SASEBO Quick Start Guide

(for SASEBO, SASEBO-G, and SASEBO-R)

[Version 1.0]

October 1, 2008

Research Center for Information Security,
National Institute of Advanced Industrial Science and Technology

1. Equipment preparation

Before setting up the SASEBO instrumental environment and running its test program, have the following equipment available:

(1) SASEBO
The SASEBO package contains the SASEBO (a parts-mounted print circuit board), two power cables, and several shunt resistors.

(2) Power supply
The SASEBO requires a power supply of 3.3 VDC at 1.0 Amps.

(3) Serial cable: Either RS-232 female-female 9-pin cable or USB cable
The SASEBO prototype (the first version of SASEBO) uses an RS-232 cable to communicate with the host PC.
SASEBO-R and SASEBO-G connect to the host PC with either an RS-232 or USB cable.

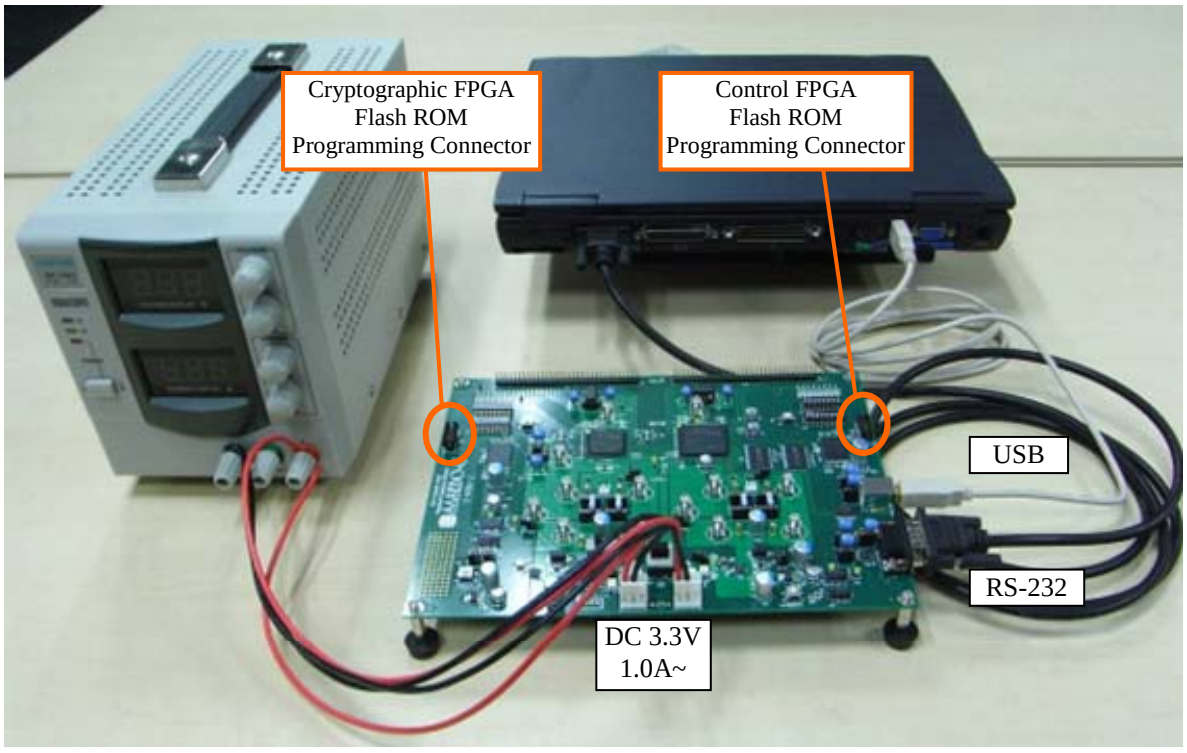
(4) Host PC
Have a middle-range Windows 2000/XP/Vista PC as the host computer of SASEBO.

(5) Software (See Section 3)
The instrumental environment requires Microsoft .Net Framework 3.5 and Xilinx ISE (WebPACK or Foundation, whichever works).
To use SASEBO-R or SASEBO-G with the USB connection, you also need the driver software D2XX and library FTD2XX_NET_DLL, both provided by FTDI.

(6) FPGA configuration cable
Have either of the Xilinx Platform Cable USB, Platform Cable USB II, or Parallel Cable III/IV available. This cable is used to program the flash ROMs connected to the FPGAs.

2. Connections

Connect the power supply to SASEBO with the power cables. Connect between SASEBO and the host PC with the USB or RS-232 cable.



3. Software installation

Download and install the following software:

(1) SASEBO test program: sasebo_tester

http://www.rcis.aist.go.jp/special/SASEBO/index-en.html
(via introduction page in English)

http://www.rcis.aist.go.jp/special/SASEBO/
(via introduction page in Japanese)

(2) Microsoft .Net Framework 3.5

http://www.microsoft.com/downloads/details.aspx?FamilyID=333325fd-ae52-4e35-b531-508d977d32a6
(English version)

http://www.microsoft.com/downloads/details.aspx?FamilyID=333325fd-ae52-4e35-b531-508d977d32a6&displaylang=ja
(Japanese version)

(3) Xilinx ISE WebPACK

http://www.xilinx.com/ise/logic_design_prod/webpack.htm
(English version)

http://japan.xilinx.com/ise/logic_design_prod/webpack.htm
(Japanese version)

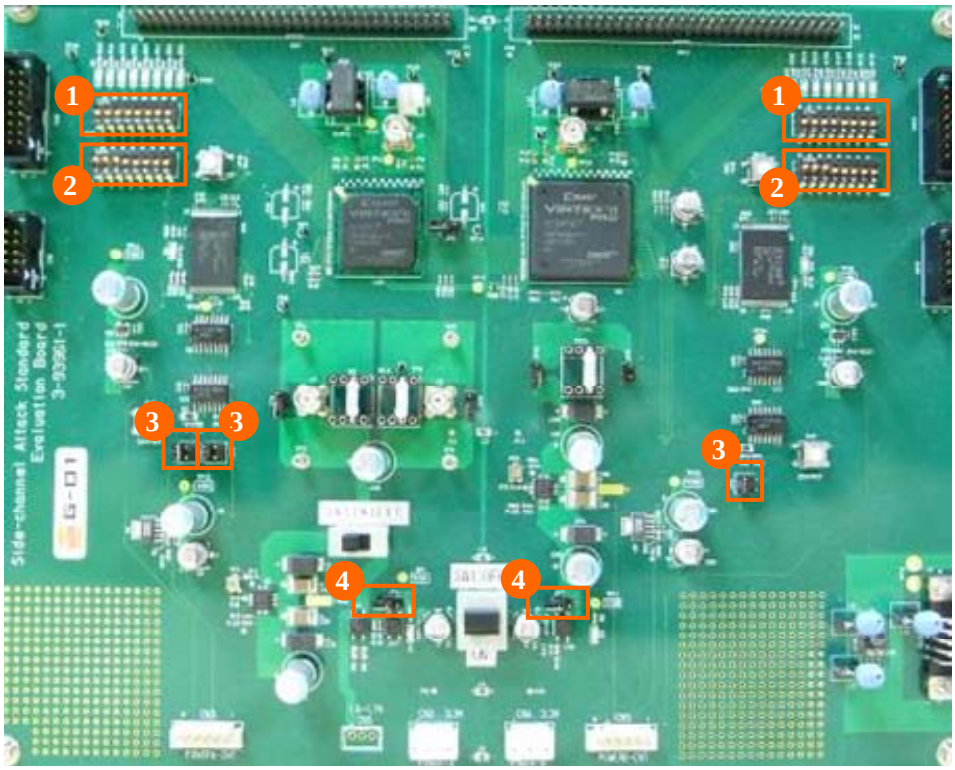
(4) FTDI D2XX driver and FTD2XX_NET_DLL

http://www.ftdichip.com/Drivers/D2XX.htm
(D2XX driver)

http://www.ftdichip.com/Projects/CodeExamples/CSharp.htm
(FTD2XX_NET_DLL)
Place FTD2XX_NET_DLL in the directory where the application files of sasebo_tester have been installed.

4. Setting up SASEBO

- DIP switch and jumper settings for SASEBO (protptype)



(1) SW5, SW9

All OFF.

(2) SW4, SW8

Turn ON 1, 2, and 3.

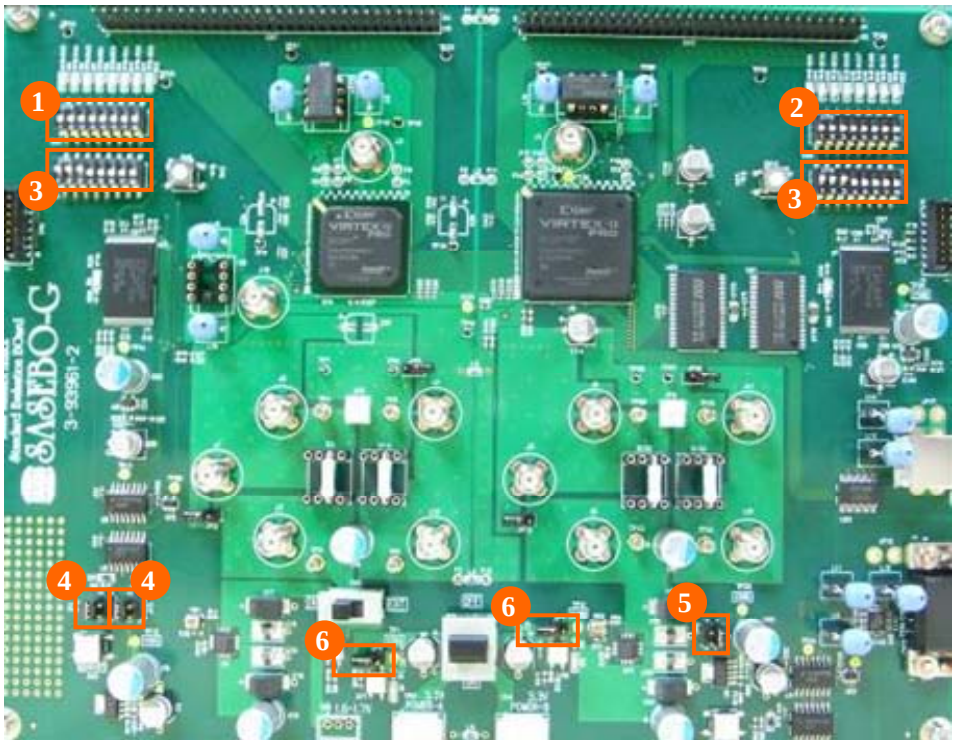
(3) JP1, JP2, JP6

Place a jumper on the left pins.

(4) JP4, JP7

Open.

➢ DIP switch and jumper settings for SASEBO-G



(1) SW5

All OFF.

(2) SW9

All OFF for RS-232. Turn 1 ON for USB.

(3) SW4, SW8

Turn ON 1, 2, and 3.

(4) JP1, JP2

Place a jumper on the left pins(1,2).

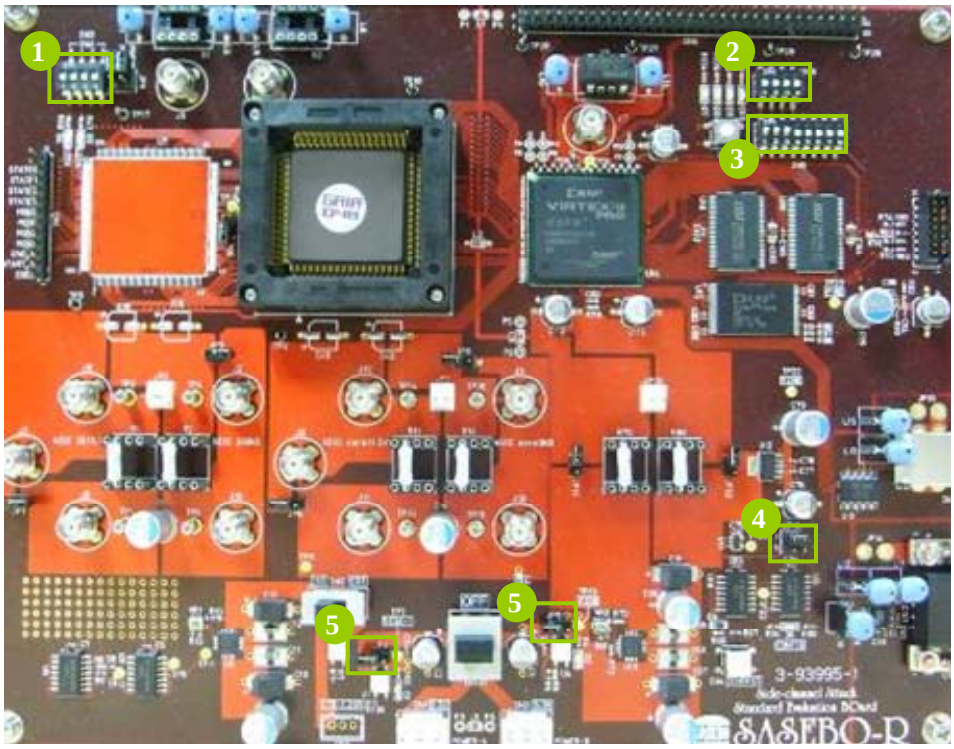
(5) JP6

Place s jumper on the right pins(1,2).

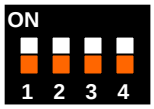
(6) JP4, JP7

Open.

➢ DIP switch and jumper settings for SASEBO-R

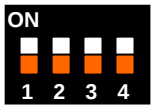


(1) SW3



All OFF.

(2) SW6



All OFF for RS-232. Turn 1 ON for USB.

(3) SW5

Turn ON 1, 2, and 3.

(4) JP10


Place a jumper on the upper pins(1,2).

(5) JP4, JP5


Open.

➢ FPGA configuration

To reprogram the flash ROM (XCF16P) for the control FPGA, attach the configuration cable to CN10 for the SASEBO prototype and SASEBO-G or to CN5 for SASEBO-R. For configuration, use the provided mcs file sasebo_v2p30_ctrl_fpga.mcs for the SASEBO prototype and SASEBO-G or sasebo_v2p30ctrl_lsi.mcs for SASEBO-R. On the programming property screen of the iMPACT programming software, check Verify and Erase Before Programming, and uncheck Parallel Mode.

For the SASEBO prototype and SASEBO-G, reprogram the flash ROM (XCF8P) for the cryptographic FPGA with the provided mcs file sasebo_v2p7_aes_comp.mcs as well. Connect the configuration cable to CN6. The reprogramming steps are the same as for the control FPGA.

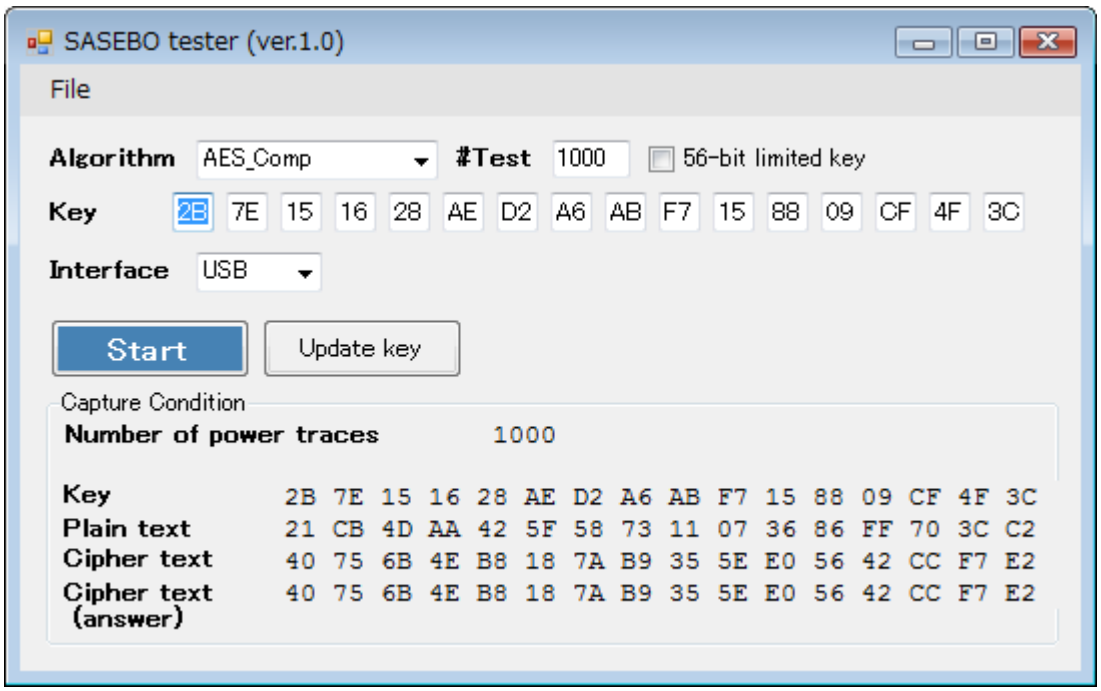
The SASEBO prototype comes with an adapter that connects between the configuration cable and the on-board connector.

To configure the FPGA immediately after reprogramming of the flash ROM, you need to cycle the power because flash ROM reprogramming does not automatically configure the FPGA.

5. Encryption test

Switch the power of SASEBO on and you should see LEDs D1, D3, D4 and D14 (D1, D2 and D6 for SASEBO-R) turn on. If D1 and D3 (or D1 and D2) do not light, it indicates a problem with the power supply. If D4 and D14 (D6) are off, it implies a power supply problem, SASEBO setting problem, or failure in reprogramming the flash ROM.

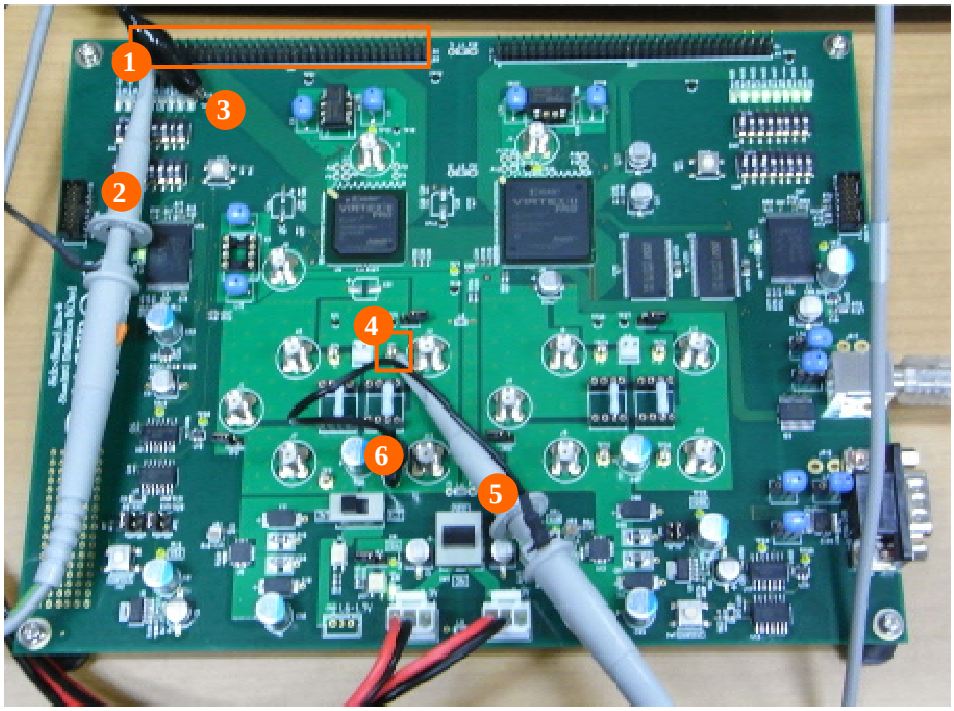
Make sure everything appears right so far, then run the sasebo_tester test software. The software will show the following screen so that you can assure the system works normally and see that the plaintext sent to SASEBO is correctly ciphered.



6. Power Consumption Measurement

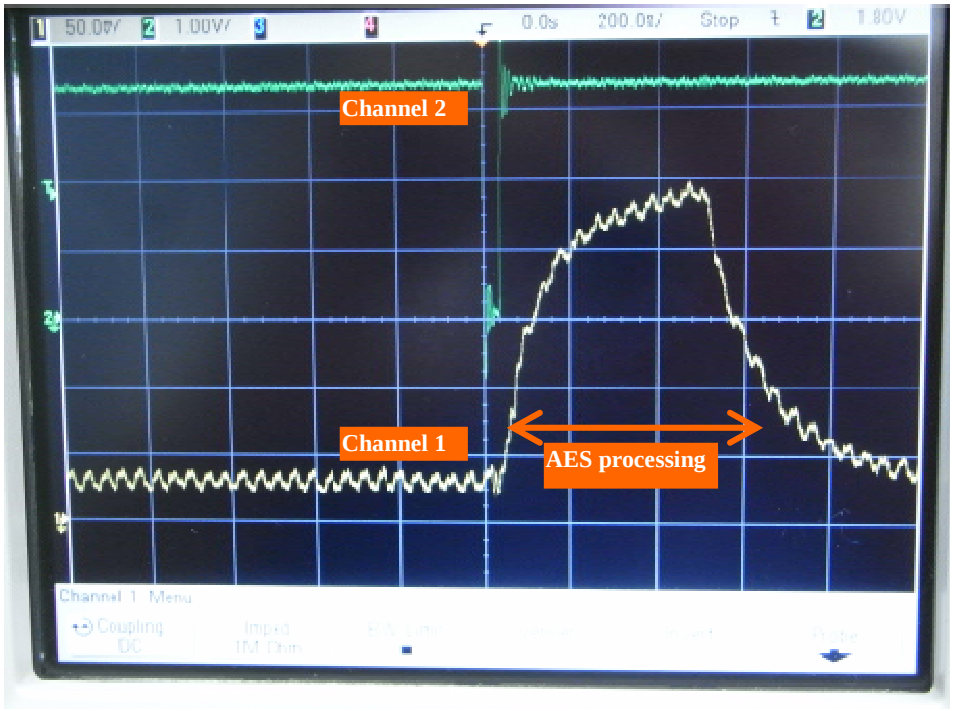
To carry out measurement of power consumption of the board, have an oscilloscope and two probes.

- Example measurement for SASEBO-G



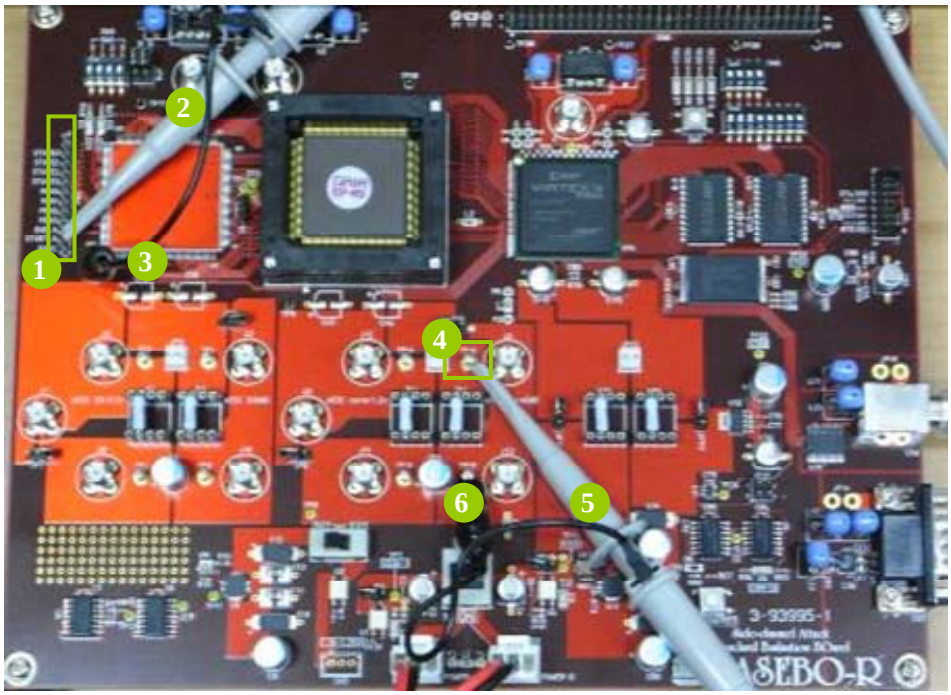
Grab the trigger signal on pin 1 of CN7(1) with the probe connected to channel 2(2). The ground wire of the probe should be connected to TP20(3). Take the power consumption waveform from TP6(4) via the channel 1 probe(5). Connect the probe ground to TP5(6).

For channel 1, set the vertical scale to 50 mV/div, the offset to 150 mV, and enable 20MHz BWL. For channel 2, set the vertical scale to 1 V/div and the offset to 0 V. Set the trigger source to channel 2 and the triggering mode to negative edge.



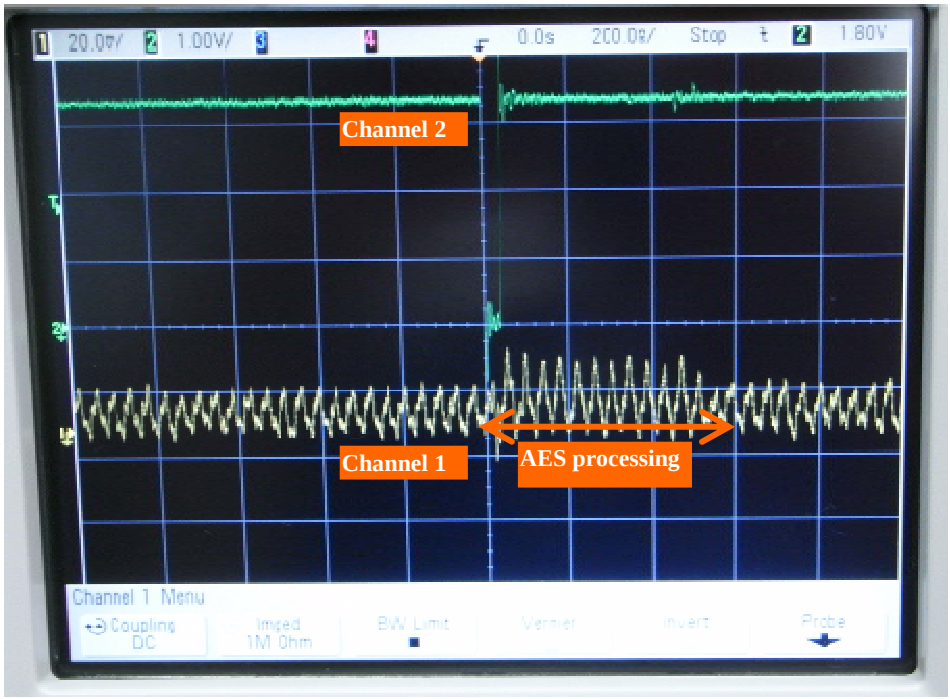
A power consumption waveform like the one in the above picture is expected.

➢ Example measurement for SASEBO-R



Grab the START_N pin of CN4(1) with the channel 2 probe(2). Connect the ground wire of the probe with TP5(3). Take the power consumption waveform from TP16(4) via the channel 1 probe(5). Connect the probe ground to TP15(6).

For channel 1, set the vertical scale to 20 mV/div, the offset to 20 mV, and enable 20 MHz BWL. For channel 2, set the vertical scale to 1 V/div and the offset to 0 V. Set the trigger source to channel 2 and the triggering mode to negative edge.



A power consumption waveform like the one in the above picture is expected.

Technical inquiries:

National Institute of Advanced Industrial Science and Technology (AIST)

Research Center for Information Security (RCIS)

Akihabara-Daibiru 11F Room 1102

1-18-13 Sotokanda, Chiyoda-ku, Tokyo 101-0021, Japan

TEL: +81-3-5298-4722

FAX: +81-3-5298-4522