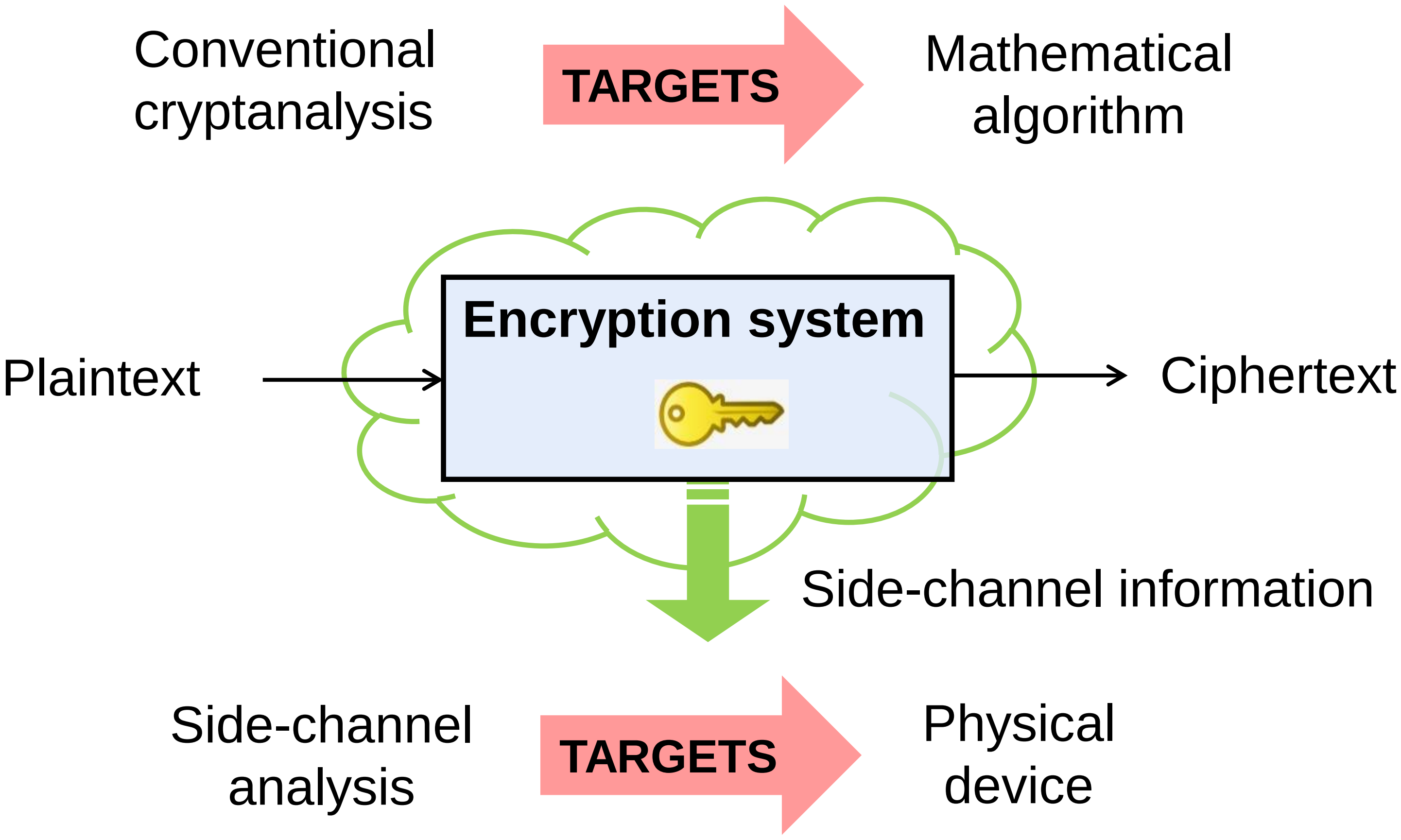
Side-Channel Vulnerability and Threat Analysis with Machine Learning in Focus

Elena Dubrova
School of Electrical Engineering and Computer Science
Royal Institute of Technology (KTH)

What is a side-channel attack?



Conventional cryptanalysis

TARGETS

Mathematical algorithm

Plaintext

Encryption system

Ciphertext

Side-channel information

Side-channel analysis

TARGETS

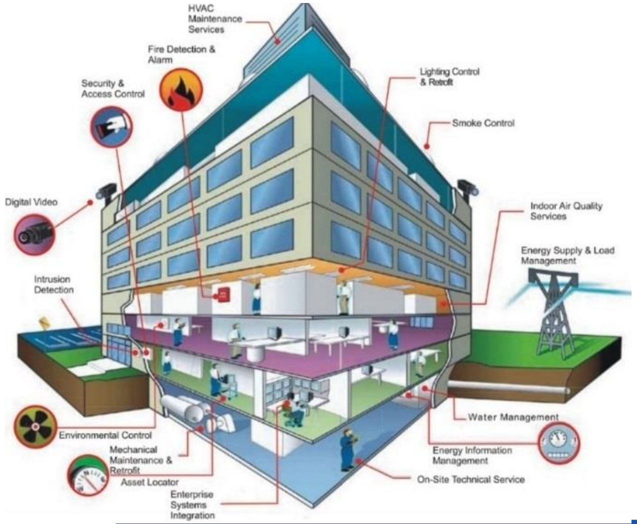
Physical device

Motivation: In the near future …

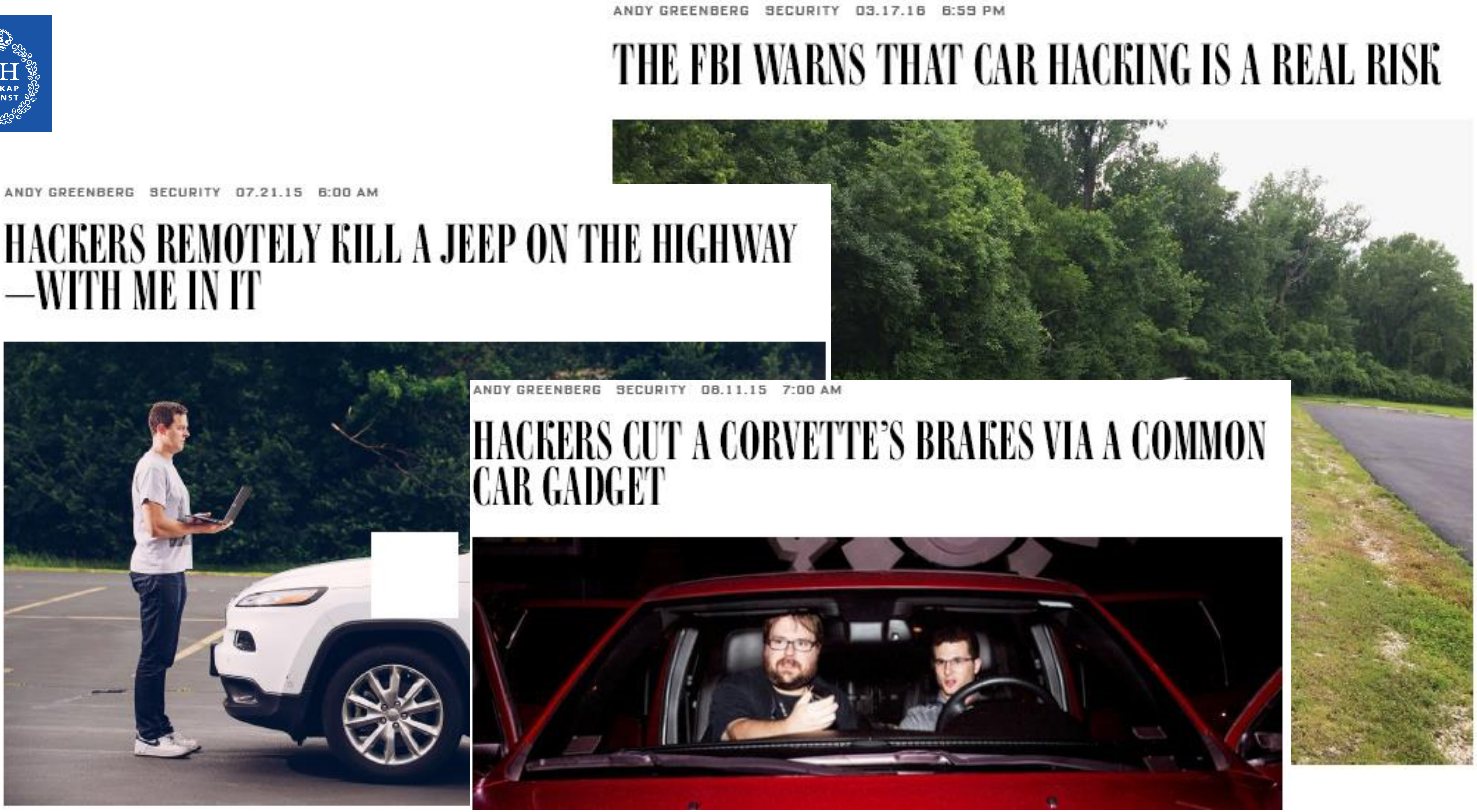
- Millions not so well protected Internet-connected devices will be involved in services related to confidential data
  - Wearables
  - Connected cars
  - Smart home

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

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


HVAC Maintenance Services
Fire Detection & Alarm
Security & Access Control
Lighting Control & Retrofit
Smoke Control
Digital Video
Indoor Air Quality Services
Energy Supply & Load Management
Intrusion Detection
Water Management
Environmental Control
Mechanical Maintenance & Retrofit
Energy Information Management
Asset Locator
On-Site Technical Service
Enterprise Systems Integration

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



ANDY GREENBERG SECURITY 03.17.16 6:59 PM

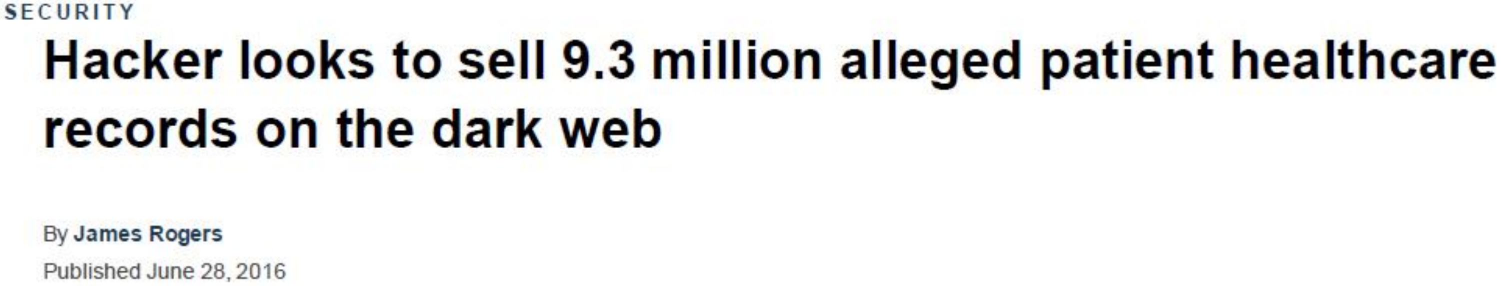
THE FBI WARNS THAT CAR HACKING IS A REAL RISK

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

MSB project structure

- 5-year project granted by MSB (2021-03-15 - 2026-03-14)
- Two partners:
  - **KTH**

    Elena Dubrova and one PhD student
  - **LTH**

    Thomas Johansson and one PhD student

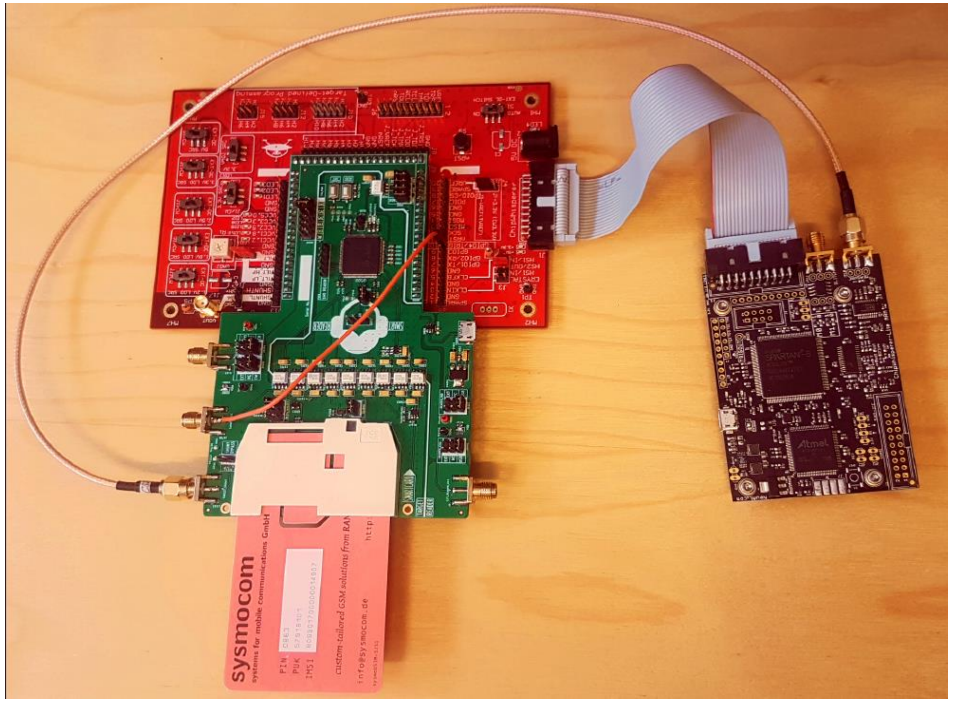


photo credit: Martin Brisfors

MSB project goals

- Advance state-of-the-art in side-channel analysis using the toolbox of machine learning
- Develop new methods for side-channel leakage assessment
- Design countermeasures against side-channel attacks and supporting tools

photo credit: Katerina Gurova

Results so far

3 journal and 5 conference/workshop papers published

1. A Side-Channel Attack on a Masked IND-CCA Secure Saber KEM, K. Ngo, E. Dubrova, Q. Guo, T. Johansson, TCHES’2021
2. A Key-Recovery Side-Channel Attack on Classic McEliece Implementations, Q. Guo, A. Johansson, T. Johansson, TCHES’2022
3. Don’t Reject This: Key-Recovery Timing Attacks Due to Rejection-Sampling in HQC and BIKE, Q. Guo, C. Hlauschek, T. Johansson, N. Lahr, A. Nilsson, R. L. Schröder, TCHES’2022
4. Breaking Masked and Shuffled CCA Secure Saber KEM by Power Analysis, K Ngo, E Dubrova, T. Johansson, ASHES’2021
5. Side-Channel Analysis of the Random Number Generator in STM32 MCUs, K. Ngo, E. Dubrova, GLSVLSI’2022
6. Side-Channel Analysis of Saber KEM Using Amplitude-Modulated EM Emanations, R. Wang, K. Ngo and E. Dubrova, DSD’2022
7. A Message Recovery Attack on LWE/LWR-Based PKE/KEMs Using Amplitude-Modulated EM Emanations, R Wang, K Ngo, E Dubrova, ICISC’2022
8. Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste, E Dubrova, K Ngo, J Gärtner, Real World Crypto Symposium 2023

Side-channel analysis of CRYSTALS-Kyber

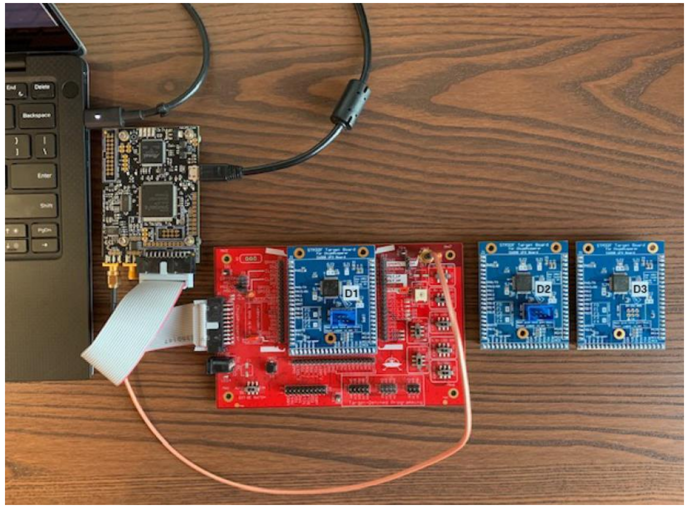
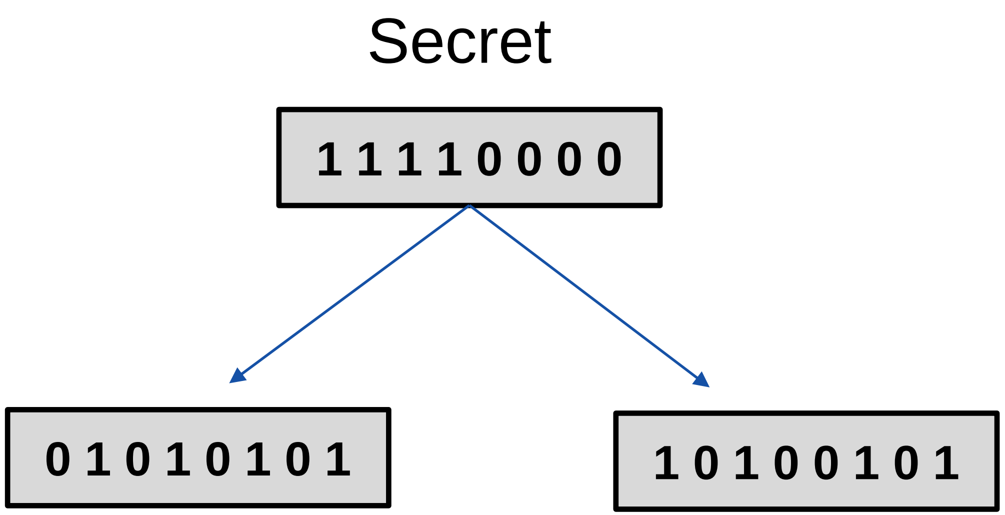


photo credit: Kalle Ngo

- In July 2022 NIST selected CRYSTALS-Kyber as a new public-key encryption and key encapsulation algorithm to be standartized
- NSA included CRYSTALS-Kyber in the suite of cryptographic algorithms recommended for national security systems

1. Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste, E Dubrova, K Ngo, J Gärtner, RWC’2023
2. A Message Recovery Attack on LWE/LWR-Based PKE/KEMs Using Amplitude-Modulated EM Emanations, R Wang, K Ngo, E Dubrova, ICISC’2022
3. Secret Key Recovery Attacks on Masked and Shuffled Implementations of CRYSTALS-Kyber and Saber**,** *L. Backlund, K. Ngo, J.* Gärtner, E. Dubrova, submittted to DAC’2023
4. A Side-Channel Attack on a Hardware Implementation of CRYSTALS-Kyber, Y. Ji, R. Wang, K. Ngo, E. Dubrova, L. Backlund, submitted to ETS’2023
5. Higher-Order Boolean Masking Does Not Prevent Side-Channel Attacks on LWE/LWR-based PKE/KEMs, K. Ngo, R. Wang, E. Dubrova, N. Paulsrud, submitted to ISMVL’2023

Masking and shuffling counteremeasures



Secret

1 1 1 1 0 0 0 0

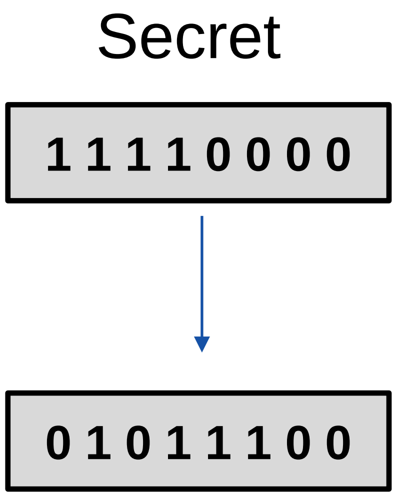
0 1 0 1 0 1 0 1

1 0 1 0 0 1 0 1

Random mask

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

Masking (first-order)



Secret

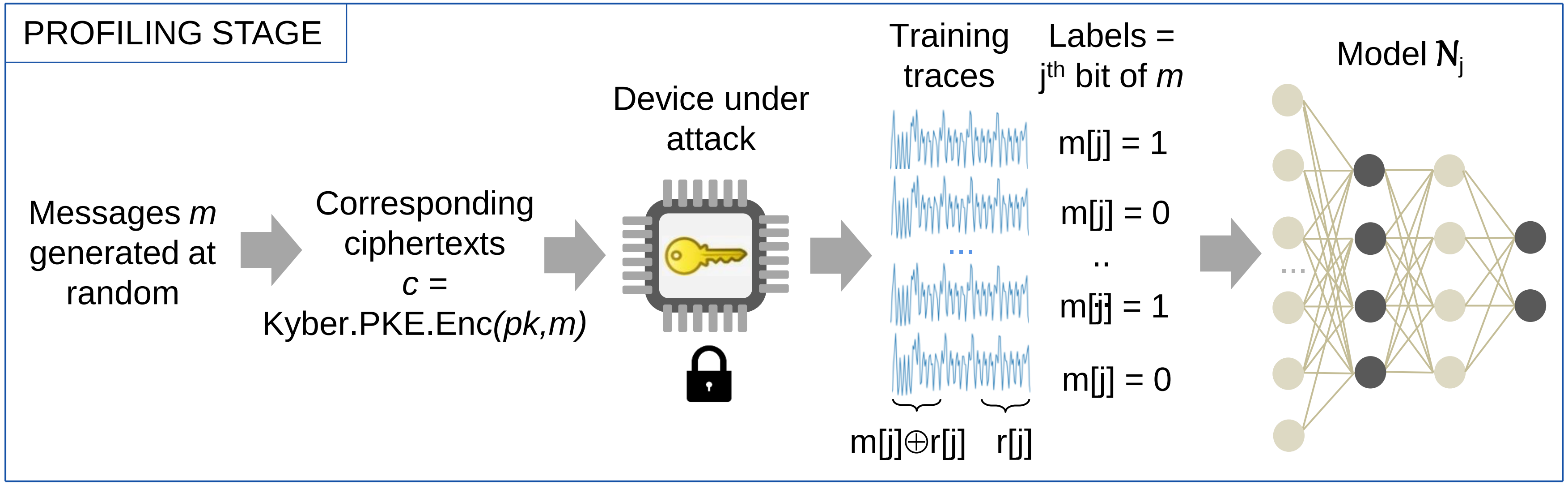
1 1 1 1 0 0 0 0

0 1 0 1 1 1 0 0

Random
permutation of bits

Shuffling

How deep learning helps break masking



PROFILING STAGE

Messages *m* generated at random

Corresponding ciphertexts *c* = Kyber.PKE.Enc*(pk,m)*

Device under attack

Training traces

Labels = j^{th} bit of *m*

m[j] = 1

m[j] = 0

..

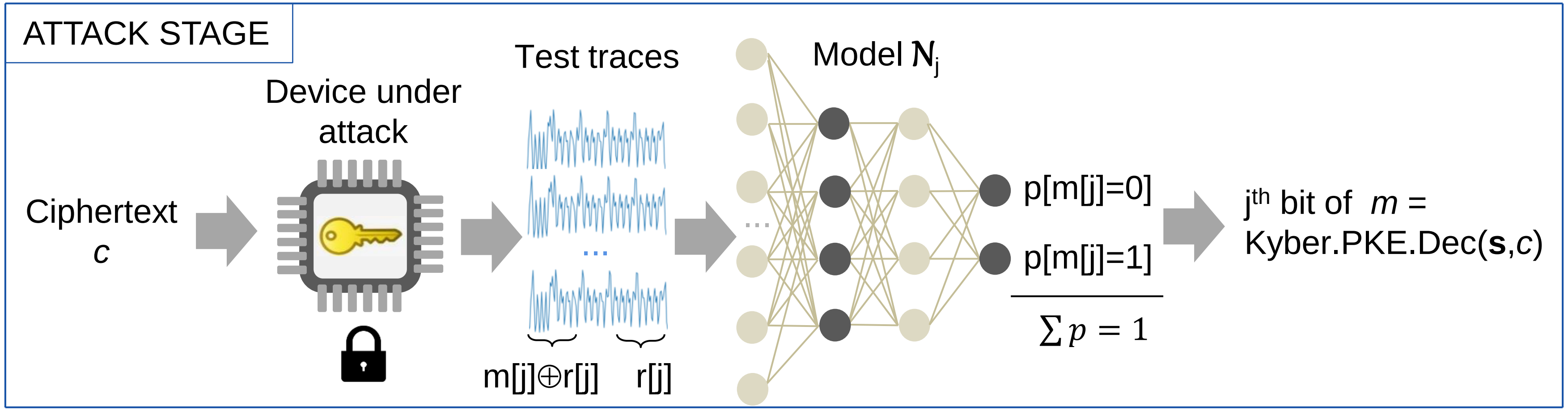
m[j] = 1

m[j] = 0

m[j]⊕r[j]

r[j]

Model $\mathbf{N}_j$



ATTACK STAGE

Ciphertext *c*

Device under attack

Test traces

m[j]⊕r[j]

r[j]

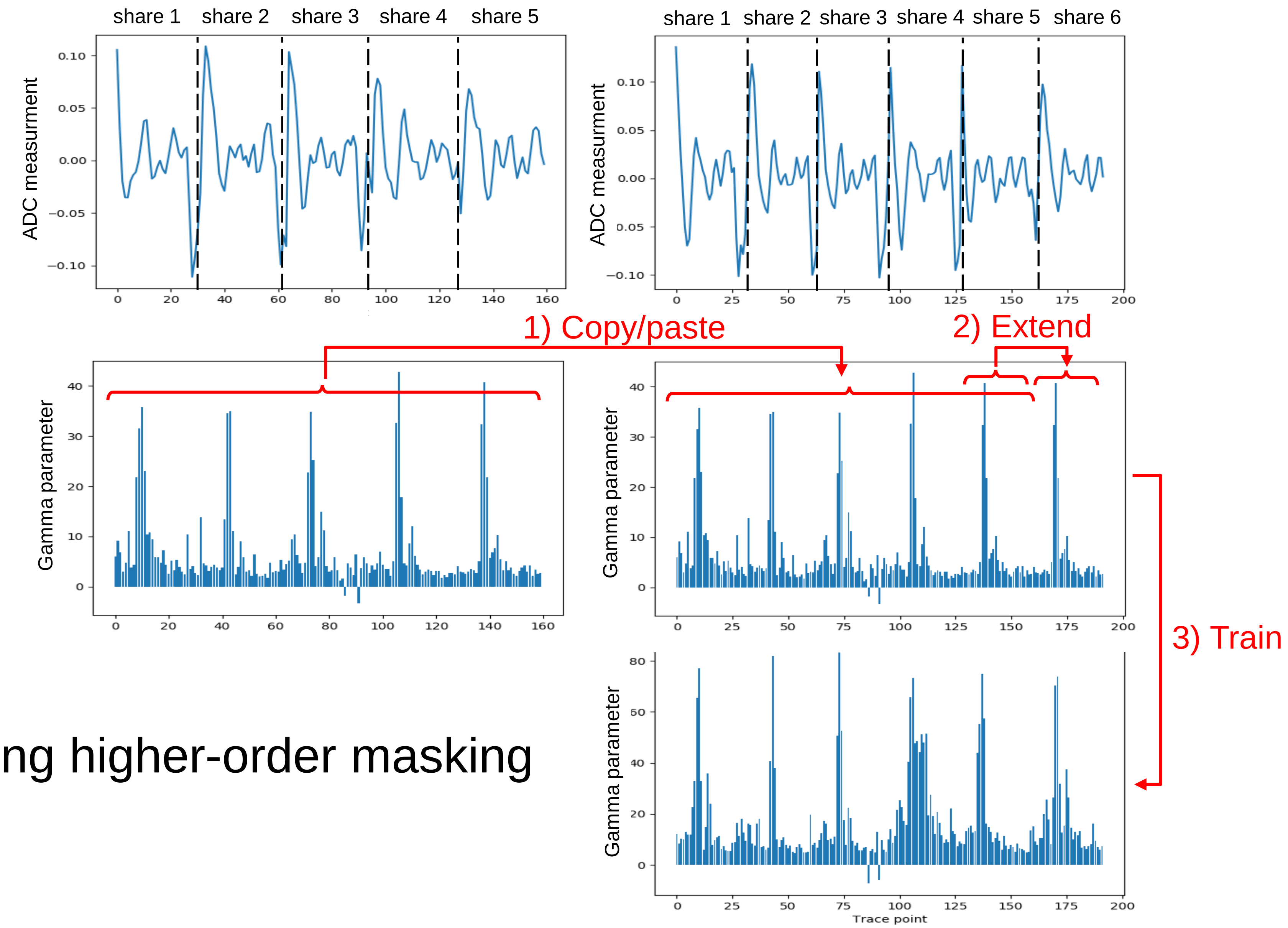
Model $\mathbf{N}_j$

p[m[j]=0]

p[m[j]=1]

$\sum p = 1$

j^{th} bit of *m* = Kyber.PKE.Dec(**s**,*c*)



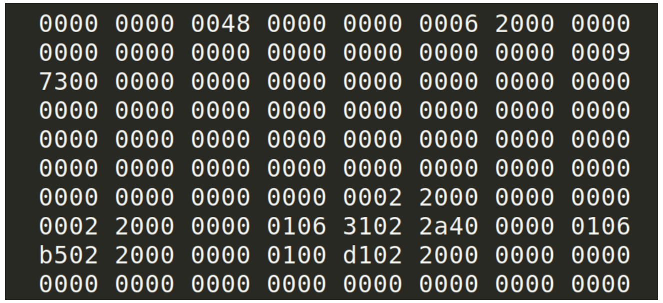
Breaking higher-order masking

Securing Reconfigurable Hardware in the Era of AI

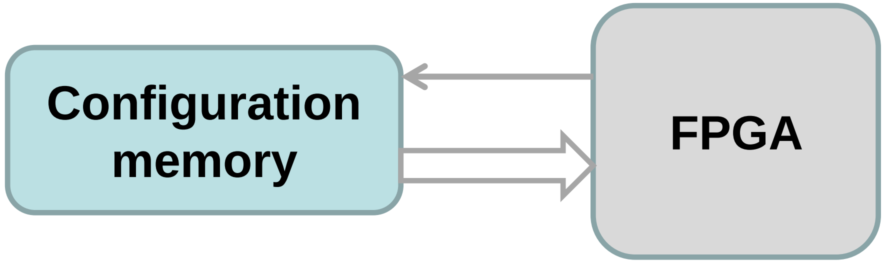
Elena Dubrova
School of Electrical Engineering and Computer Science
Royal Institute of Technology (KTH)

FPGA background

- Reconfigurable hardware, such as Field Programmable Gate Arrays (FPGAs), is widely used for implementing cryptographic algorithms and accelerating AI-related workloads
- Available countermeasures do not provide adequate protection against physical attacks using ML techniques



```
0000 0000 0048 0000 0000 0006 2000 0000
0000 0000 0000 0000 0000 0000 0000 0009
7300 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0002 2000 0000 0000
0002 2000 0000 0106 3102 2a40 0000 0106
b502 2000 0000 0100 d102 2000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
```



VINNOVA project structure

- 26 months project granted by VINNOVA (2021-07-01 - 2023-08-31)
- Two partners:
  - **KTH**

    Elena Dubrova and two PhD students
  - **Ericsson**

    Håkan Englund and Niklas Lindskog, Platform Security Group, Ericsson Research

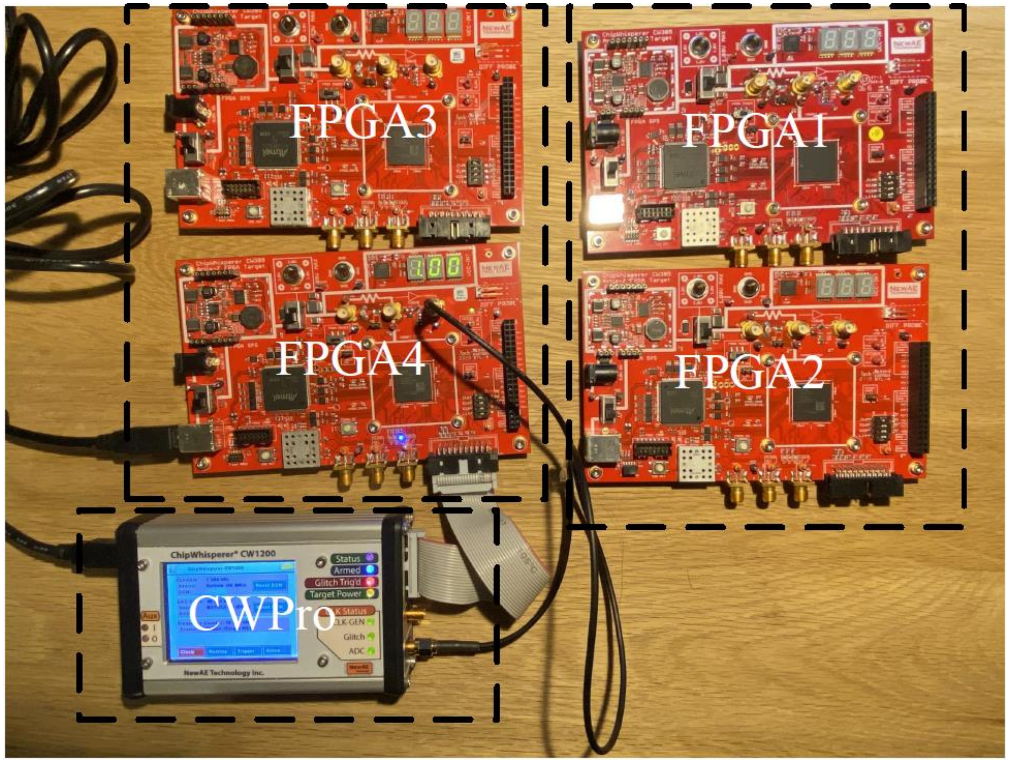
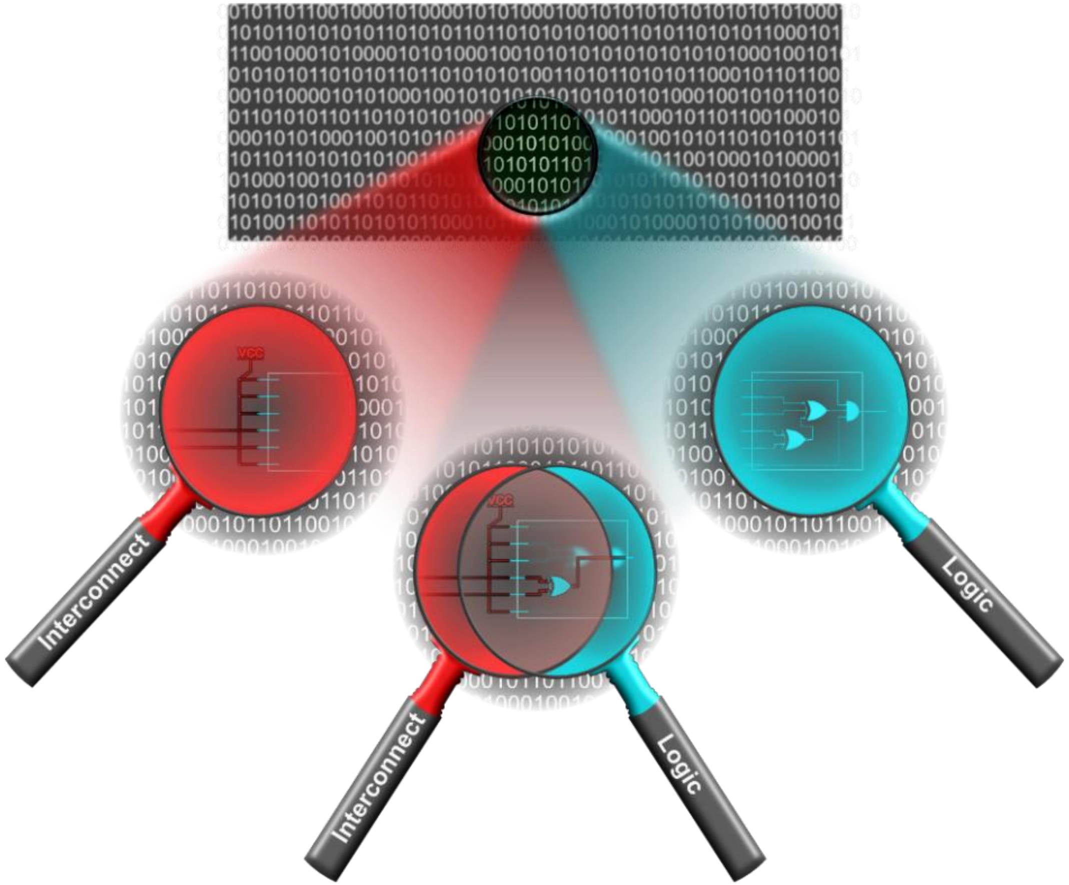


photo credit: Yang Yu

VINNOVA project goals

- Develop new FPGA security assessment methods
- Design countermeasures against physical attacks on FPGA implementations



picture credit: Michail Moraitis

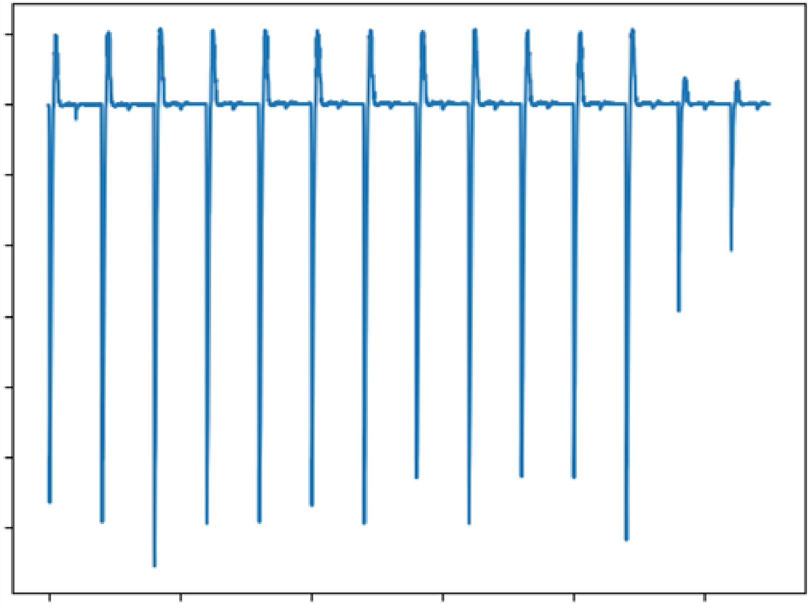
Results so far

- 6 patent applications submitted
- 1 journal and 3 conference papers published

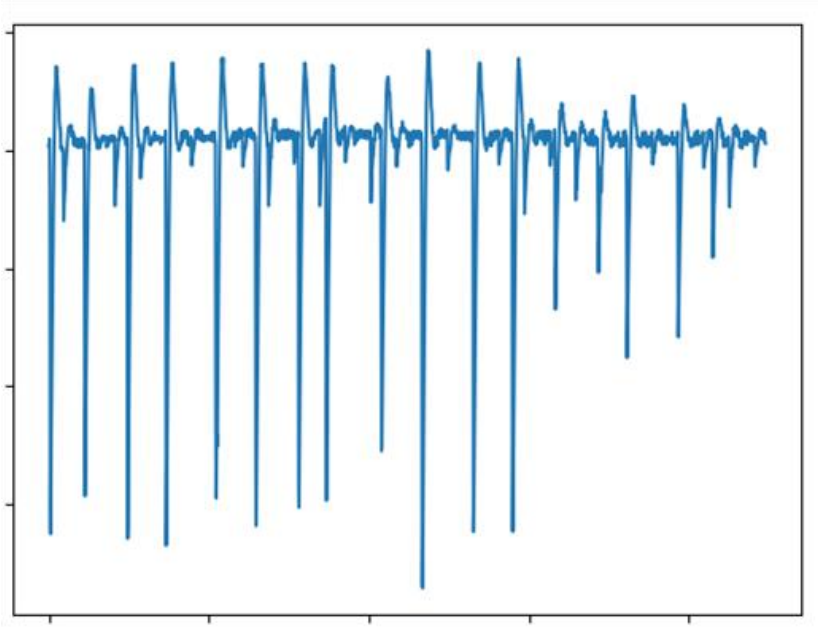
1. FPGA Design Deobfuscation by Iterative LUT Modifications at Bitstream Level, M Moraitis, E Dubrova, Journal of Hardware Security, 2023
2. Do Not Rely on Clock Randomization: A Side-Channel Attack on a Protected Hardware Implementation of AES, M. Brisfors, M. Moraitis, E Dubrova, FPS’2022
3. Towards Generic Power/EM Side-Channel Attacks: Memory Leakage on General-Purpose Computers, C. Aknesil, E. Dubrova, VLSI-SOC’2022
4. A Side-Channel Resistant Implementation of AES Combining Clock Randomization with Duplication ", M. Moraitis, M. Brisfors, E. Dubrova, N. Lindskog, H. Englund, ISCAS'2023

Clock randomization countermeasure (Kocher'99)

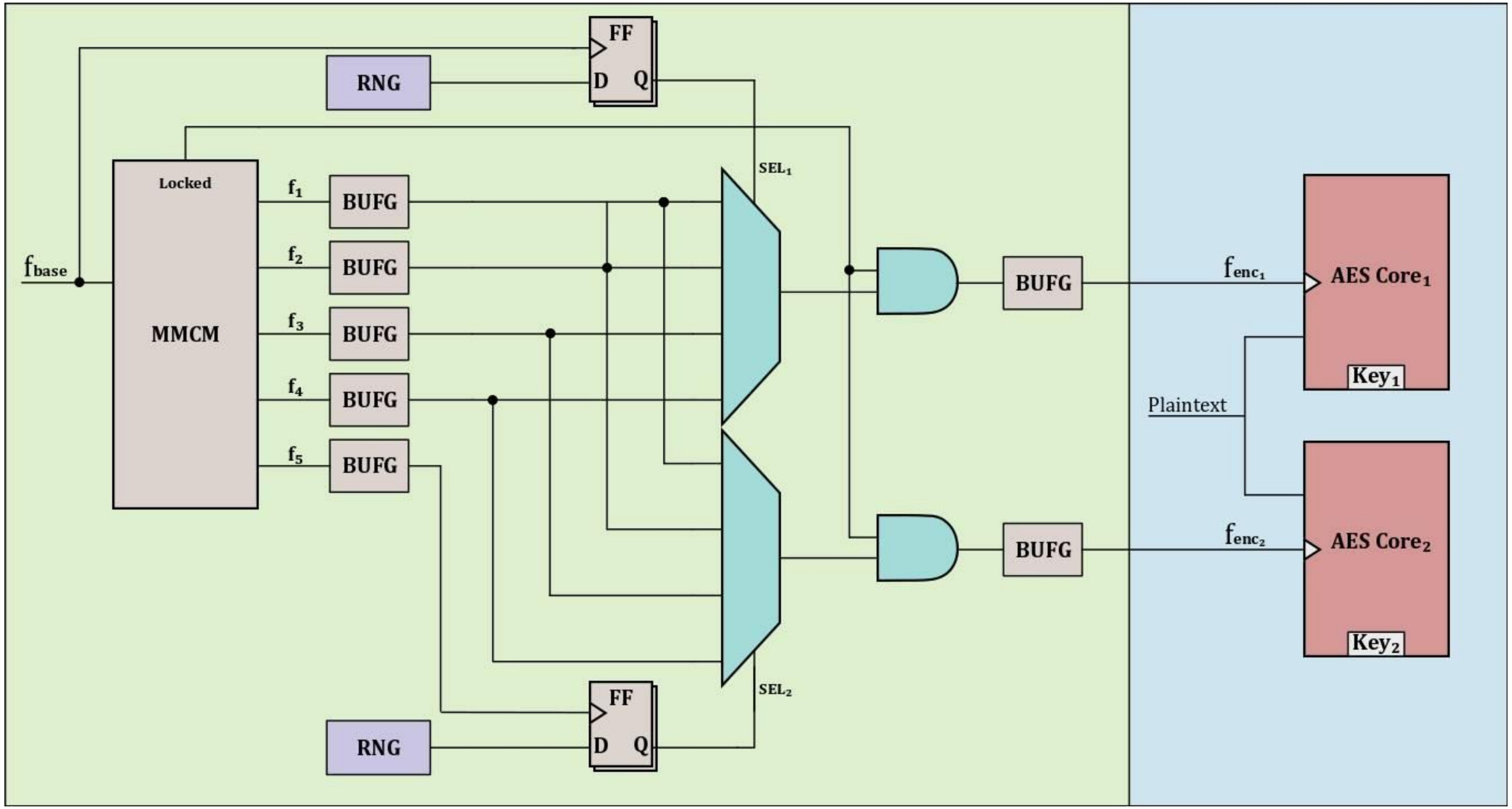
Stable clock power trace



Randomized clock power trace



New counteremeasure



AES key recovery

AES-128 Implementation	# Power traces (mean for 1000 tests)
Unprotected	116
Duplicated with stable clock	220
Duplicatied with one randomized clock	265
Duplicatied with two randomized clocks	-

Advantages of new countermeasure:

- Simplicity of implementation
- Application independence
- Glitch immunity
- Universality of coverage

Summary

Current status:

- Deep learning side-channel attacks are very powerful; they can overcome traditional countermeasures such as masking, shuffling, randomized clock, etc.
- We introduced a DL-resistant countermeasure suitable for hardware implementations

Future steps:

- Develop DL-resistant countermeasure suitable for software implementations

KTH VETENSKAP OCH KONST

VINNOVA

MSB Myndigheten för samhällsskydd och beredskap

Thank you!

CDIS

TECOSA

Vetenskapsrådet