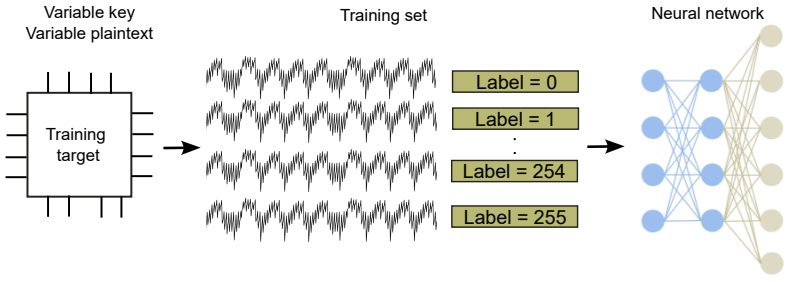
SCADL: A Side-Channel Attack Tool Based on Deep Learning

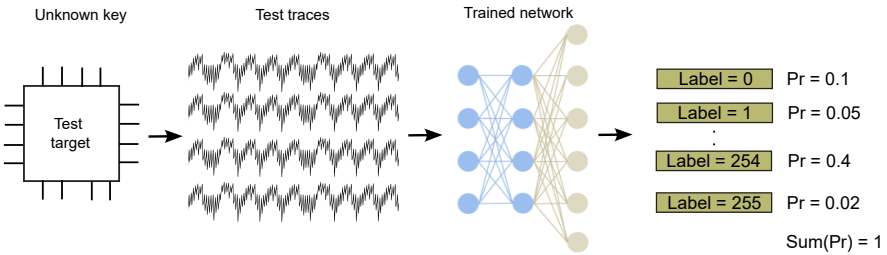
Karim M. Abdellatif

DL-based SCAs



Profiling phase

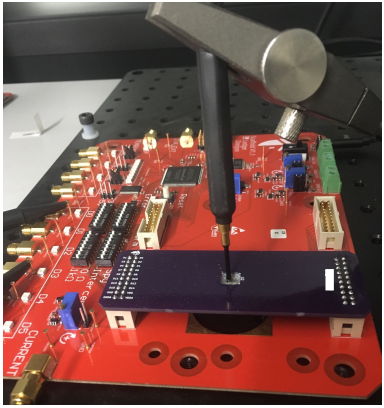
DL-based SCAs



Test phase

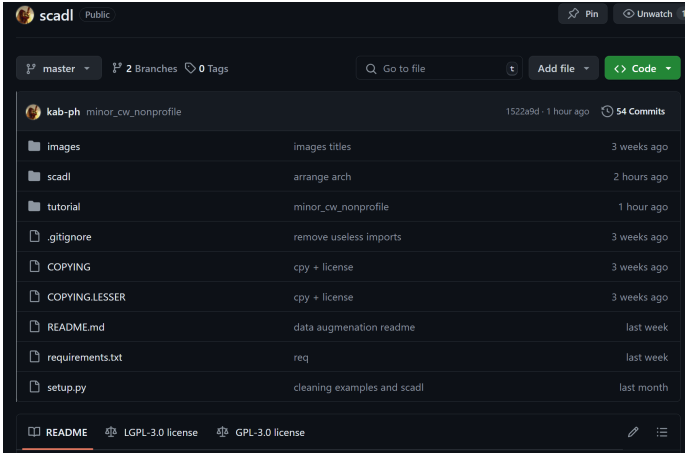
Motivation

- Limited DL features in lascar [1]
- A recent DL-based tool for the internal usage in addition to muscat [2]
- Open-source a DL-based SCA tool for the community



EM-based SCA setup

[1] https://github.com/Ledger-Donjon/lascar
[2] https://github.com/Ledger-Donjon/muscat



[3]https://github.com/Ledger-Donjon/scadl

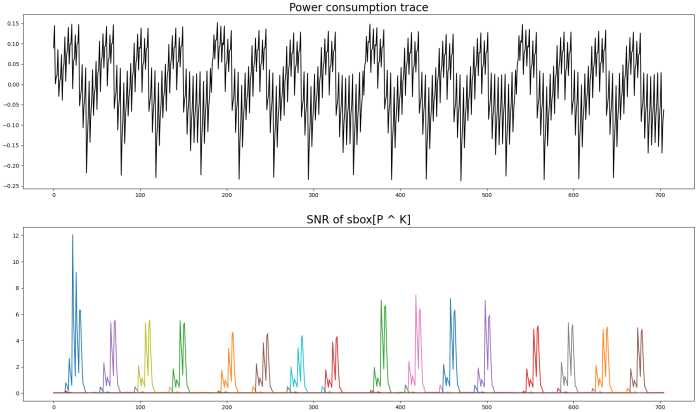
Previous tools and SCADL

	Profiling	Multi-label	Non-profiling	Data augmentation
lascar [4]	√	x	x	x
scaaml [5]	√	x	x	x
scadl [6]	√	√	√	√

[4] https://github.com/Ledger-Donjon/lascar
[5] https://github.com/google/scaaml
[6] https://github.com/Ledger-Donjon/scadl

DATASETS USED IN SCADL

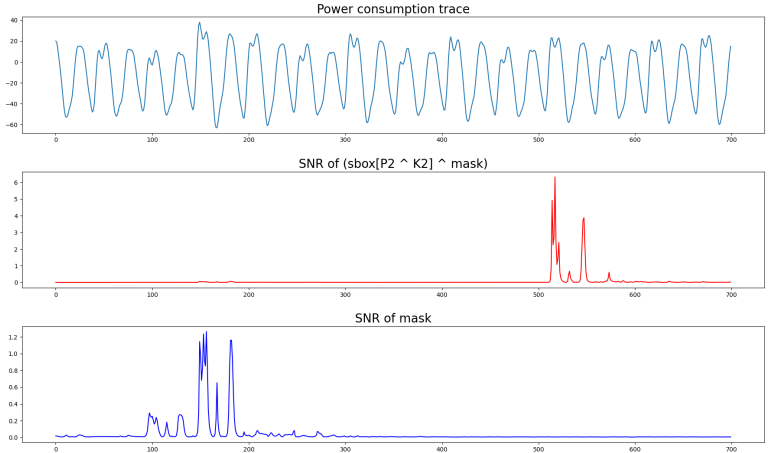
AES-128 on ChipWhisperer-Lite [7]



SubBytes calculation

[7] https://www.newae.com/products/nae-cwlite-arm

ASCAD database [8]



[8] https://github.com/ANSSI-FR/ASCAD

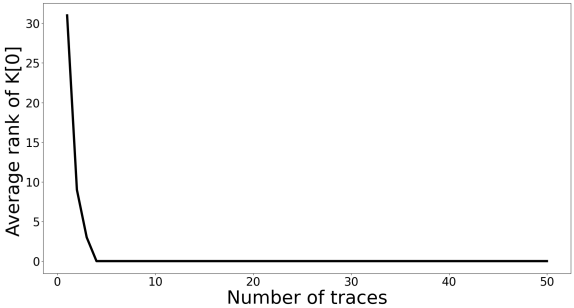
DL-BASED PROFILING ATTACKS

MLP-based example

```
def mlp_model(sample_len, range_outer_layer):
    model = Sequential()
    model.add(Dense(20, input_dim=sample_len, activation=tf.nn.relu))
    model.add(Dense(10, activation=tf.nn.relu))
    model.add(Dense(range_outer_layer, activation=tf.nn.softmax))
    model.compile(
        optimizer="adam",
        loss="categorical_crossentropy",
        metrics=["accuracy"],
    )
    return model
```

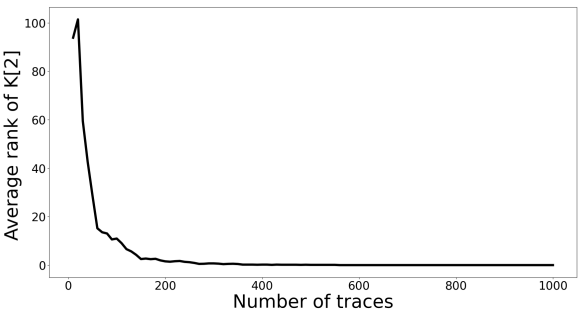
Example of unprotected design

- AES-128 on STM-32
- MLP architecture
- 50K traces for profiling
- 1K traces for test
- Labels on Sbox output



Example of ASCAD

- ASCAD dataset
- Masked AES
- MLP architecture
- 50K traces for profiling
- 10K traces for test
- Labels on Sbox output

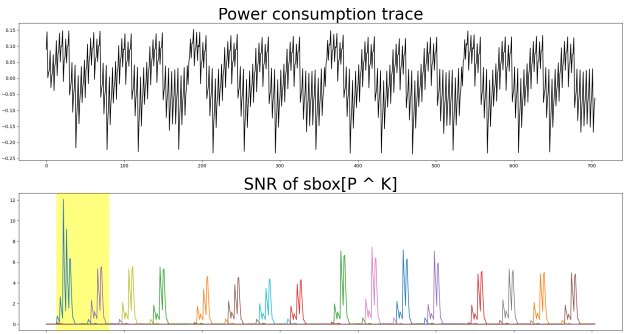


MULTI-LABEL

POI selection under countermeasures

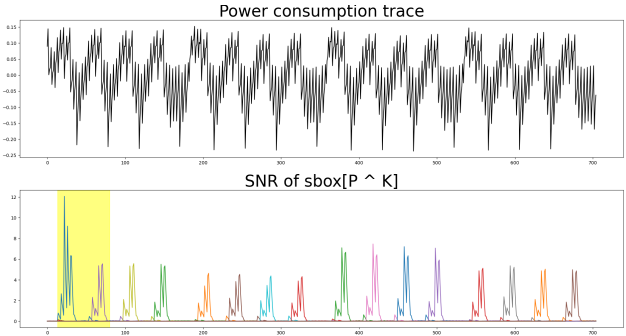
- Desynchronization
- Masking
- Power masking

Feeding the model with a window that may contains several labels.



Multi-label classification in SCAs [9]

- Targeting more than one operation (multiple keys)
- Reducing evaluation time
- More efficiency against masked designs

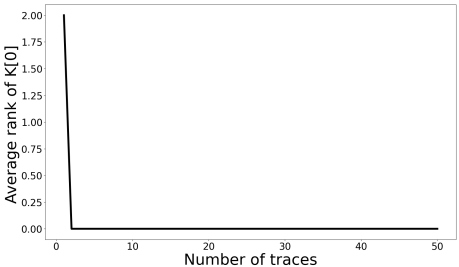


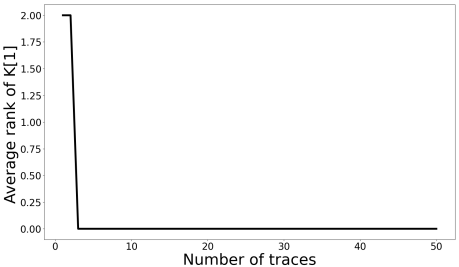
[9] Houssem Maghrebi, "Deep learning based side-channel attack: a new profiling methodology based on multi-label classification", ePrint 2020

MLP-based example

```
def mlp_multi_label(node=50, layer_nb=4):
    model = Sequential()
    model.add(Dense(node, activation="relu"))
    for i in range(layer_nb - 2):
        model.add(Dense(node, activation="relu"))
    model.add(Dense(512, activation="sigmoid"))
    optimizer = "adam"
    model.compile(loss="binary_crossentropy", optimizer=optimizer,
    metrics=["accuracy"])
    return model
```

Attacking two keys using one model





DATA AUGMENTATION

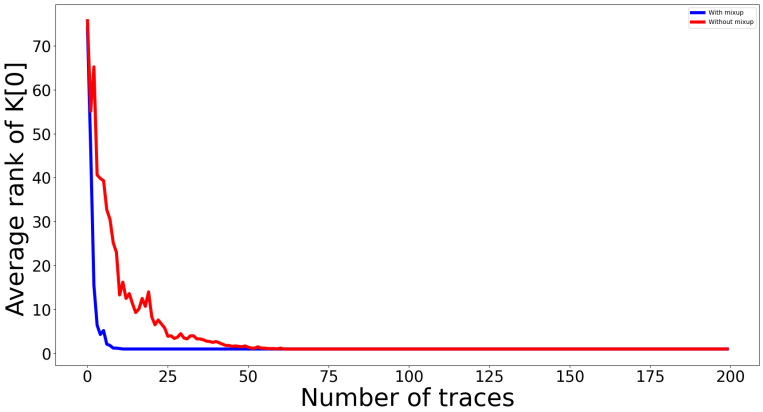
Data augmentation

- It's used to boost the DL efficiency
- Add-remove deformation and shift were used to Improve CNN performance against jitter-based designs [10].
- Mixup also was used against masked designs [11]

[10] E. Cagli, C. Dumas, and E. Prouff "Convolutional neural networks with data augmentation against jitter-based countermeasures: Profiling attacks without pre-processing", CHES 2017

[11] K. Abdellatif "Mixup Data Augmentation for Deep Learning Side-Channel Attacks ", ePrint 2021.

Mixup


With mixup
Without mixup
Average rank of K[0]
0
10
20
30
40
50
60
70
0
25
50
75
100
125
150
175
200
Number of traces

NON-PROFILING DL

Non-profiling DL [12]

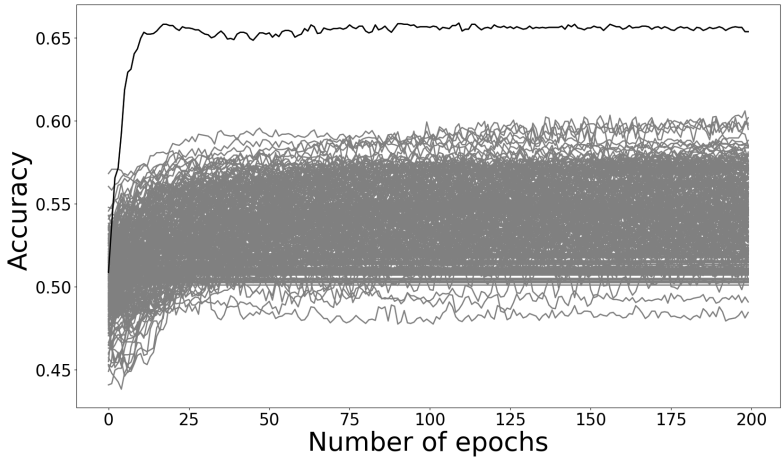
- Similar concept to Non-Profiled attacks (CPA and DPA)
- The correct guess gives the best accuracy
- It outperforms Non-Profiled attacks because of the ability to break designs with countermeasures (ex: jitter and masking)
- Sometimes it can be combined with DA techniques

[12] Benjamin Timon "Non-Profiled Deep Learning-based Side-Channel attacks with Sensitivity Analysis", CHES 2019

- Leakage function:
  - LSB
  - MSB
  - HW

```
accuracy = np.zeros((key_len, epochs))
for guess in range(key_len):
    labels = GenerateLabels(guess)
    accuracy[i] = ModelCompile(labels, leakages)
key = np.argmax(np.max(accuracy, axis=0))
```

Result on unprotected AES-128



CONCLUSION

- **SCADL** [13] is an open-source tool which has the following features:
  - Single and multi-label profiling attacks
  - Non-profiling attacks
  - Data augmentation
- Features to be added soon:
  - Multi-tasking DL attacks
  - Sensitivity analysis
- Your contribution to **SCADL** is welcomed!

[13] https://github.com/Ledger-Donjon/scadl

THANK YOU. QUESTIONS?

Karim M. Abdellatif, PhD
e-mail: karim.abdellatif@ledger.fr