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

[Version 0.9]

SAKURA-W

October 19, 2014

Satoh Laboratory,

The University of Electro Communications

Revision Record

Date	Version	Record
2014/10/19	0.9	Released

Contents

1. Overview

This document briefly describes instruction to conduct side channel attack experiments using an IC on SAKURA-W 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-W board.

1. SAKURA-W bard
   An IC card R/W board to be stacked on SAKURA-G
2. SAKURA-G bard
   This board is used as a mother board for SAKURA-W.
3. IC card
   ATMega8515 card delivered with SAKURA-W, which contains DES and AES binary codes.
4. 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.
5. Personal computer
   Windows Vista/7 middle-range personal computer to control SAKURA-G.
6. 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 and W. 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

SAKRA-W is controlled by Xilinx Spaltan-6 FPGA on SAKURA-G, and thus SAKURA-G must be setup as follows.

Fig. 1 shows major parts on the SAKURA-G board and locations of DIP switches and setup for the switch SW2 is shown in Tables 1. SW5 and SW10 are not used for SAKURA-W control.

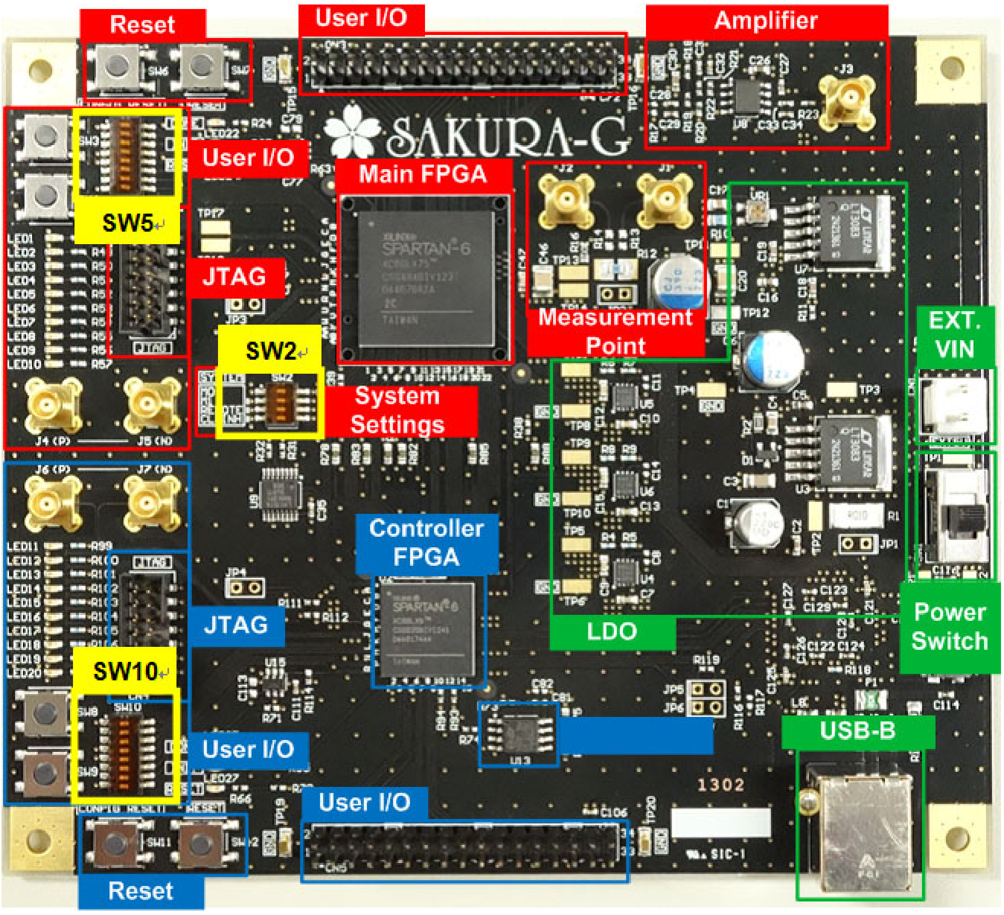


Fig. 1 Major parts on SAKURA-G board.

Table 1. SW2 set up

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

4.2 Download SAKURA-W Tool Package

Access to the following SAKURA-W Webpage.

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

Then, download following four files, and unzip them into the PC connected to SAKURA-G and -W.

1. SAKURA-G interface circuits in VCP mode for SAKURA-W control
   This file contains Verilog-HDL codes, a ucf file, and ROM files (bit and mcs) for the controller FPGA XC6SLX9 on SAKURA-G.

2. SAKURA-W DES Checker
   This file contains a Windows program to test a DES function of the ATMega8515 card in “Release” folder.

3. SAKURA-W AES Checker
4. This file contains a Windows program to test a AES function of the ATMega8515 card in “Release” folder.

5. SAKURA-W Quick Start Guide
   This document.

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. 2. 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.

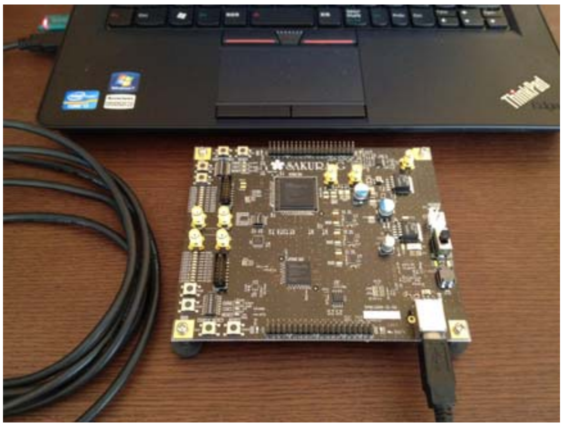


Fig. 2 SAKURA-G connected to PC by a USB cable.

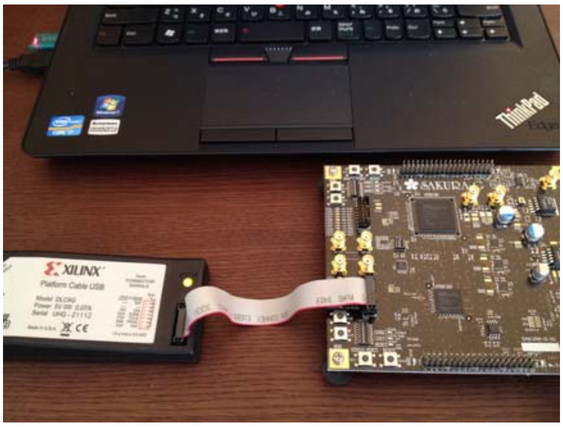
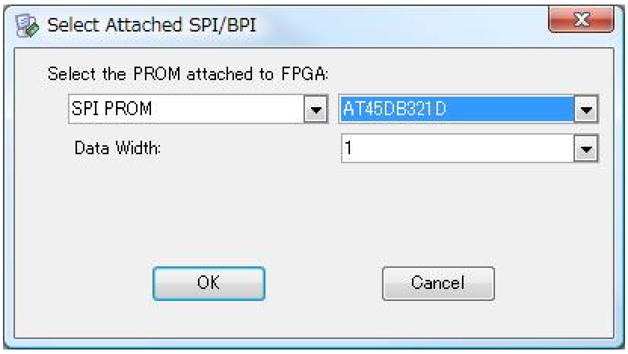


Fig. 3 Configuration cable attached to a JTAG connector of the control FPGA.

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 a configuration file “sakura_w_vcp_mode.mcs” in the unzipped directory. Then select SPI PROM / AT45DB321D as shown in Fig. 4, and write the mcs file into PROM.



Select Attached SPI/BPI

Select the PROM attached to FPGA:

SPI PROM

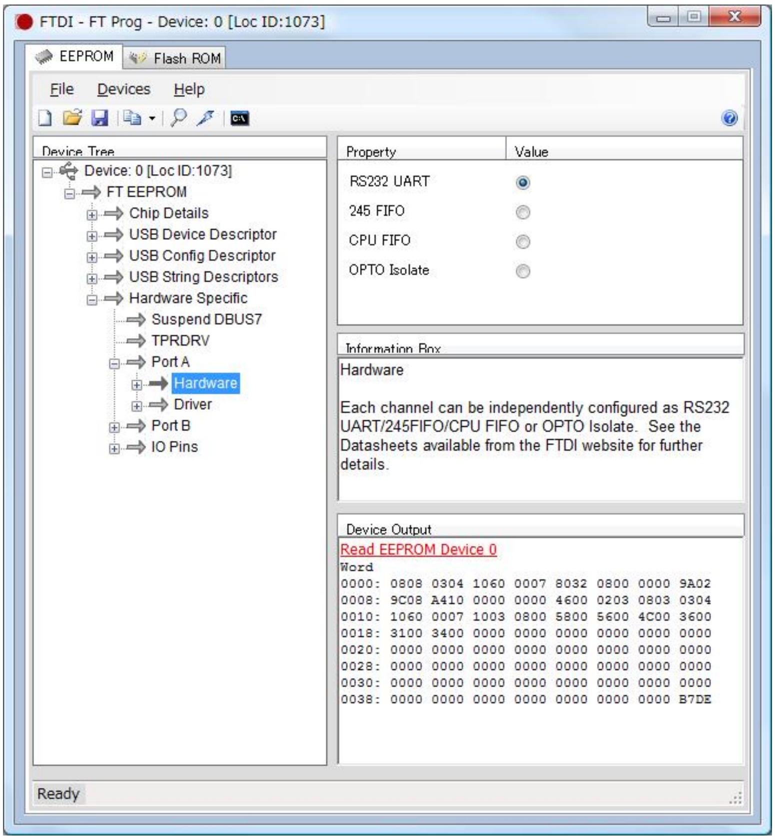
AT45DB321D

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 “RS232 UART” from four modes as shown in Fig. 5. Then, select driver mode “Virtual COM Port” as shown in Fig. 6. The selection is applied only to port A. 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	○

Information Box

Hardware

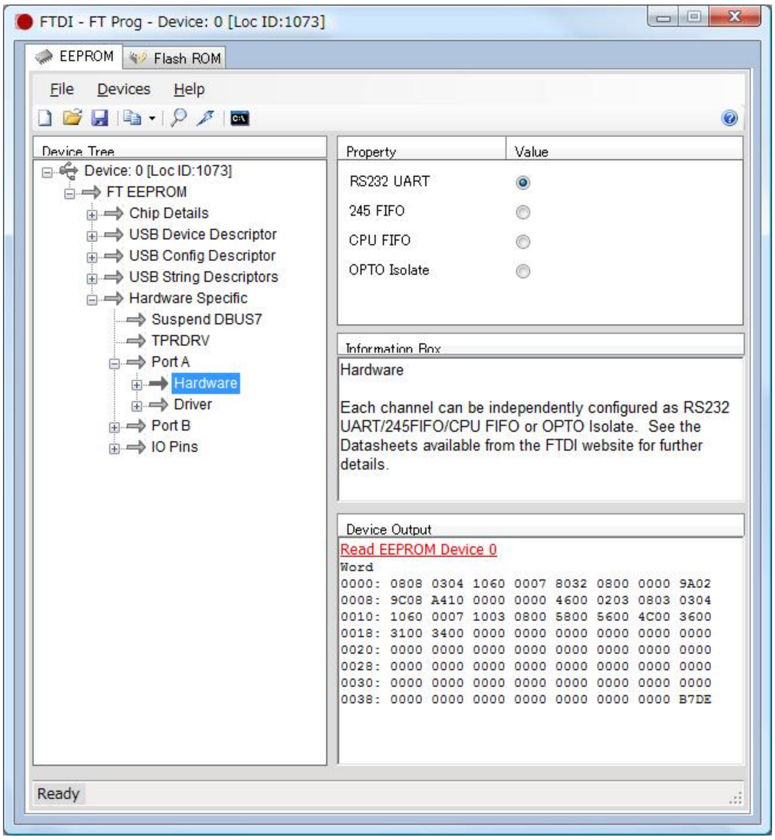
Each channel can be independently configured as RS232 UART/245FIFO/CPU FIFO or OPTO Isolate. See the Datasheets available from the FTDI website for further details.

Device Output

Read EEPROM Device 0

```
Word
0000: 0808 0304 1060 0007 8032 0800 0000 9A02
0008: 9C08 A410 0000 0000 4600 0203 0803 0304
0010: 1060 0007 1003 0800 5800 5600 4C00 3600
0018: 3100 3400 0000 0000 0000 0000 0000 0000
0020: 0000 0000 0000 0000 0000 0000 0000 0000
0028: 0000 0000 0000 0000 0000 0000 0000 0000
0030: 0000 0000 0000 0000 0000 0000 0000 0000
0038: 0000 0000 0000 0000 0000 0000 0000 B7DE
```

Fig. 5 Operation mode selection



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

Information Box

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.

Device Output

Read EEPROM Device 0

```
Word
0000: 0808 0304 1060 0007 8032 0800 0000 9A02
0008: 9C08 A410 0000 0000 4600 0203 0803 0304
0010: 1060 0007 1003 0800 5800 5600 4C00 3600
0018: 3100 3400 0000 0000 0000 0000 0000 0000
0020: 0000 0000 0000 0000 0000 0000 0000 0000
0028: 0000 0000 0000 0000 0000 0000 0000 0000
0030: 0000 0000 0000 0000 0000 0000 0000 0000
0038: 0000 0000 0000 0000 0000 0000 0000 B7DE
```

Fig. 6 Driver mode selection

6. SAKURA-W Setup

Turn off the power switch and disconnect the USB cable for SAKURA-G, and mount SKURA-W on SAKURA-W as shown in Fig. 7. There are five jumper headers JP1-JP5, but JP1 and JP2 are not used in this VCP mode. JP3-JP5 are used to set a power supply voltage to the IC card as follows.

JP3 : 1.8V
JP4 : 3.0V
JP5 : 1.0-3.8V (Adjustable)

For the ATMega8515 card, set a jumper plug to JP4.

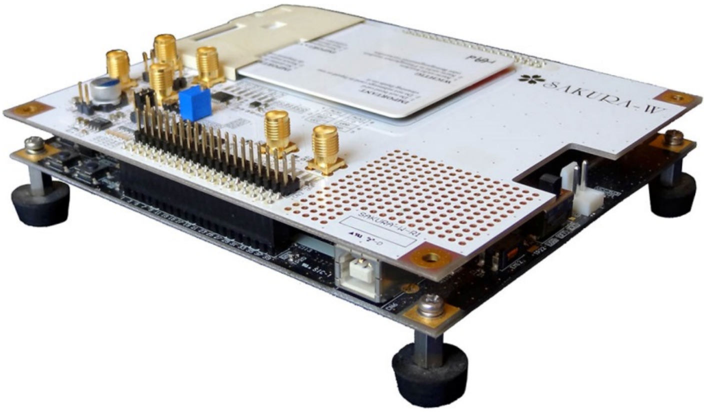


Fig. 7 SAKURA-W on SAKURA-G

7. Operation

7.1 Power on SAKURA-G

When the SAKURA-W is setup properly, connect a USB cable to SAKURA-G and turn on the power switch. Then LED10-LED20 of SAKURA-G and LED1-5 of SAKURA-W are as shown in Tables 4 and 5, respectively. If the status is different, data may not be written in the ROMs for FPGA and USB properly.

Table 4 Status LED of SAKURA-G

No.	Status	No.	Status
LED11	off	LED16	off
LED12	off	LED17	off
LED13	off	LED18	off
LED14	on	LED19	off
LED15	off	LED20	off

Table 5 Status LED of SAKURA-W

No.	Status
LED16	off
LED17	off
LED18	off
LED19	off
LED20	off

7.2 Execute SAKURA-W Checker

Execute the AES function check program for the ATMega8515 card "SAKURA_W_VCP_Checker/bin/Release/SAKURA_W_VCP_Checker.exe" downloaded and unzipped as described in Chapter 3. Fig. 7 shows the initial window of the checker. Followings are explanation of each part in the window. The checker to test DES operations of the card is almost the same except the key length.

COM port

Selection of COM port connected to SAKURA-G as shown in Fig. 8.

#Traces

Input a number of encrypt operations to be performed.

Key

A 128-bit secret key used for the encryption.

Change Key

The 128-bit secret key is changed randomly by clicking this button.

56-bit Key

A length of the secret key for the ATMega8515 card delivered with SAKURA-W is limited to 56 bit (72 bits from MSB side are fixed to "01 23 45 67 89 AB CD EF 01") due to an export regulation. Therefore, it is required to check this box to execute the AES function as shown in Fig. 8. A user can re-program the card with a 128-bit key AES code on the SAKURA-W page.

Start/Stop

When Start button is clicked, encrypt operation starts and the button changes to "Stop" button window changed as shown in Fig. 9. When the Stop 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.

#Traces

A number of encrypt operations performed.

Plaintext

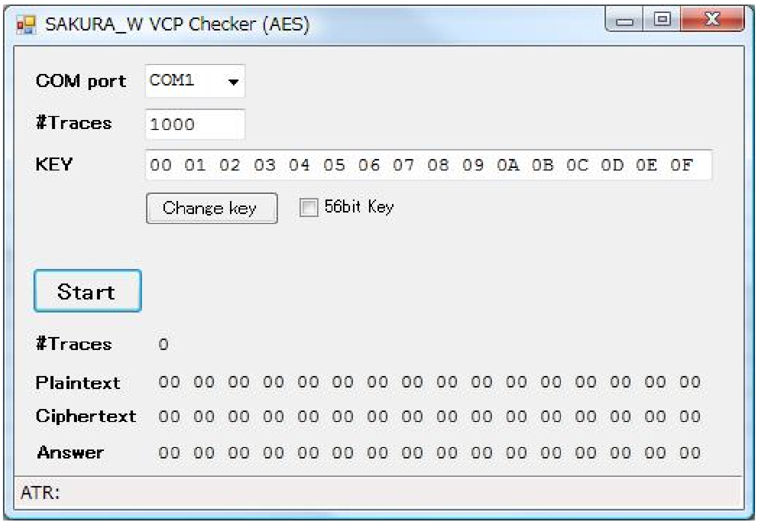
A 128-bit plaintext being encrypted. The plaintexts are generated randomly.

Cipher text

A 128-bit cipher text encrypted from the plaintext.

Answer

A 128-bit cipher text returned from the IC card through SAKURA-W and -G.



COM port COM1

#Traces 1000

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

☐ 56bit Key

#Traces 0

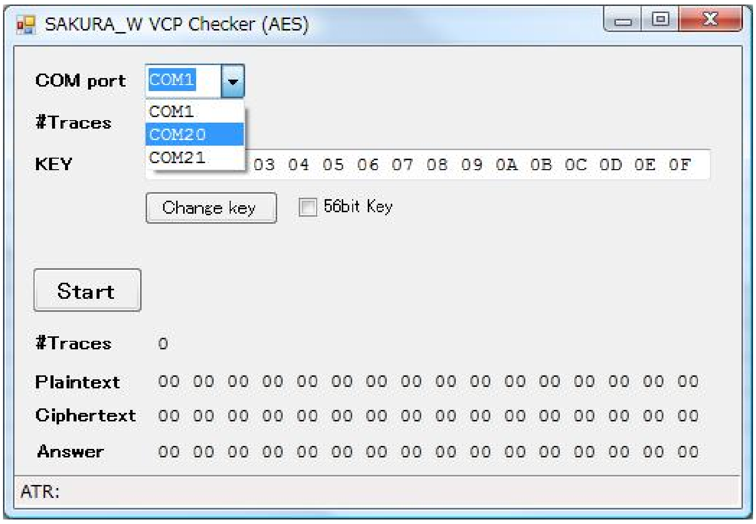
Plaintext 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

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

ATR:

Fig. 7 Initial window of SAKURA_W_VCP_Cheker (AES)



COM port COM1

#Traces

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

☐ 56bit Key

#Traces 0

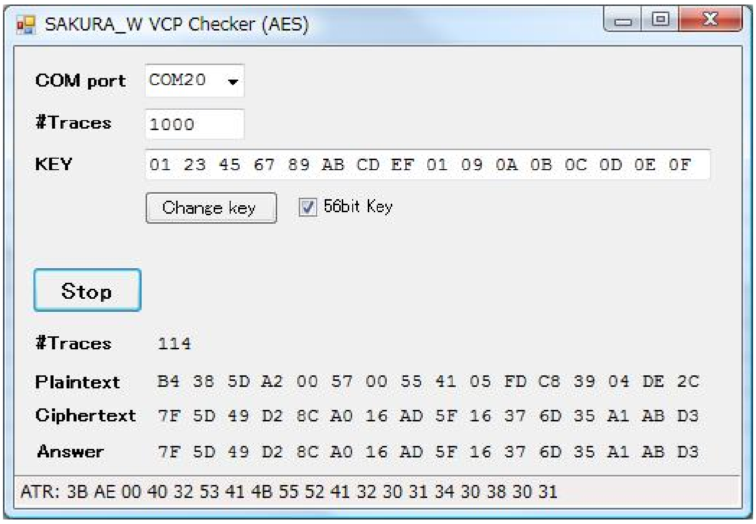
Plaintext 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

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

ATR:

Fig. 8 COM port selection



COM port COM20

#Traces 1000

KEY 01 23 45 67 89 AB CD EF 01 09 0A 0B 0C 0D 0E 0F

☑ 56bit Key

#Traces 114

Plaintext B4 38 5D A2 00 57 00 55 41 05 FD C8 39 04 DE 2C

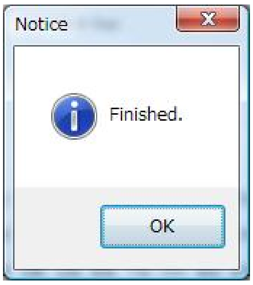
Ciphertext 7F 5D 49 D2 8C A0 16 AD 5F 16 37 6D 35 A1 AB D3

Answer 7F 5D 49 D2 8C A0 16 AD 5F 16 37 6D 35 A1 AB D3

ATR: 3B AE 00 40 32 53 41 4B 55 52 41 32 30 31 34 30 38 30 31

Fig. 9 Encrypt operation with 56-bit key

When the encrypt operation is repeated the number indicated by #Trace and no error occurred, the message dialog box shown in Fig. 10 appears. Thus click “ok” button.


Notice

Finished.

Fig. 10　Successful completion

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/