SASEBO-GII Quick Start Guide

[Version 1.0]

September 3, 2009

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

1. Equipment preparation

******设备的准备：
在建立SASEBO-G2工作环境及调试项目之前，必须拥有的设备包括板子，USB线，主机软件+FPGA线：Xilinx Platform Cable线，Platform线，或平行线

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

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

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

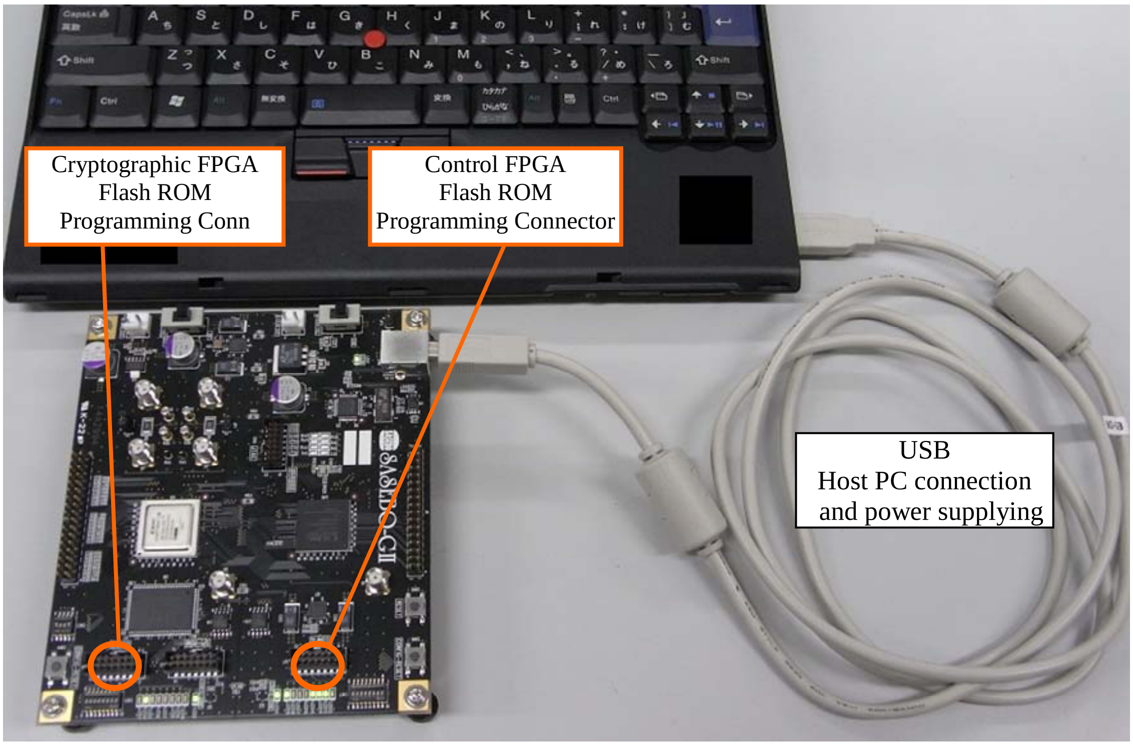
(3) Host PC
Have a middle-range Windows XP/Vista/7 PC with USB ports as the host computer of SASEBO-GII.

(4) Software (See Section 3)
The instrumental environment requires Microsoft .Net Framework 3.5 and Xilinx ISE (WebPACK or Foundation, whichever works).
To use USB communication, you also need the driver software D2XX provided by FTDI.

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

2. Connections

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



******软件安装：

3. Software installation

Download and install the following software:

(1) Software for testing AES/DES module on SASEBO-GII: SASEBO_AES_Checker, SASEBO_DES_Checker

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)

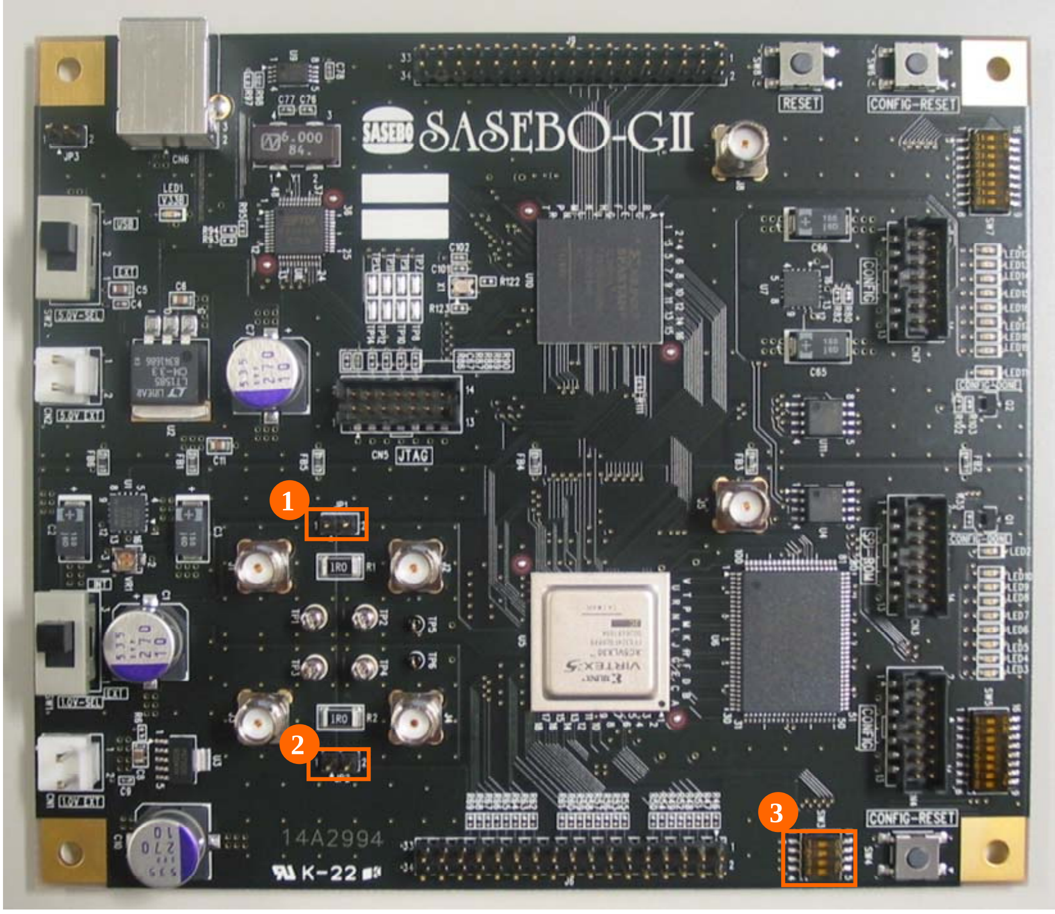
http://japan.xilinx.com/ise/logic_design_prod/webpack.htm
(Japanese version)

(4) FTDI D2XX driver and FTD2XX_NET_DLL

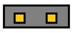
http://www.ftdichip.com/Drivers/D2XX.htm
(D2XX driver)

4. Setting up SASEBO

- DIP switch and jumper settings for the SASEBO prototype

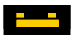


(1) JP1



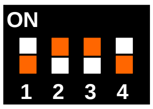
Open.

(2) JP2



Place a jumper.

(3) JP1, JP2, JP6



Turn on 2 and 3.

- FPGA configuration

To reprogram the flash ROM (ST45DB16D, U11) for the control FPGA (Spartan-3A), attach the configuration cable to CN7. For configuration, use the provided mcs file sasebo_gii_ctrl.mcs.

Reprogram the flash ROM (ST45DB16D, U4) for the cryptographic FPGA (Virtex-5 LX30) with the provided mcs file sasebo_aes_comp_lx30.mcs as well. Connect the configuration cable to CN4.

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

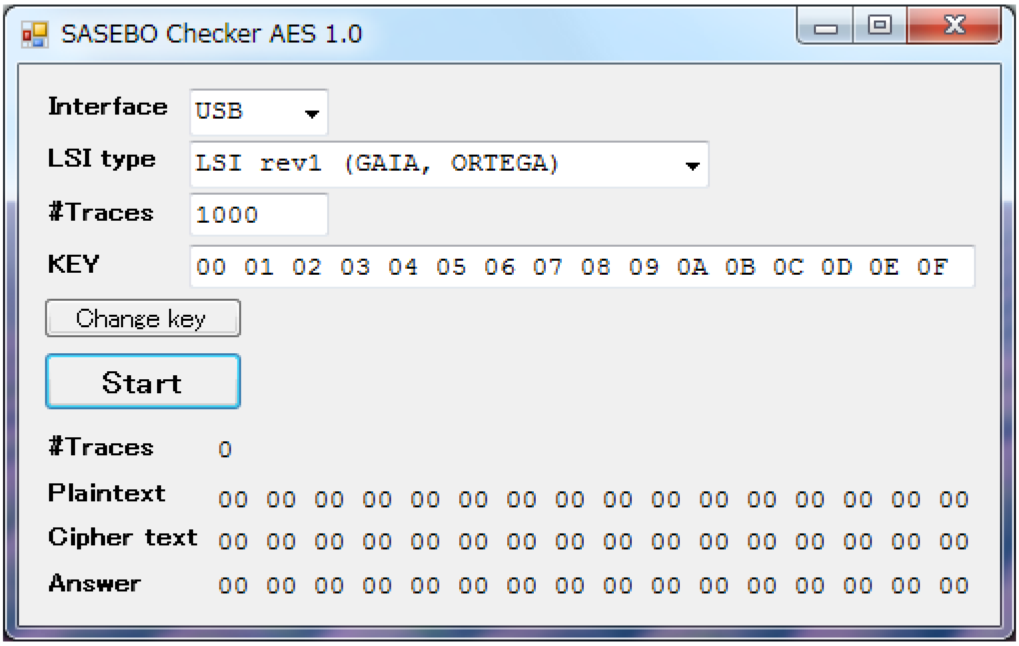
5. Encryption test

******加密测试部分：如果显示灯没有正常亮对应的各种问题：供电问题+设置问题+改遍闪存出现的问题

Switch the power of SASEBO-GII on and you should see LEDs D1, D2, and D11 turn on. If D1 does not light, it indicates a problem with the power supply. If D2 and D11 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, and then run the SASEBO_AES_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-GII is correctly ciphered.

******直至确保一切正常后才能运行AES（高级加密标准）的检查软件



SASEBO Checker AES 1.0

Interface: USB

LSI type: LSI rev1 (GAIA, ORTEGA)

#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

Cipher text: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

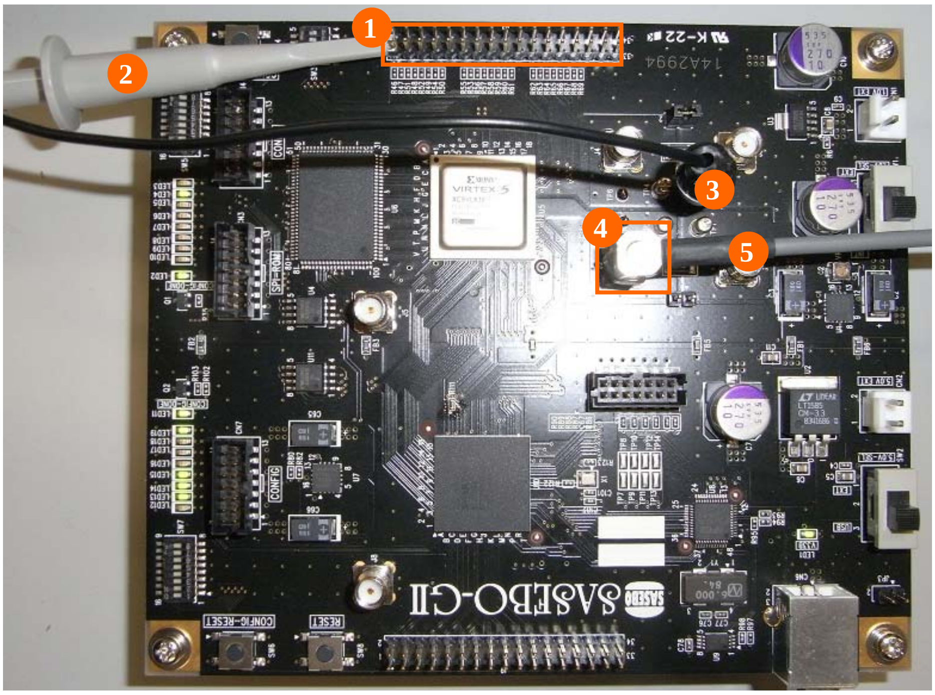
Answer: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

******功耗测量：
由于我们进行旁道攻击分析主要是靠功耗攻击的，所以功耗测量是一个关键。
必须要有的：示波器+探针+SMA-BNC线

6. Power Consumption Measurement

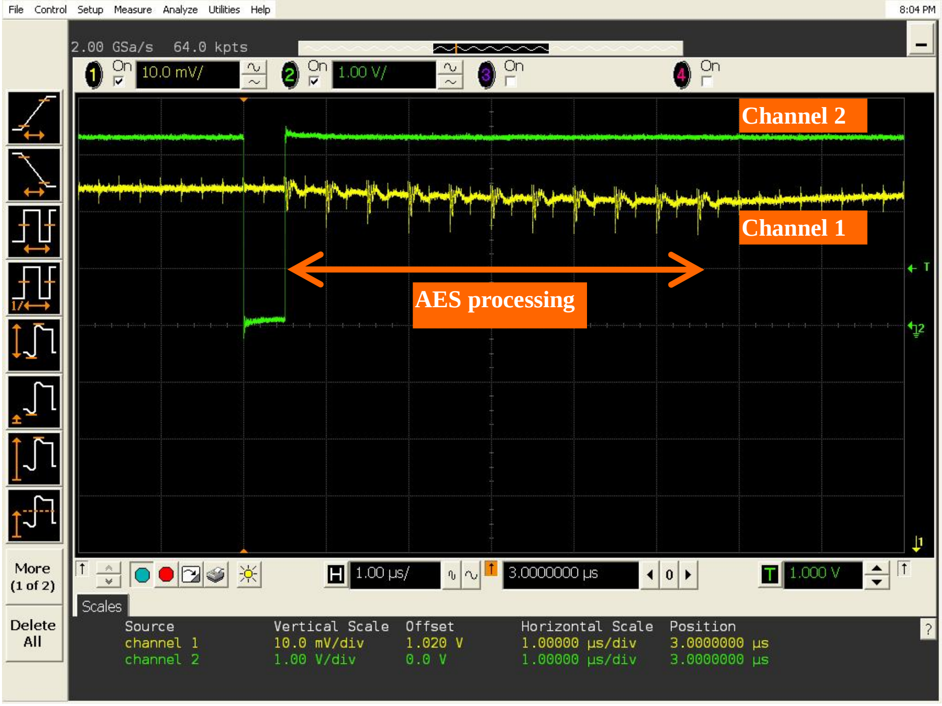
To carry out measurement of power consumption of the board, have an oscilloscope, a passive probe, and a SMA-BNC cable.

- Example measurement for SASEBO-G



Grab the trigger signal on pin 1 of J6(1) with the probe connected to channel 2(2). The ground wire of the probe should be connected to TP3(3). Take the power consumption waveform from J2(4) via the channel 1 SMA-BNC 50 ohms cable(5).

For channel 1, set the vertical scale to 10 mV/div, and the offset to 1.0 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.



```
Source      Vertical Scale  Offset    Horizontal Scale  Position
channel 1   10.0 mV/div     1.020 V   1.00000 µs/div    3.0000000 µs
channel 2   1.00 V/div      0.0 V     1.00000 µs/div    3.0000000 µs
```

******
对于信道1来说，
竖直方向的标度为10mV/格，
偏移量为1.0V/div
信道2保持相同的竖直标度
但是零偏移，
这样可以直接比较，
我们可以发现在处理ASE解密
的阶段功耗是有明显的差异。

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

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

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