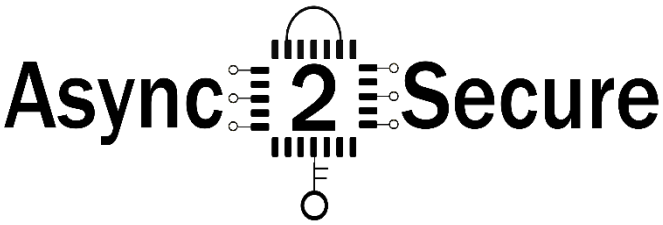

Side Channel Attack (SCA) Toolkit Quick-Start Guide

(For Arty-A7 and Arty-S7)

Version 1.0

(Updated: 09/10/2020)

List of Equipment and Software

Table 1 lists the hardware components needed for the experimental setup.

Table 1: Hardware components

No	Items	Functions/Description
1	Evaluation board (Arty A7 or S7)	• To run a cryptographic program such as Advanced Encryption Standard (AES)
2	USB 2.0 A-Male to Micro B Cable	• To power on the evaluation board • To connect the evaluation board to a personal computer for data communication
3	Board-to-board connectors	• To connect oscilloscope probes for trace measurements
4	Electromagnetic (EM) probes	• To pick-up the EM information on the FPGA chip running AES operations
5	Oscilloscope (provided by users)	• To collect the EM traces for SCA
6	A personal computer (provided by users)	• To transfer/send data for AES operation • To perform the SCA evaluation

Table 2 lists the software and files needed for the experimental setup.

Table 2: Software and files needed

No	Items	Functions/Description	From
1	Async2Secure SCA Evaluation tool	• To perform SCA evaluation on the implemented AES	Note 1
2	AES Sender/Checker Program	• To record the plain text and cipher text when running the AES program	Note 2
3	AES sample bit file and AES project file for the evaluation board	• AES sample files which are compatible for Arty evaluation board	Note 3
4	Vivado Webback Design/Design Suite	• To implement an AES hardware on the Xilinx FPGA of the evaluation board	Note 4

Note 1: Visit http://async2secure.com/products/tools for more information and enquires
Note 2: Visit http://async2secure.com/resources for more information
Note 3: Visit http://async2secure.com/resources for more information
Note 4: Visit https://www.xilinx.com/support/download.html .

System Requirements (recommended)

No	Host PC	Recommended Requirements
1	Operating Systems	• Windows 10 (tested) • Linux (Tested on Ubuntu 18.04 LTS 20.04 LTS)
2	Processors	• Minimum: Any Intel or AMD x86-64 processor • Recommended: With four logical cores
3	RAM	• Minimum: 8 GB • Recommended: 16 GB

Hardware Setup

1. Download the sample AES bit file (AES_ARTY_TOP_####.bit) from our website, http://async2secure.com/resources. #### denotes the 4-digit code of the board version. For example, #### is A735 for Arty-A735T board, and S725 for Arty-S725 board.

2. Download and install the AES sender/checker program from our website, http://async2secure.com/resources.

3. Download and install the latest Vivado WebPACK/ Design suite from Xilinx website, https://www.xilinx.com/support/download.html .

4. After installation, launch Vivado. Click “Open Hardware Manager” in Vivado WebPACK under “Tasks” as shown in Figure 1.

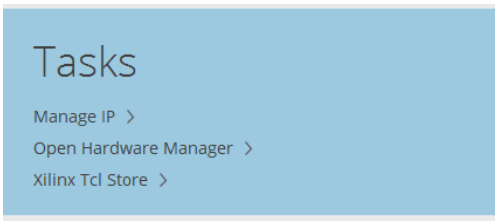

Figure 1: Vivado View

5. Connect ARTY board to the PC using USB cable given in our Toolkit. Click on “Auto Connect” under Hardware Window.

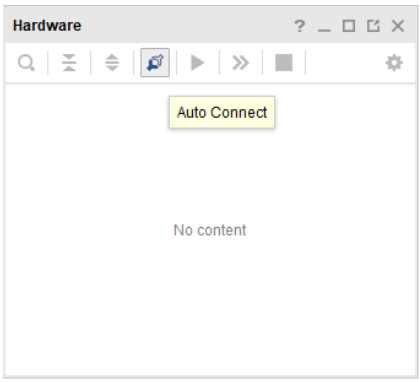

Figure 2: Connecting to FPGA Board

6. When the devices appear in the Hardware window, right click on the FPGA name, and select “Program Device”. Browse and select the bit file (AES_ARTY_TOP_####.bit). Click “Program” and wait until it is successfully programmed.

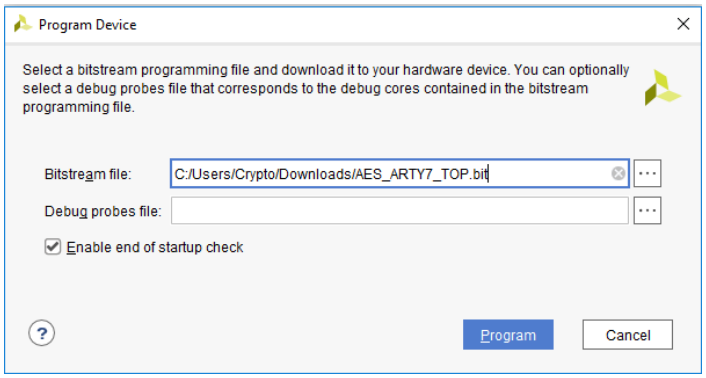

Figure 3: Programming FPGA

7. To start the FPGA, set the switches, i.e. SW3 = SW2 = SW1 = ‘DOWN’, SW0 = ‘UP’, as shown in the Figure 4.

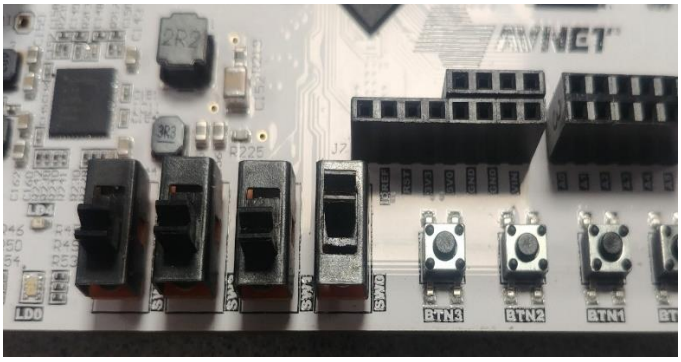

Figure 4: Switches to start the FPGA

8. Connect an EM probe and a passive probe to the oscilloscope. Connect the passive probe to the pin IO0 as the Trigger signal for data capturing, as shown in Figure 5. Set the switching threshold for the Trigger signal to 1.65V since the Trigger signal is operating within 3.3V.

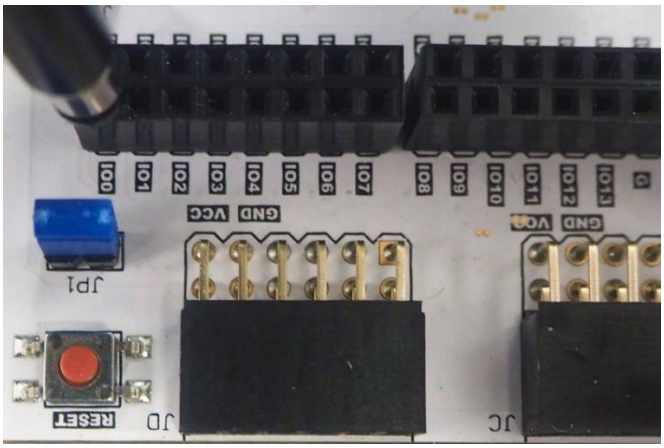

Figure 5: IO0 pin location for oscilloscope probe

9. Connect the Ground of the oscilloscope probe to any of the GND pins available on the board, as shown in Figure 6.

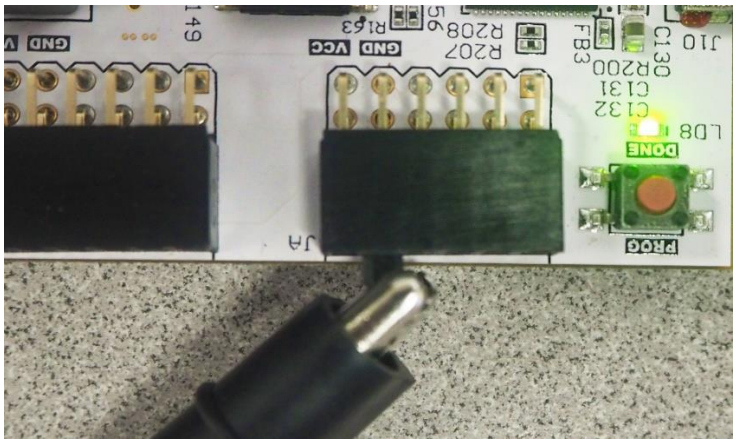

Figure 6: GND connection for your oscilloscope probe

10. Connect the EM probe to oscilloscope and place the EM probe tip onto the FPGA chip as shown in Figure 7.

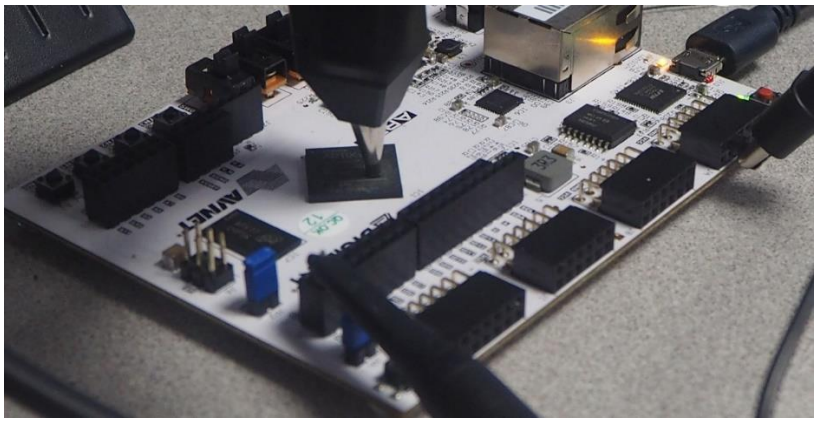

Figure 7: EM probe placed on the main FPGA chip

11. Launch the AES sender program in the PC. Set the Baud rate to 9600 and click “Connect”. Type in “No. of Traces” you would like to collect and click “Start”.

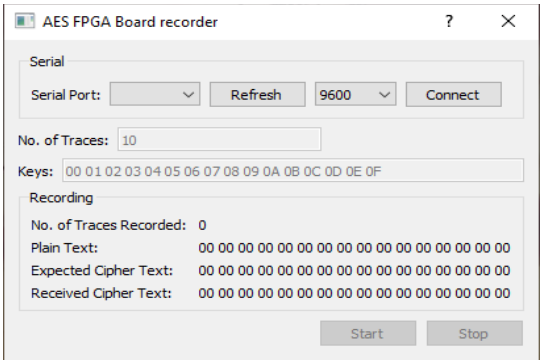

Figure 8: AES sender program used for sending plain text to the board

12. The waveforms of EM signal and Trigger signal can be observed as shown in Figure 9. Record the EM signal waveforms for a total of 450ns before the Trigger signal for SCA evaluation.

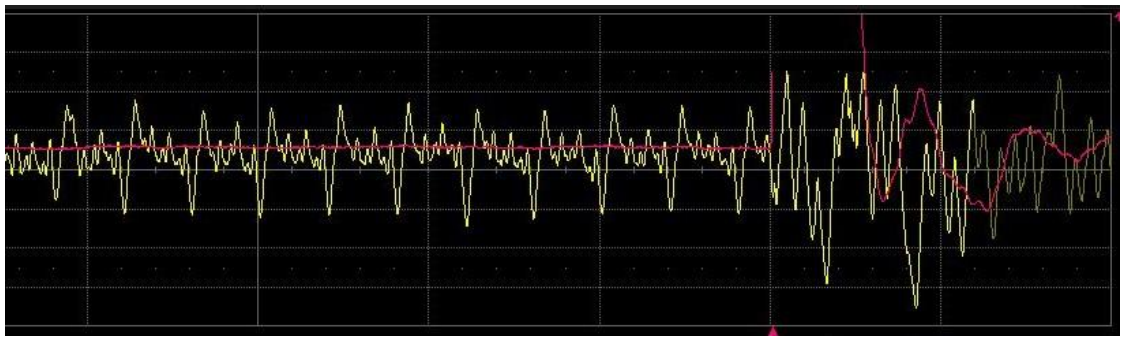

Figure 9: EM waveform with Trigger signal on Oscilloscope

Software Setup

1. First, log in with your account after the application is launched as shown in Figure 10.

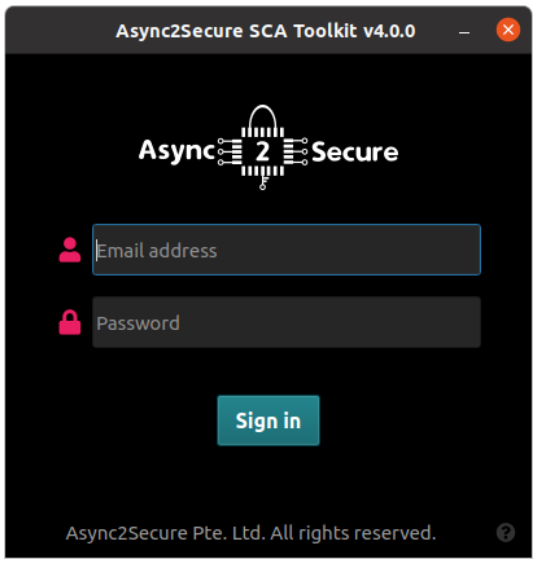

Figure 10: Login screen

2. Data Conversion – To convert the collected traces from the oscilloscope into *.h5 file format.
   - From the Menu, go to *'Data Conversion' > 'Periodic Data to Samples'.*
     (i) Click '*Load Files*' to load traces file in CSV format as shown in Figure 11.
     (ii) Click '*Save As*' to save all trace files as a single file in *.h5 file format, e.g. "568_traces.h5".
     (iii) Then click '*Process*' to perform the conversion.

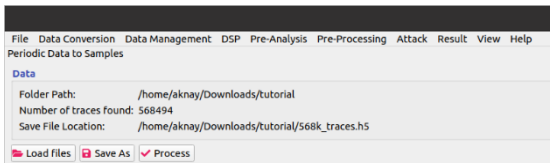

Figure 11: Periodic data to samples in data conversion

3. Building Project File – to generate a single project by combining traces, plain text, cipher text with the following steps.
   - From the Menu, go to '*Data Management' > 'Build Project File'* as shown in Figure 12. Click '*Load Files*'.

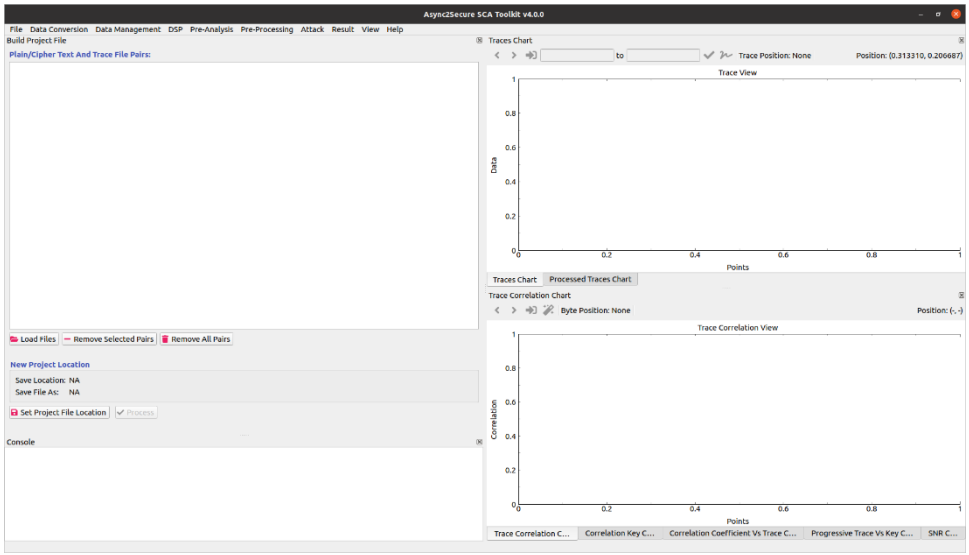

Figure 12: Building a project file

- The "Add Files" window is displayed as shown in Figure 13.
  (i) Click '*Load Trace File*' to load *.h5 file (generated from above step 2 – Data Conversion).
  (ii) Click '*Load Plain Text File*' (generated during the trace collection step).
  (iii) Click '*Load Cipher Text File*' similarly.
  (iv) Click '*Set Key*' (i.e. AES key used for generating traces during the trace collection step).
  (v) Finally, click '*Add to Project File*' to add those pair (traces, plain text, cipher text and key) to the project file.

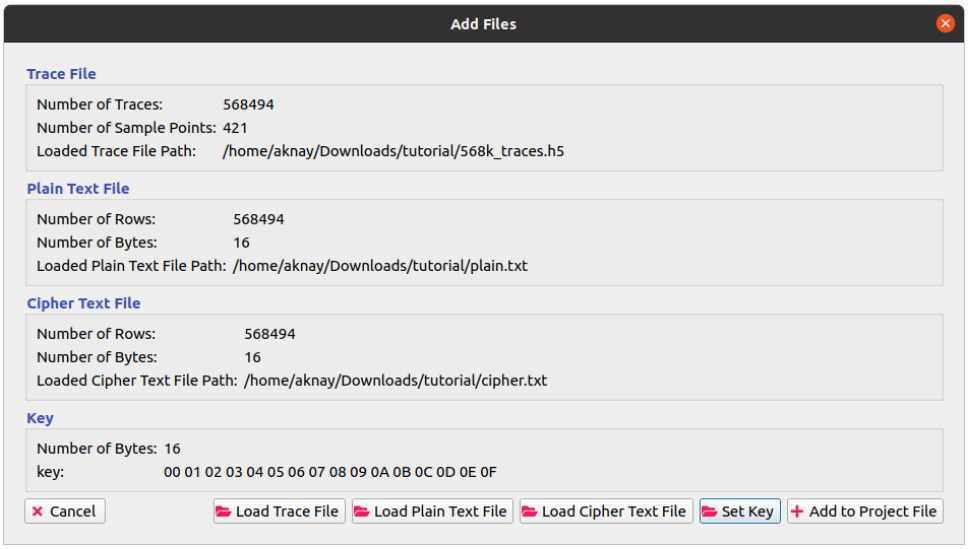

Figure 13: Add files to the project file

- Thereafter, the current window "Add Files" is closed, and the previous window "Build Project File" is displayed again as shown in Figure 14.
  (i) As seen, the pair (traces, plain text, cipher text and key) is displayed as a list.
  (ii) Once confirmed, click '*Set Project File Location*' to save the project file.
  (iii) Then click 'Process' to generate a project file.
  (iv) Side Note: More pairs can be added to the project similarly to build a list of different pairs.

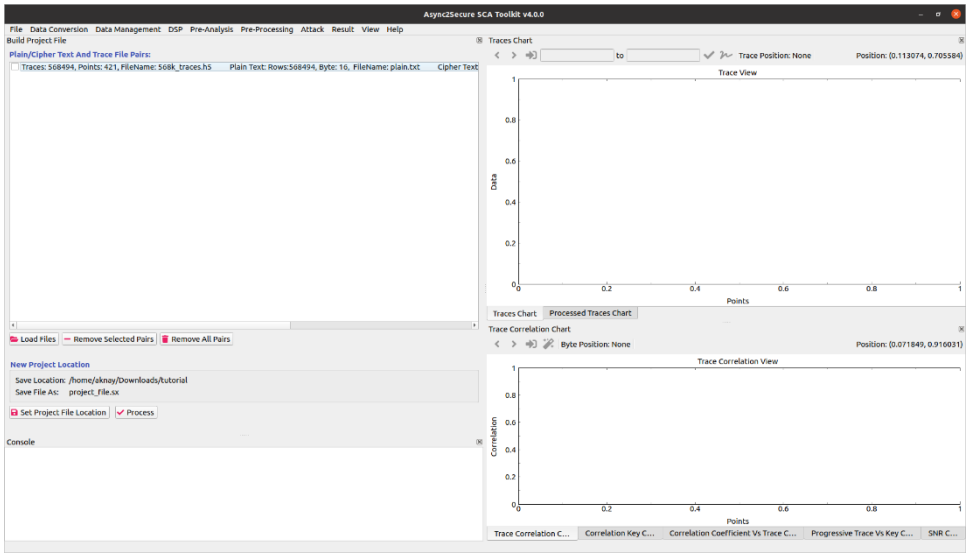

Figure 14: After adding files to the project file

4. Attacking Phase – to specify the SCA settings and to perform SCA evaluation.
   - From the Menu, go to '*File*' > '*Project*' > '*Open Project*' to load the project file (generated from the previous step 3 – Building Project File).

   - Once the project file is loaded, go to '*Attack*' > '*Correlation*' from the menu. The "Correlation" window is displayed as shown in Figure 15.
     (i) Specify the trace sample region (points of interest) at '*Samples*' under the '*Range*' panel.
     (ii) Choose either CPA or DPA for the attack.
     (iii) Choose the appropriate round, model and target to match the hardware leakage.
     (iv) In this current setup, the 'CPA' attack, 'Last' round, 'Hamming Distance' model and 'SR^ISB' target are selected for the attack.
     (v) Tick the options under the 'View' panel for different kinds of analysis
     (vi) Then click '*Process*' for the analysis.

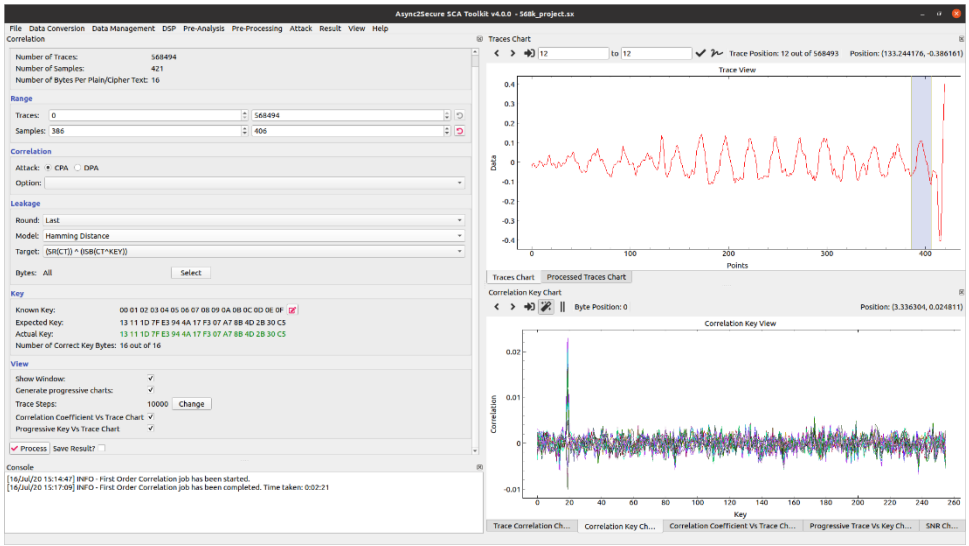

Figure 15: Attacking and analysing the collected traces

5. Analysis Phase – to check whether the key can be retrieved successfully or not, as shown in Figure 15.
    - Under the 'Key' panel, the 'Actual Key', i.e. key guess from the correlation will be compared with the 'Expected Key', i.e. calculated key at the selected round.
    - After the correlation is performed, there are two possible outcomes, i.e. the key guess is correct (highlighted in green), and the key guess is wrong (highlighted in red).
    - Users can further analyze each byte's leakage at time in the correlation key chart and trace correlation chart.

Technical and Sales Support

Please contact us at contact@async2secure.com for technical and sales supports We welcome any feedback.

Appendix: AES Interface

Figs. A1 (a) depicts the default interface signals for the AES cipher used. If a custom AES having different interface signals, the custom AES needs to be re-designed having the same interface signals to allow the AES Sender/Checker Program to function properly. This can be done easily with a Verilog interface wrapper. Table A1 tabulates the definition of the interface signals and Fig. A2 depicts the waveform pattern of the interface signals. Please follow the interface pattern for your custom AES design.

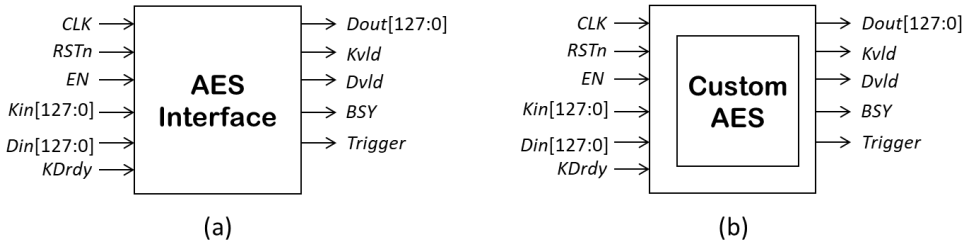

Fig. A1: Interface signals for AES (a) default, and (b) embodying a custom AES

Table A1 The definition of the interface signals

No	Signal Name	Input/Output	Remark
1	*CLK*	Input	Clock signal
2	*RSTn*	Input	Active low reset signal
3	*EN*	Input	Active high enable signal
4	*Kin*[127:0]	Input	Key
5	*Din*[127:0]	Input	Plaintext
6	*KDrdy*	Input	Start signal (for both Key and Plaintext)
7	*Dout*[127:0]	Output	Ciphertext
8	*Kvld*	Output	Key valid signal
9	*Dvld*	Output	Data valid signal (after *N* cycles)
10	*BSY*	Output	Busy signal (for operation)
11	*Trigger*	Output	Trigger signal (for oscilloscope triggering)

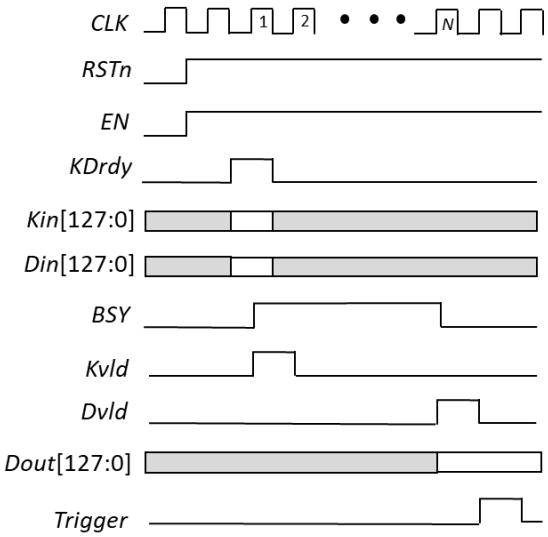

Fig. A2: Interface signals Pattern for a Proper Operation