PROCEEDINGS OF SCIENCE

Research on Power Attack Comprehensive Experiment Platform Based on SAKURA - G Hardware Circuit

Ge Jiao [1][2]

College of Computer Science and Technology,Hengyang Normal University,Hunan Provincial Engineering Laboratory for Technology of Traditional Settlements Digitalization,Hunan Provincial Key Laboratory of Intelligent Information Processing and Application
Hengyang Hunan 421002, China
E-mail: jiaoge@126.com

Lang Li[a], **Yi Zou**[b]

College of Computer Science and Technology,
Hengyang Normal University, Hengyang Hunan 421002, China
E-mail: [a]lilang911@126.com;[b]zou_zouyi@163.com

The power attack of the hardware circuit is going through the steps of algorithm writen in FPGA, power consumption, data processing and analysis. In order to solve the problem of the existing power attack experimental platform because the processing steps are too scattered, feature complex operations and other issues, we've thus developed a higher degree of integration of the experimental platform. The advanced encryption standard (AES) algorithm is taken as an example to illustrate the whole process of implementing the correlation power analysis (CPA) attack on the experimental platform. The AES algorithm will be downloaded to the SAKURA-G experiment board, acquire the algorithm runtime power leakage, carry out the energy analysis because related attacks on information may leak location, and restore the AES first round of the first byte of the key. Empirical results show that the comprehensive experimental platform will integrate these steps into a platform, simplify the operation process, ensure the accuracy of power acquisition, realize the parallel data processing and improve the accuracy and efficiency of power attack.

CENet2017
July 22-23, 2017
Shanghai, China

[1]Speaker

[2]This study is supported by the National Natural Science Foundation of China (Grant No.: 61572174), Hunan Provincial Natural Science Foundation of China (Grant No.: 2017JJ2010), The Scientific Research Fund of Hunan Provincial Education Department (Grant No.:16B039), The open fund project of Hunan Provincial Engineering Laboratory for Technology of Traditional Settlements Digitalization (Grant No.: CT16K03), The Science and Technology Plan Project of Hunan Province（Grant No.: 2016TP1020）and The Science and Technology Plan Project of Hengyang（Grant No.: 2015KJ26）.

PoS(CENet2017)044

1 . Introduction

In 1999, Kocher[1] proposed a differential power analysis (DPA), the hardware implementation of DPA attack for encryption algorithm by measuring the leakage of cryptographic devices to get the key information of differential power. The scholars have carried on related researches on the power consumption attack experiment platform. In 2011, Yue Daheng[2] constructed an analysis platform based on FPGA power attack, and the conventional cryptographic algorithm successfully attack; In 2012, Li Lang [3] constructed a AT89C51 based DES encryption algorithm power attack physical experiment platform; in 2016, Li Zonghua [4] developed a software to simulate the power consumption of embedded chip, the successful implementation of the DES round key plus differential power attack.

However, the power attack hardware implementation to each clock cycle will perform more operations, which stimulate the energy consumption than software implementation is much more complex, and the existing experimental platform also exists in power acquisition, data processing, attack analysis dispersion problems, aiming at the above problems is constructed a hardware circuit based on power attack experiment platform SAKURA-G.

In this paper, the advanced encryption standard (AES) algorithm is taken as an example to illustrate the whole process of implementing the correlation power analysis (CPA) attack on the experimental platform. The AES algorithm will be downloaded to the SAKURA-G experiment board, acquire the algorithm runtime power leakage, carry out energy analysis and related attacks on information may the leak location, restore the AES first-round of the first byte of the key.

The paper will describe the establishment of a comprehensive experimental platform in Section 2. The work flow of the comprehensive experimental platform will be given in Section 3. Section 4 will briefly introuce the power attack and experimental results for AES algorithm, and in Section 5 we will describe the conclusion.

2. Establishment of Comprehensive Experimental Platform

2.1 Platform Architecture

The comprehensive experimental platform can realize the power of information AES encryption for password chip acquisition leakage, carry on the corresponding processing to the collected data, and then carry out CPA attack experiment to get the key of AES cipher chip.

2.2 Hardware Environment

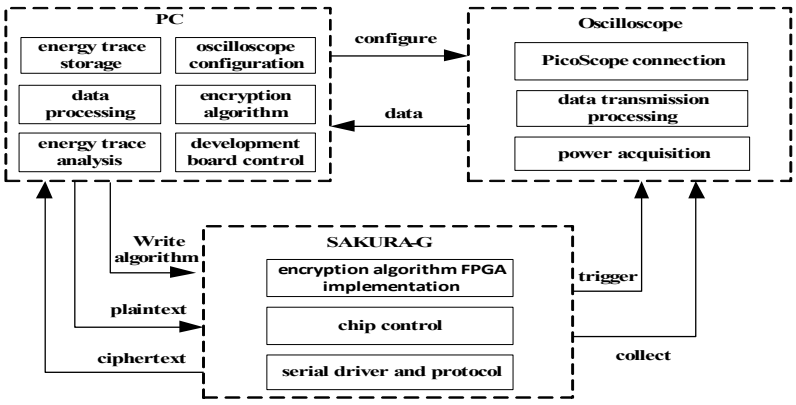

Figure 1: Hardware Module

The hardware composition of the integrated experimental platform includes SAKURA-G hardware encryption development board, oscilloscope and PC. The integrated experimental platform module diagram is shown in Fig. 1.

The power acquisition process and the connection method of hardware environment are as follows:

(1) SAKURA-G two FPGA chip ROM has been written to the official AES circuit and control circuit. The power will be automatically loaded to the FPGA chip [5]. If the user uses other encryption algorithms to modify the circuit, the Xilinx downloader will connect to SAKURA-G CN2 or CN4, to FPGA 1# and FPGA 2# download program.

(2) PC host through the USB interface to connect the encryption device SAKURA-G CN6 and power supply for the SAKURA-G.

(3) PC sends plaintext data to SAKURA-G through the experimental platform.

(4) Power acquisition device PicoScope oscilloscope Channel 1 and high resistance probe connection, probe hook connected to the AKURA-G CN3 of the Pin, the probe clip is connected to the SAKURA-G of any one of the outer edge of the SMA block. SMA is used to connect the BNC line oscilloscope inChannel 2, where the SMA head is connected to the SMA block J3, BNC head connected to the low-pass filter, and through the low-pass filter connected to the oscilloscope channel of 2 SAKURA-G. When the power is collected, the SAKURA-G runs 1 times of the AES encryption algorithm channel to generate trigger signal, and Channel 2 collects the relevant power consumption data.

(5) After the encryption is completed, the SAKURA-G sends back the ciphertext data to the PC machine, and the oscilloscope returns the power consumption data and stores the data in the computer.

(6) Comprehensive experimental platform for FPGA data files acquires power data files, carries out CPA attack analysis to obtain the experimental results .

2.3 Software Design

The software function of the integrated experiment platform includes power consumption collection module, data processing module and CPA analysis processing module. Main functions of each module is showns as follows:

(1) The power consumption acquisition module: including the selection of USB interface of the hardware test board, the selection of the target device, the selection of the oscilloscope, the location of data storage, FPGA data acquisition, power consumption data acquisition.

(2) The data processing module: to collect a large number of data files to modify the file name in a batch manner and copy them to the same folder.

(3) The CPA analysis and processing: select the FPGA data files and collecte data by CPA analysis, carry out CPA attack analysis and processing, and the corresponding waveform display.

3. Experimental Operation Process

For the workflow of the comprehensive experimental platform, specific procedures are shown as follows:

(1) First open the SAKURA-G test board, oscilloscope and other hardware equipment;

(2) Open the power acquisition and CPA attack experimental platform for data acquisition;

(3) The FPGA data are collected on the experimental board and collect the power data by the oscilloscope, and store the same on the local file;

(4) Batch processing of a large number of data files as saved;

(5) The FPGA data and power consumption data were analyzed by CPA;

(6) The waveform is successfully displayed and analyzed, otherwise return to Step (2).

3.1 Actual Power Acquisition

The steps of power consumption are shown as follows:

(1) Open power acquisition and CPA attack experimental platform, the main interface is shown in Fig. 2.

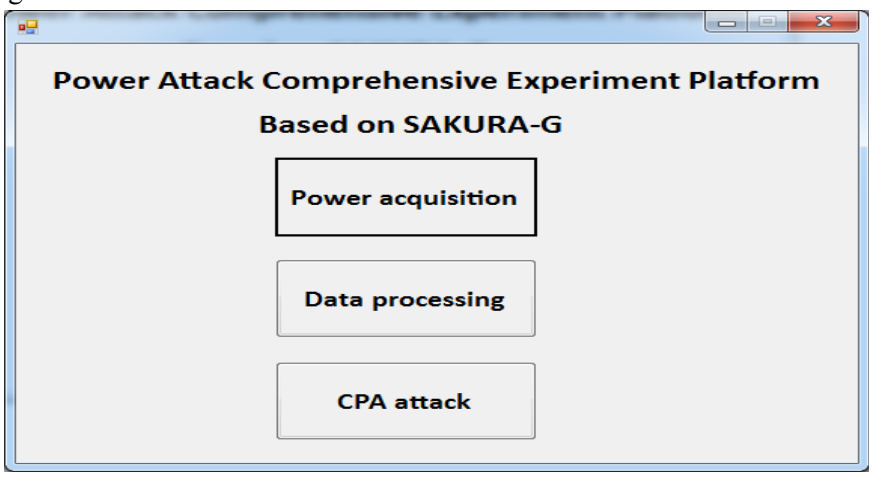

Figure 2: Software Main Interface

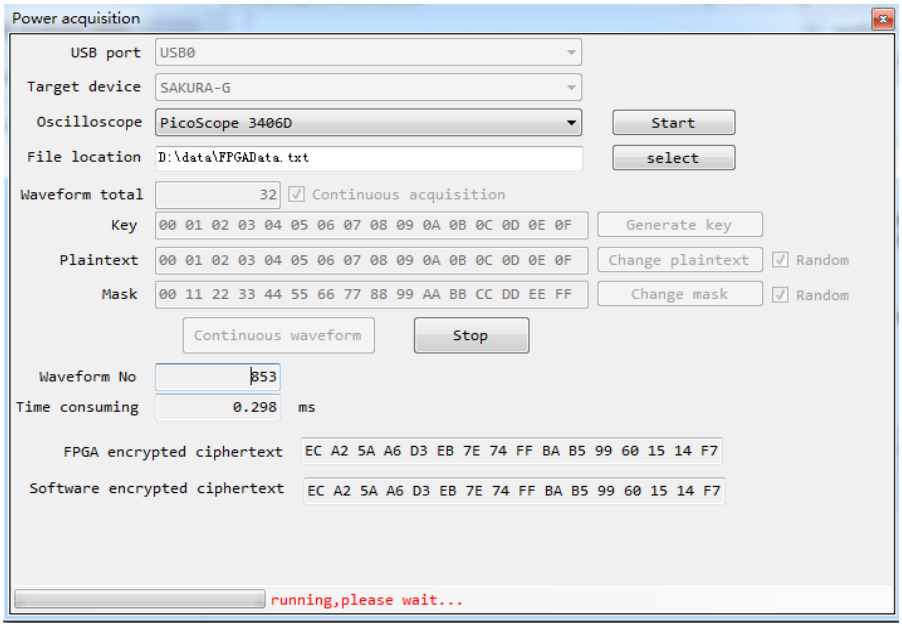

Figure 3: Power Acquisition Interface

(2) Click the "power acquisition" button on the main interface to enter the power capture main interface, as shown in Fig. 3.

(3) Select the target device as "SAKURA-G", select the target device by using the USB interface, select the oscilloscope “PicoScoper 3406D”, Click “start", run PicoScope 6 program. You should make the following settings:

- Channel A range:5V
- Channel B range:20mV
- Timebase: 2μs/div, x2 (zoom), 1 MS (samples)
- Trigger channel: A

- Trigger height:200mV
- Trigger: repeat

(4) Click Select File Save Location to specify the path to save the FPGA data file.

(5) Click the "generate key", "change plaintext", "change mask", "random", can randomly generate 128 bit key, plaintext and mask.

(6) Click the "continuous waveform" can start the SAKURA-G experiment board to run AES, at the same time,see the input to the SAKURA-G experiment board through SAKURA-G experiment board plaintext encrypted ciphertext and ciphertext encrypted by AES software. At the same time, there are 2016 groups of data including the number, plaintext, ciphertext, mask and key to save to FPGAData.txt.

(7) At the same time, the oscilloscope data acquisition, PicoScoper 3406D for the first time the number of waveforms are collected for up to 32 and stored in a folder with the file name: i.txt(i={1,2,…,32}); so collect 63 times, 1-63 named folder, Waveform file saved as text type, a total of 2016 waveform data acquisition.

(8) Click stop to stop SAKURA-G experiment board by running AES algorithm.

3.2 Power Consumption Data Processing

As the 63 power consumption data in the folder to save the same file name, needs to be modified as a batch j.txt （j={1,2,…,2016}） , 2016 waveform power files are copied to the same folder. The specific operations are shown as follows:

(1) Click the "data processing" button on the main interface of the experimental platform to enter the power consumption data processing interface, as shown in Fig. 4.

(2) Click the “Batch File Rename” tab, click the select folder, select the collected power data files to be treated, automatically display the number of statistics folder contains a selected folder, click the batch rename button to complete the file batch rename. Click the “View Folder” button to open the file directory and view the file name changes.

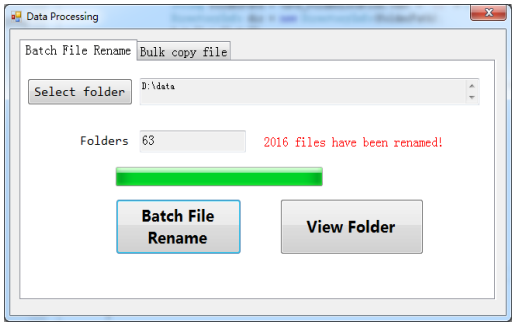

Figure 4: Batch Modify the File Name

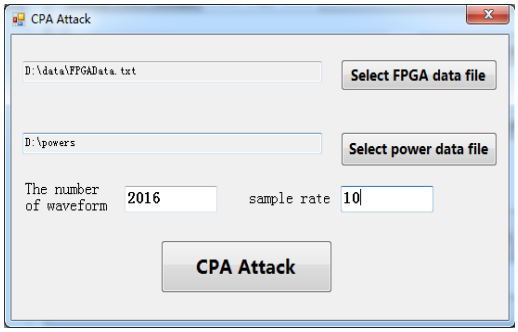

Figure 5: CPA Attack Analysis

(3) Click the “Bulk Copy file” tab, click Select folder, select a target folder to deal, click a target folder, select a target folder to copy, click the “Bulk copy” button, complete the batch file copy.

(4) Click the “Browse file” button to open the file directory and view the bulk copy of the file.

4.Power Attack and Experimental Results for AES Algorithm

4.1 CPA Attack Analysis Process

(1) Click on the main interface of the CPA attack analysis and the CPA attack analysis interface, as shown in Fig. 5.

(2) Click Select FPGA data file and select the saved FPGA data file.

(3) Celect the power consumption data file and select the data file that has been processed.

(4) The number of waveform acquisition automatically generated, the number of input points, according to the ratio of 10:1 sampling.

(5) Click the "CPA attack analysis" button to get the experimental results.

4.2 Theoretical Cower consumption

Select the S-box of input as the point of power attacks. Assuming the key value of 0 to 255, the key value of the first byte substitution hypothesis with the plaintext encryption process, calculate the intermediate results.

The leakage model of SAKURA-G AES circuit is Hamming distance model, which describes the energy consumption of CMOS circuit much better than the Hamming weight model, the power and the first encrypted ciphertext and the encryption state (plaintext and key XOR) showed a linar relationship between the Hamming distance, the Matlab program that converts the assumed intermediate result to the power data value is as follows:

```
for keyGuess=0:255
for plaintextNo=1: 2016
  midValue=bitxor(plaintext(plaintextNo,1),keyGuess);
            if plaintextNo>1
             midValue =bitxor(midValue,ciphertext(plaintextNo-1,1));
end
HDPower(keyGuess+1,plaintextNo)=bitand(midValue,128)/128+bitand(midValue,
64)/64+bitand(midValue,32)/32+bitand(midValue,16)/16+bitand(midValue,8)/8+bitand(
midValue,4)/4+bitand(midValue,2)/2+bitand(midValue,1);
end
end
```

4.3 CPA Analysis

The correlation coefficient is a measure of the linear relationship between data, CPA takes the correlation coefficient to determine the correct key. The correlation coefficient between the actual power consumption and the theoretical power consumption is calculated. The input of the S-box is attacked by CPA. Only the first byte of the first round key is attacked.

Click the "CPA Attack" button, call the Matlab function (Matlab function to generate a dynamic link library) and generate the corresponding waveform. The correct key is assumed to be 56 at the highest peak, the successful guess key. The results of CPA attack are shown in Fig. 6.

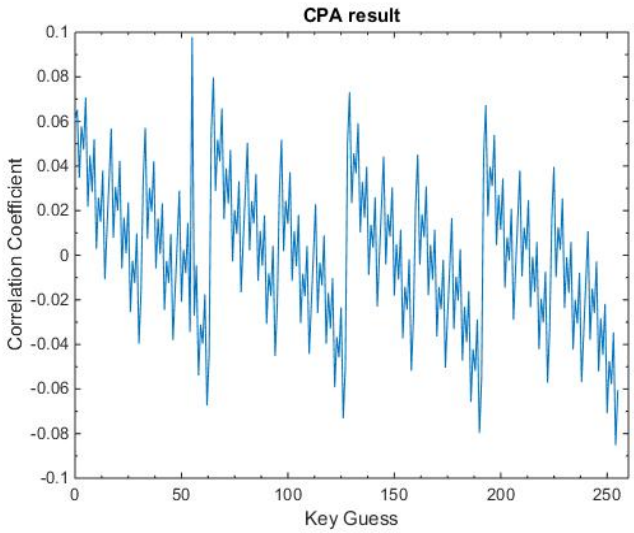

Figure 6: Result of CPA attack

5. Conclusion

The power attack is a method to obtain the key by using the power consumption information leaked in the working process. Aiming at the existing power attack experiments, the majority power waveforms are realized by the simulation software. In comparison with the actual hardware circuit, the energy consumption is quite different. The power consumption of data acquisition, processing and analysis of attack dispersion problems, build a hardware circuit based on power attack comprehensive experimental platform of SAKURA-G, and the experimental correlation power attack AES. The experimental results show that the platform has the characteristics of high integration, flexible hardware circuit, convenient power consumption and high efficiency of data processing.

References

[1]P. Kocher, J. Jaffe, B. Jun, *Differential power analysis*, International Cryptology Conference on Advances in Cryptology, Berlin:Springer-Verlag, 1999:388-397.

[2]D.H. Yue, *Research on circuit-level design agasinst power analysis attack for cryptographic chip*, National university of defense technology,2011. (in chinese)

[3]L. Li, K.L. Li, G. Jiao Ge, et al, *Research of power analysis physical experiment platform based AT89C51*, Application research of computers, 2012,(07):2681-2682. (in chinese)

[4]Z.H. Li, *Design and implementation of differential power analysis attack platform*, South china university of technology,2016. (in chinese)

[5]W.J. HU, A. WANG, L.J. Wu, et al, *Power attack of SM4 hardware implementation based on SAKURA-G board*, Microelectronics & computer, 2015,(04):15-20. (in chinese)