



## FPGA Evaluation Boards for Side-Channel-Attack (SCA)

Many choices of FPGA evaluation boards are available and compatible with our SCA evaluation platform. Construct your design for SCA evaluation.

Async2Secure is dedicated to provide solutions to mitigate and evaluate hardware attacks on Integrated Circuits (IC). There are a wide range of SCA evaluation boards that can be used with our SCA evaluation platform. Fig. 1 depicts the block diagram how an FPGA evaluation board can be used for SCA evaluation. We provide the interface block (in FPGA) that can transfer the data between a

### Key Features

- Many FPGA boards available and ready for SCA evaluations
- Built-in interface block (in FPGA) to transfer data from/to a personal computer (PC)
- Built-in programmable data/key generator (in the PC) to generate various data/key
- Built-in AES output checker (in the PC) to verify the results
- Support FPGA programmer (in the PC) to realize various AES designs
- Fully compatible for our SCA platform (to receive data and EM/power traces)
- AES design examples available
- Tutorial available

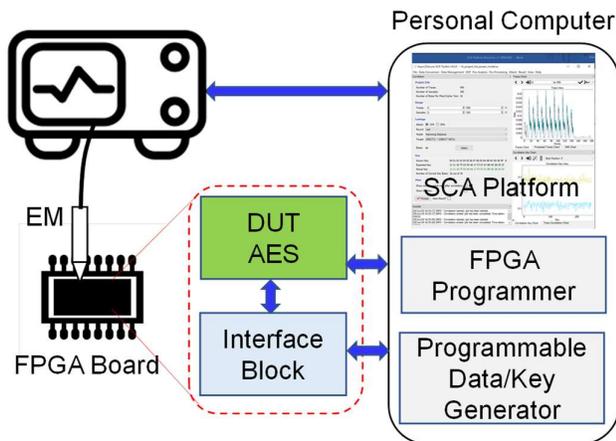


Fig. 1: The block diagram to link an FPGA board embodying an AES device-under-test (DUT) for SCA evaluations

personal computer (PC) and an FPGA chip. A programmable data/key generator (in the PC) is available to easily generate data and key for the SCA evaluations. Different AES design architectures are possible to be realized without changing the interface block, enabling simple SCA evaluations using our SCA evaluation platform. Fig. 2 depicts an FPGA board under SCA evaluation.



Fig. 2: An FPGA prototype SCA evaluation using our SCA evaluation platform

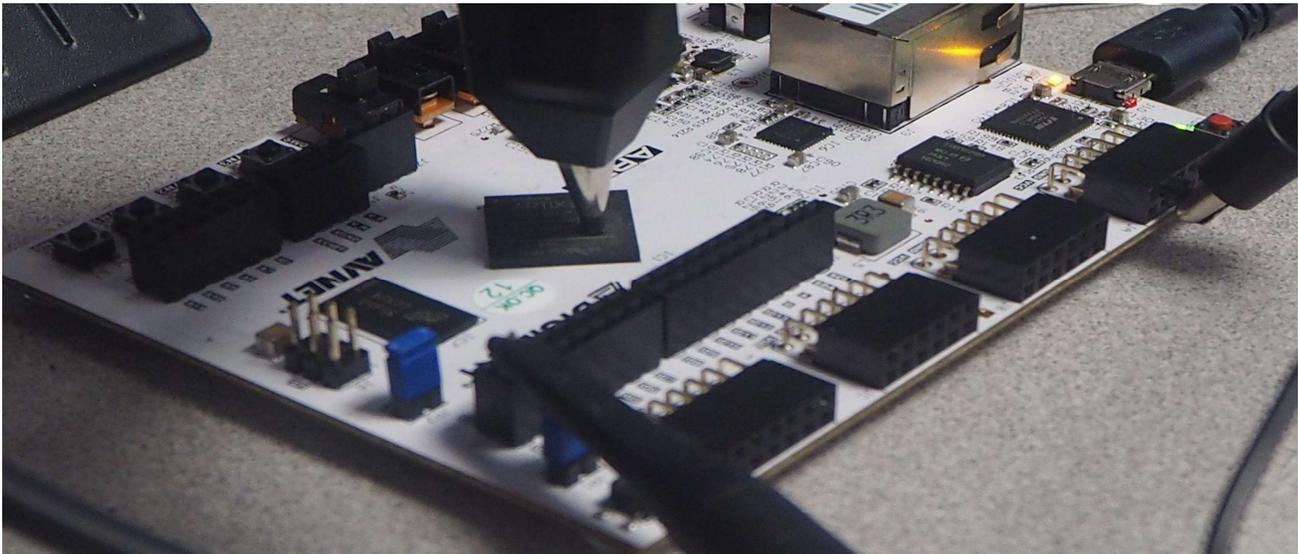
Table I lists the available Xilinx FPGA chips within various FPGA evaluation boards for SCA evaluation. Table II lists the available Intel FPGA chips within various FPGA evaluation boards for SCA evaluation. Please feel free to contact us to explore the preferred FPGA evaluation boards.

Table I  
Xilinx FPGA Chips within the Evaluation Boards

No	FPGA	Logic Cells
1	Artix-7 XC7A35TICSG324-L	32,280
2	Spartan-7 XC7S50-CSGA324	52,160
3	Zynq-7000 XC7Z020-1CLG400C	85,000
4	Artix-7 XC7A100TCSG324-1	101,440

Table II  
Intel FPGA Chips within the Evaluation Boards

No	FPGA	Logic Cells
1	MAX-10 10M08SAU169C8G	8,000
2	Cyclone-IV EP4CE22F17C6N	22,320
3	MAX-10 10M50DAF484C7G	50,000
4	Cyclone-V 5CSEBA6U23I7	110,000



For more information, visit <http://Async2Secure.com>

Async2Secure Pte Ltd, TCH TechCentre #05-07, 71. Toh Guan Road East, Singapore 608596  
Contact: [contact@async2secure.com](mailto:contact@async2secure.com)