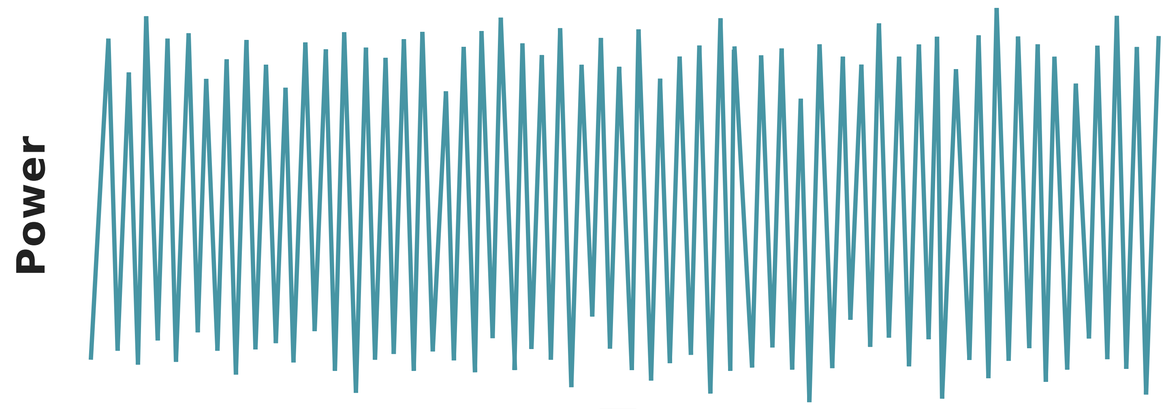
Towards Robust Deep-Learning Cryptographic Localization in Side-Channel Traces

Giuseppe Chiari, Davide Galli, Davide Zoni
{name.surname}@polimi.it

A **successful side-channel attack** needs the attacker to:

- **Locate** in a side-channel trace the cryptographic operations (COs)
- **Align** in time the measured data

This work presents a **deep-learning technique** to accurately **locate cryptographic operations** in a side-channel trace, even in trace deformations. We validated our proposal through a successful attack against a variety of unprotected and protected cryptographic primitives that have been executed on an FPGA-implemented RISC-V CPU.



Slice the input into sub-windows and feed them to a CNN.
Depending on whether the window has been classified as the beginning of the CO or not, a higher or lower class score is assigned.

Clean the input into a square wave signal by comparing each sample with a threshold. Then, a median filter is applied to improve the accuracy further. This step returns the samples identifying the rising edges. Such points represent the beginning of each CO in the analyzed input trace.

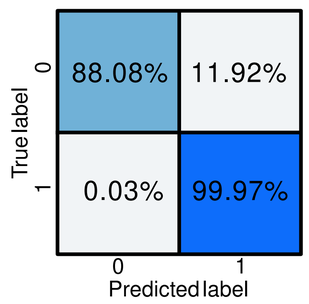
Match the side-channel trace with the segmentation's samples.

Target the sub-byte intermediate of the AES chiper. A minor aggregation over time is used to fix the rough estimation of the beginning of the COs and to mitigate the presence of random delay.

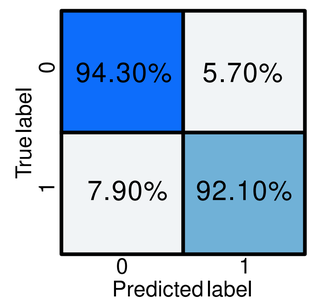
Experimental Evaluation

- 5 COs: Clefia, Simon, Camellia, AES, AES mask
- Up to 2 (or 4) consecutive random delay instructions
- Interleave with noisy applications (or consecutive COs)

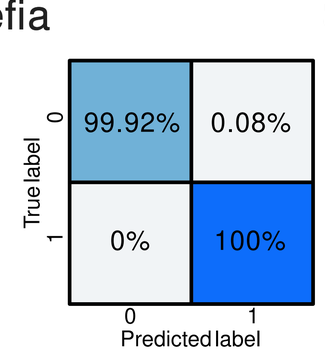
We are able to find **100%** of the COs for every tested configuration.
CPA is successful with less than 4000 COs.



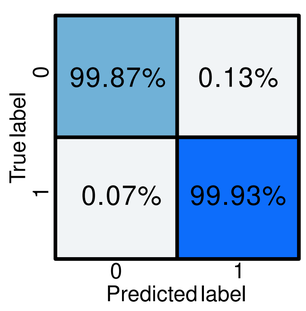
Clefia



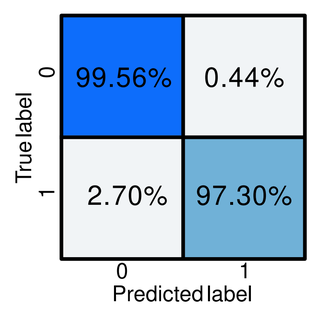
Simon



Camellia



AES mask



AES

References

[1] G. Chiari, D. Galli, F. Lattari, M. Matteucci and D. Zoni, "A Deep- Learning Technique to Locate Cryptographic Operations in Side-Channel Traces," 2024 Design, Automation & Test in Europe Conference & Exhibition (DATE), Valencia, Spain, 2024, pp. 1-6.
[2] D. Galli, A. Galimberti, W. Fornaciari, and D. Zoni, “On the effectiveness of true random number generators implemented on fpgas,” in International Conference on Embedded Computer Systems. Springer, 2022, pp. 315–326.

20th International Summer School on Advanced Computer Architecture and Compilation for High-Performance Embedded Systems (ACACES) | July 14th – 20th, 2024, Fiuggi, Italy