SASEBO-GIII Quick Start Guide

[Version 1.0]

April 25, 2013

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

1. Equipment preparation

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

(1) SASEBO-GIII
The SASEBO-GIII package contains the SASEBO-GIII (a parts-mounted print circuit board)

(2) USB cable
The SASEBO-GIII uses a USB cable to communicate and supply board power with the host PC.

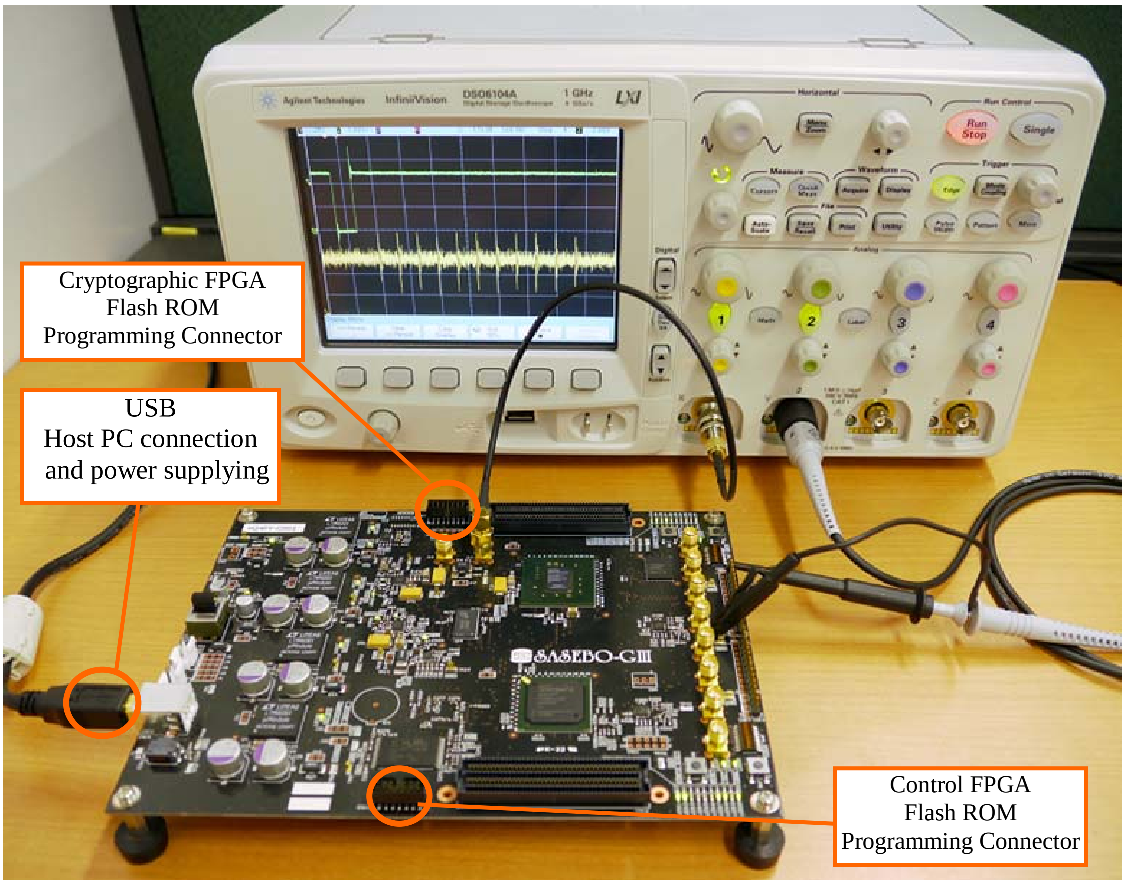
(3) Host PC
Have a middle-range Windows XP/Vista/7 PC with USB ports as the host computer of SASEBO-GIII.

(4) Software (See Section 3)
The instrumental environment requires Microsoft .Net Framework 4.0 and Xilinx ISE (WebPACK or Foundation, whichever works).

(5) FPGA configuration cable
Have either of the Xilinx Platform Cable USB or Platform Cable USB II available. This cable is used to program the flash ROMs connected to the FPGAs.

2. Connections

Connect between SASEBO-GIII and the host PC with the USB cable.



3. Software installation

Download and install the following software:

(1) Software for testing AES module on SASEBO-GIII: SASEBO_G_Checker

http://www.risec.aist.go.jp/project/sasebo/
(via introduction page in English)

(2) Microsoft .Net Framework 4.0

http://www.microsoft.com/en-us/download/details.aspx?id=17851
(English version)

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

(3) Xilinx ISE WebPACK

http://www.xilinx.com/products/design-tools/ise-design-suite/ise-webpack.htm
(English version)

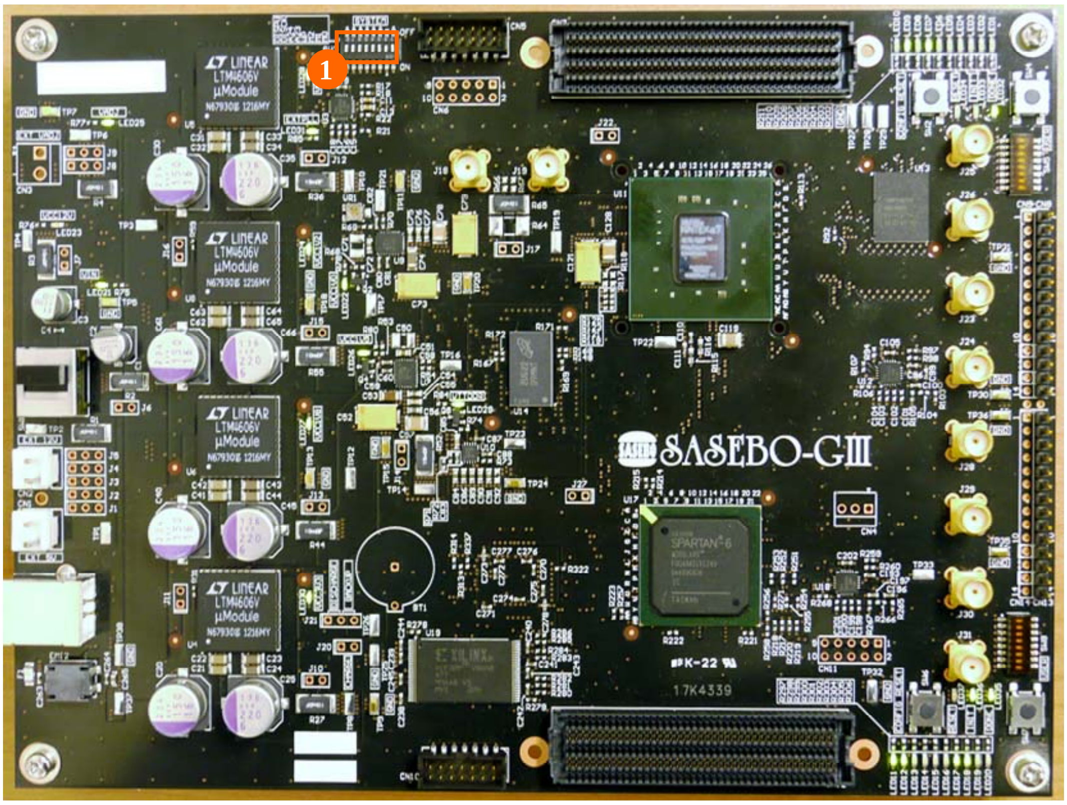
http://japan.xilinx.com/products/design-tools/ise-design-suite/ise-webpack.html
(Japanese version)

(4) FTDI FT_Prog software

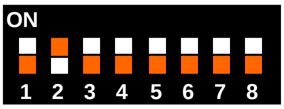
http://www.ftdichip.com/Support/Utilities.htm

4. Setting up SASEBO-GIII

➢ DIP switch and jumper settings for the SASEBO-GIII



(1) SW3



Turn on 2.

➢ FTDI USB configuration

To reprogram the configuration ROM of FT2232H (U21), attach the USB cable and use FT_Prog software. For configuration, use the provided the template file sasebo_giii.xml.

➢ FPGA configuration

To reprogram the flash ROM (XCF32P, U19) for the control FPGA (Spartan-6), attach the configuration cable to CN10. For configuration, use the provided MCS file sasebo_giii_ctrl.mcs.

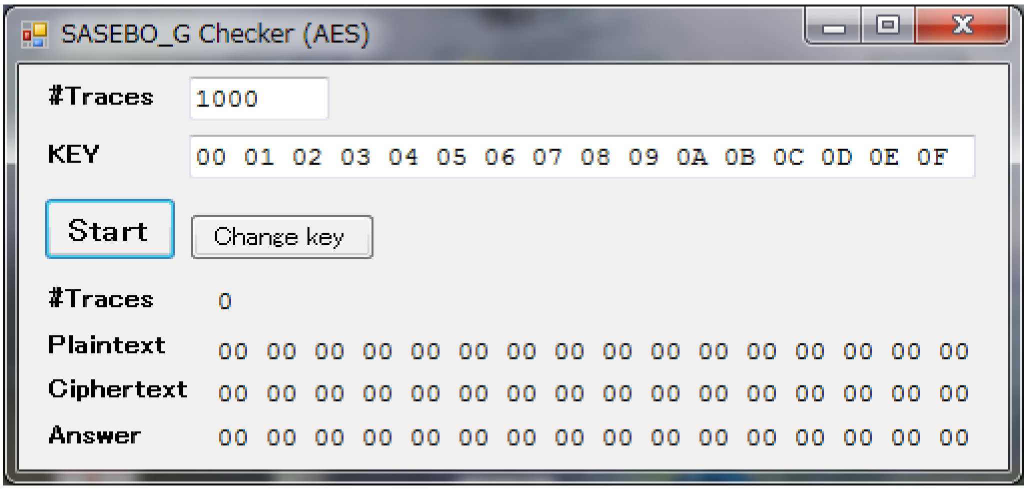
Reprogram the flash ROM (28F128P30B, U13) for the cryptographic FPGA (Kintex-7) with the provided MCS file sasebo_giii_aes.mcs as well. Connect the configuration cable to CN5.

To configure the FPGA immediately after reprogramming of the flash ROM, cycle the power.

5. Encryption test

Switch the power of SASEBO-GIII on and you should see LEDs turn on. If LED “VCC**V” does not light, it indicates a problem with the power supply. If LED32 and 35 are off, it implies a setting problem, or failure in reprogramming the flash ROM.

Make sure everything appears right so far, and then run the SASEBO_G_Checker 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-GIII is correctly ciphered.



#Traces 1000

KEY 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

#Traces 0

Plaintext 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

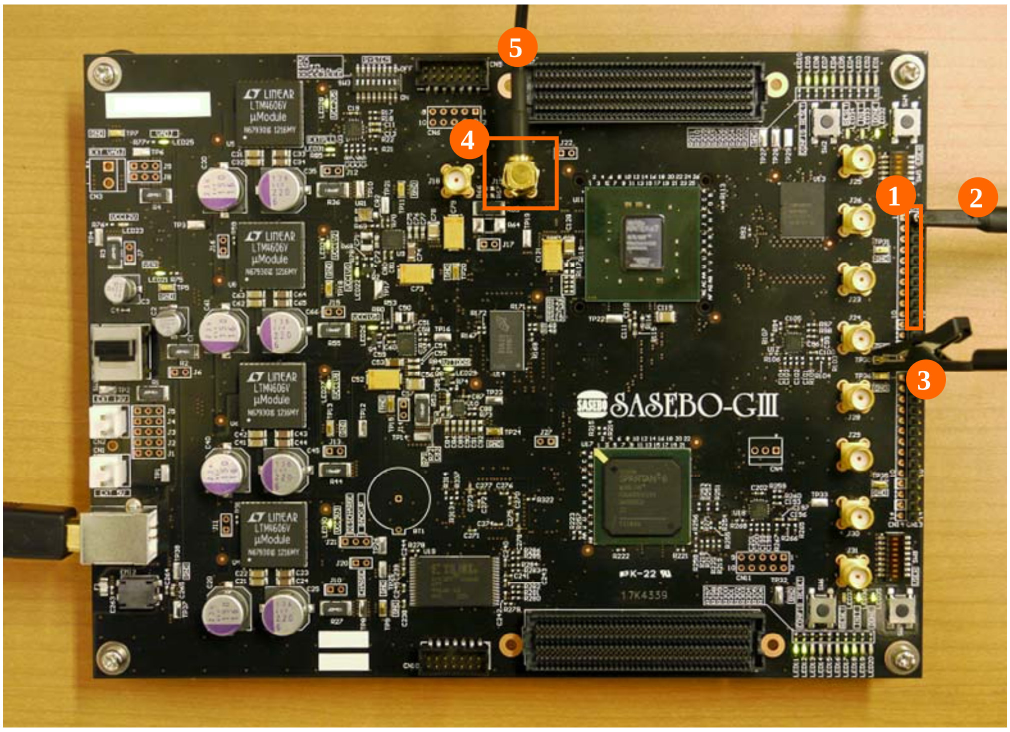
Ciphertext 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Answer 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

6. Power Consumption Measurement

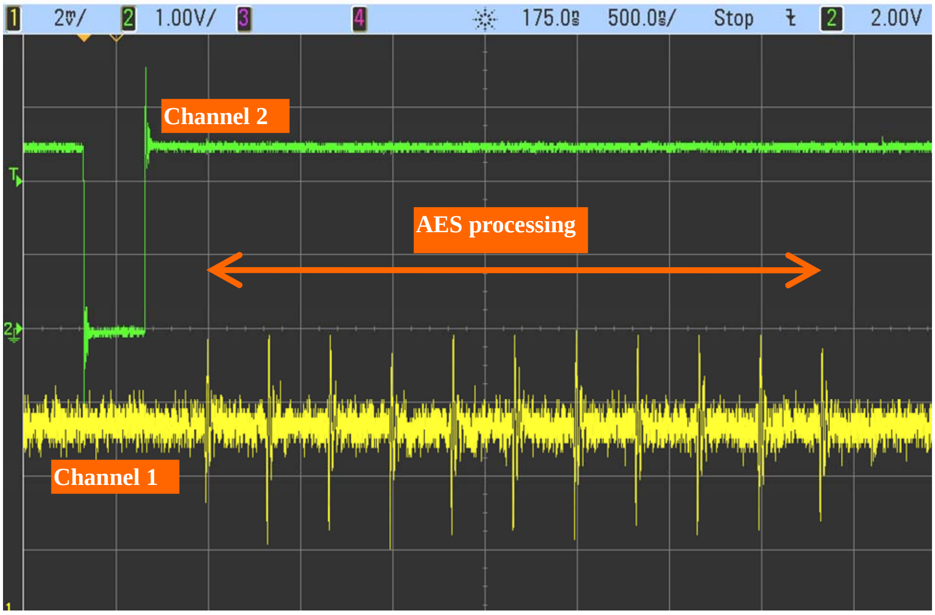
To carry out measurement of power consumption of the board, have an oscilloscope, a passive probe, and a SMA-BNC cable.

➢ Example measurement for SASEBO-GIII



Grab the trigger signal on pin 1 of CN8(1) with the probe connected to channel 2(2). The ground wire of the probe should be connected to TP30(3). Take the power consumption waveform from J19(4) via the channel 1 SMA-BNC 50 ohms cable(5).

For channel 1, set the vertical scale to 2 mV/div, and the offset to 1.05 V/div. For channel 2, set the vertical scale to 1.0 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.

The SASEBO-GIII board was developed by AIST undertaking projects sponsored by JST (Japan Science and Technology Agency)

4. The specifications of this product are subject to revision without notice.

Technical inquiries:

National Institute of Advanced Industrial Science and Technology (AIST)

AIST Tsukuba Central 2 Room 4408

1-1, Umezono 1-Chome Tsukuba-shi, Ibaraki 305-8568, Japan

TEL: +81-29-861-2984

FAX: +81-29-861-5285