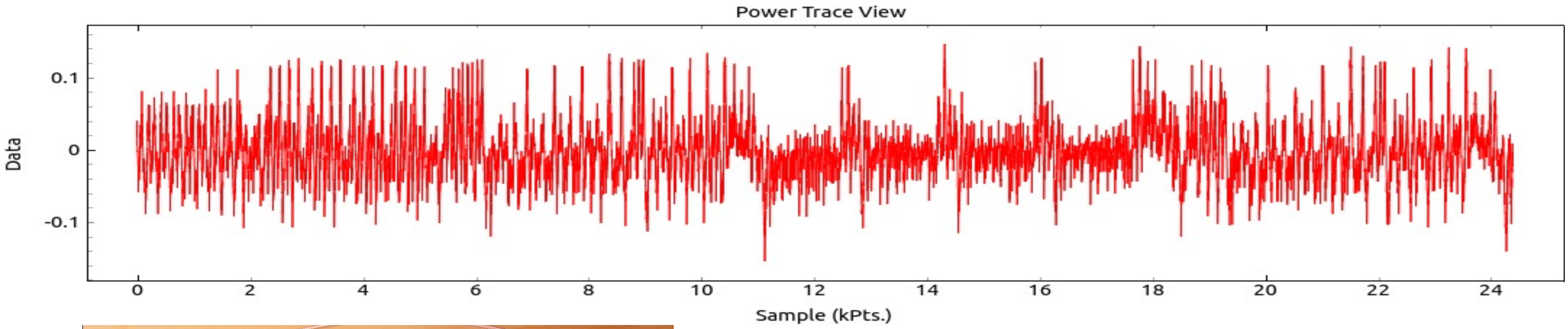
Locating the attack point in trace



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



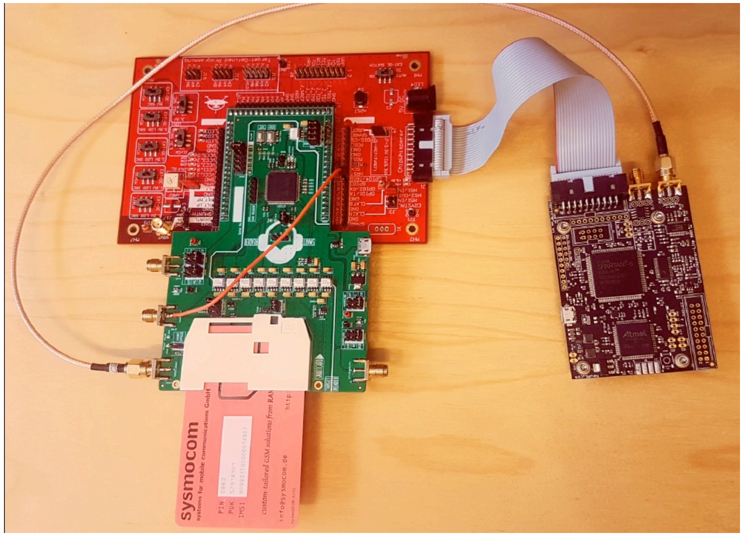
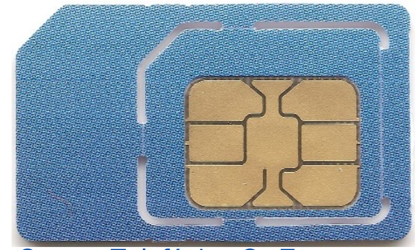


photo credit: Martin Brisfors

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

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

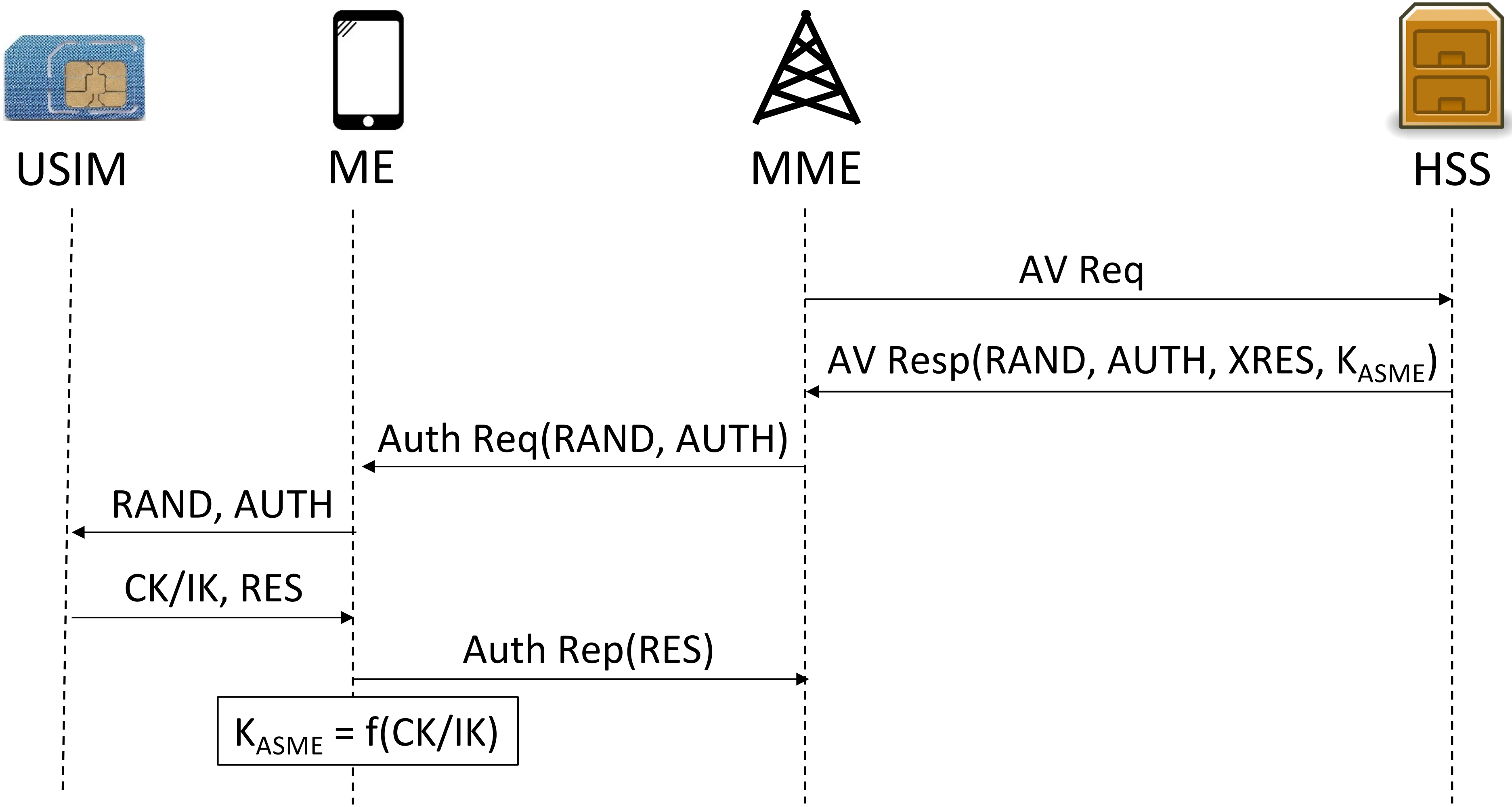
Universal Subscriber Identity Module (USIM)



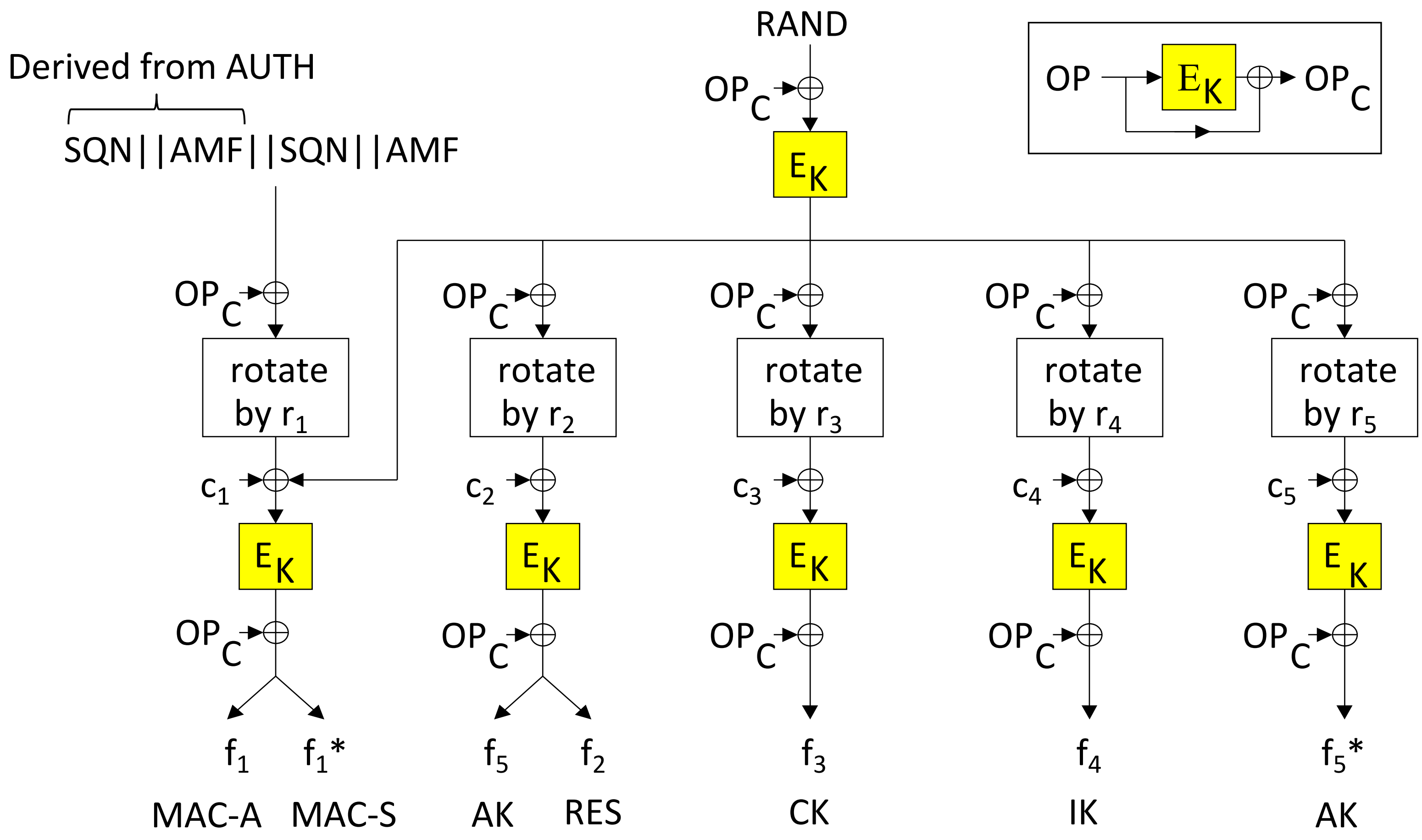
Source:Telefónica O_2 Europe

- 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

Authentication and Key Agreement (AKA) in 4G



MILENAGE algorithm

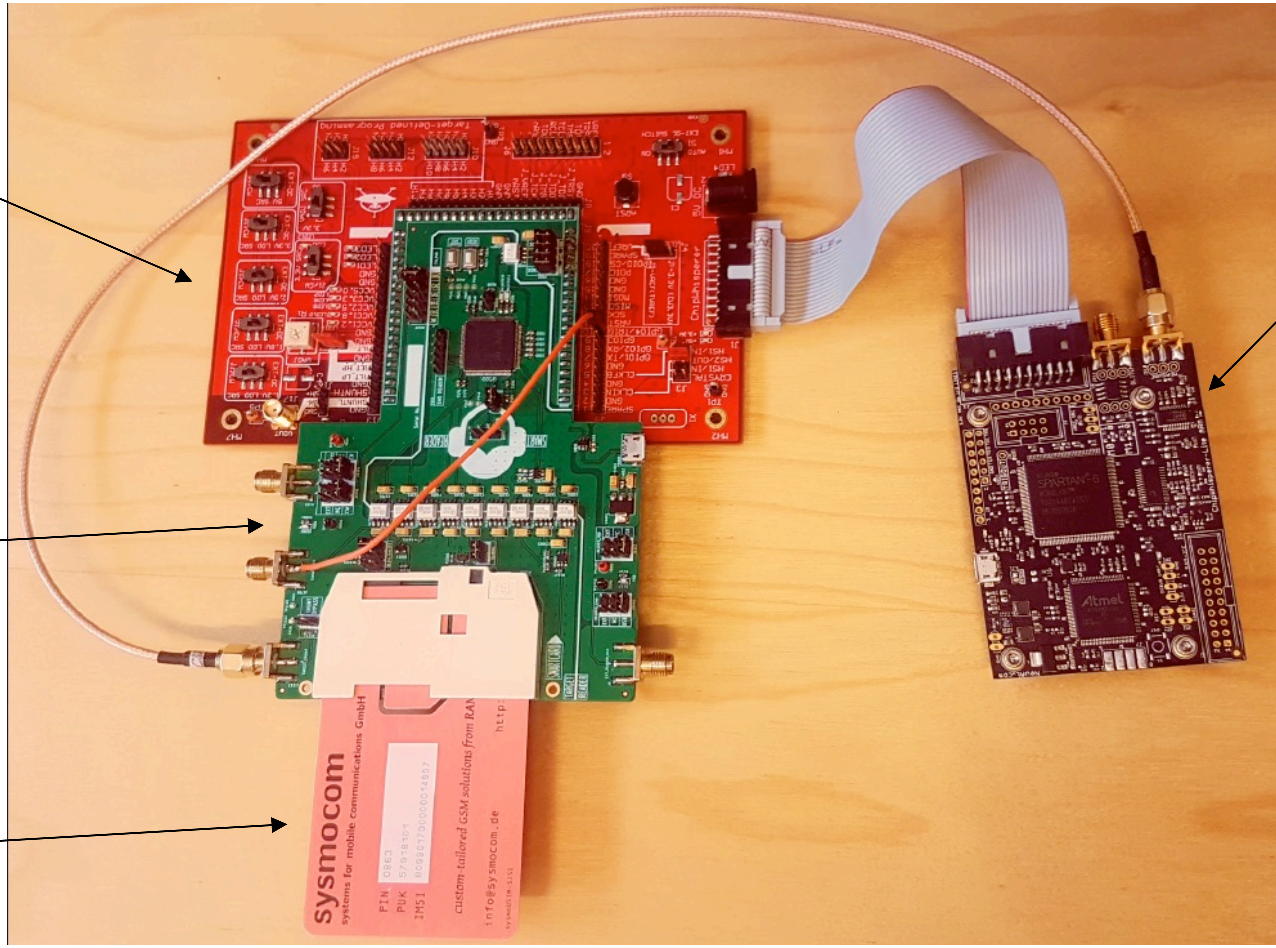


Measurment setup

CW308 UFO

LEIA

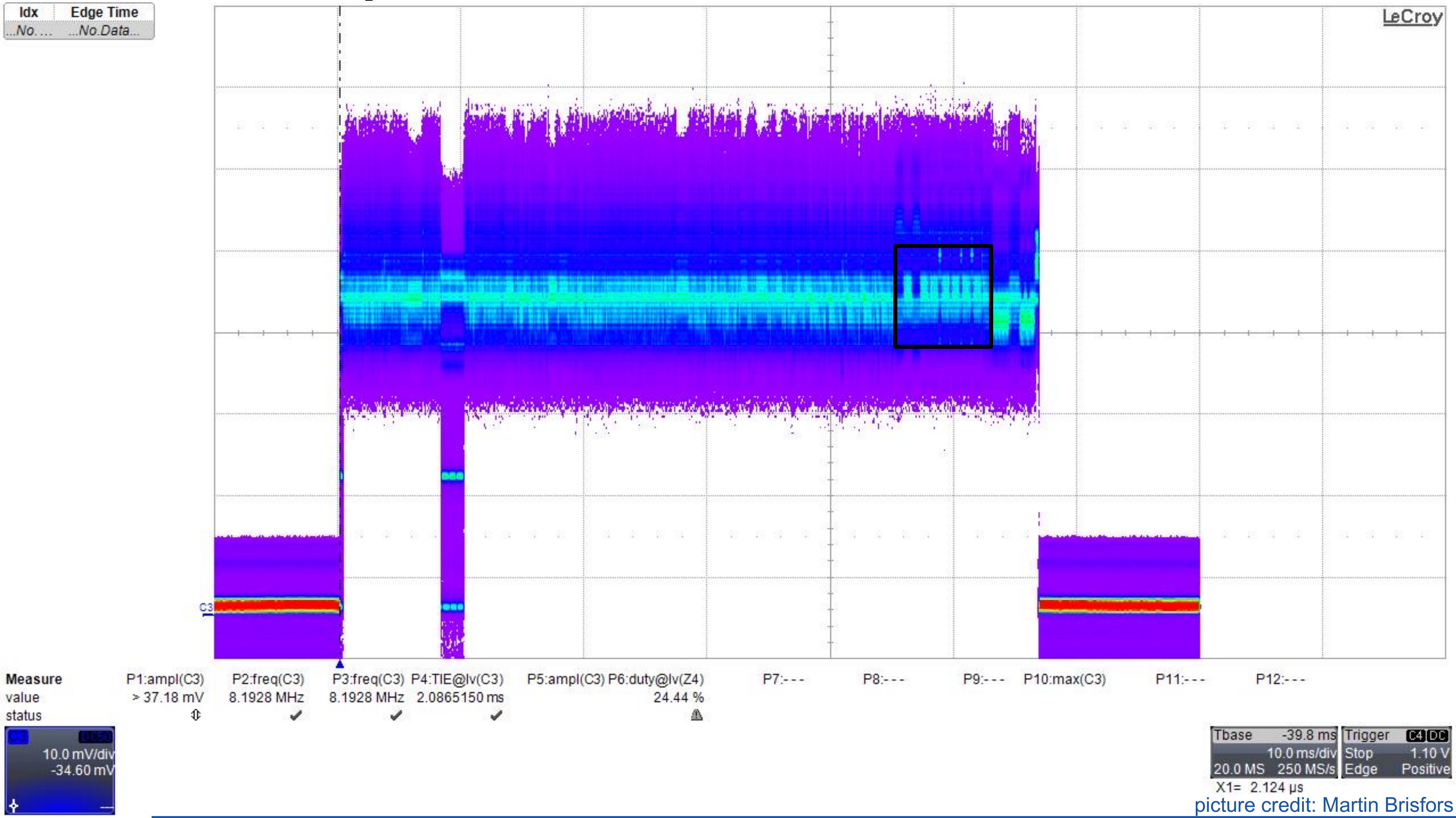
USIM



ChipWisperer

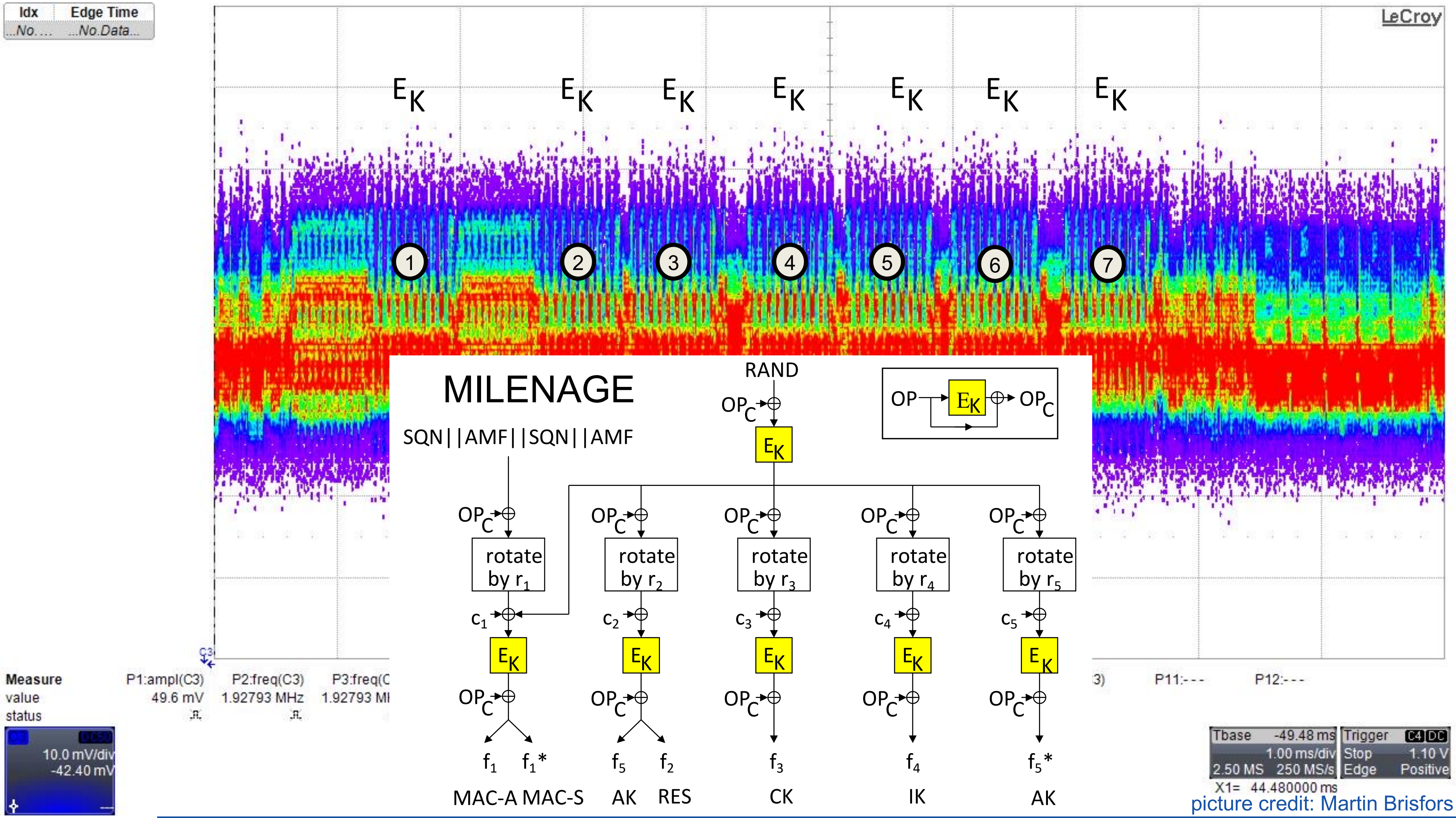
photo credit: Martin Brisfors

USIM power trace for one MILENAGE call



picture credit: Martin Brisfors

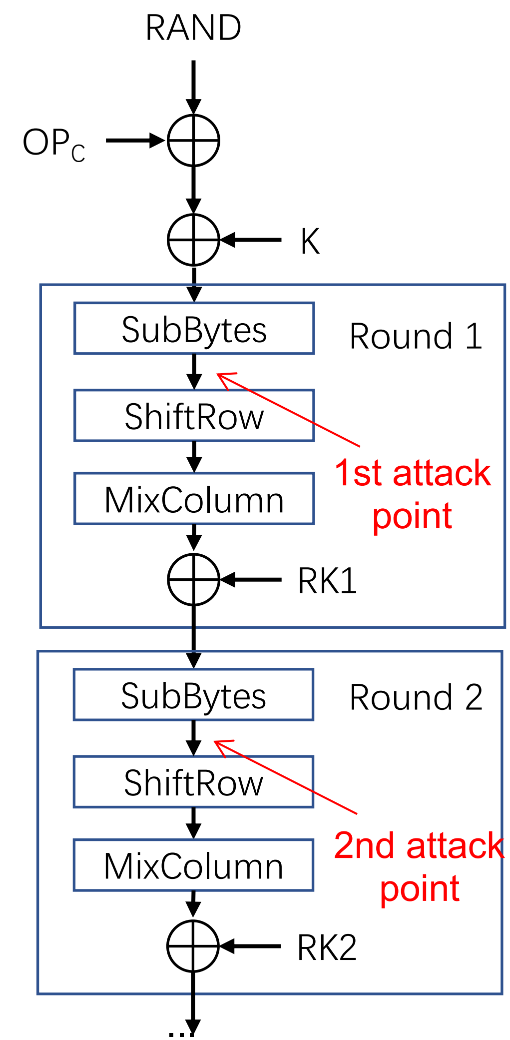
Zoomed interval of MILENAGE execution



picture credit: Martin Brisfors

Attack steps

- In MILENAGE, RAND $\oplus$ 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. $OP_C = (OP_C \oplus K) \oplus K$



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

USIM key recovery demo 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

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

Example 3: NIST PQC candidates analysis

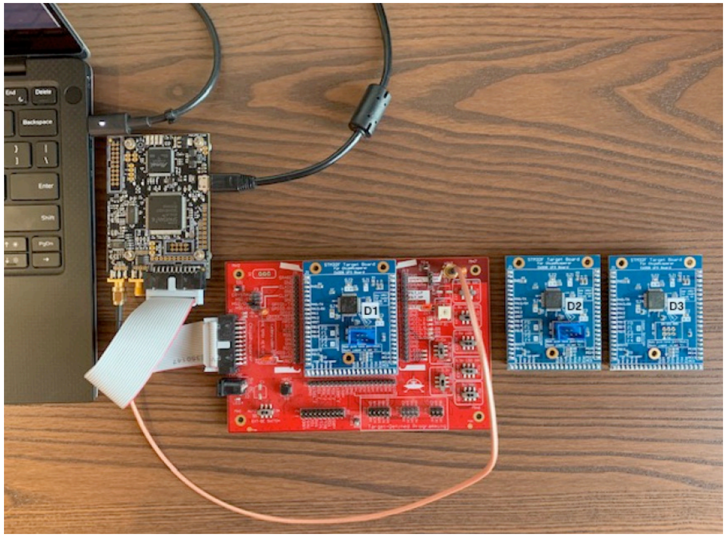


photo credit: Kalle Ngo

- Kyber and Saber are candidates of the ongoing NIST post-quantum cryptography standartization process
- Key Encapsulation Mechanisms (KEM)
  - public-key, lattice-based
- Kyber is already chosen for standardization

1. *Side-Channel Attack on a Masked IND-CCA Secure Saber KEM,* K. Ngo, E. Dubrova, Q. Guo, T. Johansson, TCHES'2021
2. *Breaking Masked and Shuffled CCA Secure Saber KEM by Power Analysis*, K.Ngo, E.Dubrova, T.Johansson, ASHES'2021
3. *Side-Channel Attacks on Lattice-Based KEMs Are Not Prevented by Higher-Order Masking*, K.Ngo, R.Wang, E.Dubrova, N.Paulsrud, Cryptology ePrint Archive, 2022/919
4. *Making Biased DL Models Work: Message and Key Recovery Attacks on Saber Using Amplitude-Modulated EM Emanations,* R.Wang, K.Ngo, E.Dubrova, Cryptology ePrint Archive, 2022/852
5. *A Side-Channel Attack on a Hardware Implementation of CRYSTALS-Kyber,* Y. Ji, R. Wang, K.Ngo, E.Dubrova, L. Backlund, Cryptology ePrint Archive, Oct. 2022

Masking and shuffling countermeasures

Secret

1 1 1 1 0 0 0 0

0 1 0 1 0 1 0 1

Random mask changed at every execution

1 0 1 0 0 1 0 1

Secret ⊕ Random mask
``⊕´´ is bitwise XOR

Secret

1 1 1 1 0 0 0 0

0 0 1 0 1 0 1 1

Secret permuted

Saber KEM algorithm

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**

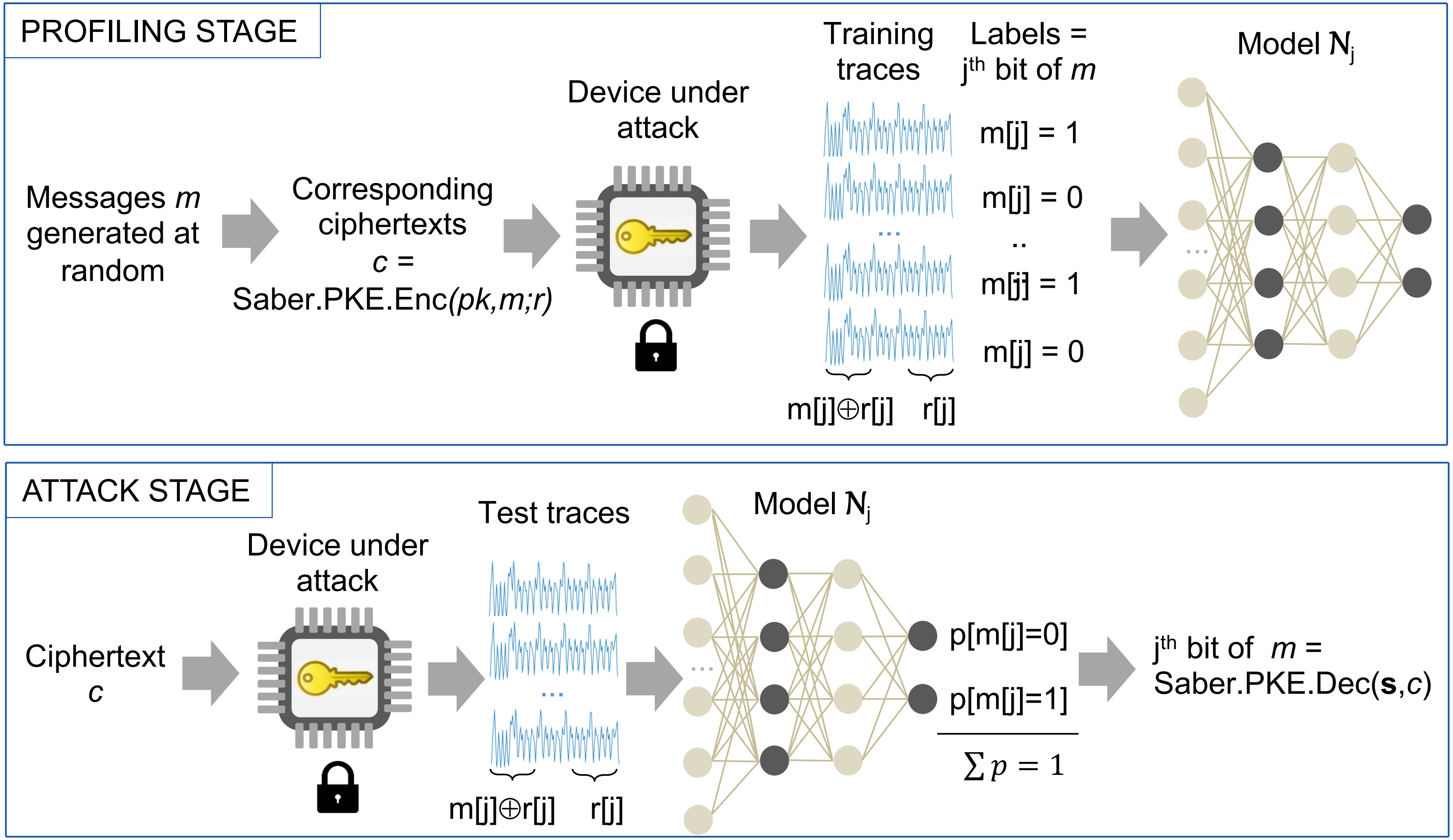
  return $K = \mathcal{H}(\hat{K}', c)$

else

  return $K = \mathcal{H}(z, c)$

end if

How deep learning helps break masking



Empirical probability to recover a message bit from a single trace

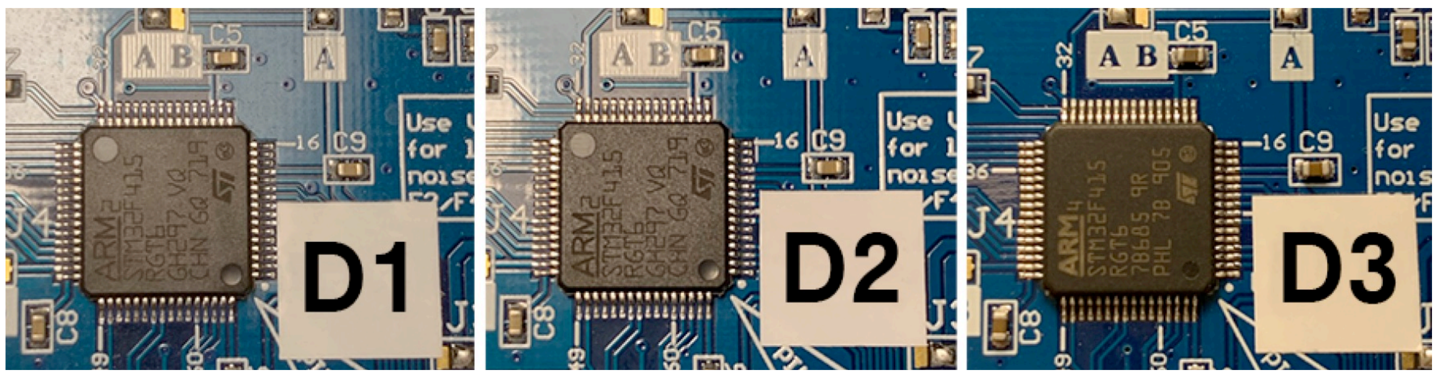
Device	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	average
D_1	0.993	0.999	0.998	1.000	0.997	0.998	0.999	0.995	0.997
D_2	0.987	0.998	0.999	0.999	0.997	0.998	0.998	0.999	0.997
D_3	0.982	0.966	0.976	0.962	0.966	0.954	0.968	0.941	0.964
average	0.987	0.988	0.991	0.987	0.987	0.983	0.988	0.978	0.986

used for training

similar to D_1

different from D_1

$0.9974^{256} = 0.5135$



Results

- Long-term secret key can be recovered from
  - 24 chosen ciphertexts for a masked software implementation of Saber
  - 61,680 chosen ciphertexts for a masked and shuffled software implementation of Saber
- Messages/session keys can be recovered from
  - 5120 traces for an unprotected FPGA implementation of Kyber

Saber Key Recovery demo: https://youtu.be/5ydQAenyGSQ

Summary

- Deep learning-based side-channel attacks can overcome traditional countermeasures such
  - Masking
  - Shuffling
  - Unstable clock
  - Random delay insertion
  - Noise-based
  - …
- We need stronger, deep learning resistant countermeasures

KTH VETENSKAP OCH KONST

Vetenskapsrådet

MSB Myndigheten för samhällsskydd och beredskap

CDIS

Thank you!

TECOSA

VINNOVA