

The Database for Side Channel Attacks

Testbed for Side Channel Analysis and
Security Evaluation (TeSCASE)

URL: <http://tescase.coe.neu.edu>

Northeastern University Energy-efficient and Secure Systems
(NUEESS) Lab



What TESCASE Provides

- **Data sets**
 - Real power measurements
 - EM measurements
 - Timing information (from simulations)
- **Side-channel attacks**
 - First-order power/EM attacks
 - Second-order power/EM attacks
 - Timing analysis attack and simulators
- **Implementation**
 - Various cryptographic HW and SW imple.
 - Measurement setup and boards imple.
- **Documents/publications**





NUEESS, Northeastern University

Purpose of TeSCASE Database

- Free researchers up from tedious data acquisition and lengthy implementation process
- Align side-channel research by providing common data sets and hardware and software platform
- Lower the barrier for research on hardware security



What TeSCASE Provides Now

- Data sets (power measurements)
 - AES FPGA implementation
 - Masked AES FPGA implementation
 - MAC-Keccak FPGA implementation
 - MAC-Keccak software implementation
- Attack library
 - CPU CPA on AES, GPU CPA on AES (OpenCL)
 - 2O-CPA on masked AES with profiling
 - 2O-CPA on masked AES without profiling
 - CPA on MAC-Keccak



How to download

1

- Visit <http://tescase.coe.neu.edu>

2

- Go to *Downloads* page

3

- No registration required
- Just enter your information and we send download links to you

4

- Please cite our webpage and publications if you use our traces or attack library for publications



Tescase | Welcome x

tescase.coe.neu.edu/?current_page=softwarepage

TeSCASE - Testbed for Side Channel Analysis and Security Evaluation

Home People Projects Publications Downloads

Power Trace Data

Request Information

Data Type: AES Mask: Masked Number Of Traces: 50000

Downloader Information

First Name* Last Name* Phone Number

Email Address* Company/Organization*

Mailing Address

Type Of Organization* Purpose* Research Area*

Please select one. Please select one. Please select one.

If you chose "Other" for any field above, please clarify here:

evvrzsl1vd

Enter the text shown above:

Analysis library

- Implementation of CPA on AES (CPU+GPU)
 - Supports for both AMD GPUs (OpenCL) and Nvidia GPUs (CUDA)
- Easy setup and usage
 - Library will configure itself and build a GPU component based on the device found on the computer
 - Easy to use command line interface



Download at <http://tescase.coe.neu.edu>

Source Codes

Side Channel Analysis Library

9/01/2013 – present

Licensed Under the [MIT License](#)

Download

The Side Channel Analysis Tool is an open source tool written in C++ that allows the user to recover encryption keys from leakage data obtained through some form of Side Channel Analysis. Currently only Correlation Power Analysis (CPA) for the AES-128 encryption algorithm is supported but we hope to continue supporting and expanding the range of analysis and encryption algorithms for the future.

Build Instructions

The Side Channel Analysis Tool has several dependencies that must be installed before use:

1. [CMake](#) - CMake is a family of tools used to simplify the compilation process. The minimum required version of CMake for the SCA Tool is 2.8
2. [OpenMP](#) - OpenMP is an API that allows for multithreading and is used throughout the tool to speed certain processes.

<http://tescase.coe.neu.edu>



NUEESS, Northeastern University