Side-Channel Vulnerability and Threat Analysis with Machine Learning in Focus

Elena Dubrova, KTH

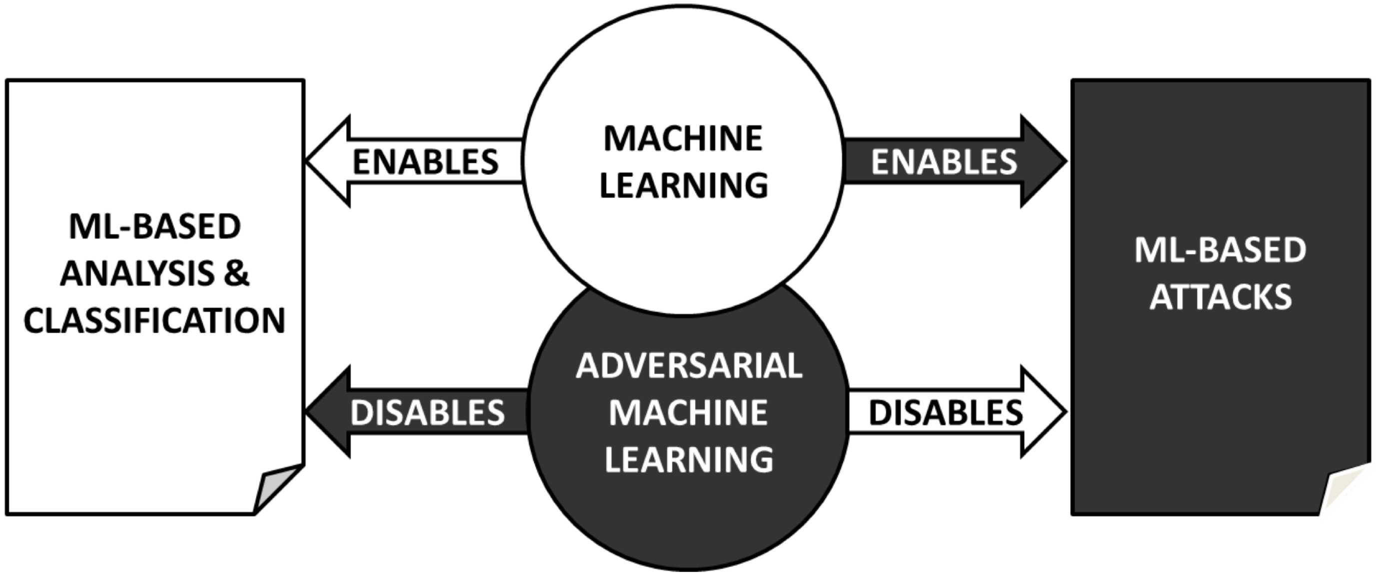
CDIS Spring Conference 2022
KTH Royal Institute of Technology
Tuesday, May 24, 2022

Overview

- Project goals
- Background on side-channel analysis
- Project results:
  - Saber power analysis
  - Saber amplitude-modulated EM emanations-based analysis
  - TRNG power analysis
  - USIM card power analysis
- Summary and future work

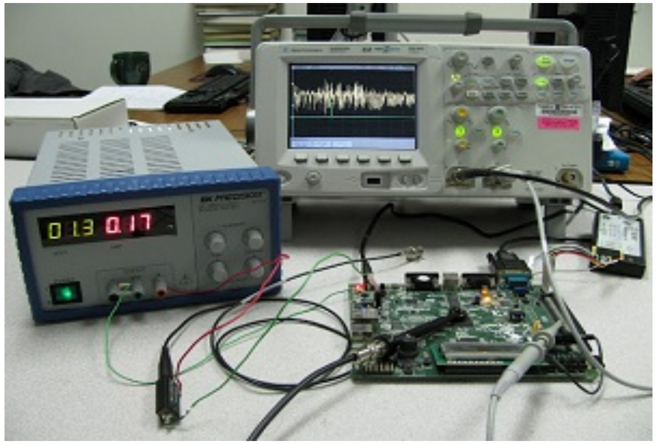
Project goals

- Develop new hardware security assessment methods
- Design countermeasures against side-channel attacks on implementations of cryptographic algorithms



How side-channel attacks work

- Crypto 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

Protected Saber side-channel analysis

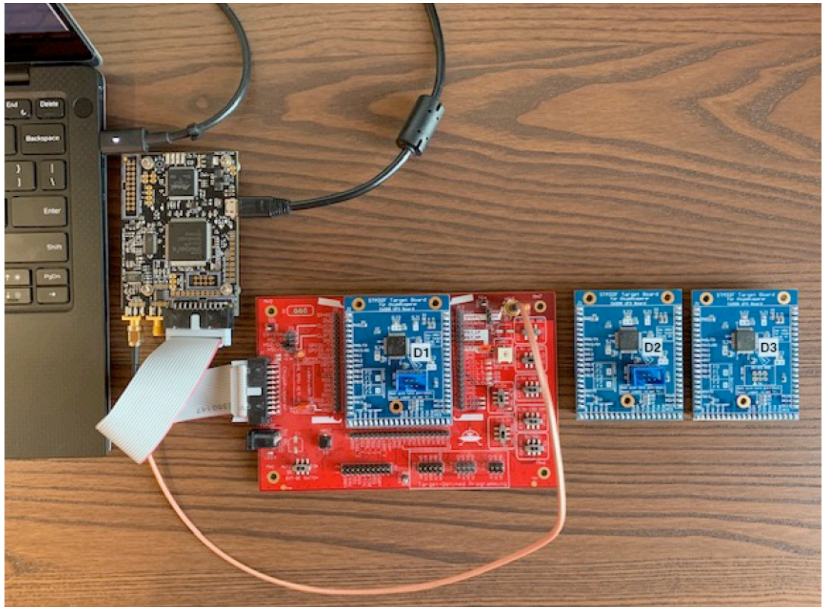


photo credit: Kalle Ngo

- Saber is one of the finalists of ongoing NIST post-quantum cryptography standartization competition
- Key Encapsulation Mechanism (KEM)
  - Security relies on the hardness of the Learning With Rounding (LWR) problem

1. *A Side-Channel Attack on a Masked IND-CCA Secure Saber KEM,* K. Ngo, E. Dubrova, Q. Guo, T. Johansson, Trans. on Cryptographic Hardware and Embedded Systems, 2021, 4, 676-707
2. *Breaking Masked and Shuffled CCA Secure Saber KEM by Power Analysis*, K. Ngo, E. Dubrova, T. Johansson, Workshop on Attacks and Solutions in Hardware Security, Nov. 19, 2021
3. *Side-Channel Analysis of Saber KEM Using Amplitude-Modulated EM Emanations*, R. Wang, K. Ngo, E. Dubrova, submitted to DSD'2022

Saber KEM algorithm

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

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

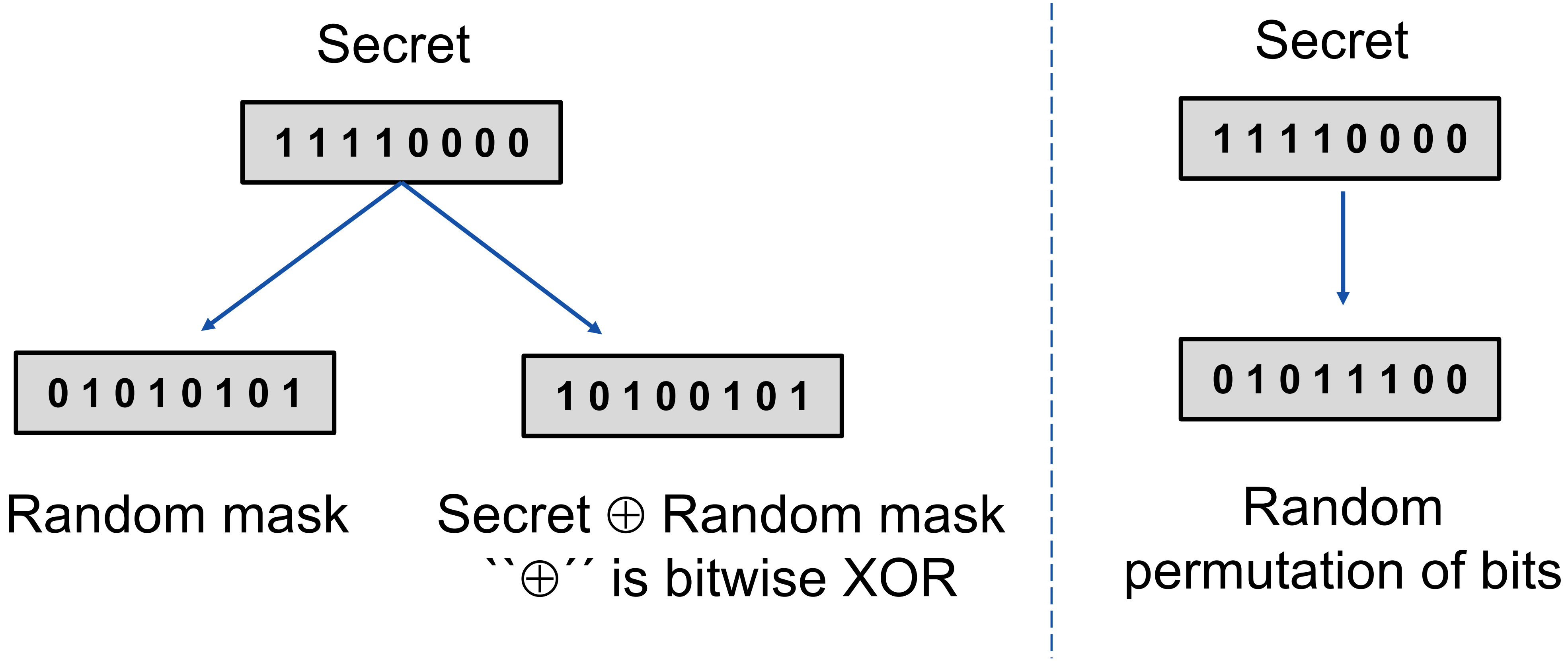
session key

public key secret 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

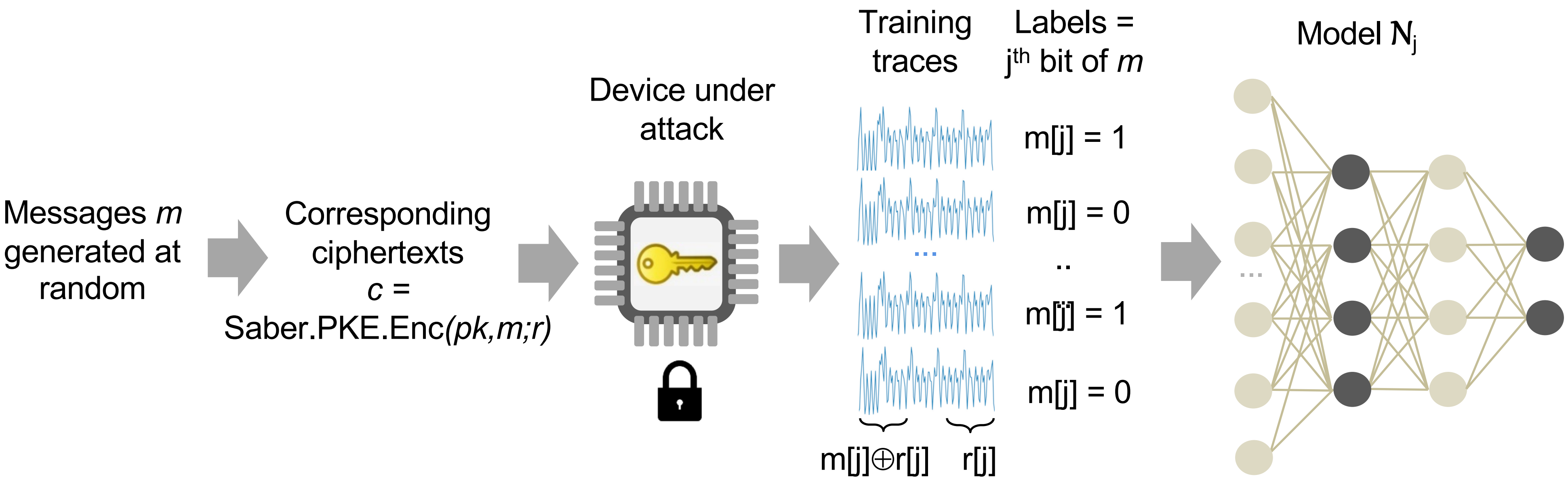
Masking and shuffling counteremeasures



Masking

Shuffling

How deep learning breaks masking



Empirical probability to recover a message bit from a single power trace

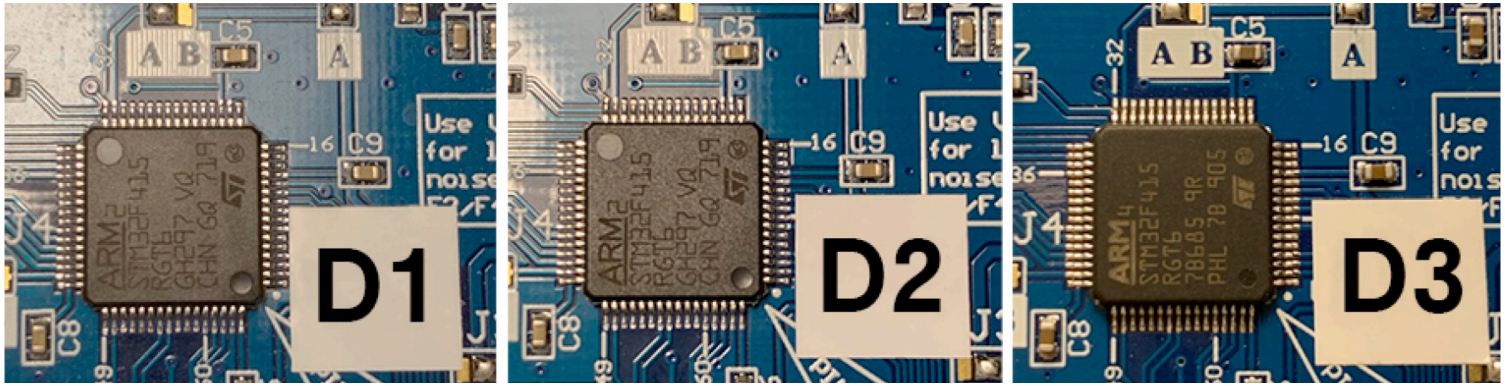
Device	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	average
D_1	0.993	0.999	0.998	1.000	0.997	0.998	0.999	0.995	0.997
D_2	0.987	0.998	0.999	0.999	0.997	0.998	0.998	0.999	0.997
D_3	0.982	0.966	0.976	0.962	0.966	0.954	0.968	0.941	0.964
average	0.987	0.988	0.991	0.987	0.987	0.983	0.988	0.978	0.986

used for training

similar to D_1

different from D_1

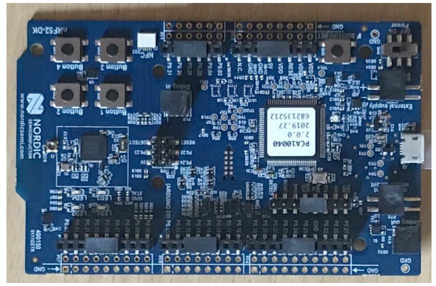
$0.9974^{256} = 0.5135$

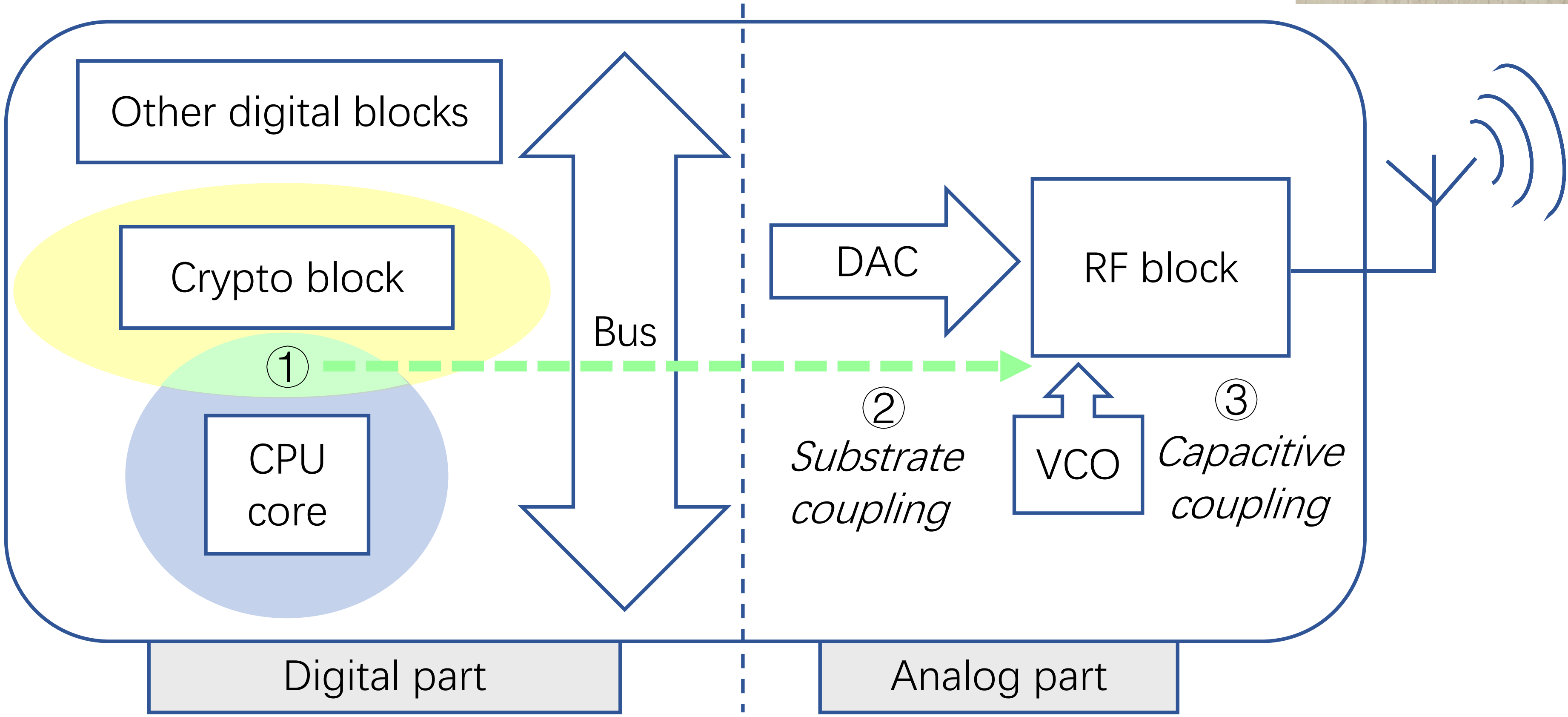


Secret key recovery

- Session key can be derived directly from the message
- Secret key can be recovered from
  - 24 chosen ciphertexts for a masked Saber
    https://www.youtube.com/watch?v=lZ3DbvDRfOQ&t=12s
  - 61,680 chosen ciphertexts for a masked and shuffled Saber
    https://youtu.be/LFCTiqvIask
- Ongoing work
  - analysing higher-order masking countermeasure
  - analysing an FPGA implementation of Saber
  - recovering shuffling indexes directly

Amplitude-modulated EM emanations based analysis of Saber





Sources of EM emanations in a mixed-signal circuit

Experimental setup

Grid Parabolic Antenna TL-ANT2424B

Ettus Research USRP N210 SDR

target board nRF52DK

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)

Empirical probability to recover a message bit from *M* EM traces captured by a coaxial cable from an unprotected Saber

M	1	10	20	30	40	50
14K	0.710	0.853	0.879	0.886	0.899	0.911
23K	0.700	0.840	0.890	0.898	0.915	0.921
32K	0.708	0.865	0.890	0.904	0.908	0.921
average	0.706	0.853	0.883	0.896	0.907	0.918

TRNG power analysis

- We can recover Hamming weight of 32-bit random numbers generated by the TRNG in a STM 32MCU with ≈ 80% probability

- First passive side-channel attack on a hardware TRNG in a commercial IC

"Side-Channel Analysis of the Random Number Generator in STM32 MCUs", K. Ngo, E. Dubrova,GLSVLSI'2022

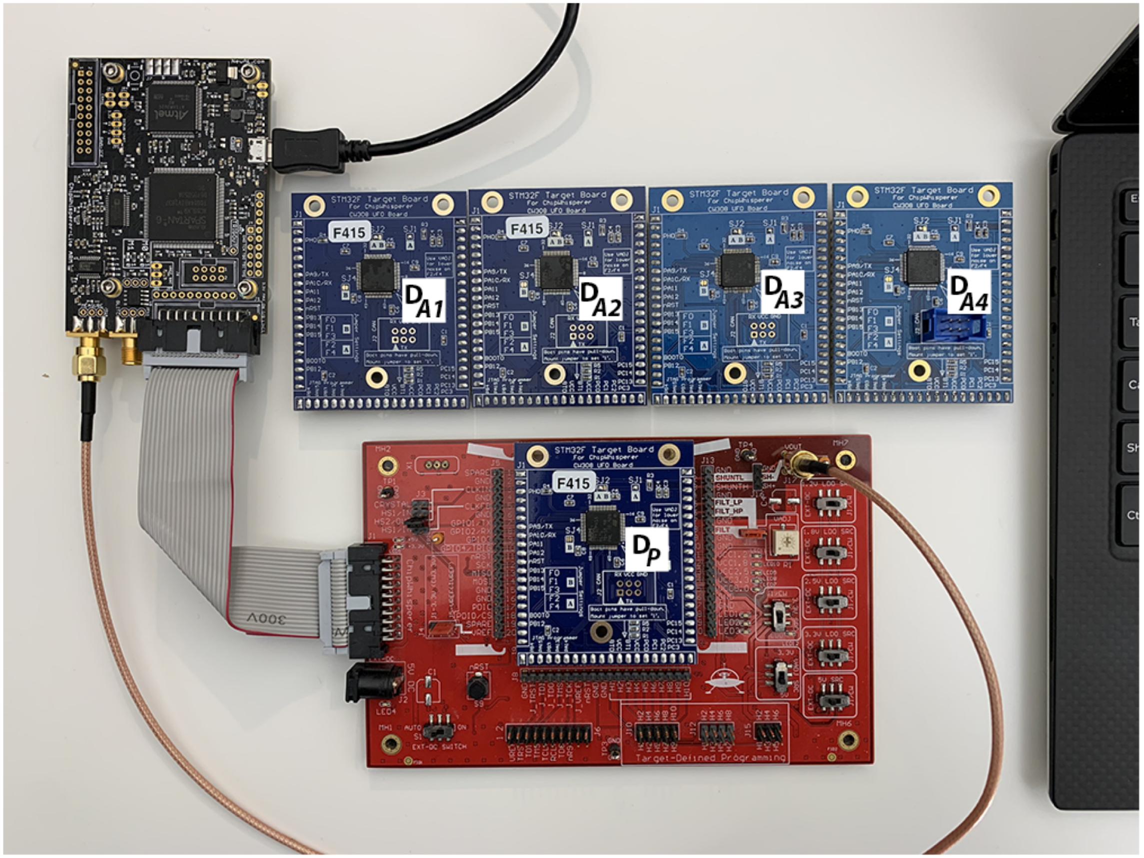
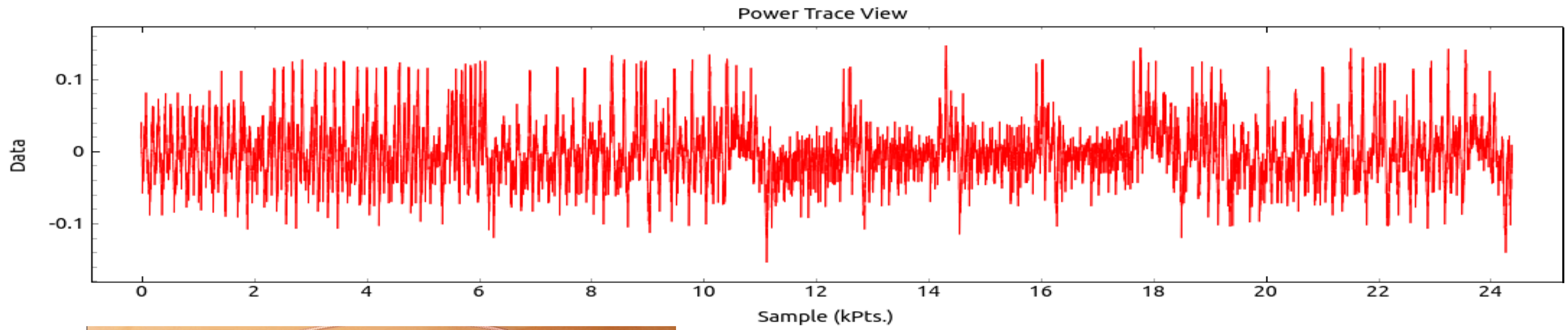


photo credit: Kalle Ngo

USIM card power analysis



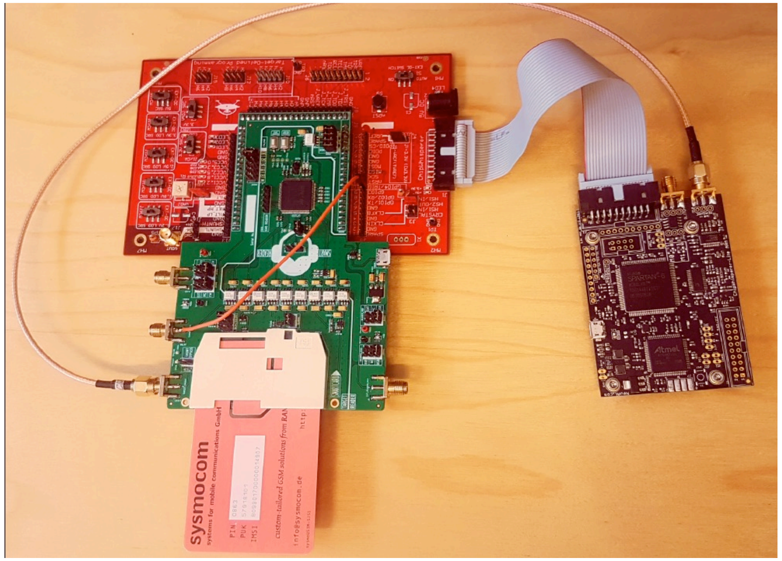
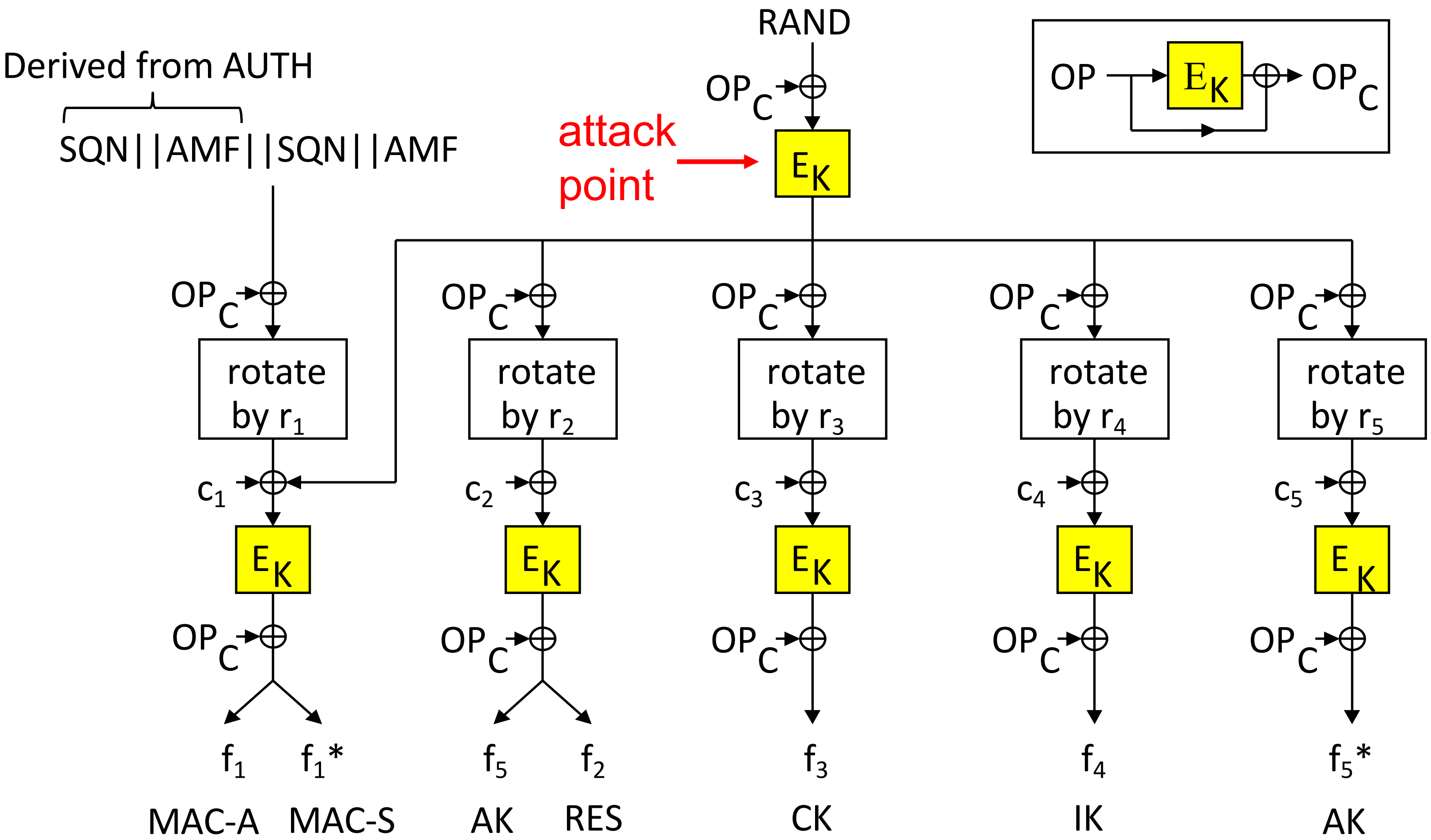


photo credit: Martin Brisfors

USIM's long-term key can be extracted by power analysis

1. *How Deep Learning Helps Compromising USIM*, M. Brisfors, S. Forsmark, E. Dubrova, CARDIS'2020
2. *Single-Trace Attacks on USIM: Myth or Reality?*, M. Brisfors, E. Dubrova, draft

MILENAGE algorithm



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

- See demo at:

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

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

→ Realistic threat

Summary and next steps

- Deep learning side-channel attacks are very powerful
- They can overcome traditional countermeasures such as
  - Masking
  - Shuffling
  - Random delay insertion
  - Noise-based
- Future work
  - Designing stronger, DL-resistant countermeasures
  - Neural network model extraction by side-channel analysis