Side-channel AttacK User Reference Architecture SAKURA-G Quick Start Guide

– SASEBO-GII compatible mode –

[Version 0.9]

SAKURA-G

August 1st, 2014

Satoh Laboratory,

The University of Electro Communications

Revision Record

Date	Version	Record
	0.9	Released

Contents

1. Operation

This document briefly describes instruction to conduct side channel attack experiments on SAKURA-G board. Required hardware devices, device drivers and basic tools, board configuration, and boar operation are described below.

2. Hardware Device

The following equipment are required to operate the SAKURA-G board.

1. SAKURA-G bard
   A product package contains only SAKURA-G board.
2. USB cable
   A standard USB B-A type cable to connect the SAKURA-G board and a personal computer. 5-V power is supplied from the computer to SAKURA-G through this cable.
3. Personal computer
   Windows Vista/7 middle-range personal computer to control SAKURA-G.
4. FPGA configuration cable
   The cable is used to configure control and cryptographic FGAs on SAKURA-G. Xilinx platform cable USB II is highly recommended.

3. Download and install software on PC

Some Windows drives and tools are required to download from the following URLs to configure and to control SAKURA-G. Please follow instructions of each software to for installation and operation.

1. Microsoft.Net Framework 4.0
   <Japanese version>
   http://www.microsoft.com/downloads/details.aspx?FamilyID=333325fd-ae52-4e35-b531-508d977d32a6&displaylang=ja
   <US version>
   http://www.microsoft.com/downloads/details.aspx?FamilyID=333325fd-ae52-4e35-b531-508d977d32a6
2. Xilinx ISE 14.6
   <Japanese version>
   http://japan.xilinx.com/ise_eval/index.htm
   <US Version>
   http://www.xilinx.com/ise_eval/index.htm
3. Two FTDI drivers
   <D2XX driver>
   http://www.ftdichip.com/Drivers/D2XX.htm

<FTD2XX_NET_DLL>

http://www.ftdichip.com/Projects/CodeExamples/CSharp.htm

FTD2XX_NET_DLL should be copied into the same directory where SAKURA_Checker.exe is copied.

4. FT_prog

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

FT_prog.exe is a stand-alone tool, and thus no installation process is required.

4. SAKURA-G Setup

4.1 DIP Switch

Fig. 1 shows major parts on the SAKURA-G board and locations of DIP switches and setup for the switches are shown in Tables 1-3. SW2 is used for system setting such as configuration mode of the cryptographic FPGA. SW5 is connected to the control FPGA for arbitrary use. Table 2 shows a setup of SW5 for the control circuit "sakura_g_control.v." SW10 is connected the cryptographic FPGA for arbitrary use, and the AES circuit "sakura_g_aes128.v" does not use the switch. A setup for SW10 is shown in Table 3.

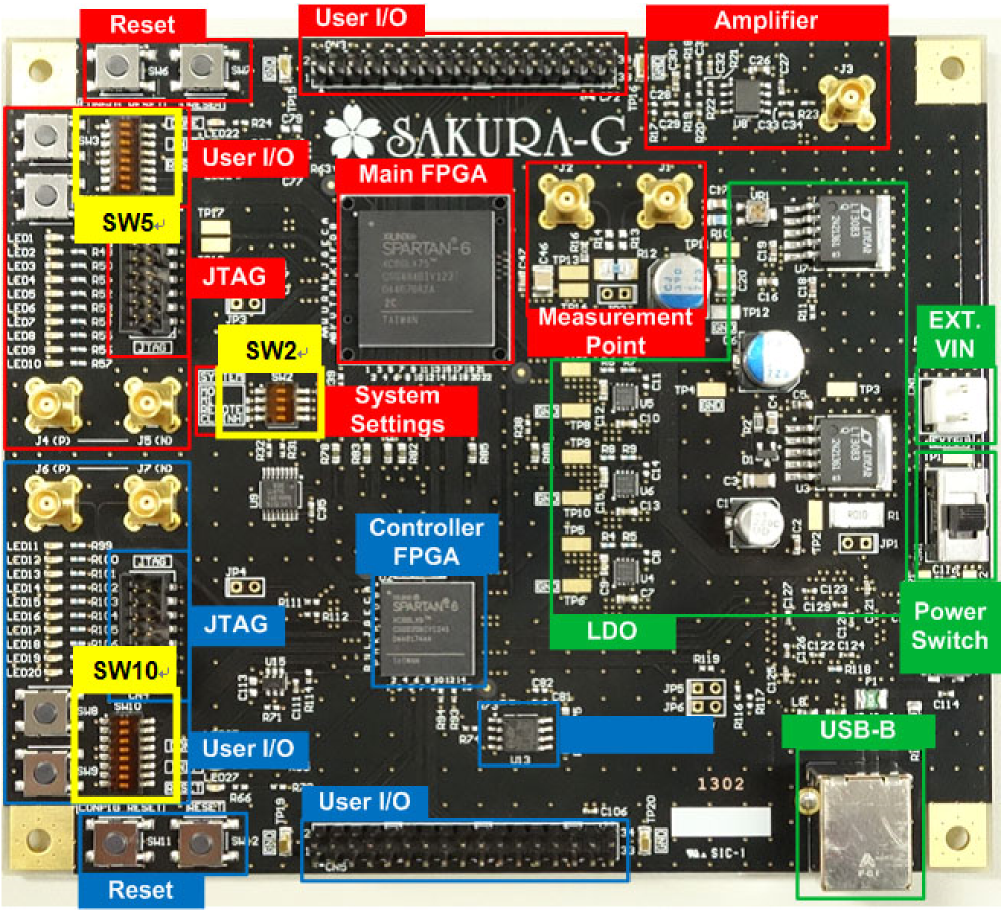


Fig. 1 Major parts on SAKURA-G board.

Table 1. SW2 set up

Pin	Setup	Remarks
1	ON	M0
2	OFF	M1
3	OFF	REMOTE
4	OFF	CLKINH

Table 2. SW5 setup

Pin	Setup	Remarks
1	OFF	Selection of operating Frequency for cryptographic FPGA
2	OFF	Selection of operating Frequency for cryptographic FPGA
3	OFF	Selection of operating Frequency for cryptographic FPGA
4	OFF	FT2232H port selection
5	OFF	Not used
6	OFF	Not used
7	OFF	Not used
8	OFF	Not used

Table 3. SW10 setup

Pin	Setup	Remarks
1	OFF	Not used
2	OFF	Not used
3	OFF	Not used
4	OFF	Not used
5	OFF	Not used
6	OFF	Not used
7	OFF	Not used
8	OFF	Not used

4.2 Download SAKURA-G Tool Package

Access to the following SAKURA-G Webpage.

http://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-G.html

Then, download following four files in the Quick Start Guide section, and unzip them into the PC connected to SAKURA-G.

1. SAKURA-G Quick Start Guide Source and Binary Codes

This file contains following three folders:

SAKURA_Checker_AES: This folder contains a Windows binary program to execute AES operations on SAKURA-G. This program is stand-alone and does not use Windows registry. There for no installation process is required

sakura_g_aes128: This folder contains Verilog-HDL source files and a configuration mcs ROM file for the cryptographic FPGA.

sakura_g_control: This folder contains Verilog-HDL source files and a configuration mcs ROM file for the control FPGA.

2. SAKURA-G Verilog-HDL Top Models and ucf Files

This file contains following two folders:

sakura_g_aes128: This folder contains a Verilog-HD top module, ucf fies, and a Xilinx ISE project file of the AES circuit for the cryptographic FPGA.

sakura-g_control: Tis folder contains a Verilog-HDL top module, ucf file, and a Xilinx ISE project file for the control FPGA.

3. SAKURA-G Quick Start Guide

This document.

4. SAKURA-G Checker

This file contains a Windows program for initial test for SAKURA-G in “Release” folder.

5. SAKURA-G Configuration

5.1 FPGA Configuration

After confirming the power switch SW1 is set to OFF (center position), connect SAKURA-G (connecter CN6) to PC by using USB cable as shown in Fig. 3. In order to configure SPI ROM for the controller FPGA XC6SLX9, connect a configuration cable to the JTAG connector CN4 as shown in Fig. 3. The board should be kept power-off during the cable connection.

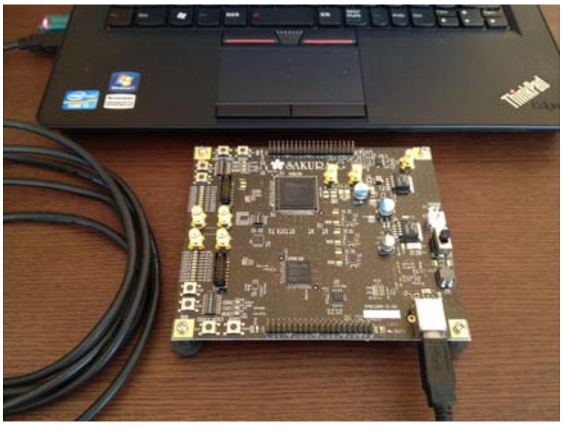


Fig. 2 SAKURA-G connected to PC by a USB cable.

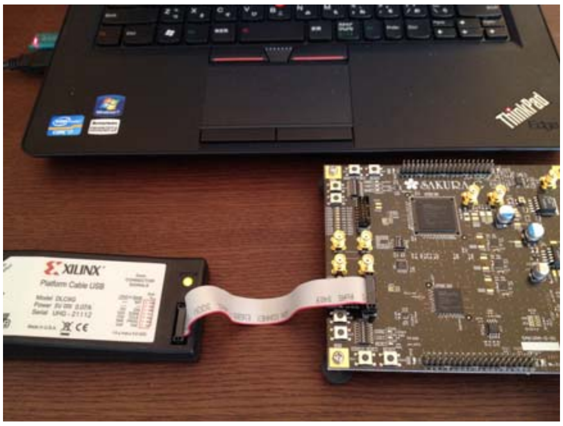


Fig. 3 Configuration cable attached to a JTAG connector of the control FPGA.

In order to configure the FPGA, turn on the power witch SW1 (set to the USB side), and execute iMACT software on PC. In the iMPAC, select he following configuration file in the unzipped directory.

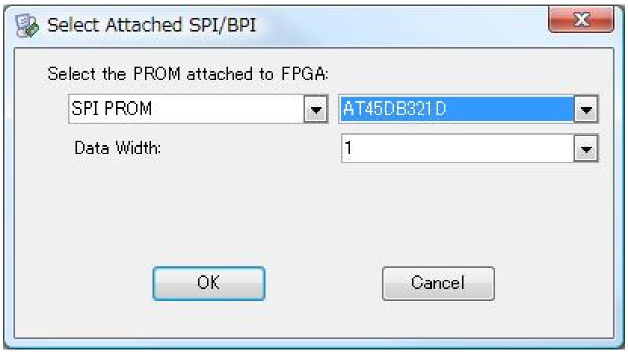
sakura_g_control /sakura_g_control/ rom_sakura_g_control.mcs.

Then select SPI PROM / AT45DB321D as shown in Fig. 3, and write the mcs file into PROM.

Similarly, connect SAKURA-G (connecter CN2) to PC after turn off the power of SAKURA-G. Then power on SAKURA-G and run iMPACT. Select the following configuration file in the unzipped directory.

akura_g_aes128/sakura_g_aes128/rom_sakura_g_aes128.mcs.

Select SPI PROM / AT45DB321D, and write the mcs file into PROM.



Select the PROM attached to FPGA:

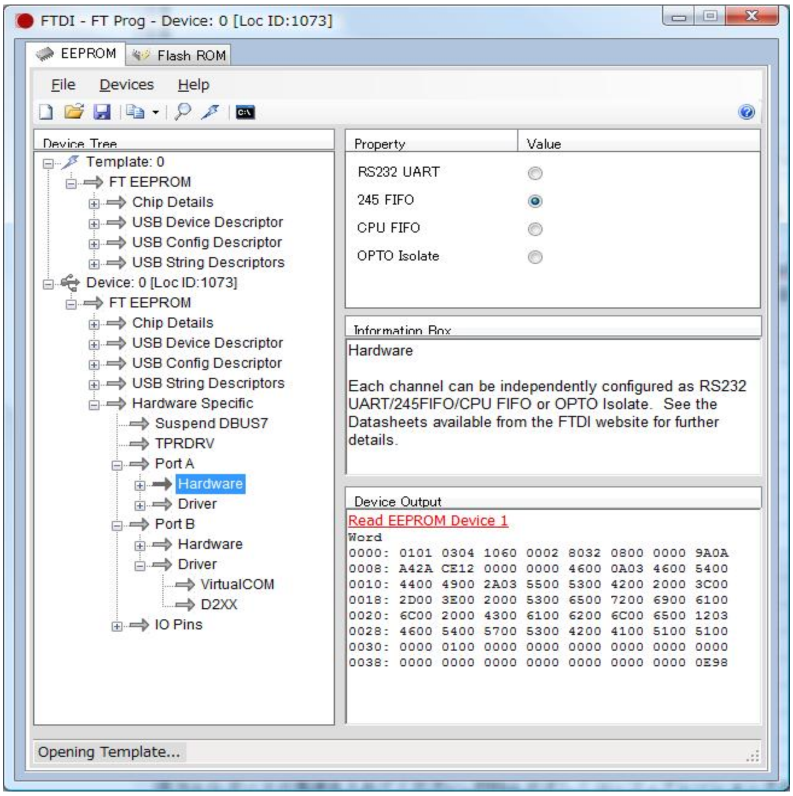
SPI PROM AT45DB321D

Data Width: 1

Fig. 4　ROM selection.

5.2　USB Controller Configuration

In order to enable the USB interface of SAKURA-G, a USB controller chip should be configured using FT_Prog.exe downloaded from FTDI’s Website in chapter 3. First, select hardware operation mode “245FIFO” from four modes as shown in Fig. 5. Then, select driver mode “D2XX Direct” as shown in Fig.6. The selection is applied to both port A and B. After that, write the setting into EEPROM of the USB controller chip. More details please refer FTDI’s user’s manual.



Property	Value
RS232 UART	○
245 FIFO	●
CPU FIFO	○
OPTO Isolate	○

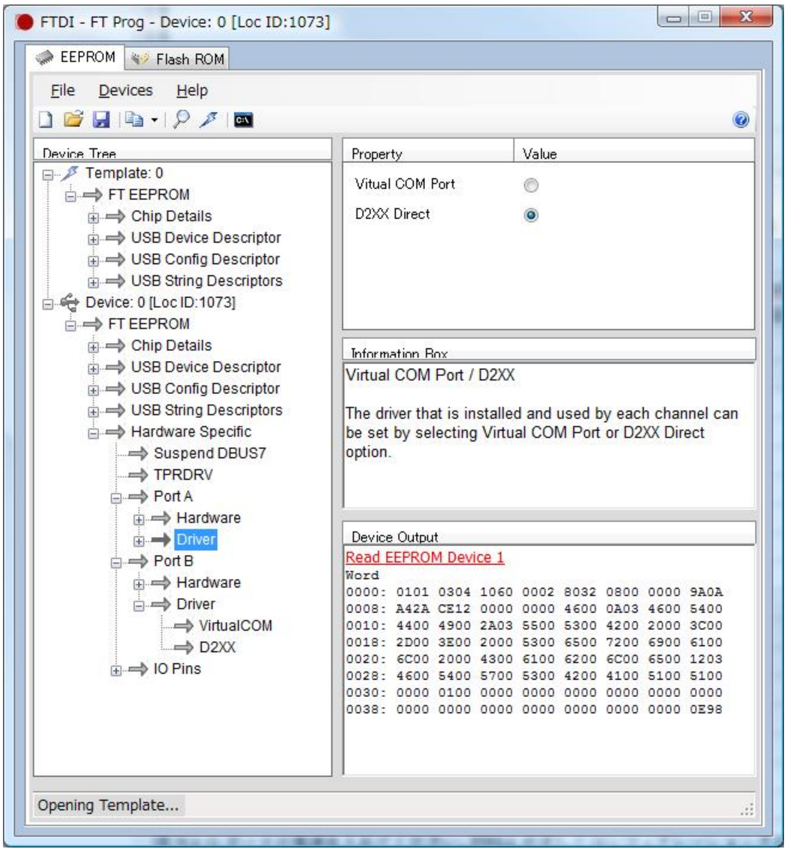
Hardware

Each channel can be independently configured as RS232 UART/245FIFO/CPU FIFO or OPTO Isolate. See the Datasheets available from the FTDI website for further details.

Read EEPROM Device 1

```
Word
0000: 0101 0304 1060 0002 8032 0800 0000 9A0A
0008: A42A CE12 0000 0000 4600 0A03 4600 5400
0010: 4400 4900 2A03 5500 5300 4200 2000 3C00
0018: 2D00 3E00 2000 5300 6500 7200 6900 6100
0020: 6C00 2000 4300 6100 6200 6C00 6500 1203
0028: 4600 5400 5700 5300 4200 4100 5100 5100
0030: 0000 0100 0000 0000 0000 0000 0000 0000
0038: 0000 0000 0000 0000 0000 0000 0000 0E98
```

Fig. 5　Operation mode selection



Vitual COM Port ○

D2XX Direct ●

Virtual COM Port / D2XX

The driver that is installed and used by each channel can be set by selecting Virtual COM Port or D2XX Direct option.

Read EEPROM Device 1

```
Word
0000: 0101 0304 1060 0002 8032 0800 0000 9A0A
0008: A42A CE12 0000 0000 4600 0A03 4600 5400
0010: 4400 4900 2A03 5500 5300 4200 2000 3C00
0018: 2D00 3E00 2000 5300 6500 7200 6900 6100
0020: 6C00 2000 4300 6100 6200 6C00 6500 1203
0028: 4600 5400 5700 5300 4200 4100 5100 5100
0030: 0000 0100 0000 0000 0000 0000 0000 0000
0038: 0000 0000 0000 0000 0000 0000 0000 0E98
```

Fig. 6 Driver mode selection

6. Operation

6.1 Power on SAKURA-G

When the FPGA and USB chip configuration is completed, turn off and then turn on the SAKURA-G board. Then status of LED1-LED20 is as shown in Table 4. If the status is different, data may not be written in the ROMs for FPGA and USB properly.

Table 4 Status of LED

No.	Status	No.	Status
LED1	off	LED11	blink (inverse of LED20)
LED2	on	LED12	off
LED3	off	LED13	on
LED4	off	LED14	on
LED5	on	LED15	off
LED6	off	LED16	off
LED7	off	LED17	on
LED8	off	LED18	on
LED9	blink (inverse of LED10)	LED19	off
LED10	blink (inverse of LED9)	LED20	blink (inverse of LED11)

6.2 Execute SAKURA-G Checker

Execute the board check program “SAKURA_G_Cheker.exe” downloaded and unzipped in the folder “SKURA_G_Checker/Release” as described in Chapter 3. Fig. 7 shows the initial window of the checker. Followings are explanation of each part in the window

Plaintext

A 128-bit plaintext being encrypted by this tool and SAKURA-G, which is generated randomly.

Chiper text

A 128-bit cipher text encrypted from the plaintext by this tool.

Answer

A 128-bit cipher text returned from SAKURA-G.

Traces

A number of encrypt operations.

FT2232H Port

A USB port used for communication between PC and SAKURA-G (fixed to device USB0).

Key

A 128-bit secret key used for the encryption. The value can be changed by using “Change key” button.

Traces

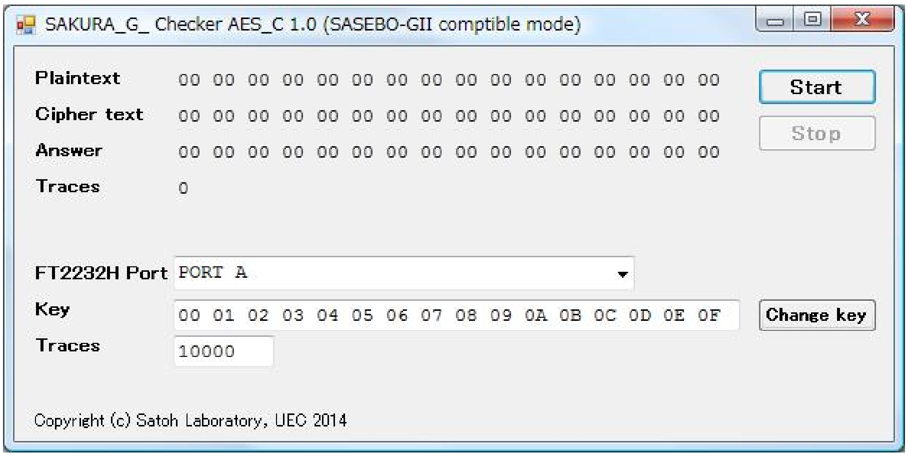
Input a number of encrypt operations to be performed.

Start

When this button is clicked, encrypt operation starts and the window changed as Fig. 7.

Stop

When this button is clicked, encrypt operation is stopped. Even if this button is not clicked, encrypt operation is stopped when encryption is repeated the number of times indicated by “Traces” or error occurs.



SAKURA_G_ Checker AES_C 1.0 (SASEBO-GII comptible mode)

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

Traces 0

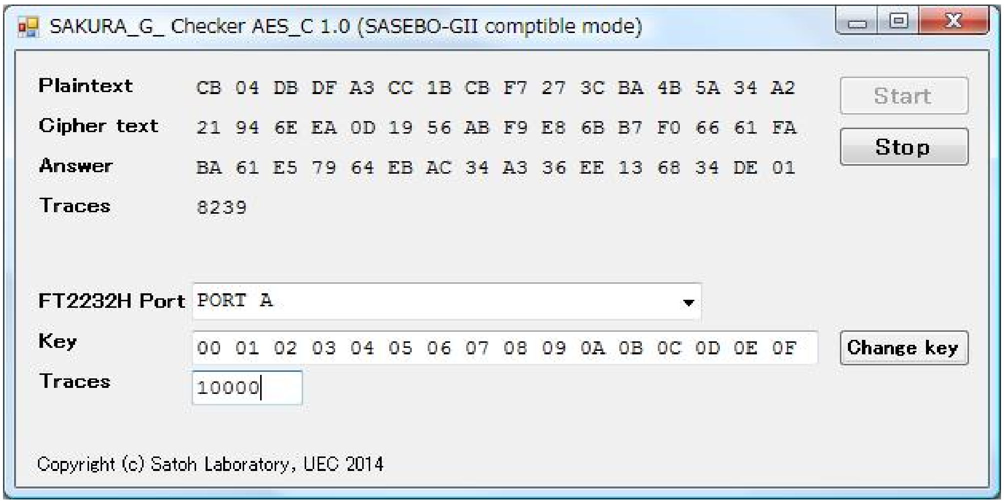
FT2232H Port PORT A

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

Traces 10000

Copyright (c) Satoh Laboratory, UEC 2014

Fig. 7 Initial window of SAKURA_G_Cheker_AES



SAKURA_G_ Checker AES_C 1.0 (SASEBO-GII comptible mode)

Plaintext	CB 04 DB DF A3 CC 1B CB F7 27 3C BA 4B 5A 34 A2
Cipher text	21 94 6E EA 0D 19 56 AB F9 E8 6B B7 F0 66 61 FA
Answer	BA 61 E5 79 64 EB AC 34 A3 36 EE 13 68 34 DE 01
Traces	8239
FT2232H Port	PORT A
Key	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
Traces	10000

Copyright (c) Satoh Laboratory, UEC 2014

Fig. 8 SAKURA_G_Cheker_AES in encrypt operation

Department of Communication Engineering and Informatics
The University of Electro-Communications
1-5-1 Chofugaka, Chofu, Tokyo, 182-8585, Japan

sakura@mtmsystems.jp
http://satoh.cs.uec.ac.jp/SAKURA/