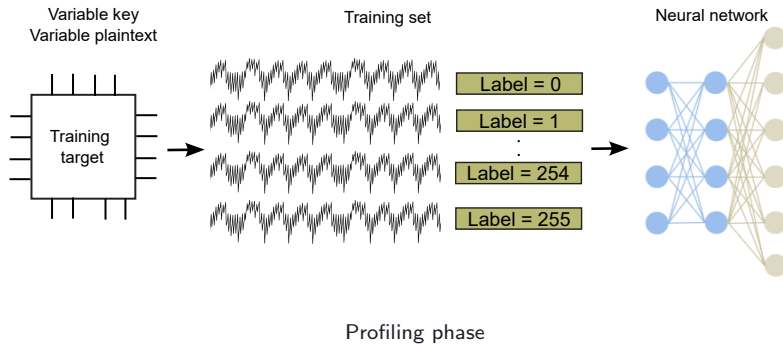


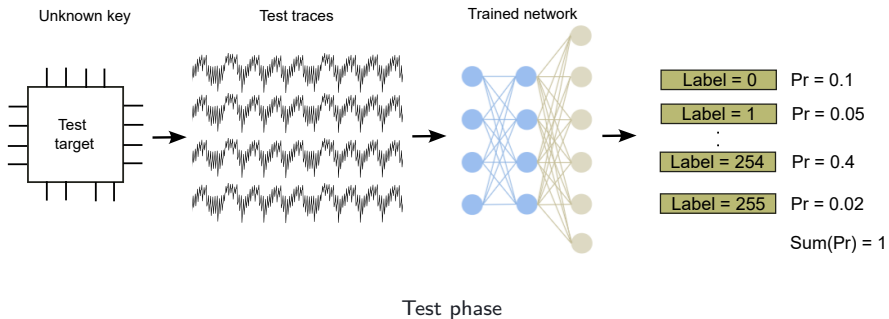


## SCADL: A Side-Channel Attack Tool Based on Deep Learning

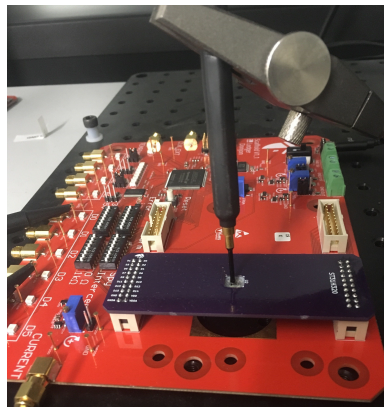
Karim M. Abdellatif







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

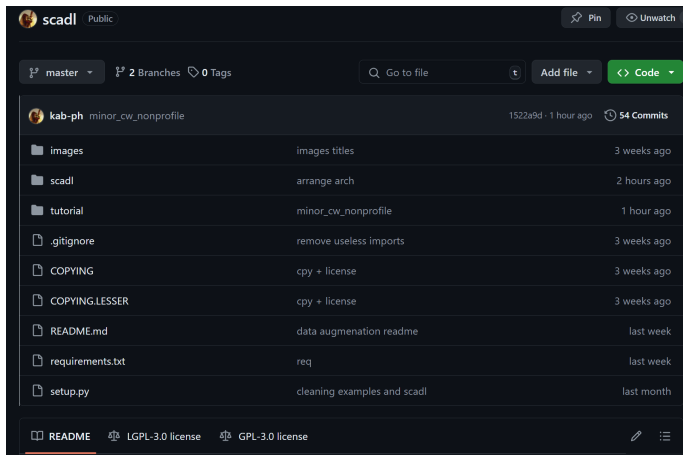


EM-based SCA setup

---

<sup>1</sup><https://github.com/Ledger-Donjon/lascar>

<sup>2</sup><https://github.com/Ledger-Donjon/muscat>



<sup>3</sup><https://github.com/Ledger-Donjon/scadl>



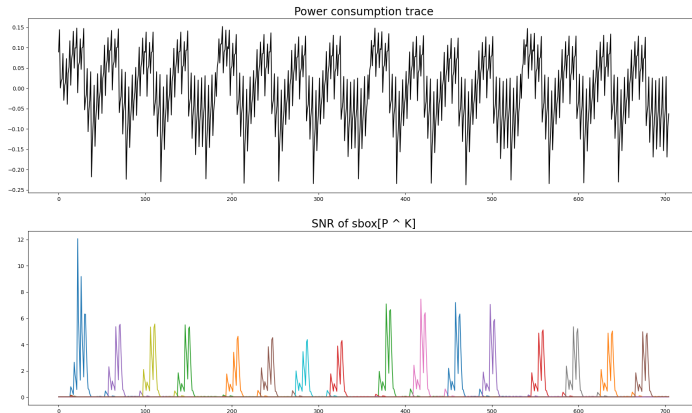
	Profiling	Multi-label	Non-profiling	Data augmentation
lascar <sup>4</sup>	✓	x	x	x
scaaml <sup>5</sup>	✓	x	x	x
scadl <sup>6</sup>	✓	✓	✓	✓

<sup>4</sup><https://github.com/Ledger-Donjon/lascar>

<sup>5</sup><https://github.com/google/scaaml>

<sup>6</sup><https://github.com/Ledger-Donjon/scadl>

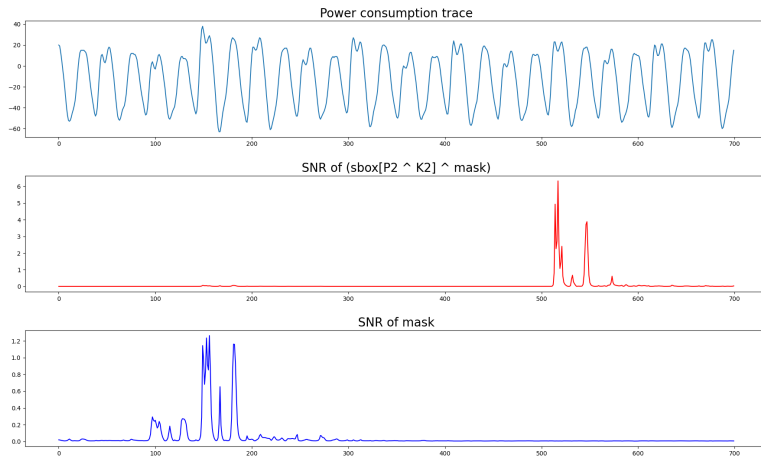
## DATASETS USED IN SCADL



SubBytes calculation

<sup>7</sup><https://www.newae.com/products/nae-cwlite-arm>





<sup>8</sup><https://github.com/ANSSI-FR/ASCAD>

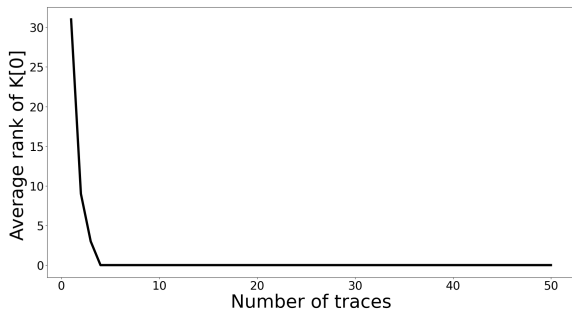
# DL-BASED PROFILING ATTACKS



```
1 def mlp_model(sample_len, range_outer_layer):
2     model = Sequential()
3     model.add(Dense(20, input_dim=sample_len, activation=tf.nn.relu))
4     model.add(Dense(10, activation=tf.nn.relu))
5     model.add(Dense(range_outer_layer, activation=tf.nn.softmax))
6     model.compile(
7         optimizer="adam",
8         loss="categorical_crossentropy",
9         metrics=["accuracy"],
10    )
11    return model
```

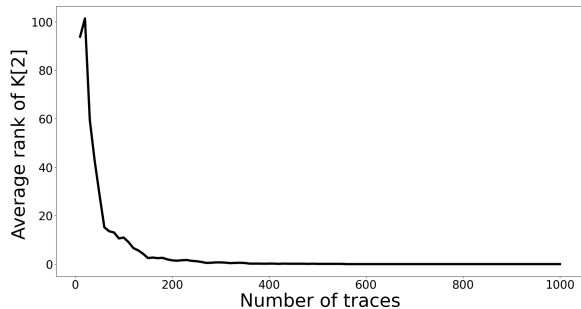


- AES-128 on STM-32
- MLP architecture
- 50K traces for profiling
- 1K traces for test
- Labels on Sbox output





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

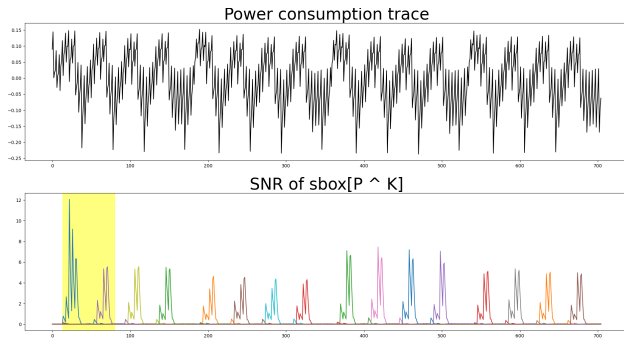


**MULTI-LABEL**



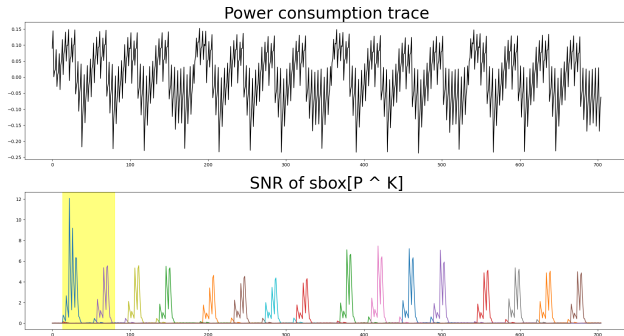
- Desynchronization
- Masking
- Power masking

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





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



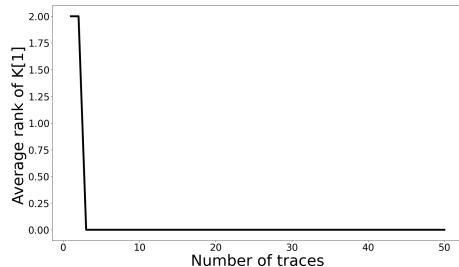
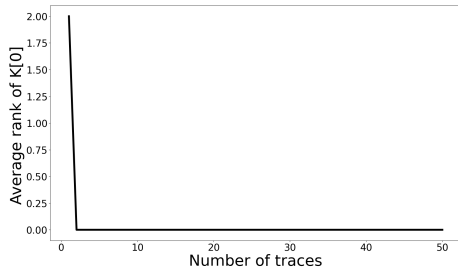
<sup>9</sup>Houssem Maghrebi, "Deep learning based side-channel attack: a new profiling methodology based on multi-label classification", ePrint 2020





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

## Attacking two keys using one model



# DATA AUGMENTATION

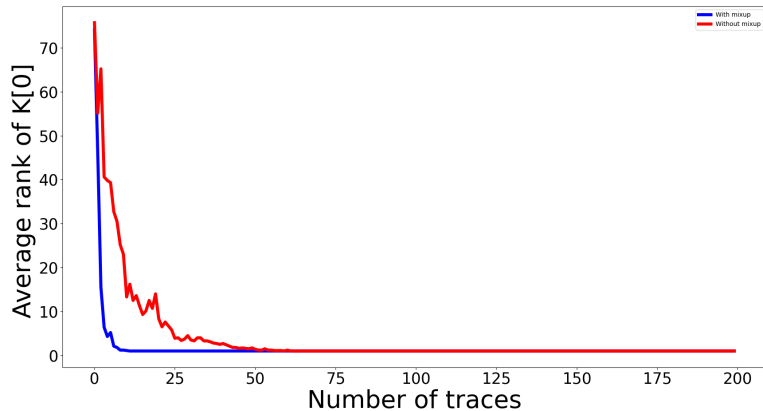


- It's used to boost the DL efficiency
- Add-remove deformation and shift were used to Improve CNN performance against jitter-based designs <sup>10</sup>.
- Mixup also was used against masked designs <sup>11</sup>

---

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

<sup>11</sup>K. Abdellatif "Mixup Data Augmentation for Deep Learning Side-Channel Attacks ", ePrint 2021.



**NON-PROFILING DL**



- 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

---

<sup>12</sup>Benjamin Timon "Non-Profiled Deep Learning-based Side-Channel attacks with Sensitivity Analysis ", CHES 2019

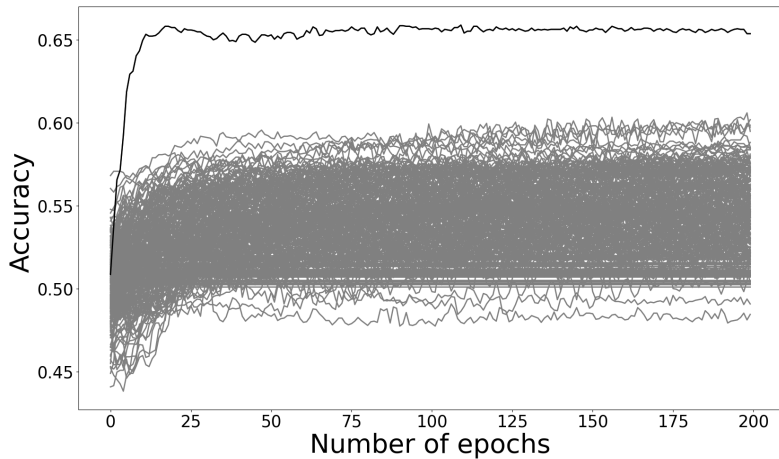


- Leakage function:
  - LSB
  - MSB
  - HW

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



## Result on unprotected AES-128



## CONCLUSION



- **SCADL**<sup>13</sup> 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!

---

<sup>13</sup><https://github.com/Ledger-Donjon/scadl>

THANK YOU. QUESTIONS?



Karim M. Abdellatif, PhD  
e-mail: [karim.abdellatif@ledger.fr](mailto:karim.abdellatif@ledger.fr)