DPA Attack Flow

Author : Antarpreet Singh
Version : 1.0

- DPA Attack is a Makefile based Flow.
- Internally, it uses combination of various Perl scripts and C++ to perform actual DPA attack

Makefile targets are explained as below :

DPA :

It is a top-level target which will do everything from :

- Generating the spice file
- Generating stimuli required
- Generating nanosim cfg file
- Run nanosim simulation
- Perform DPA attack
- Generating Current Variance and Mean data

run_nanosim :

It'll only perform Nanosim simulation, given the spice file and stimuli is properly in place.

gen_spice :

It'll generate the spice file and stimuli required to perform DPA attack

gen_cfg :

Generate configuration file for nanosim simulation.

Currvar :

Generate current variance and Mean of current drawn from supply.

Clean :

Clean unused files

Clean_data :

Clean data files

In order to perform DPA Attack, it is important to set Makefile parameters correctly, otherwise one or other script will fail.

Makefile Parameters :

SCRIPTS_PATH :

Directory Path where all scripts are kept

NO_OF_KEY_BITS :

Number of Keys bits we are trying to find by performing DPA attack

KEY :

The value of Key for Test. The stimuli is generated according to this KEY value and while performing DPA attack, flow checks if it is able to find the correct Key.
Has to be between 0 and 2^(NO_OF_KEY_BITS) – 1.

NO_OF_IP_BITS:

Number of plain text input bits.

No_OF_OP_BITS:

Number of cipher text output bits.

NO_OF_VECTORS:

Number of random vectors to be generated to perform the DPA attack

SPICE_NETLIST:

Full Path of Spice netlist File to perform nanosim simulation.

SOURCE:

Source files 'PREFIX' for the stimuli source files to be used while performing DPA Attack. Useful when you have to use same stimuli over and over to test different scenarios.

TARGET:

Target files 'PREFIX' for output files.

OVERWRITE :

When OVERWRITE=0, stimuli from 'SOURCE' parameter is used to perform nanosim simulation instead of generating new stimuli. OEVRWRITE has to be 1 if new stimuli has to be generated.

Ideally, SOURCE = TARGET and OVERWRITE =1 when you are starting fresh.
Then, modify only the TARGET and set OVERWRITE=0 to use same stimuli for testing different scenarios.

PRECHARGE :

For DDL Logics, PRECHARGE has to be set to 1.
When PRECHARGE = 1, stimuli is generated with precharge after each vector input and also while performing DPA attack, overlap window is increased to two clock cycles.

METHOD :

Method for DPA Attack.
Values supported are CPA, CPA_HD, OPB, OPB_HD, HD, HW.

CPA – Correlation based DPA Attack
CPA_HD - Correlation based DPA Attack using Hamming Distance instead of Hamming weight.
OPB – DPA Attack based on Partitioning current waveform wrt Output Bits Hamming Weight and Then calculating Difference of means

for each Output Bit. (Kocher's Method)

OPB_HD - DPA Attack based on Partitioning current waveform wrt Output Bits Hamming Distance and Then calculating Difference of means for each Output Bit.

HW – Purely Hamming Weight Based Attack. Calculating Hamming Weight of Output Bits and Partitioning Based on that to Calculate Difference in Means.

HD – Purely Hamming Distance Based Attack. Calculating Hamming Weight of Output Bits and Partitioning Based on that to Calculate Difference in Means.

ALGORITHM :

Encryption Algorithm to be Attacked.
Valid Values are : DES10
Currently, Flow only supports Single stage Sbox-8 implementation of DES Encryption Algorithm.

INPUT_TOGGLE_PERIOD :

Time Difference between Input Signal Toggling in ns.

CLK_PERIOD :

CLK Period in ns.

Usually, INPUT_TOGGLE_PERIOD = CLK_PERIOD.

ACCUARCY :

Accuracy (or time resolution) with which current data is captured from nanosim simulation.
Default = 0.01 (ns)

SPICE_TRAN_START_TIME :

Start time for current data to be captured from nanosim simulation.
Default = 0 (ns)

INITIAL_DELAY :

Initial Delay during which are inputs are zero. Stimuli and CLK generation starts only after initial delay.

START :

DPA Attack is performed iteratively till all the Vectors are exhausted. START defines the initial value of number of vectors to be used for performing DPA attack

STEP :

STEP is the number of vectors incremented during each step till all vectors are exhausted for DPA attack

SPLITWF_START_TIME :

It is the time in ns from which you want current data to be split for DPA attack.

Ideally, it should be Equal to INITIAL_DELAY + Time before which input vectors are applied.

Example :

To perform DPA attack with just spice file and make file parameters set correctly :

make DPA OVERWRITE = 1