Deep Learning for SCA

Train intelligent machines to extract keys

Evaluating the resilience of cryptographic algorithms to side channel analysis (SCA) is required by several national and private certification schemes.

A typical SCA evaluation requires a complex end-to-end procedure: an initial leakage assessment stage, an optional dimensionality reduction phase, a signal processing step (e.g., static alignment, filtering, resampling), and finally the application of one or several attack methods.

Recently, deep learning has been introduced as an alternative framework, and used successfully as an all-in-one tool for SCA.

> **Did you know?**
>
> Since 2017, several national and private schemes mandate the application of deep learning in side channel analysis evaluations of secure products.

If you are interested in or obligated to keep your knowledge in synch with state-of-the-art SCA methodologies, look no further than our deep learning for SCA (short: deep SCA) training.

The goal of this one-day workshop is to introduce you to deep learning for side channel analysis. After the workshop you will be able to use neural networks to evaluate both private and public key crypto algorithms.

Key learning objectives:

- Determine the number of traces to use for training
- Assess the learning performance of your network
- Interpret the intermediate and final output
- Make choices about of the network architecture
- Understand the effect of key parameters, such as the number of hidden layers, the activation function, etc.
- Optimize and automate the hyper-parameter search

The workshop is interactive with tailored exercises of varied difficulty levels for effective knowledge transfer.

riscure

Course Syllabus

Introduction to machine learning for SCA

- Machine learning
  - Key notions: classes, labels, features
  - Supervised vs Unsupervised learning
  - Applications
- Deep learning for SCA
  - Compare and contrast

Deep learning essentials

- Artificial Neural Networks (ANN)
  - Multi-Layer Perceptron (MLP)
- Convolutional Neural Network (CNN)
  - CNN vs multilayer perceptron
  - Convolution and pooling layers
  - Using CNN to extract information
- Architecture of a typical neural network:
  - Input/Hidden/Output layers
  - Activation functions
- Epochs and Mini-Batches
- Forward and Backward propagation
- Regularization and generalization

Extracting cryptographic keys with deep learning

- Introduction to profiled attacks
- Preparing the datasets
- Optimizing the parameter search

Optimization and automation

- Data augmentation for SCA traces
- Random search vs genetic algorithms

Analyzing symmetric crypto algorithm implementations

- Leakage model selection
- *Exercise: extract key from a SW AES implementation*
- *Exercise: extract key from a SW AES in the presence of jitter (manual hyper-parameter selection)*

Remarks and conclusions

- No-free lunch theorem
- Estimate time and effort for training your network
- Recent developments in the field

RISCURE INSPECTOR
Side Channel Analysis

RISCURE TRAINING ACADEMY
DEEP LEARNING

While the concepts we teach are generic and can be replicated using different equipment, during the training we use our Riscure Inspector tool. **Workshop participants with an Inspector license will receive a Deep Learning license valid for 30 days.**