

# **SASEBO-W Quick Start Guide**

**Version 1.1**



**August 18, 2012**

**Morita Tech Co., Ltd.**

# 1. FPGA Configuration

Set the jumper pins and switches on the SASEBO-W board as follows:

- JP1: Short
- JP2: Open (+1.8V), Short (+3.0V), Open (PROG)
- JP3: Short
- JP5: Open
- JP7: Open
- JP8: Short
- SW1: INT
- SW2: INT
- SW8: EXT
- SW3: On (1), On (2), Off (3), Off (4)
- SW4: Off (1), Off (2), Off (3), Off (4)
- SW6: Off (1), On (2), On (3), On (4)

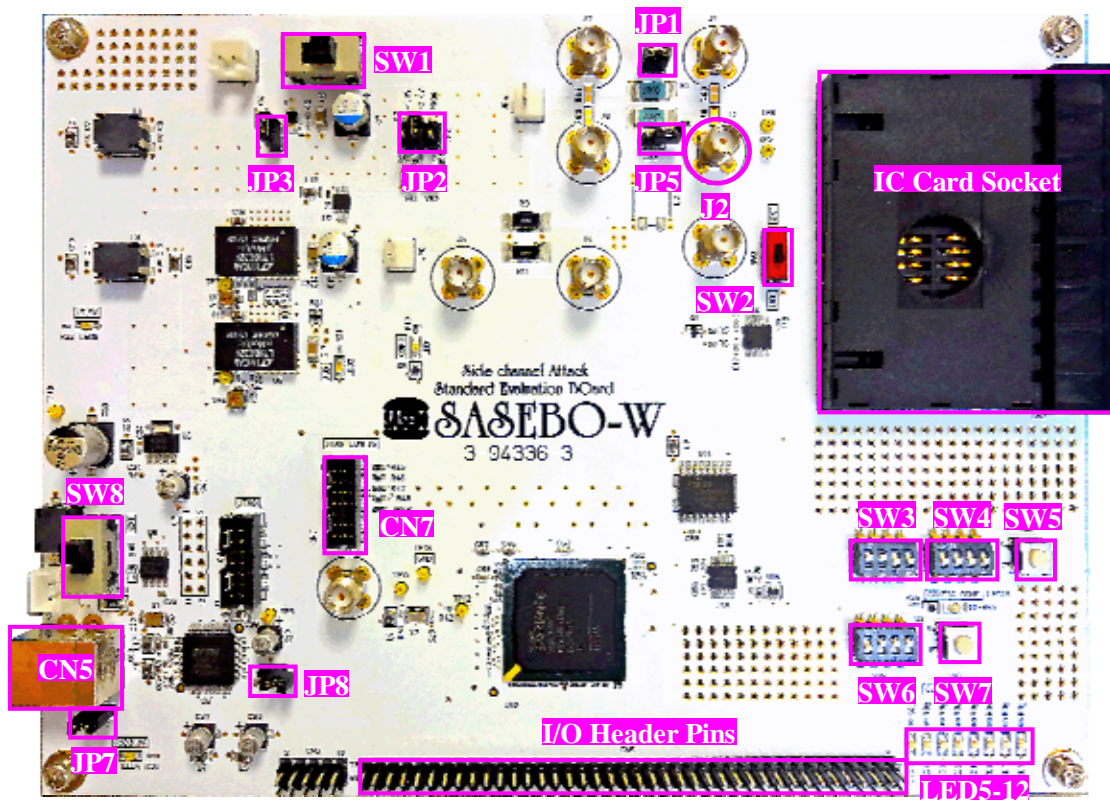


Fig 1. SASEBO-W

Begin by connecting a USB cable to the USB port (CN5) and a Xilinx download cable to the JTAG CONFIG connector (CN7), as shown in Fig. 2. Next, power up the board by switching SW8 from "EXT" to "USB." LED1, LED2, LED3, and LED4 should turn on.

Download the zip file from the following URL:

[http://www.morita-tech.co.jp/SAKURA/en/resource/sasebo\\_w\\_quick\\_start\\_guide\\_v1\\_1.zip](http://www.morita-tech.co.jp/SAKURA/en/resource/sasebo_w_quick_start_guide_v1_1.zip)

Unzip the file on your PC, and write the ROM image file "sasebo\_w\_vcp\_1\_3.mcs" under the unzipped directory "sasebo\_w\_vcp\ysasebo\_w\_vcp\_1\_3." into the SPI-ROM M25P64.

Disconnect the download cable and press the configuration reset switch SW7. If the FPGA Spartan-6 has been configured properly, the config done light LED13 will be on. Next, press switch SW5 which should turn LED6 and LED12 on.

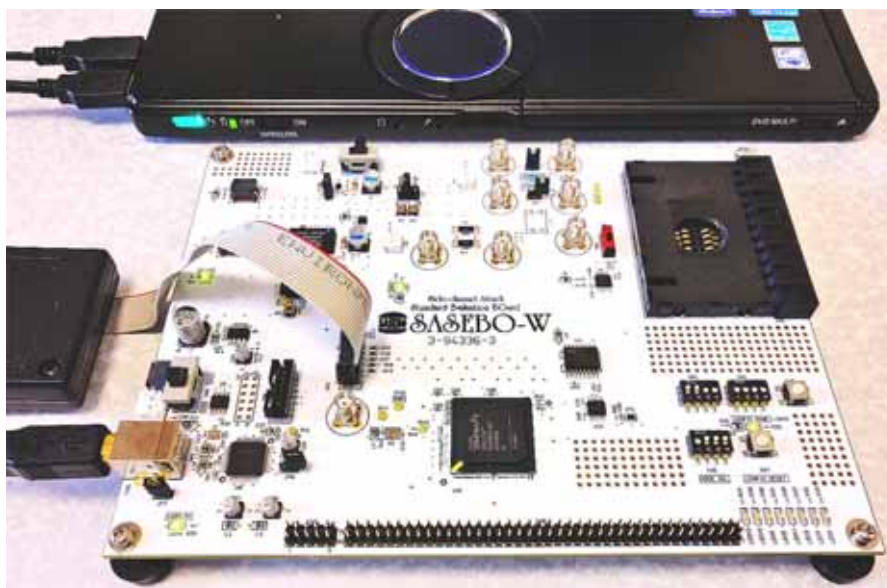


Fig 2. FPGA configuration of SASEBO-W

## 2. IC Card Programming

Set the mode switch SW3 on the SASEBO-W board as follows.

SW3: On (1), On (2), On (3), On (4)

Download the Virtual COM Port (VCP) Driver for FTDI devices (CDM20824\_Setup.exe) from the following URL and install the drivers. Remember the COM port assigned to FTDI device FT2232H.

<http://www.ftdichip.com/Drivers/VCP.htm>

An FTDI driver installation guide is available at

[http://www.ftdichip.com/Support/Documents/AppNotes/AN\\_119\\_FTDI\\_Drivers\\_Installation\\_Guide\\_for\\_Windows7.pdf](http://www.ftdichip.com/Support/Documents/AppNotes/AN_119_FTDI_Drivers_Installation_Guide_for_Windows7.pdf)

Download the EEPROM programming utility (FT\_Prog) from the following URL.

[http://www.ftdichip.com/Support/Utilities.htm#FT\\_Prog](http://www.ftdichip.com/Support/Utilities.htm#FT_Prog)

After unzipping the download file, execute FT\_Prog.exe and press the "F5" function key. The main window will come up as shown in Fig. 3. Under "FT EPROM -> Hardware Specific -> Port A" set "Hardware" to "245 FIFO" and "Driver" to "D2XX Direct," as shown in Figure 4.

As same as Port A, set " Hardware" to "245 FIFO" and "Driver" to "D2XX Direct" for Port B.

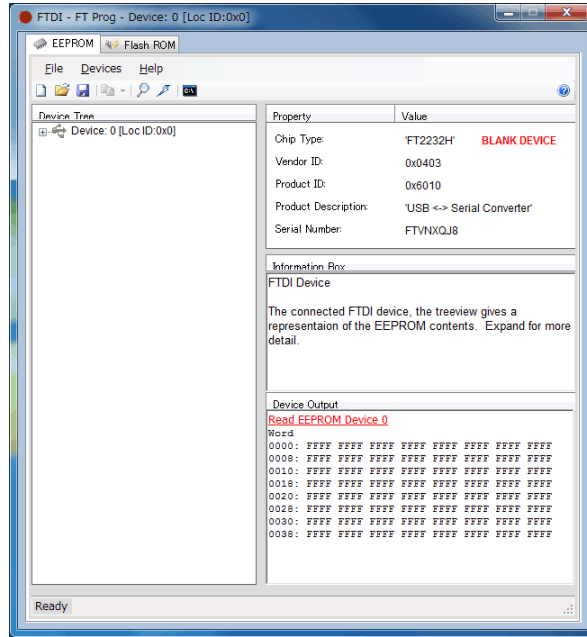


Fig 3. FT\_Prog main window

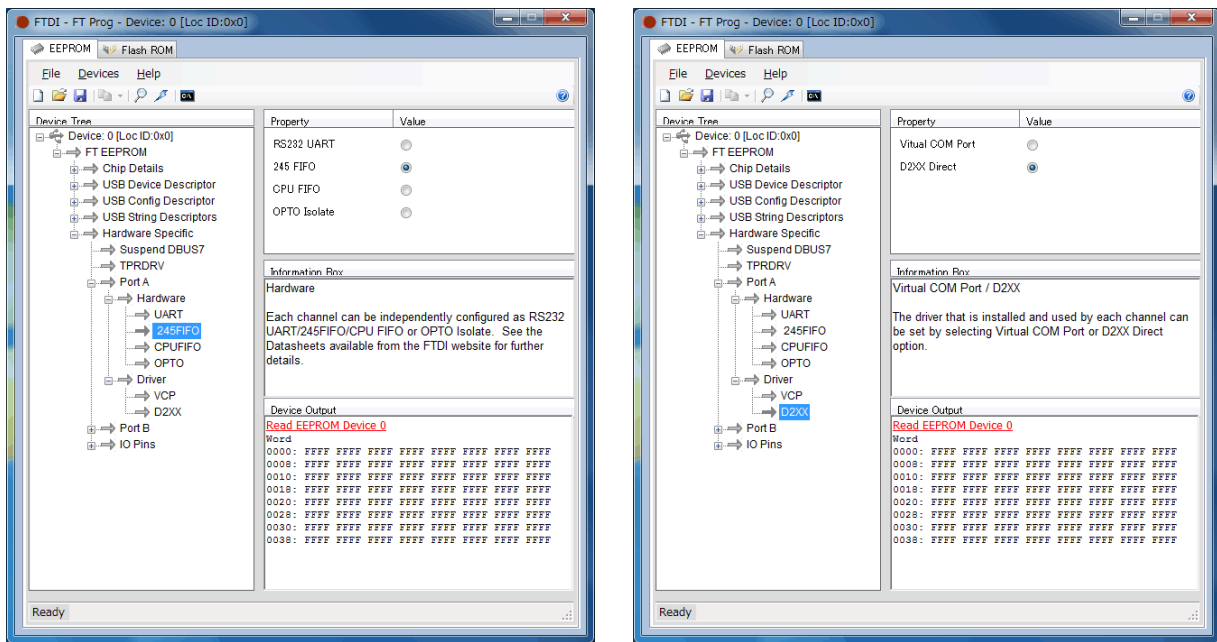


Fig 4. FTDI device parameter setup

Open the "Program Devices" window as shown in Fig. 5 by pressing Ctrl+P, and "Program" the EEPROM of the device. When programming is completed, close the window and press Ctrl+F. The programmed data will be displayed in the main window as shown in Fig. 6. Reset the SASEBO-W board by switching SW8 to "EXT" (power down) and then to "USB" (power up).

Now, insert the ATmega163 IC card facedown into the IC card socket as shown in Fig. 7. Open a command prompt window and change directory to "AVRdude" inside the directory where "sasebo\_w\_quick\_start\_guide\_v1\_1.zip" was unzipped, as described above. Execute "program.bat" in the directory. The IC card will then be programmed as shown in Fig. 8.

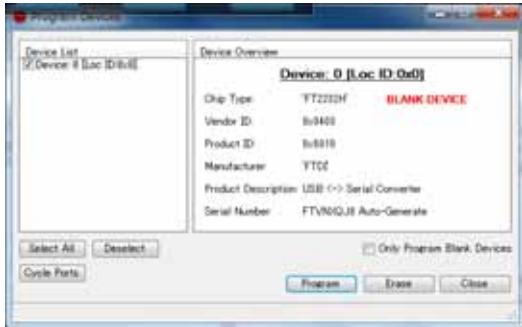


Fig 5. Program devices window

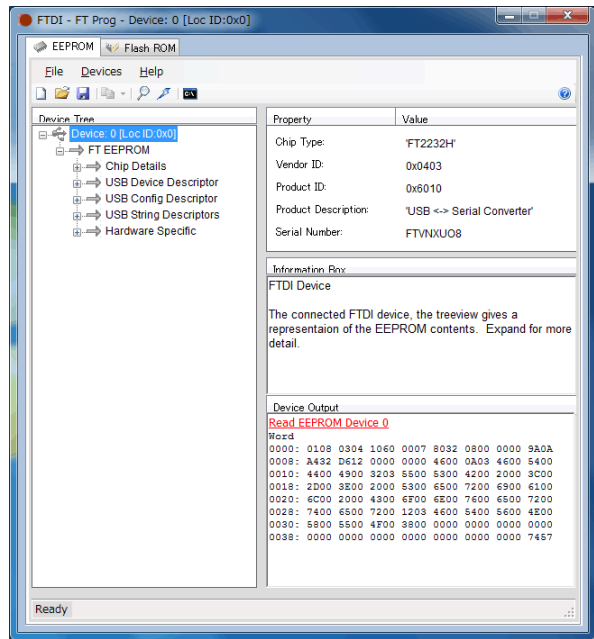


Fig 6. Programmed EEPROM data display



Fig 7. ATmega 163 IC card

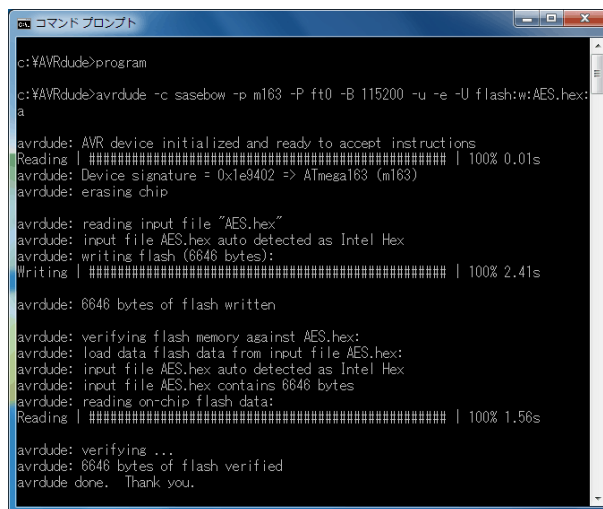


Fig 8. IC card being programmed



After the IC card programming is completed, change the FTDI device to the VCP mode. Select "RS232C UART" and "Virtual Com Port" for the Port A parameters and program the device as shown in Figs. 9 and 10. You can confirm that EEPROM data has been changed by pressing Ctr+P as shown in Fig. 11.

Finally, set the mode switch SW3 on the SASEBO-W board as follows.

SW3: On (1), On (2), Off(3), Off (4)

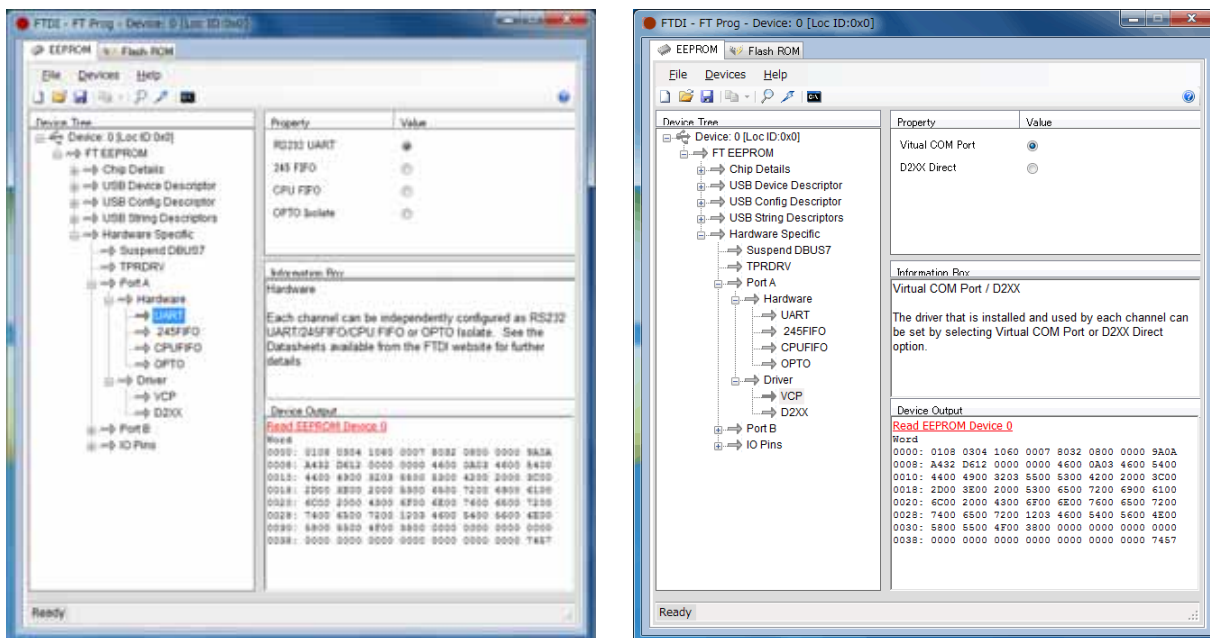


Fig 9. Change FTDI device parameter to VCP mode

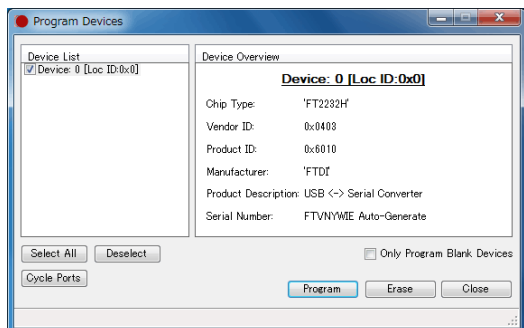


Fig 10. Program devices window

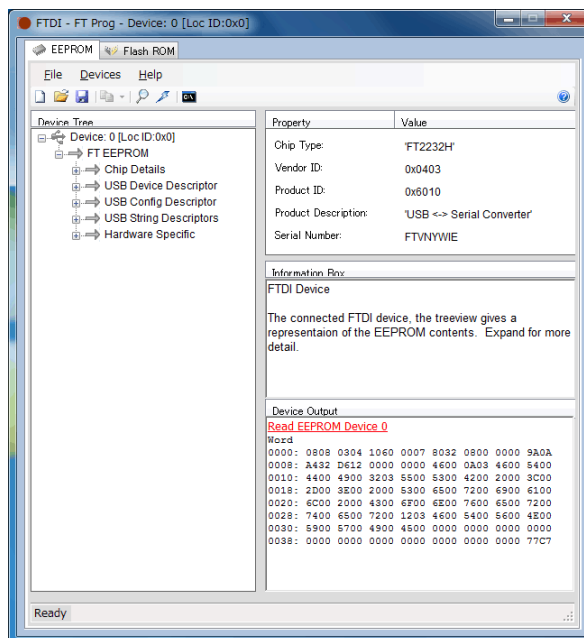


Fig 11. Programmed EEPROM data are displayed

### 3. Execute AES software on IC card

Reboot SASEBO-W by switching SW8 off (EXT) and back on (USB). When configuration completes and LED13 turns on, insert the programmed IC card into the card socket. LED11 should then turn on. Execute "sasebo\_w\_vcp\_checker.exe" in the "sasebo\_w\_vcp\sasebo\_w\_vcp\_checker" directory from the file you previously unzipped. A program window to test the AES software on the IC card will come up as shown on the left side of Fig 12. After selecting the COM port assigned to SASEBO-W, press the "Start" button. The AES operation will start on the card, and input plaintext and output ciphertext will be displayed as in the right side of Fig 12. The 16-byte (128-bit) data in the "Answer" row are calculated by your PC and are compared with the output ciphertext. If any difference is found between the answer data and the plaintext, the program stops. If you have problems, please check the COM port, and double check that you follow the procedure described above.

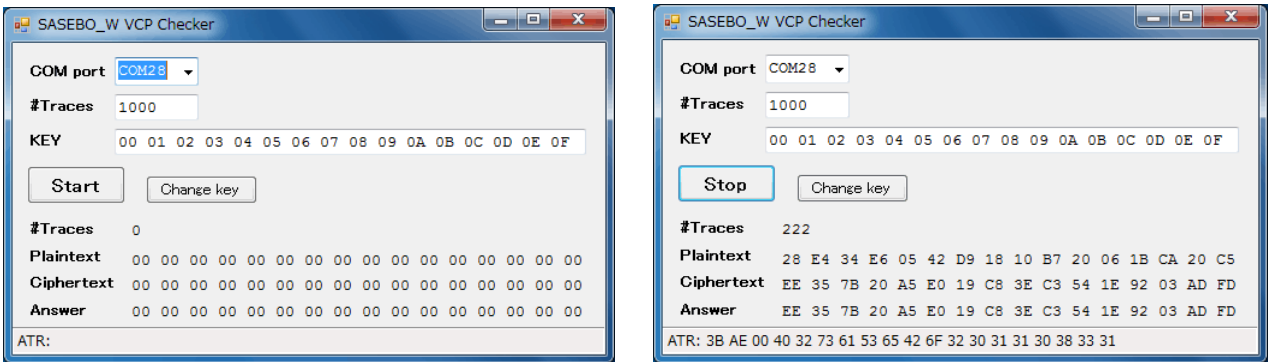


Fig 12. IC card test program window

If the program runs correctly, power traces of the AES operation can be monitored at the J2 SMA connector using an SMA-BNC 50-ohm cable. The trigger signal for the operation is output on header pin 6 of CN6. Figs 13 and 14 shows the SASEBO-W setup and a captured AES power trace.

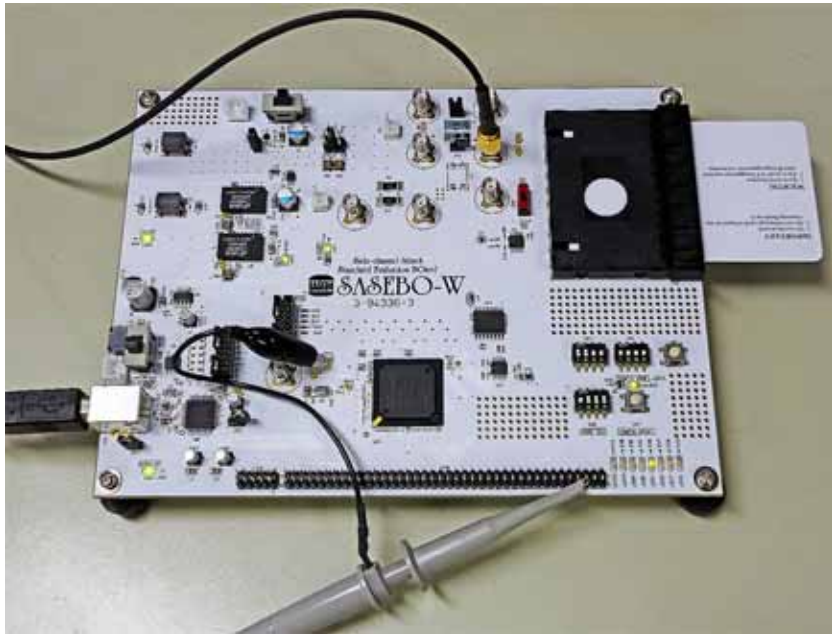


Fig 13. SASEBO-W setup to capture power traces of IC card



Fig 14. Sample power trace of AES operation in IC card



Morita Tech Co., Ltd.  
3-8-1, Kurikidai, Asou-ku, Kawasaki-shi, Kanagawa,  
215-0032, JAPAN  
TEL : 044-980-8139  
FAX : 044-980-8140  
e-mail : sakura@morita-tech.com  
Website : <http://www.morita-tech.co.jp/index.html>

