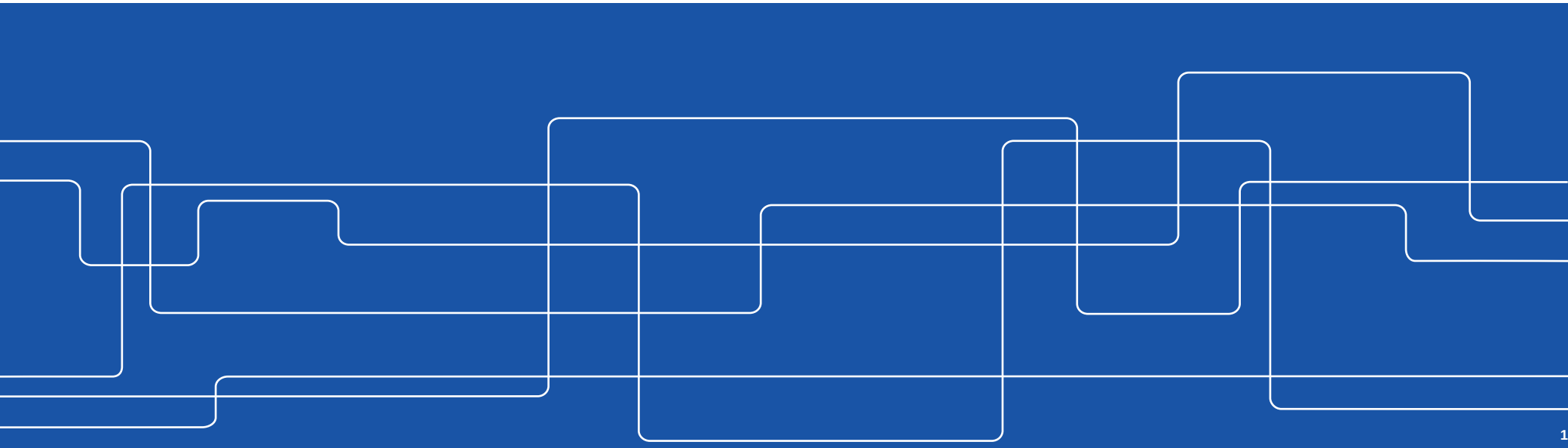
Securing Reconfigurable Hardware in the Era of AI

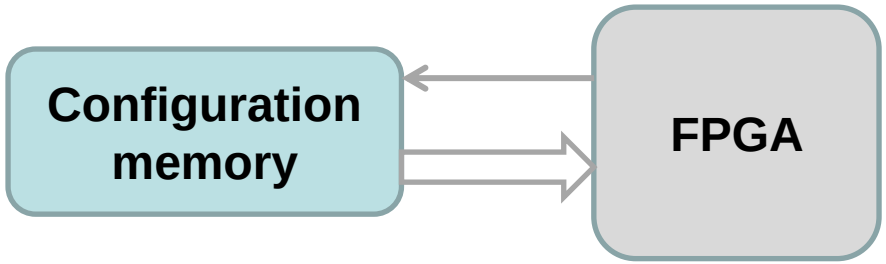
Elena Dubrova
School of Electrical Engineering and Computer Science
Royal Institute of Technology (KTH)



Motivation

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

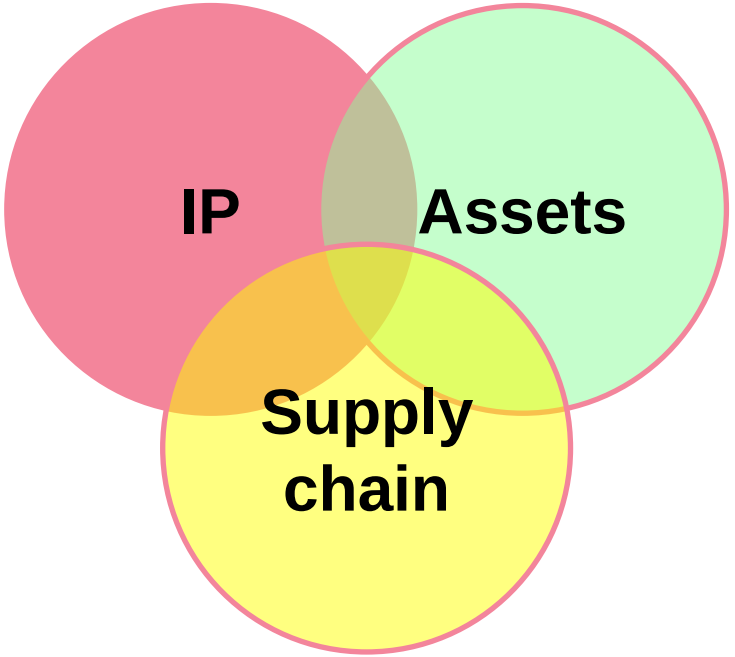
```
0000 0000 0048 0000 0000 0006 2000 0000
0000 0000 0000 0000 0000 0000 0000 0009
7300 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0002 2000 0000 0000
0002 2000 0000 0106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

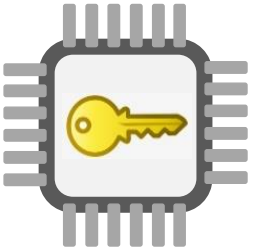


What needs protection?

Saab@MarcusWandt

Proprietary designs
Proprietary algorithms
Proprietary bitstreams

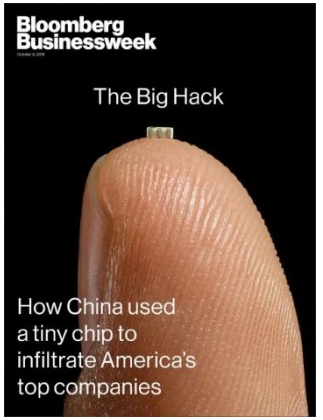




On-device data
On-device keys

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

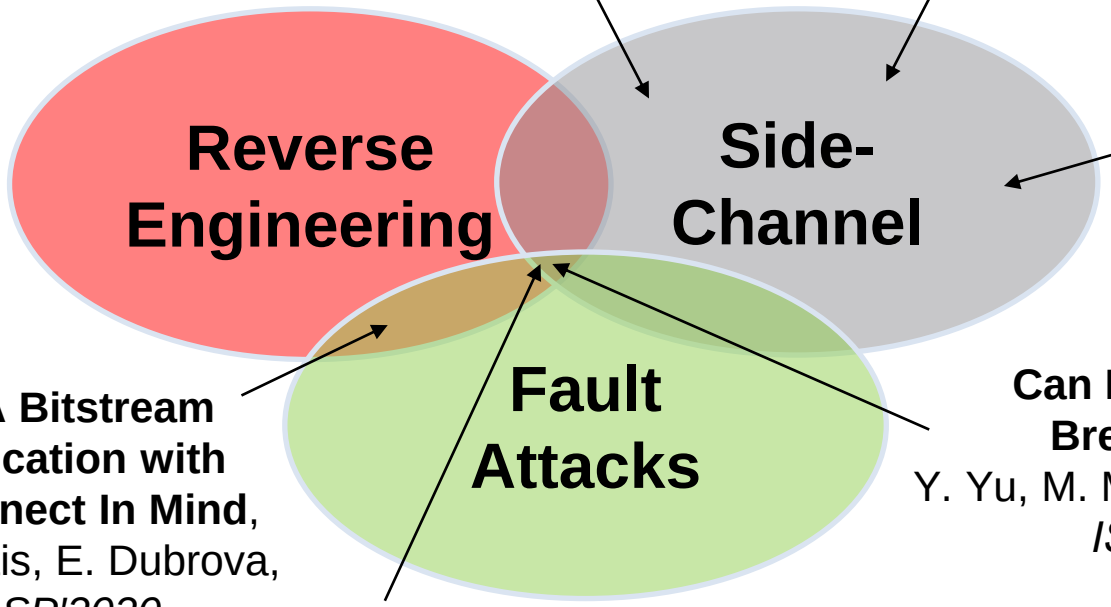
Preventing Hardware Trojans, counterfeit, overproduction



Physical attacks vectors

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

A Side-Channel Attack on a Masked IND-CCA Secure Saber KEM, K. Ngo, E. Dubrova, Q. Guo, T. Johansson, *CHES'2021*



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

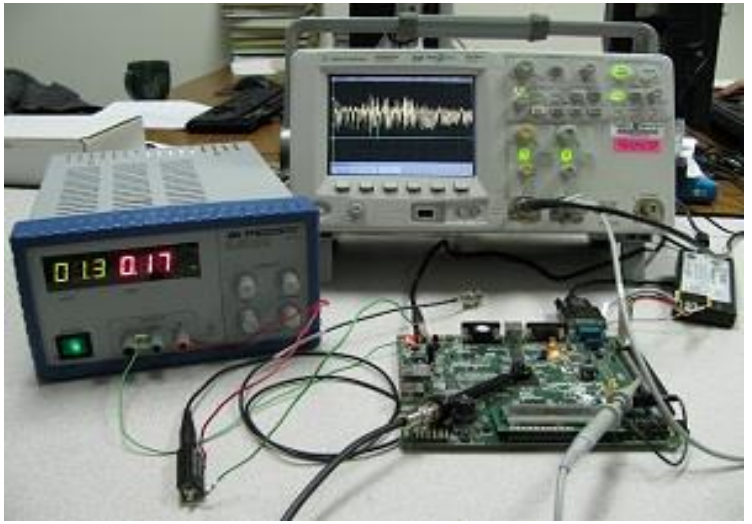
FPGA Bitstream Modification with Interconnect In Mind, M. Moraitis, E. Dubrova, *HASP'2020*

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*

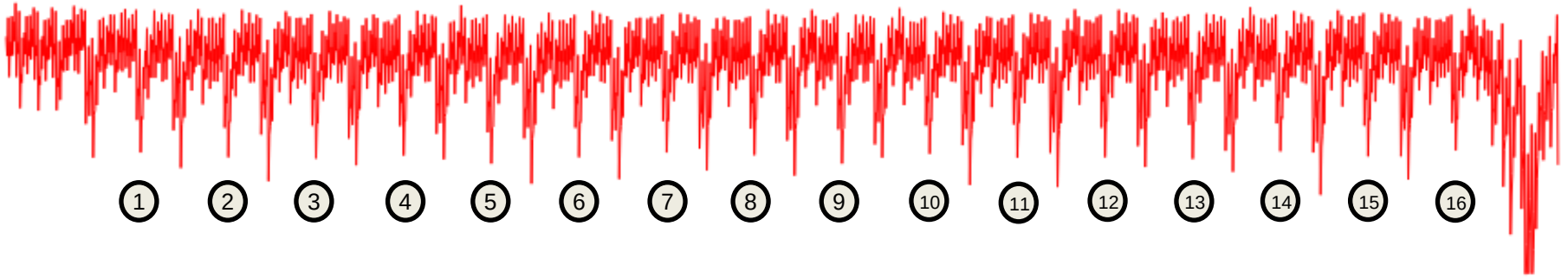
How side-channel attacks work

- Algorithms are implemented in physical devices which leak side-channel information
- It may be possible to recognize which data is processed by the device by measuring
  - Power consumption
  - Electromagnetic emission
  - Timing
  - …
- If data involves the secret key, the key may be recovered

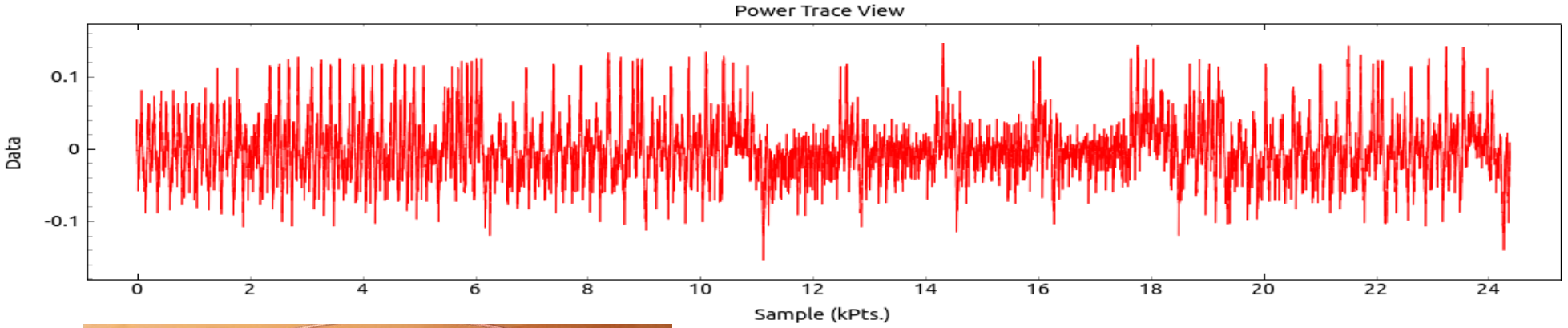


source: hackaday.com

Power trace representing 16 executions of AES S-box on 8-bit MCU (ATXmega128D4)



Previous related work: USIM power analysis



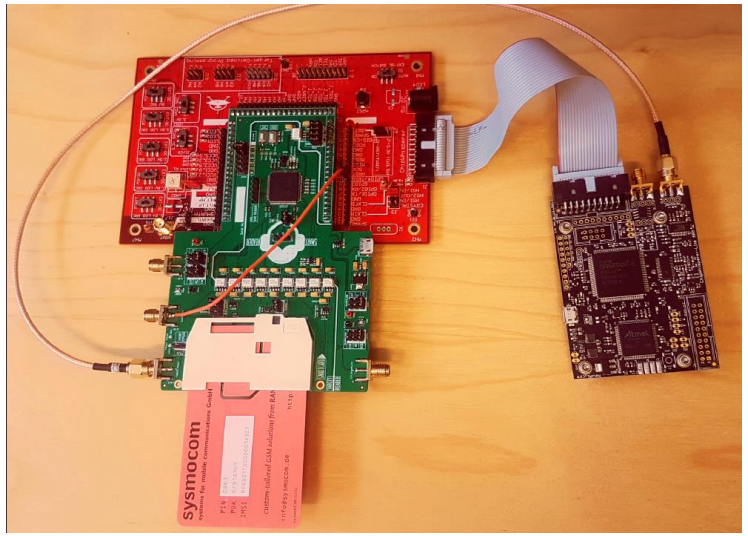


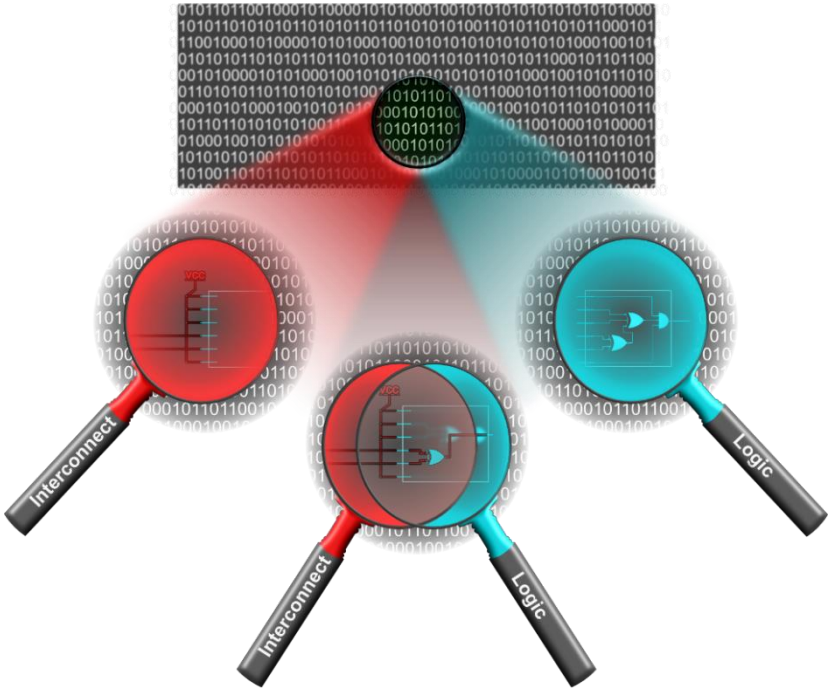
photo credit: Martin Brisfors

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

Project goal

- Develop new hardware security assessment methods
- Design countermeasures against physical attacks on FPGA implementations
  - Secret key recovery
  - Neural network model extraction
  - Bitstream modification



picture credit: Michail Moraitis

Project structure

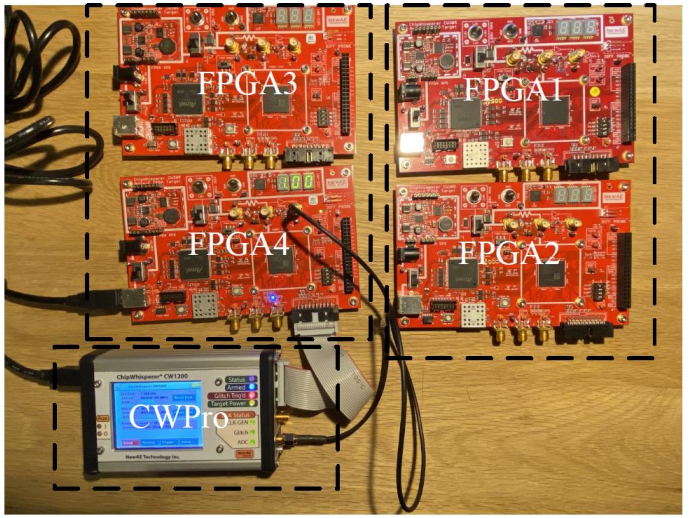


photo credit: Yang Yu

- 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

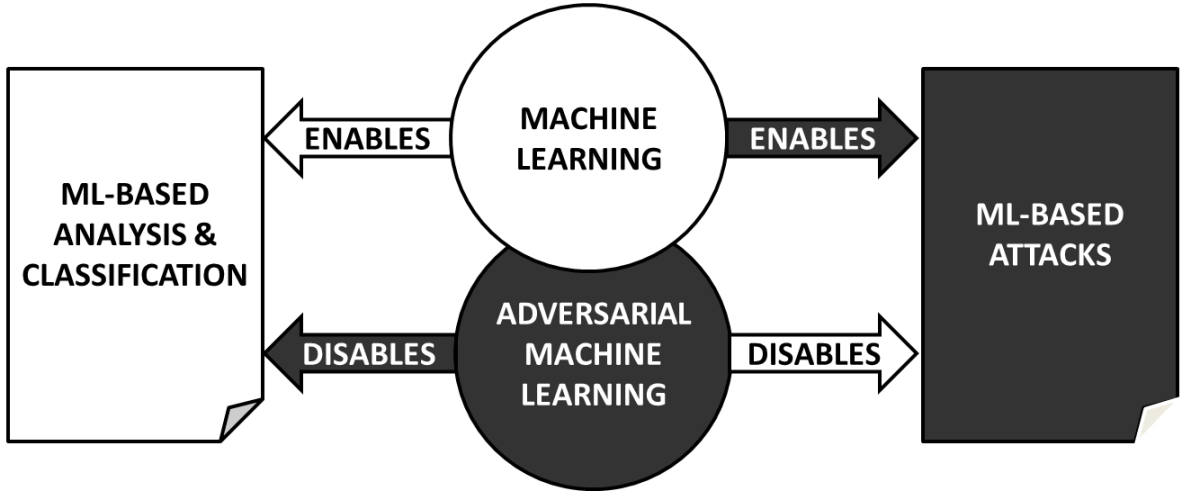
Results so far

- Work ongoing on:
  - Assesing security of bitstream encryption in Xilinx FPGAs
  - Designing countermeasures against bitstream modification
  - Searching for tamper-resistant key storage methods
- Dissemination activities
  - Hardware security course is offered as a Lifelong Learning course at KTH from 2020
  - Article in October issue of Elektroniktidningen

https://issuu.com/etndigi/docs/etn2110ld

Summary and next steps

- Deep learning side-channel attacks are very powerful, they can overcome traditional countermeasures
  - Masking, shuffling, noise addition, …
- We need to understand 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

Saber Key Recovery demo:

https://youtu.be/5ydQAenyGSQ