SCALib: Side-Channel Analysis Library
Olivier Bronchain, Gaëtan Cassiers
UCLouvain, Belgium

Available Features

Leakage Assessment:
- Signal-to-Roise Ratio
- Uni/Multi-variate higher-order T-test

Attack Tools:
- Gaussian Templates & LDA
- Soft-Analytical Side-Channel Attacks (SASCA)

Post-processing:
- Key rank estimation
  → And more to come.

Goals & Philosophy

Easy to use:
- Simple Python API.
- Detailed documentation and examples.
- On PyPI: pip install scalib.

High performance:
- Single/multi core optimizations.
- Rust/C back-end.
- Incremental API.
- Optimized RAM usage.

ANSSI’s AES-128 on STM32

Affine masking:
- Masks \( r^m \) and \( r^a \):
  \[ x_i = (r^m \otimes \text{Sbox}(pt_i \oplus k_i)) \oplus r^a_i \]
- Pre-computed masked Sbox.

Shuffling:
- Permutation on 16 Sboxes.
- Permutation on 4 MixColumns.

→ Both masking and shuffling are combined to increase side-channel protection.

Attack Description

Attack Parameters:
- 60 kSample/trace.
- 125MSample/sec with 12-bit resolution.
- 37 intermediate values are profiled.
- SNR computed with 8192 traces.
- Between 400 and 800 PoIs are used.
- Models computed with 16384 traces.

Leakage Profiling Strategy (e.g. permutation indexes)

Gaussian Templates with Dimensionality reduction

Attack Results

Attack Performance:
- SNR computed in \( \approx 40 \) sec.
- Templates are built in \( \approx 40 \) sec.
- 200 traces are required to break a key.
- One 128-bit key is recovered in \( \approx 1 \) sec.

References