Radboud University

The Chip, Mia and the Table

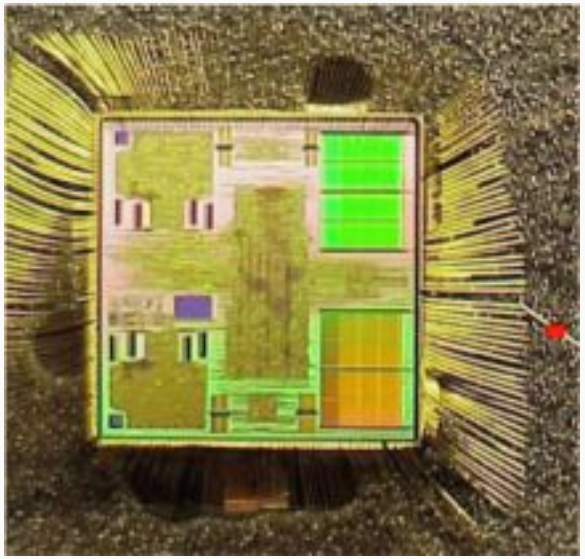
Lejla Batina

March 4, 2020

Institute for Computing and Information Sciences
Radboud University

High-Tech Women in Science and Technology
March 4, 2020, Darmstadt

The Chip, Mia and the Table



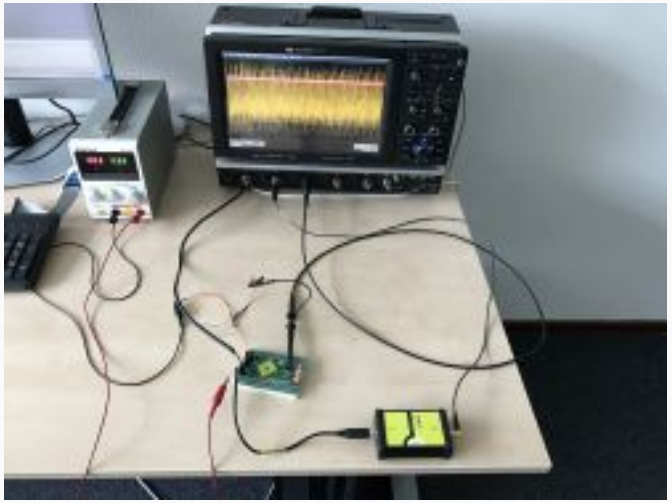
Opening

“So, you want to be a cryptographer”, Bruce Schneier’s newsletter, Oct. 1999

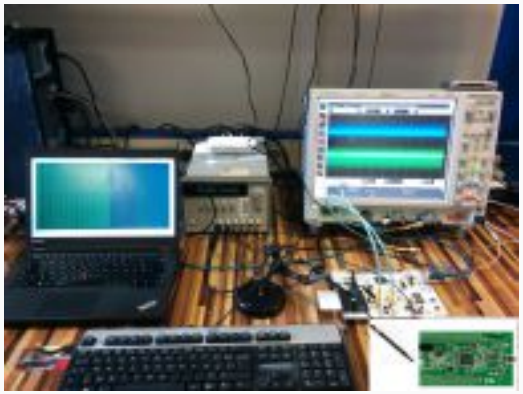
Crypto devices

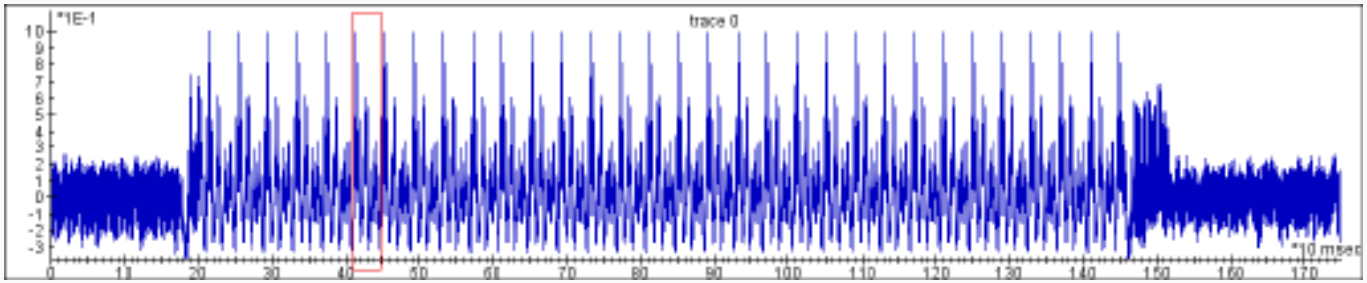
Critical infrastructure, human SCADA systems, IoT devices

Side-channel attacks

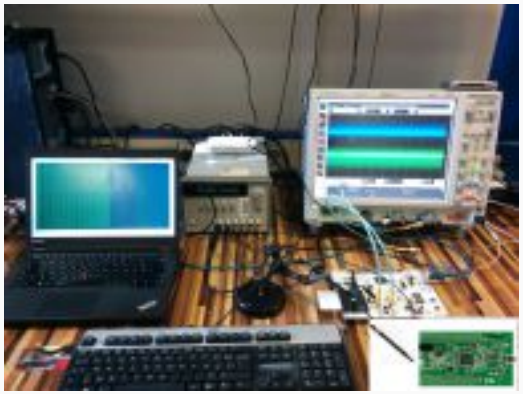


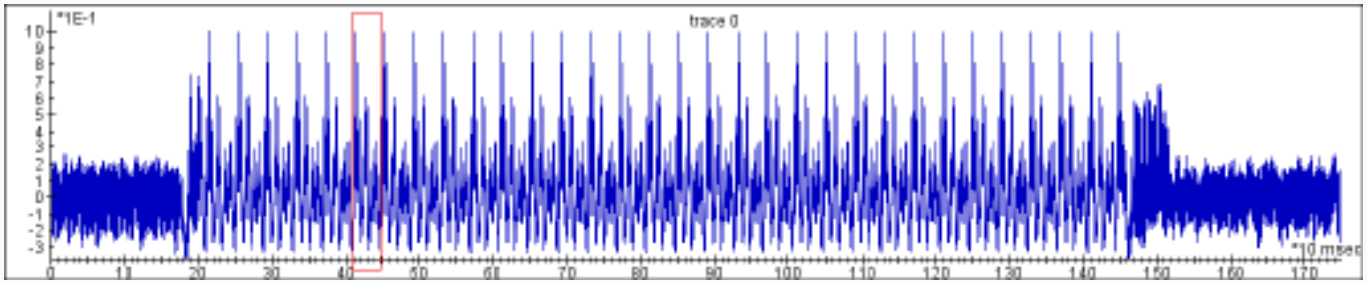
Using physical leakages





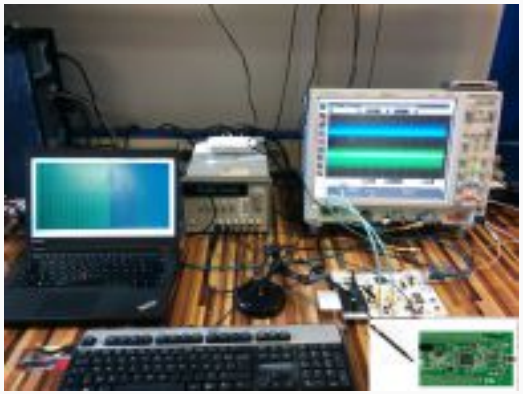
Using physical leakages

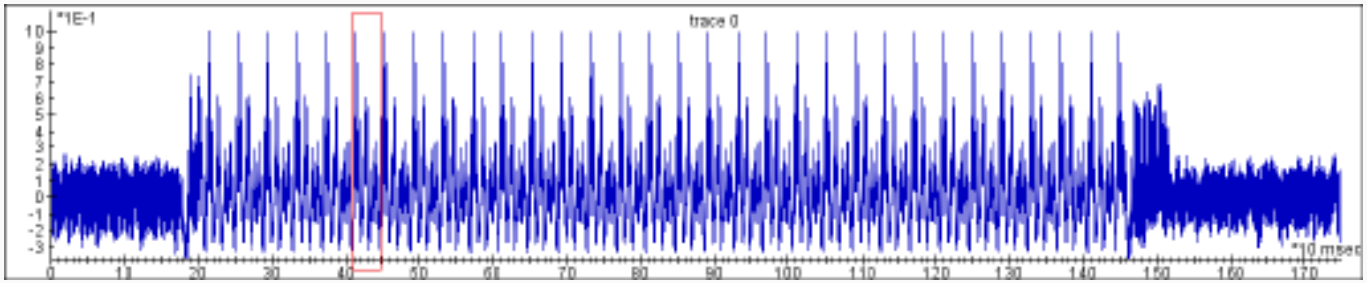




- Recovering secrets through timing, power consumption, EM

Using physical leakages





- Recovering secrets through timing, power consumption, EM
- Often, optimizations enable leakages

Relevance

September 3, 2019

Research Post: Cache Attacks on CTR_DRBG - Forgotten Assumptions

This post presents results from our paper "Pseudorandom Black Swans: Cache Attacks on CTR_DRBG". We illustrate how omissions in...

security.cohney.info

Relevance

September 3, 2019

Research Post: Cache Attacks on CTR_DRBG - Forgotten Assumptions

This post presents results from our paper "Pseudorandom Black Swans: Cache Attacks on CTR_DRBG". We illustrate how omissions in...

security.cohney.info

October 3, 2019

Relevance

November 13, 2019

September 3, 2019

Research Post: Cache Attacks on CTR_DRBG - Forgotten Assumptions

This post presents results from our paper "Pseudorandom Black Swans: Cache Attacks on CTR_DRBG". We illustrate how omissions in...

security.cohney.info

October 3, 2019

Relevance

November 13, 2019

September 3, 2019

Research Post: Cache Attacks on CTR_DRBG - Forgotten Assumptions

This post presents results from our paper "Pseudorandom Black Swans: Cache Attacks on CTR_DRBG". We illustrate how omissions in...

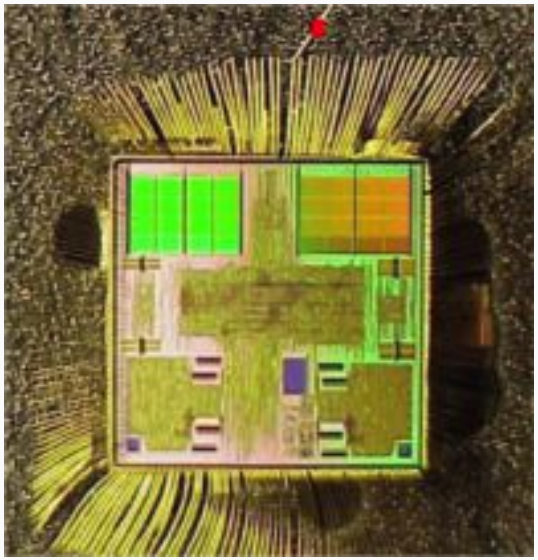
security.cohney.info

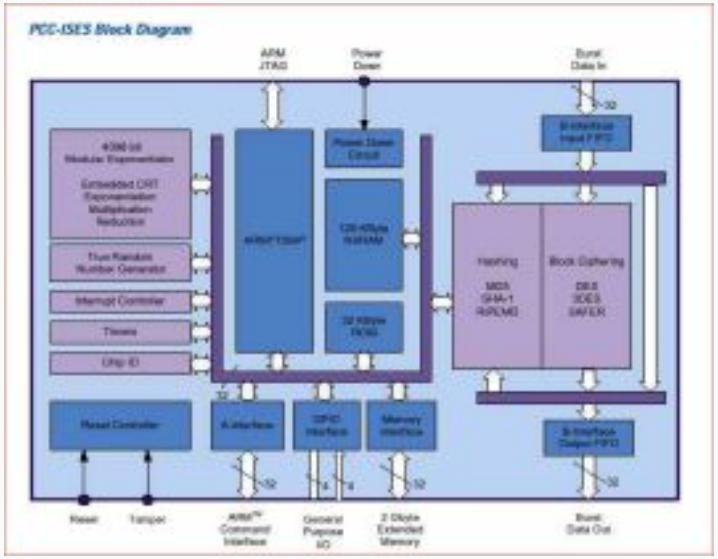
October 3, 2019

December 12, 2019

The chip

An RSA crypto chip of Pijnenburg Securealink cca year 2000

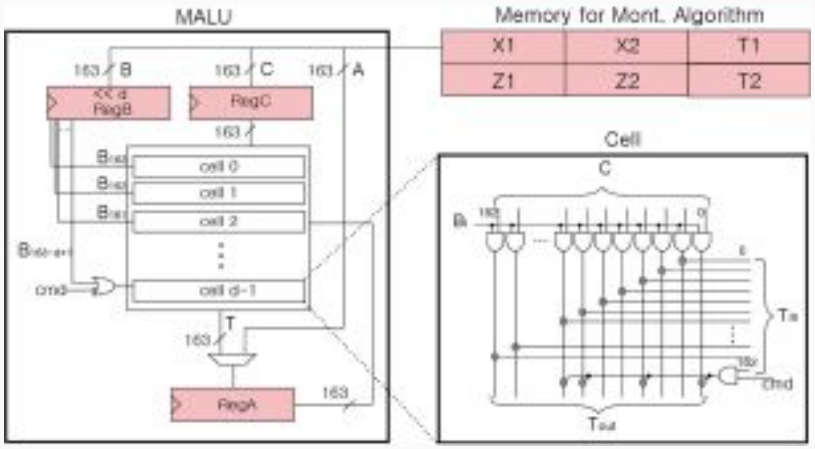




The chip featured:

- Modular exponentiator for RSA (2 units, up to 2048 bit)
- Symmetric crypto: (3)DES, SAFER
- Hashing: MD5, SHA1 and RIPEMD
- True Random Number Generator

ECC RFID chip 2007



ECC RFID chip: Results

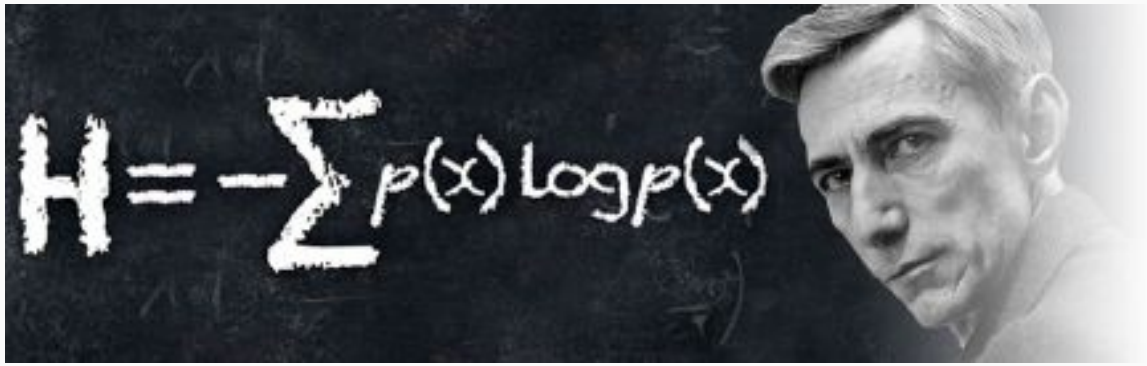
- Several protocols were designed for different RFID applications
- ECC co-processor that can compute:
  - ECC scalar multiplications
  - finite field operations
- Schnorr protocol: one scalar multiplication
  - 14K gates, 79K cycles
  - 30 μWatt@500 KHz and performance of 158 msec
  - energy of 4.8 μJoule

MIA

Information theoretic approach to side-channel analysis

Started cca 2006

- MIA was proposed as a new SCA distinguisher
- started a new line of research into information theoretic view to side-channel analysis



We introduce a Mutual Information-based distinguisher that constitutes the core of a new and generic differential side-channel attack: Mutual Information Analysis (MIA). In contrast to [17], we apply information theory to develop a powerful attack without any device characterization. The distinguisher uses only

MIA and the chip:
Location-based leakage

Motivation

- Registers, memory and other storage units exhibit identifiable and data-related leakage

Motivation

- Registers, memory and other storage units exhibit identifiable and data-related leakage when accessed
- Exploit dependence between the secret key and the location of the activated component

Motivation

- Registers, memory and other storage units exhibit identifiable and data-related leakage when accessed
- Exploit dependence between the secret key and the location of the activated component

---

Algorithm 3: Montgomery ladder

Input: $P, k = (k_{x-1}, k_{x-2}, ..., k_0)_2$

Output: $Q = k \cdot P$

$R_0 \leftarrow P$

$R_1 \leftarrow 2 \cdot P$

for $i = x - 2$ downto 0 **do**

$b = 1 - k_i$

$R_b = R_0 + R_1$

$R_{k_i} = 2 \cdot R_{k_i}$

end for

return R_0

Previous work

- Sugawara et al. considered so-called “geometric” leakage in an ASIC

Previous work

- Sugawara et al. considered so-called “geometric” leakage in an ASIC
- Heyszl et al. recovered the secret scalar by exploiting the spatial dependencies of the double-and-add-always algorithm for ECC on FPGA

Previous work

- Sugawara et al. considered so-called “geometric” leakage in an ASIC
- Heyszl et al. recovered the secret scalar by exploiting the spatial dependencies of the double-and-add-always algorithm for ECC on FPGA
- Schlosser et al. use photonic side-channel to recover the exact SRAM location accessed during the activation of an AES S-box lookup table

Previous work

- Sugawara et al. considered so-called “geometric” leakage in an ASIC
- Heyszl et al. recovered the secret scalar by exploiting the spatial dependencies of the double-and-add-always algorithm for ECC on FPGA
- Schlosser et al. use photonic side-channel to recover the exact SRAM location accessed during the activation of an AES S-box lookup table
- Algorithmic countermeasures such as register renaming were considered

Previous work

- Sugawara et al. considered so-called “geometric” leakage in an ASIC
- Heyszl et al. recovered the secret scalar by exploiting the spatial dependencies of the double-and-add-always algorithm for ECC on FPGA
- Schlosser et al. use photonic side-channel to recover the exact SRAM location accessed during the activation of an AES S-box lookup table
- Algorithmic countermeasures such as register renaming were considered
- Literature sometimes referred to those as address attacks

Previous work

- Sugawara et al. considered so-called “geometric” leakage in an ASIC
- Heyszl et al. recovered the secret scalar by exploiting the spatial dependencies of the double-and-add-always algorithm for ECC on FPGA
- Schlosser et al. use photonic side-channel to recover the exact SRAM location accessed during the activation of an AES S-box lookup table
- Algorithmic countermeasures such as register renaming were considered
- Literature sometimes referred to those as address attacks

Location-based leakage revisited

- Distinguishing the activity of small regions

Location-based leakage revisited

- Distinguishing the activity of small regions
- Exploiting the spatial dependencies of crypto algorithms

Location-based leakage revisited

- Distinguishing the activity of small regions
- Exploiting the spatial dependencies of crypto algorithms

- Forward Neural Networks classifiers exploiting location-based side-channel on the SRAM of a ARM Cortex-M4

Location-based leakage revisited

- Distinguishing the activity of small regions
- Exploiting the spatial dependencies of crypto algorithms

- Forward Neural Networks classifiers exploiting location-based side-channel on the SRAM of a ARM Cortex-M4
- 2 SRAM regions of 128 bytes each can be distinguished with 100% success rate and 256 SRAM byte-regions with 32% success rate

Adversarial model

- Implementation of a key-dependent crypto operation using certain storage components in a deterministic way e.g. a lookup-table (AES LUT)

Adversarial model

- Implementation of a key-dependent crypto operation using certain storage components in a deterministic way e.g. a lookup-table (AES LUT)
- Location leakage is caused by switching circuitry and is observable via EM emissions on the die surface

Adversarial model

- Implementation of a key-dependent crypto operation using certain storage components in a deterministic way e.g. a lookup-table (AES LUT)
- Location leakage is caused by switching circuitry and is observable via EM emissions on the die surface
- Adversary aims to infer which part of the table is active

Adversarial model

- Implementation of a key-dependent crypto operation using certain storage components in a deterministic way e.g. a lookup-table (AES LUT)
- Location leakage is caused by switching circuitry and is observable via EM emissions on the die surface
- Adversary aims to infer which part of the table is active
- Adversary uncovers the location information leading to key recovery

Experimental setup

Figure: Modified Pinata ARM STM32F417IG device.

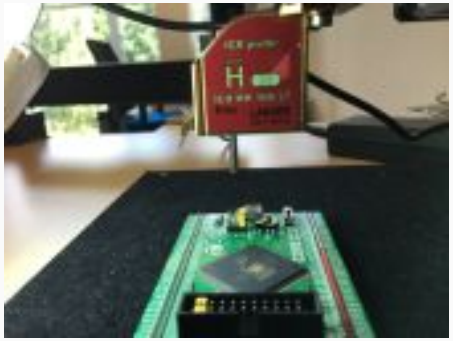


Figure: Decapsulated Pinata with Langer microprobe on top.

Setup details

- Decapsulated Piñata with ARM Cortex-M4 in 90 *nm* technology
- ICR HH 100-27 Langer microprobe $d = 100\mu m$
- Rectangular grid of 300 $\times$ 300 measurement spots
- Sampling rate of 1 Gs/sec resulting in 170k samples
- Near-field probe with positioning accuracy of 50 μm
- Sequential accesses to a cont. region of 16 KBytes in the SRAM using ARM assembly

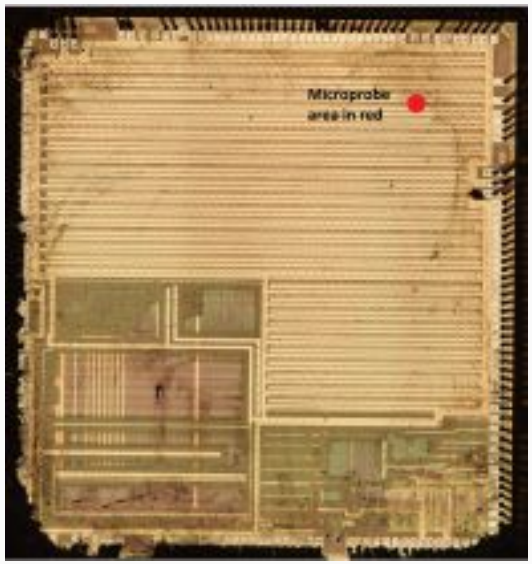


Figure: ARM Cortex-M4 after removal of the plastic layer.

Experiment

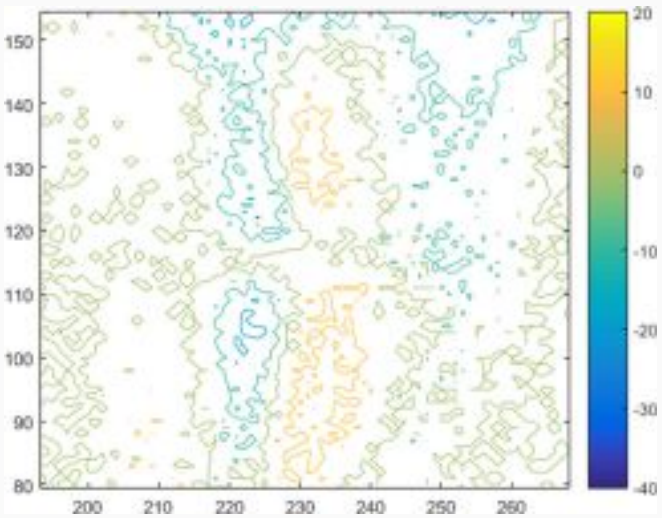


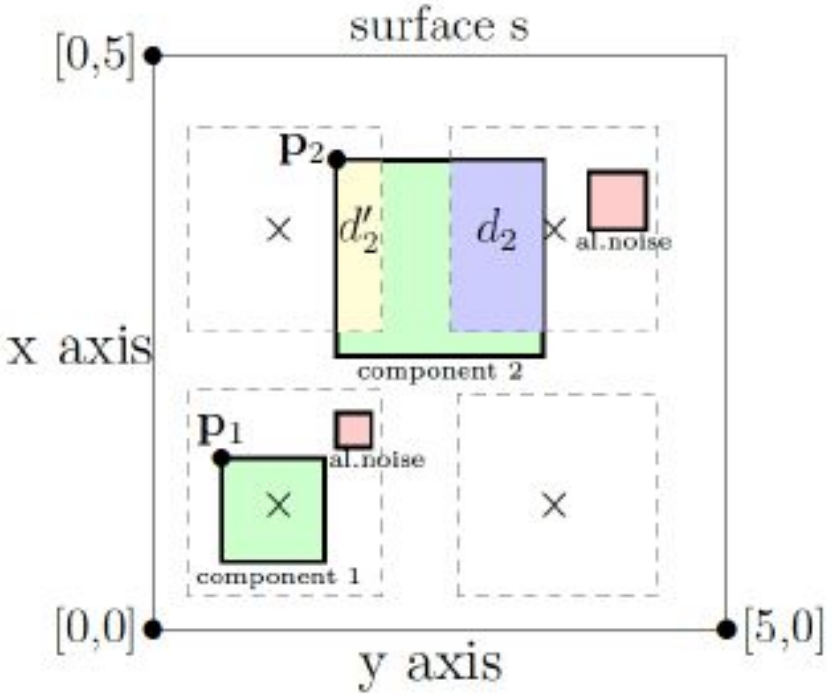
Figure: Distinguishing two 8 KByte regions of the SRAM. Yellow region = stronger leakage from class 1, blue = stronger from class 2.

Figure: Red rectangle shows the location where the highest differences were observed.

Parameters

Parameter	Description	Unit	Our example
S	chip surface area	u^2	$\leq 6\ mm^2$ (whole chip)
O	probe area	u^2	$0.03\ mm^2$
G	scan grid dimension	–	300
A	component areas	vector with 1D entries	–
P	component positions	vector with 2D entries	–

Location Leakage Model



$$l^{det}_{[x,y]}|\mathbf{v}^i = \begin{cases} 0, \text{ if comp. } i \text{ is not captured at [x,y]} \\ d_i,\ 0 < d_i < a_i, \text{ if comp. } i \text{ is partially captured at [x,y]} \\ a_i, \text{ if comp. } i \text{ is fully captured at [x,y]} \end{cases}$$

Figure: Vectors $\mathbf{p}_1, \mathbf{p}_2$ show the position of two components whose areas (a_1, a_2) are solid black-line rectangles.

Information theoretic analysis

Perceived information metric

$$PI(\mathbf{L}; R) = H[R] - H_{true,model}[\mathbf{L}|R] = H[R] + \sum_{r \in \mathcal{R}} Pr[r] \int_{\mathbf{l} \in \mathcal{L}g^2} Pr_{true}[\mathbf{l}|r] \cdot log_2 Pr_{model}[r|\mathbf{l}] \; d\mathbf{l}$$

$$\text{where} \quad Pr_{model}[r|\mathbf{l}] = \frac{Pr_{model}[\mathbf{l}|r]}{\sum_{r^* \in \mathcal{R}} Pr_{model}[\mathbf{l}|r^*]}, \; Pr_{true}[\mathbf{l}|r] = \frac{1}{n_{test}}, \; n_{test} \text{ test set size} \tag{1}$$

Experiment 1: Grid partitioning and dimension

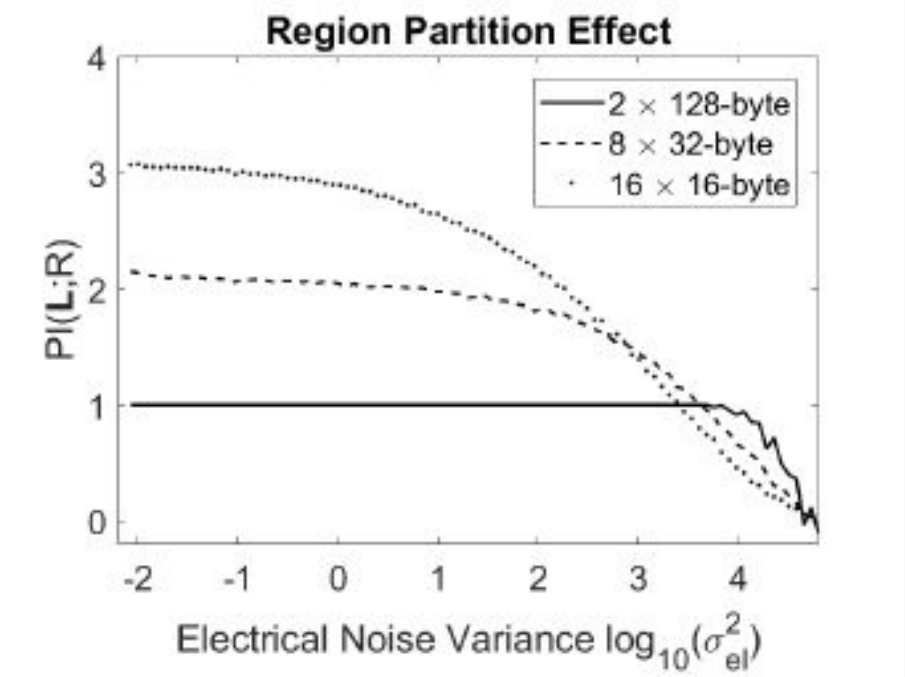


Figure: Effect of 256-byte LUT partitioning to 2, 8 and 16 regions. $\epsilon =$ $\{6\ mm^2, 0.03\ mm^2, 100, 92\ \mu m^2, \text{random}\}$

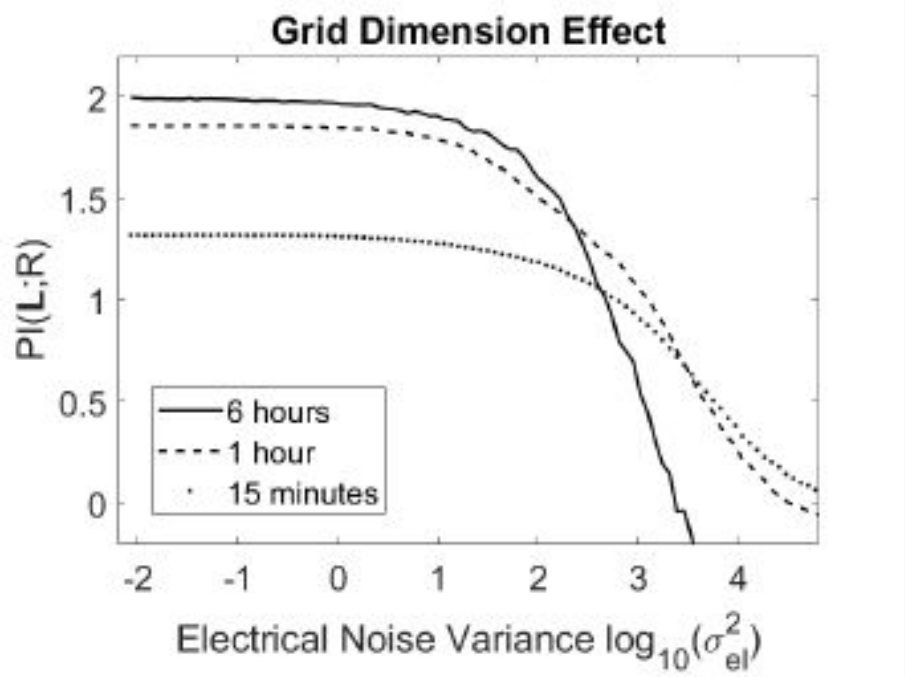


Figure: Effect of grid dim. $g = 100, 40$ and 20. $\epsilon =$ $\{6\ mm^2, 0.03\ mm^2, g, 92\ \mu m^2, \text{random}\}$.

Experiment 2: Technology scaling and algorithmic noise

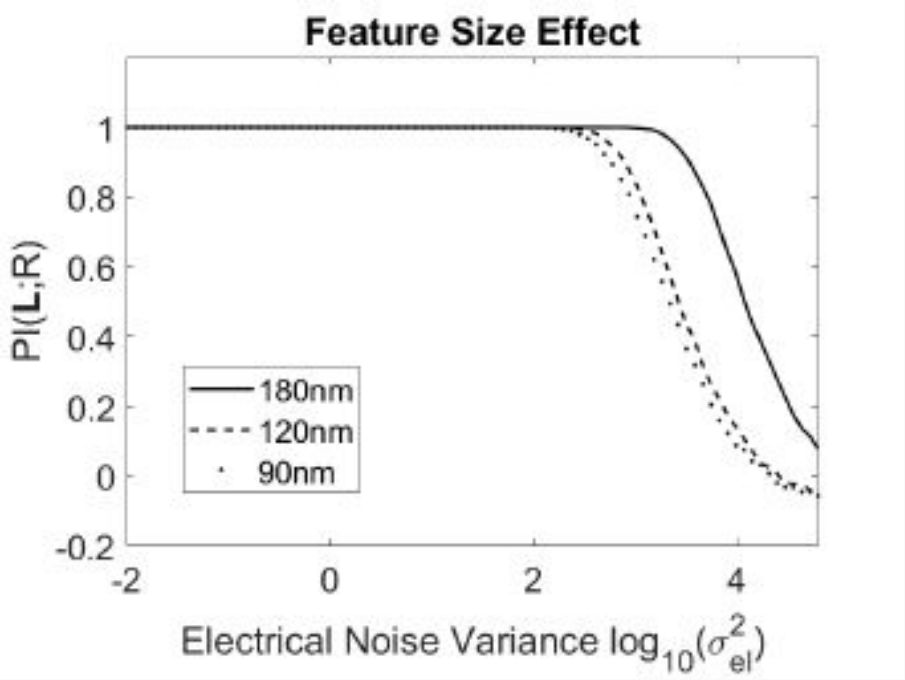


Figure: Feature size of 180 *nm*, 120 *nm*, 90 *nm* and word area $a =$ 368 μm^2, 163 μm^2, 92 μm^2. Parameters $\epsilon = \{6\ mm^2, 0.03\ mm^2, 40, a, \text{random}\}$, 2 x 128 bytes, 250 meas. per spot for 400k traces.

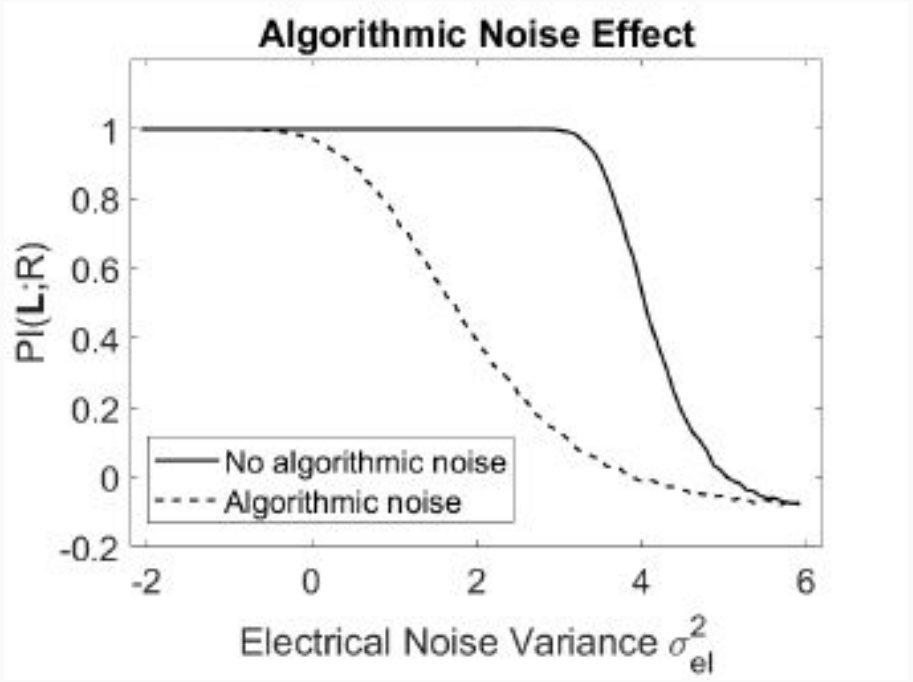


Figure: Alg. noise using 10 noise-generating words. Parameters $\epsilon = \{6\ mm^2, 0.03\ mm^2, 40, 92\ \mu m^2, \text{random}\}$, 2 x 128 bytes, 250 meas. per spot for 400k traces.

Experiment 3: Region proximity and interleaving

(1) Distant placement: ≈ 1 *mm* between 2 regions
(2) Close placement: the two regions are adjacent to each other.
(3) Interleaved placement: words of two regions are interleaved

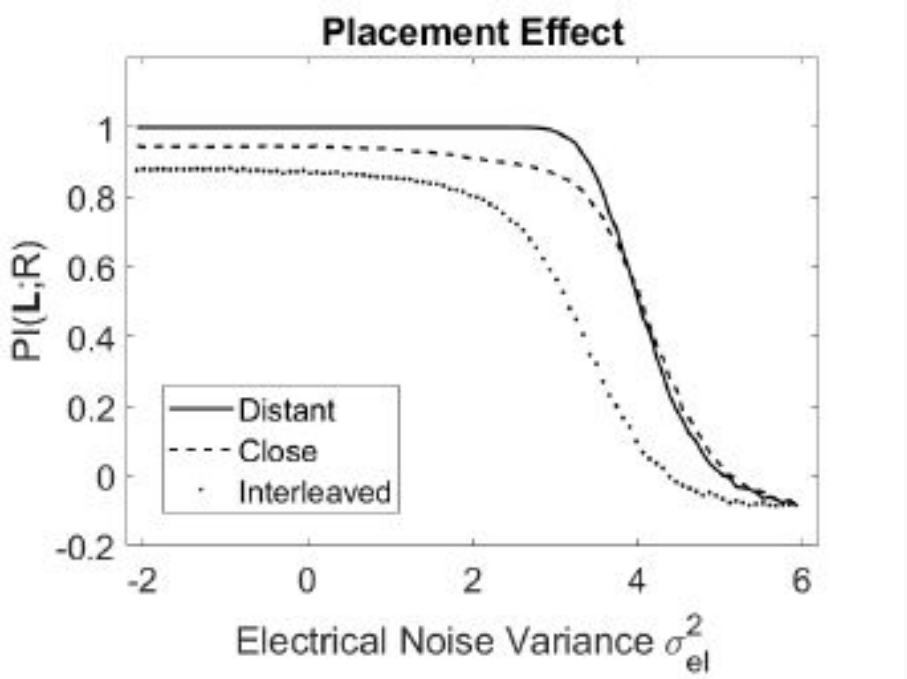
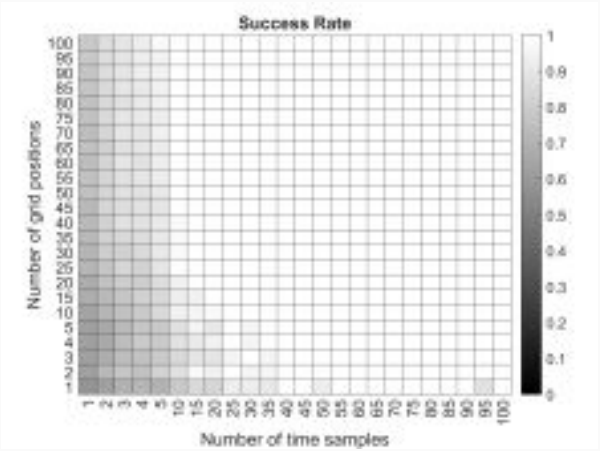
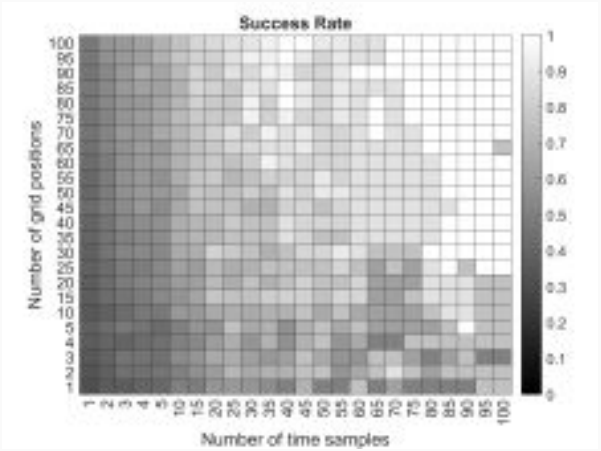
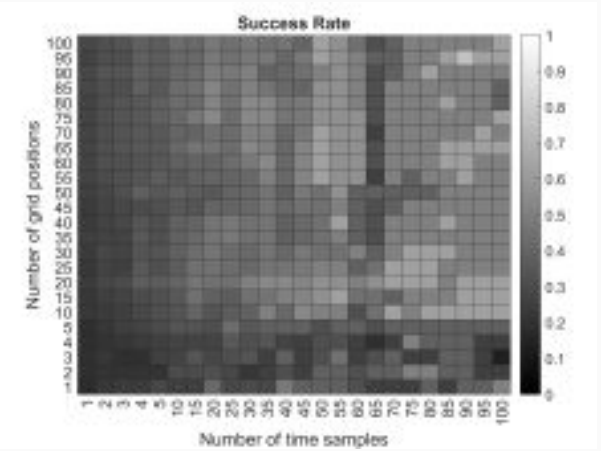


Figure: Effect of different placements. $\epsilon = \{6\ mm^2, 0.03\ mm^2, 20, 92\ \mu m^2, \text{random}\}$, 2 x 128 bytes and using 250 meas. per spot for a total of 100k traces.

Real experiment 1: Region partition

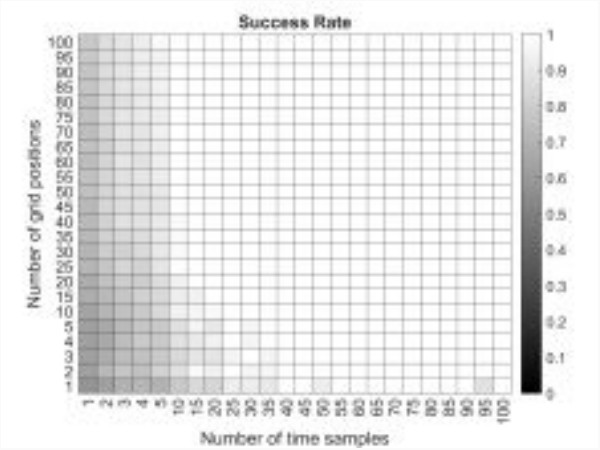


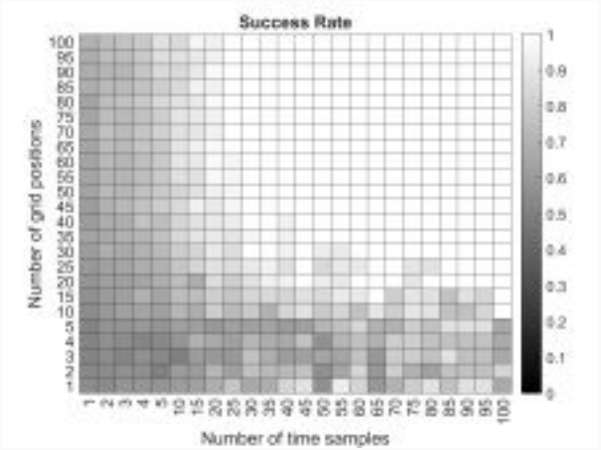


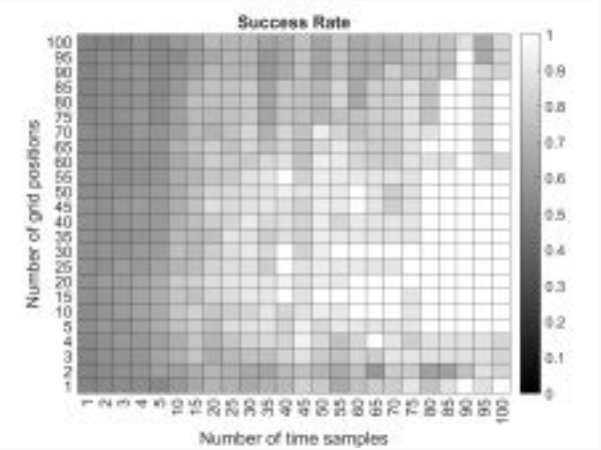


Success rate for template attacks on AES LUT (2x128, 4x64, 8x32). *Y*-axis denotes # spatial POIs, *X*-axis denotes # time samples. White – 100% SR and black – 0% SR.

Real experiment 2: Grid dimension

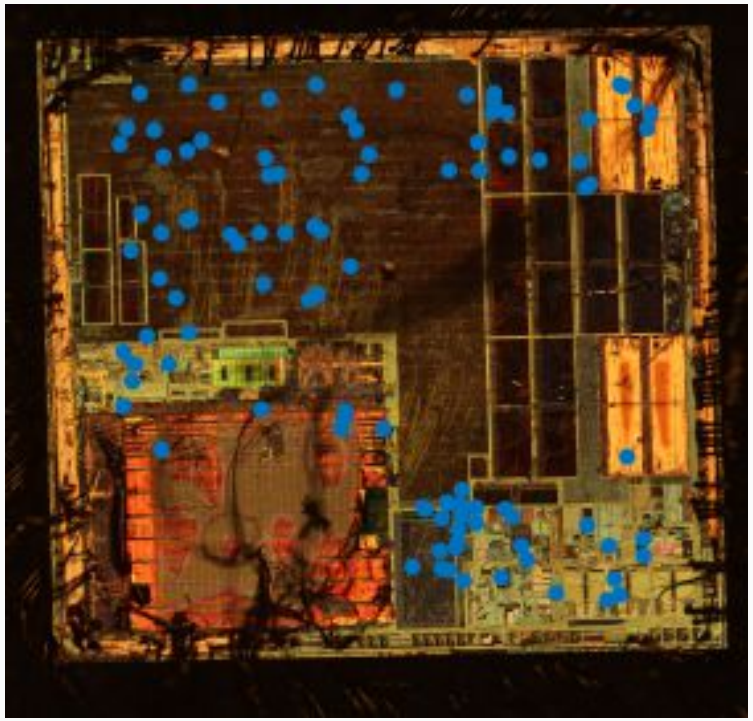






Considered full 300 x 300 grid (2-day exp.) and scaled down to 40 x 40 (1-hour) and 10 x 10 (2-minutes). The theoretical model is unable to classify correctly.

Real experiment 2: Model limitations



Can we do better?

- Machine learning (ML) proved its potential for SCA

Can we do better?

- Machine learning (ML) proved its potential for SCA
- ML used for finding POIs, profiling and non-profiling attacks, pre-processing etc.

Can we do better?

- Machine learning (ML) proved its potential for SCA
- ML used for finding POIs, profiling and non-profiling attacks, pre-processing etc.
- Deep learning (DL) found suitable in dealing with countermeasures

Can we do better?

- Machine learning (ML) proved its potential for SCA
- ML used for finding POIs, profiling and non-profiling attacks, pre-processing etc.
- Deep learning (DL) found suitable in dealing with countermeasures
- Rapid hardware advances facilitate deep learning

Deep learning experiment

- Popular pre-trained networks Convolution Neural Network (CNN) classifier
- Experiments with 2 closely placed SRAM regions of 128 bytes each
- Single-trace attacks improved compared to templates
- All 5 CNNs were trained in 2 ways: one batch and multiple-batch training
- Keras framework and Python for pre-processing
- Training, validation and test sets are of 70-20-10 ratio

Experiment with CNNs

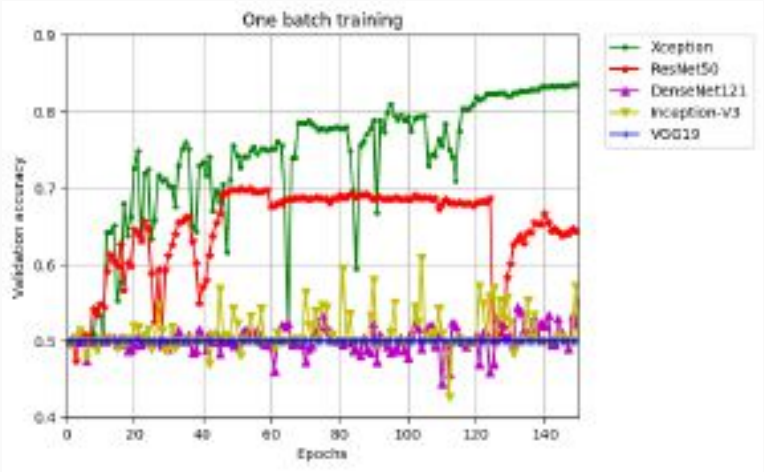


Figure: Single-batch training.

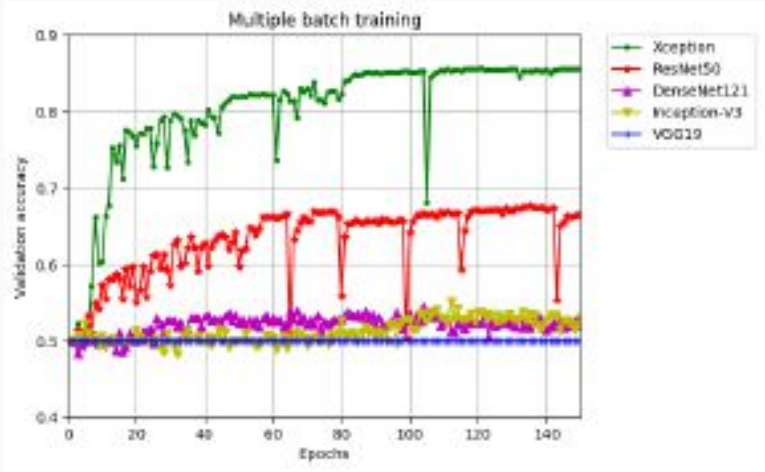


Figure: Multiple-batch training.

CNNs are surpassing the single-sample accuracy of template attacks, reaching 88%.

C. Andrikos, L. Batina, L. Chmielewski, L. Lerman, V. Mavroudis, K. Papagiannopoulos, G. Perin, G. Rassias, A. Sonnino: *Location, Location, Location: Revisiting Modeling and Exploitation for Location-Based Side Channel Leakages. ASIACRYPT (3) 2019: 285-314.*

The Table

Gender diversity: Facts

- Women are underrepresented in leadership positions
- Women Need To 'Sit At The Table', Sheryl Sandberg

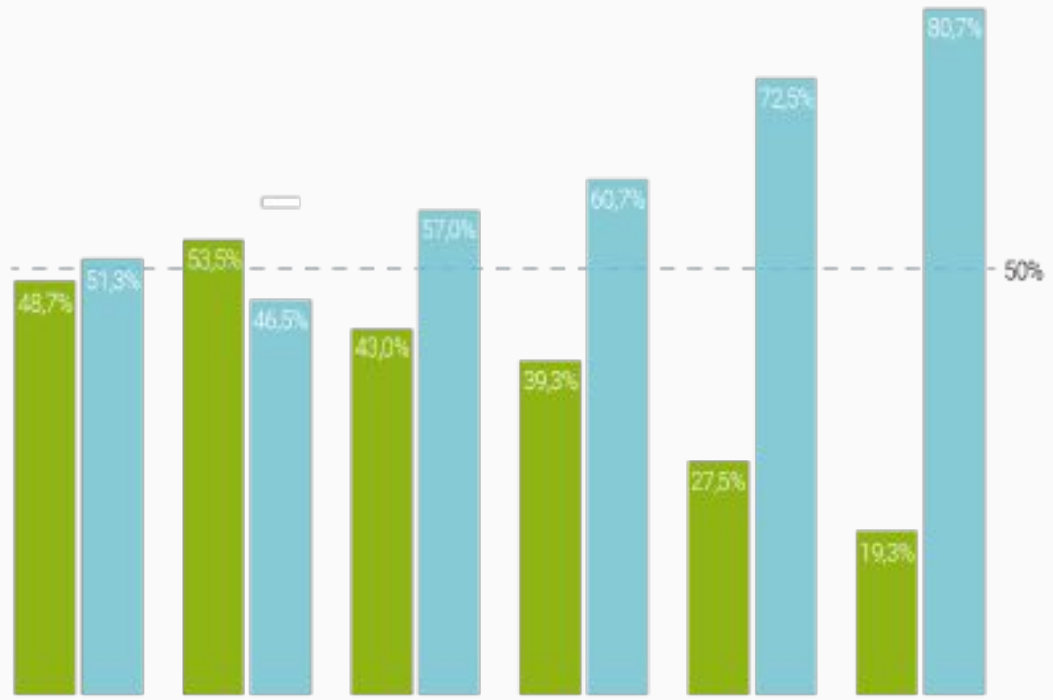
2015: with 17% of Dutch professors being female, The Netherlands had the fourth-lowest percentage of female professors in Europe

Navratilova: BBC pays McEnroe 10 times more for Wimbledon role

Tennis champion says fellow pundit John McEnroe earns at least £150,000, while she is paid £15,000

Percentages in Dutch academia

Grafiek 2.3 Percentage vrouwen en mannen van student tot hoogleraar (ultimo 2016)



Bron studenten en geslaagden: 1cHO 2016, 1 oktober 2016, in personen.
Exclusief wetenschapsgebied Gezondheid
Bron personeel: VSNU/WOPI, ultimo 2016, in fte. Exclusief wetenschapsgebied Gezondheid

Initiatives and highlights

- Gender Diversity committee was formed at Radboud University within the Faculty of Science
- University-wide mentoring program for women
- Mohrmann fellowships for women
- The Radboud Women of Computing Science (RWoCS) group was created: the main goal is to attract female students

The future is bright

- The chip: Post-quantum crypto for future embedded systems

The future is bright

- The chip: Post-quantum crypto for future embedded systems
- MIA: Deep learning for advanced security evaluation

The future is bright

- The chip: Post-quantum crypto for future embedded systems
- MIA: Deep learning for advanced security evaluation
- The Table: More diversity at all entry points

The future is bright

- The chip: Post-quantum crypto for future embedded systems
- MIA: Deep learning for advanced security evaluation
- The Table: More diversity at all entry points

Thank you

We are looking for students/PostDocs!

lejla@cs.ru.nl