SASEBO-RII (rev.3) Quick Start Guide

[Version 0.1]

May 12, 2014

Research Institute for Secure Systems
National Institute of Advanced Industrial Science and Technology

1. Equipment preparation

Before setting up the SASEBO-RII (rev.3) environment and running its test program, please ensure the availability of the following instruments:

(1) SASEBO-RII—the main board, to measure the power consumption of the target Cryptographic LSI

(2) ZUIHO—the FPGA board, to control SASEBO-RII

(3) Cryptographic LSI—the target LSI chip to apply power analysis attack. We at the National Institute of Advanced Industrial Science and Technology (AIST) do not provide a cryptographic LSI, so please provide your own LSI.

(4) Host PC—a Windows Vista/7 PC with USB ports to communicate with ZUIHO

(5) USB cable—to connect the Host PC and ZUIHO

(6) Xilinx FPGA configuration cable—to download the configuration data of FPGA on ZUIHO, e.g., Xilinx Platform Cable USB II

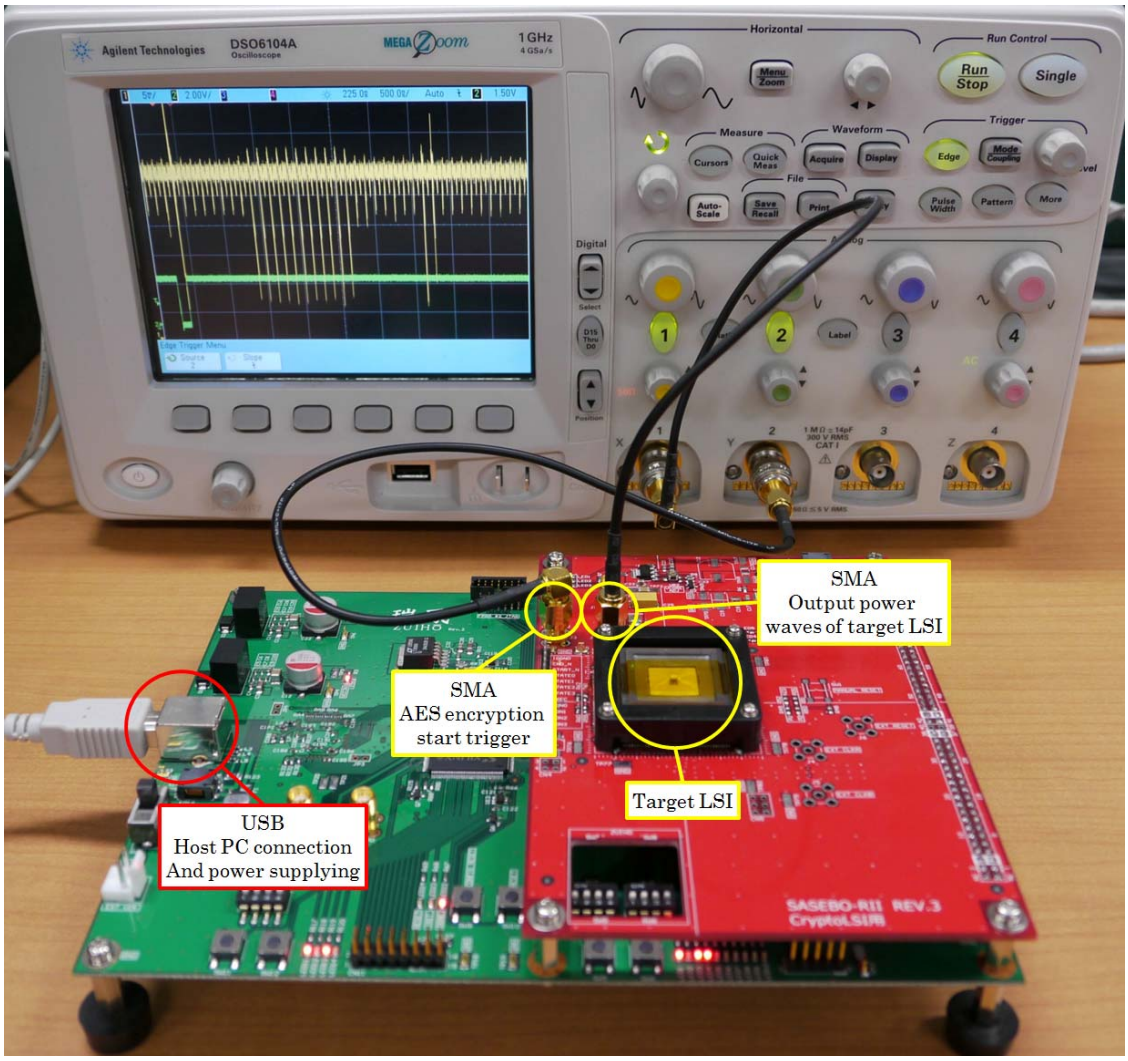
(6) Software (please see Section 3)—e.g., SASEBO_RII_Checker, Microsoft .NET Framework 4.0, and Xilinx ISE WebPACK (latest version is 14.6 on May 9, 2014)

(7) Oscilloscope—to obtain the power traces of the target LSI

(8) BNC-SMA cable (× 2)—two cables to connect SASEBO-RII and the oscilloscope: one obtains the trigger signal, and the other obtains the power traces of the target LSI. The BNC connector should be properly selected according to the termination resistance of the oscilloscope (50 Ω or 1 MΩ). If the oscilloscope supports only 1-MΩ probes, you should prepare 50-Ω terminators to connect the SMA cables to the oscilloscope. Otherwise, the typical 1-MΩ passive probes could substitute for the SMA cables.

2. Connections

1. Connect ZUIHO and the host PC using the USB cable.
2. Connect SASEBO-RII and the oscilloscope using the BNC-SMA cables.



3. Software installation

Download and install the following software:

(1) SASEBO_RII_Checker—software for testing the target LSI on SASEBO-RII. SASEBO_RII_Checker is included in the archive file “Control HW/SW,” which can be downloaded for free from the RISEC Website:

https://www.risec.aist.go.jp/project/sasebo/

(2) Microsoft .NetFramework 4.0:

http://www.microsoft.com/ja-jp/download/details.aspx?id=17851

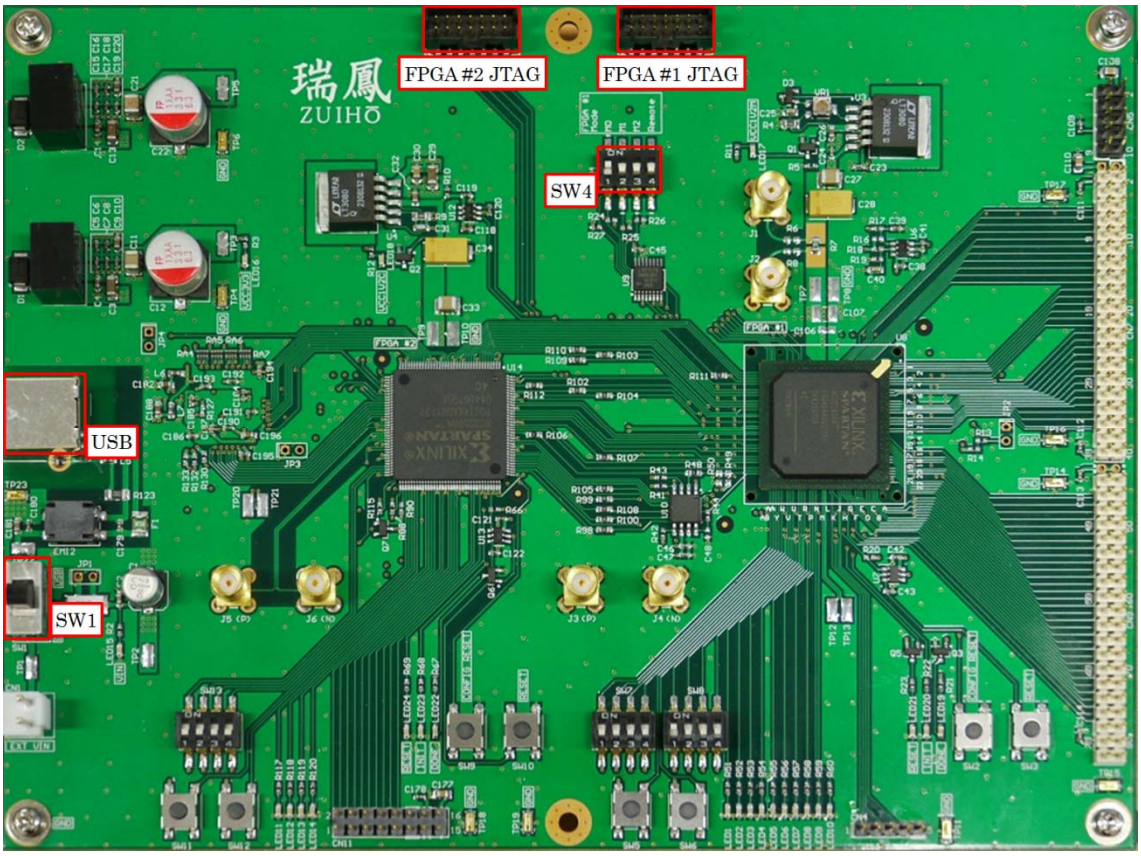
(3) Xilinx ISE WebPACK (latest version is 14.6 on May 12, 2014):

http://japan.xilinx.com/products/design-tools/ise-design-suite/ise-webpack.html

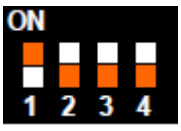
(4) FTDI driver (D2XX driver):

http://www.ftdichip.com/Drivers/D2XX.htm

4. Setting up ZUIHO



(1) SW4



Turn on 1.

(2) Configure FPGA #2 on ZUIHO.

[1] Connect the host PC and ZUIHO as follows:

・Host PC→FPGA configuration cable→FPGA #2 JTAG connector (ZUIHO)

・Host PC→USB cable→USB connector (ZUIHO)

[2] Slide SW1 to “USB” to supply power to ZUIHO via the USB cable.

[3] Start Xilinx ISE Design Suite and open project File: “File” → “Open Project” → “zuiho_ctrl¥zuiho_ctrl¥zuiho_ctrl.xise.”

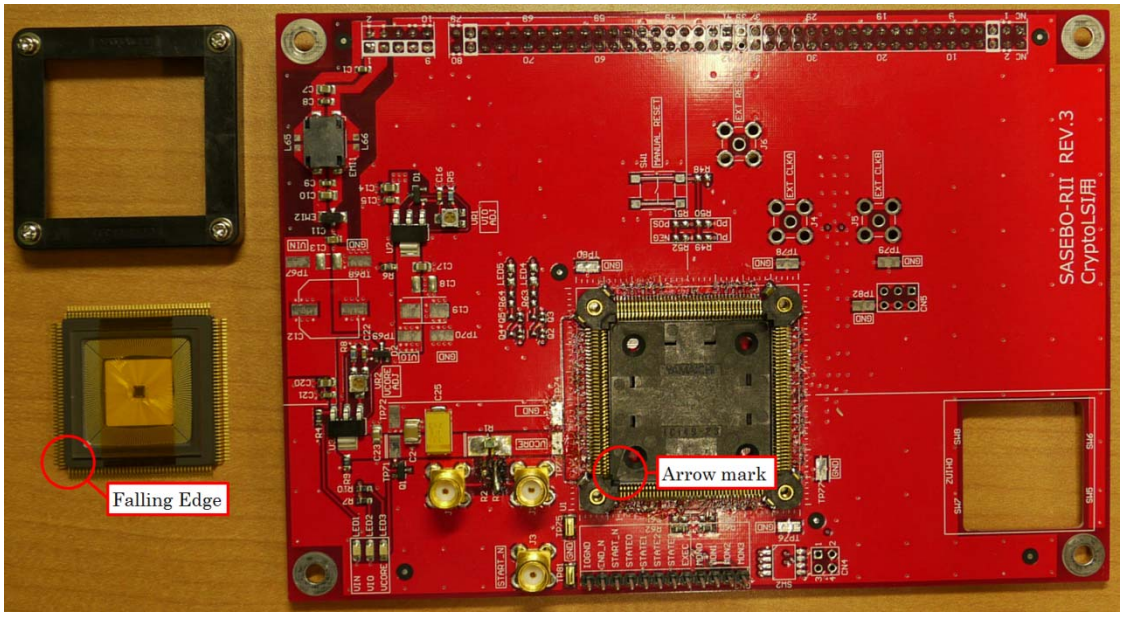
[4] Select the “Design” tab and then select “CHIP_ZUIHO_CTRL” in the Hierarchy window.

[5] Double-click “Configure Target Device” and then double-click “Boundary Scan.” Subsequently, push the “Initialize Chain” button and open the configuration file “zuiho_ctrl¥chip_zuiho_ctrl.bit.”

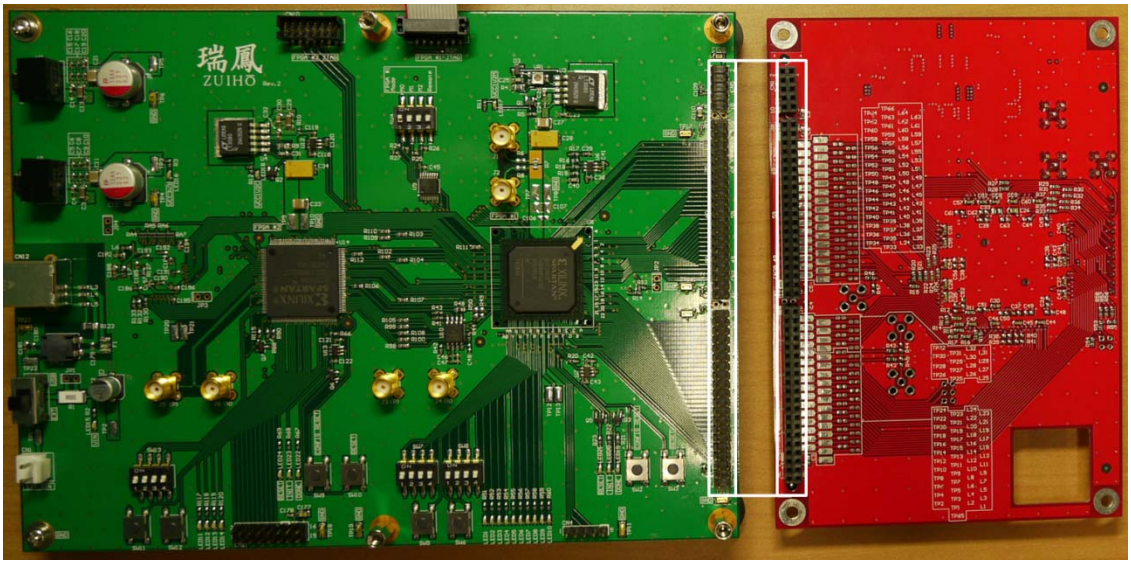
[6] Right-click “FPGA(xc3s50an)” in the ISE iMPACT window and execute “Program Flash and load FPGA ....” When the message “Program Succeeded” pops up, configuration of FPGA #2 is completed.

5. Setting up SASEBO-RII

(1) Installation of the target LSI onto SASEBO-RII



[1] PUF the target LSI so that the diagonal corner of the LSI matches the arrow mark in the SASEBO-RII socket.



[2] Join the pin headers in SASEBO-RII to the pin sockets in ZUIHO.

(2) Configuration of the Control FPGA (FPGA #1) on ZUIHO

[1] Connect the host PC and ZUIHO as follows:

・Host PC→FPGA configuration cable→FPGA #1 JTAG connector (ZUIHO)

・Host PC→USB cable→USB connector (ZUIHO)

[2] Slide SW1 to "USB" to supply power to ZUIHO.

[3] Start Xilinx ISE Design Suite and open project File: "File" → "Open Project" → "zuiho_rii_aist_rev_3¥zuiho_rii_aist_rev_3¥zuiho_rii_aist_rev_3.xise."

[4] Select the "Design" tab and then select "CHIP_ZUIHO_RII_CTRL" in the Hierarchy window.

[5] Double-click "Configure Target Device," and then double-click "Boundary Scan." Subsequently, press the "Initialize Chain" button and open the FPGA configuration file "zuiho_rii_aist_rev_3¥zuiho_rii_aist_rev_3¥chip_zuiho_rii_ctrl.bit" and the FLASH configuration file: "zuiho_rii_aist_rev_3¥zuiho_rii_aist_rev_3¥ zuiho_rii_aist_rev3.mcs." The ROM configurations are "SPI PROM" and "ST45DB081D."

[6] Confirm that the string "Identify Succeeded" is displayed. Right-click "FLASH" and execute "Program." When the message "Program Succeeded" is displayed, configuration of FPGA #1 (and FLASH) is completed.

6. Encryption test

(1) Connect the host PC, ZUIHO, and oscilloscope as follows:

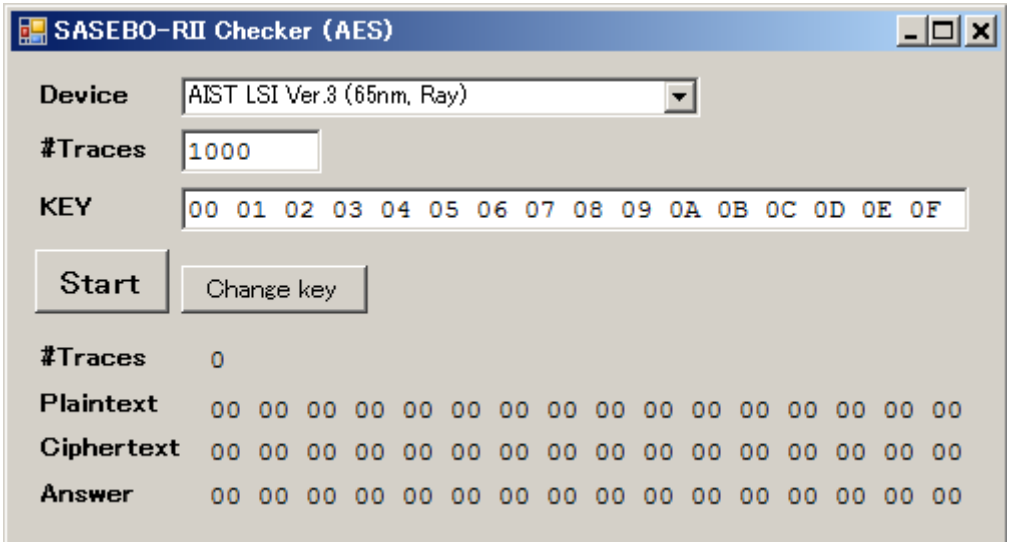
・Host PC→USB cable→USB connector (ZUIHO)

・Oscilloscope Channel1→BNC-SMA cable→J2 connector (SASEBO-RII)

・Oscilloscope Channel2→BNC-SMA cable→J3 connector (SASEBO-RII)

(2) Start

"SASEBO_RII_Checker¥SASEBO_RII_Checker¥bin¥Release¥ SASEBO_RII_Checker.exe."



(3) Set the parameters as follows:

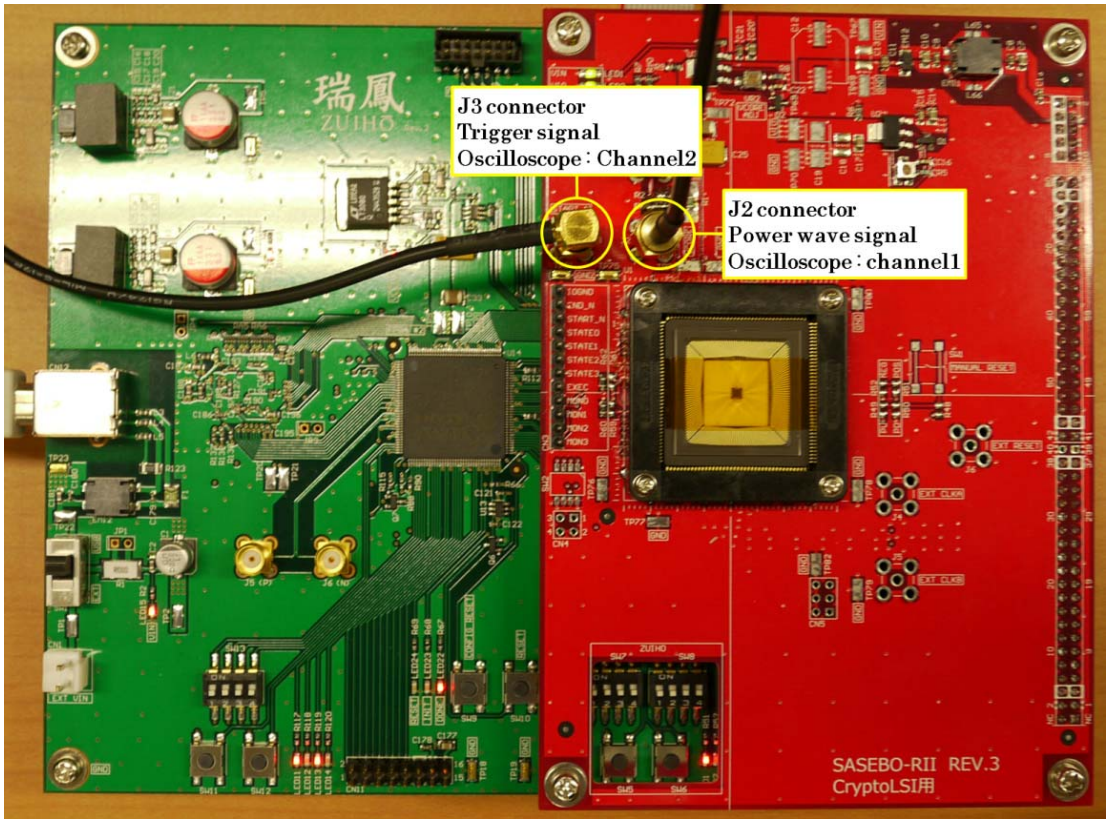
・Device: select your LSI type

・Traces: number of execution of the AES encryption

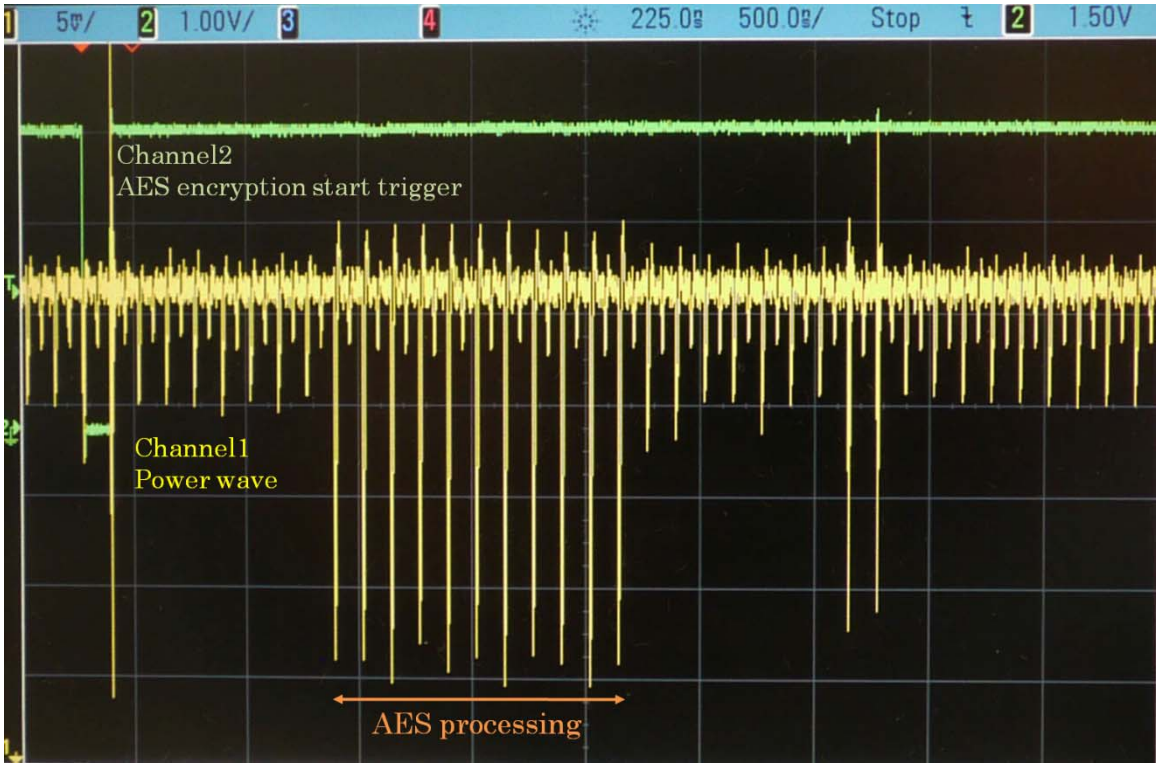
・KEY: encryption key used for the AES encryption

(4) Press the "Start" button to start the AES encryption.

7. Measuring the power consumption of the LSI



In our LSI, the trigger signal to start the AES encryption is observed at J3 on SASEBO-RII. Therefore, connect J3 and Channel2 of the oscilloscope using a BNC-SMA cable. Subsequently, connect J2 on SASEBO-RII and Channel1 of the oscilloscope using a BNC-SMA cable. The power consumption of the LSI is observed at J2. You can observe the power traces of the LSI when you run “SASEBO_RII_Checker.”



The configuration of the oscilloscope in our test environment is given below.

- Trigger source: Channel2
- Trigger category: Edge (falling)
- Trigger power voltage: 1.5 V
- Time range: 500 ns/div
- Channel1 voltage range: 5 mV/div
- Channel1 offset: 1.275 V
- Channel2 voltage: 1 V/div
- Channel2 offset: 0 V

The SASEBO-RII board was developed by the AIST in a project sponsored by the Core Research for Evolutional Science and Technology funded by Japan Science and Technology Agency.

Address technical inquiries to:
National Institute of Advanced Industrial Science and Technology (AIST)
Tsukuba HQ #3408, AIST Tsukuba Central 2
1-1-1 Umezono, Tsukuba, Ibaraki 305-8568, Japan
TEL: +81-29-861-5284
FAX: +81-29-861-5285