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

GeJiao[1,2], DeXinDing*[1], Lang Li[2]
[1]School of Environment Protection and Safety Engineering
University of South China, Hengyang Hunan 421001, China
dingdxzzz@163.com

[2]College of Computer Science and Technology
Hengyang Normal University, Hengyang Hunan 421002, China

ABSTRACT: *The power attack of the hardware circuit is going through the steps of the algorithm write in FPGA, power consumption, data processing and analysis and the existing power attack experiment platform is too decentralized for each step, where the operation is complex, requiring a high degree of integration of the experimental platform for support. The development of a hardware circuit based on power attack comprehensive experimental platform SAKURA-G, realized these steps will be integrated into a platform, simplify the operation process, to ensure the accuracy of power acquisition, and realizes parallel data processing, improve the accuracy and efficiency of power attack.*

Keywords: SAKURA-G, Power Attack Experiment Platform, AES, CPA

Received: 2 April 2019, Revised 9 July 2019, Accepted 20 July 2019

DOI: 10.6025/jes/2019/9/3/102-111

© 2019 DLINE. All Rights Reserved

1. Introduction

In 1999, Kocher[1] proposed the differential power analysis (DPA), Hardware implementation of DPA attack for encryption algorithm, by measuring the leakage of cryptographic devices and get the key information of differential power. Power attack poses a serious threat to the security of cryptographic devices, and has become a hot topic in the research of side channel attacks.

The scholars have carried on the related research to the power consumption attack experiment platform, in 2011, Le Daheng constructed an analysis platform based on FPGA power attack, and the conventional cryptographic algorithm successfully attack; In 2012, Li lang and other to establish a AT89C51 based DES encryption algorithm power attack physical experiment platform [4]; In 2016, Li Zonghua developed a software to simulate the power consumption of embedded chip, the successful implementation of the DES round key plus differential power attack [5].

However, power attack hardware implementation in each clock cycle will perform more operations, which makes the simulation of 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 (hereinafter referred to as the comprehensive experimental platform).

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

2. Establishment of Comprehensive Experimental Platform

2.1Platform Architecture

AES as a new generation of international encryption standard, because of its high efficiency and high security, it has been widely concerned and studied [6]. AES on the hardware to achieve a large number of experiments and optimization, it has a very high efficiency, so that the AES has been widely used in hardware, but also makes the AES has been a lot of attacks.

Side channel attack technology developed in recent years, especially for key power attack technology through the power consumption information leaked by the information processing process can be easy, constitutes a serious threat to the security of algorithm.

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

2.2 Hardware Environment

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

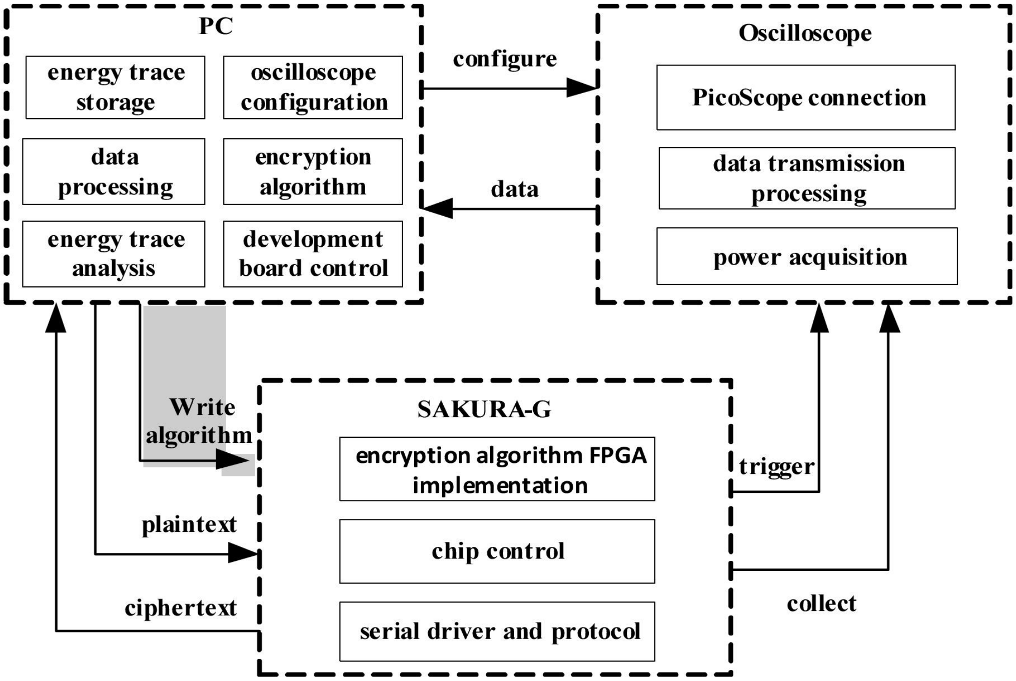


Figure 1. Hardware module

The power acquisition process and 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 [7]. If the user uses other encryption algorithms can modify the circuit, the Xilinx downloader to 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 connected to the SAKURA-G of any one of the outer edge of the SMA block. The use of SMA to connect the BNC line oscilloscope channel 2, where the SMA head 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 the 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 and the acquisition of power data files, CPA attack analysis, experimental results are obtained.

The schematic diagram of the device connection is shown in figure 2.

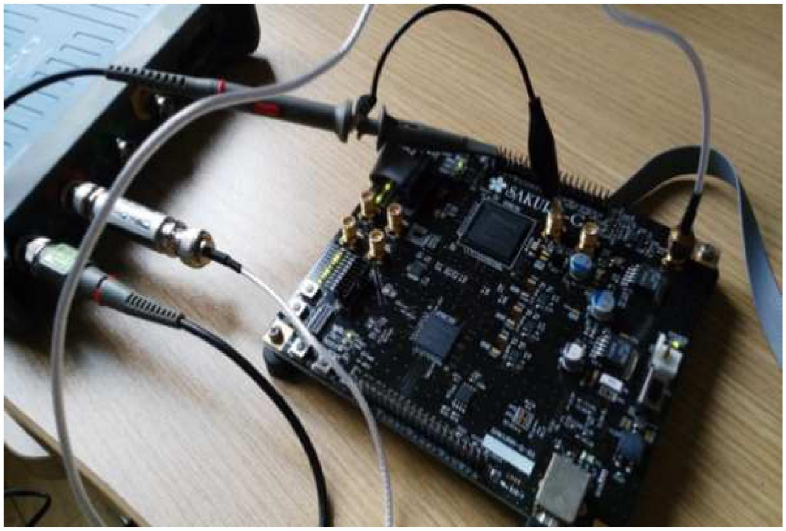


Figure 2. Actual results of the hardware environment

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. The functional structure of the software is shown in Figure 3,The main functions of each module are as follows:

(1) Power consumption acquisition module: including the selection of the 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) Data processing module: to collect a large number of data files to batch modify the file name and copy to the same folder.

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

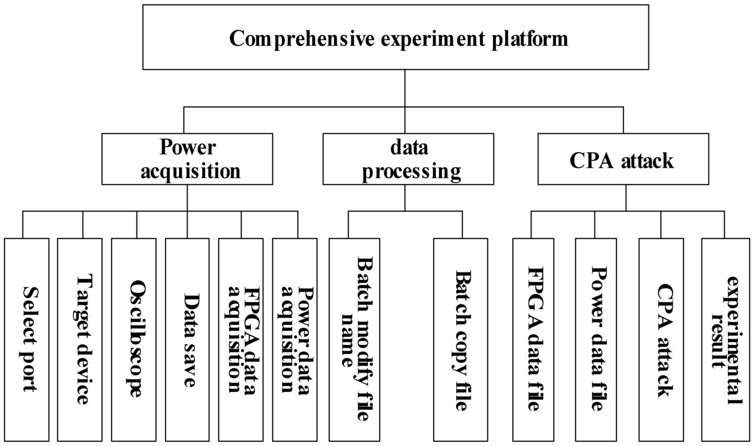


Figure 3. Software function structure

3. Experimental Operation Process

The work flow of the comprehensive experimental platform, As shown in Figure 4, Specific procedures are 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 collected on the experimental board and the power data collected by the oscilloscope are stored on the local file;

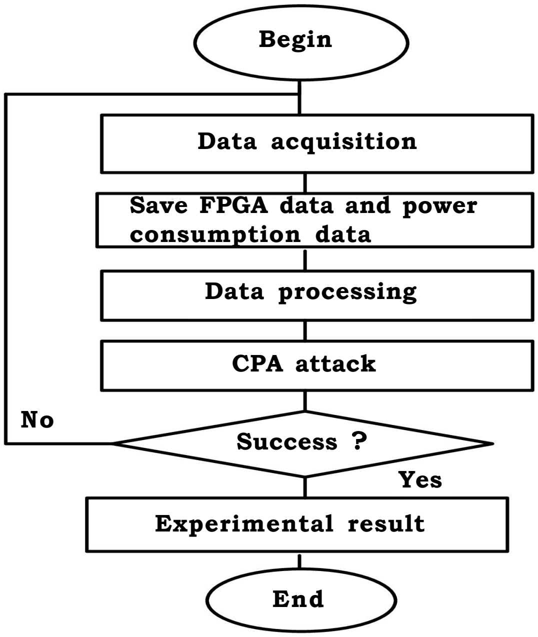


Figure 4. Experimental platform workflow

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

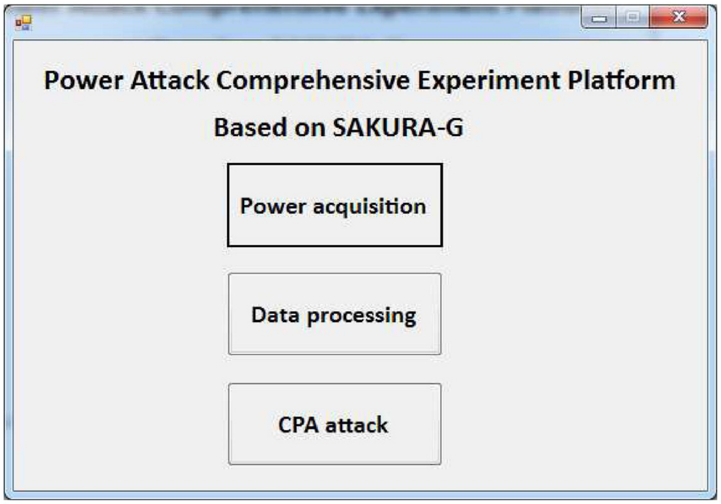
(5) The FPGA data and power consumption data were analyzed by CPA;

(6) The waveform is successfully displayed and analyzed, otherwise returned to.

3.1 Actual Power Acquisition

The steps of power consumption are as follows:

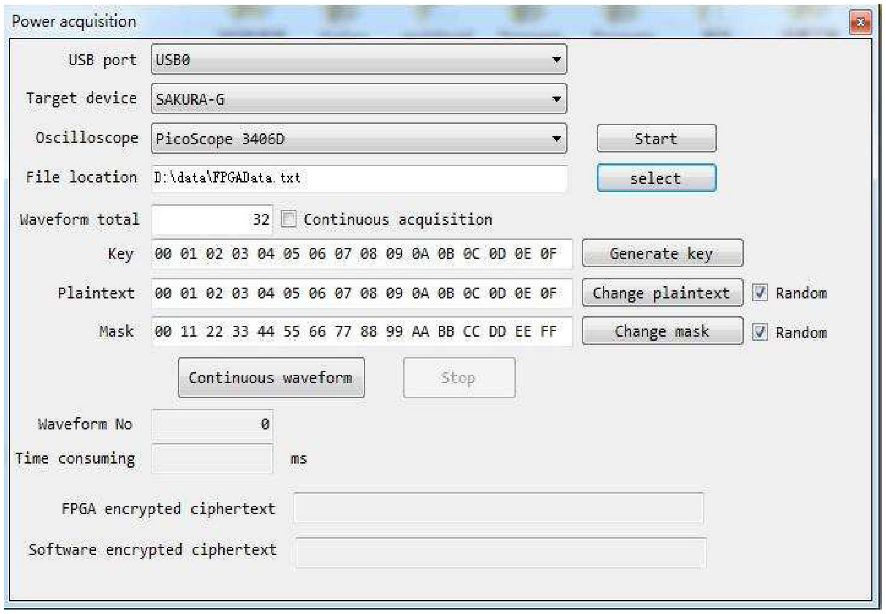
(1) Open power acquisition and CPA attack experimental platform, the main interface shown in Figure 5.



Power Attack Comprehensive Experiment Platform
Based on SAKURA-G

Figure 5. Software main interface

(2) Click the "power acquisition" button on the main interface to enter the power capture main interface, as shown in figure 6.



Power acquisition

USB port: USB0

Target device: SAKURA-G

Oscilloscope: PicoScope 3406D

File location: D:\data\FPGAData.txt

Waveform total: 32 □ Continuous acquisition

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

Plaintext: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ☑ Random

Mask: 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF ☑ Random

Waveform No: 0

Time consuming: ms

FPGA encrypted ciphertext:

Software encrypted ciphertext:

Figure 6. Power acquisition interface

(3) Select the target device as "SAKURA-G", select the target device using the USB interface, select the oscilloscope "PicoScoper 3406D", Click "start", run PicoScope 6 program. you should make the following settings (As shown in Figure 7):

- Channel A range:5V
- Channel B range:20mV
- Timebase:2is/div, x2 (zoom), 1 MS (samples)
- Trigger channel: A
- Trigger height:200mV
- Trigger: repeat

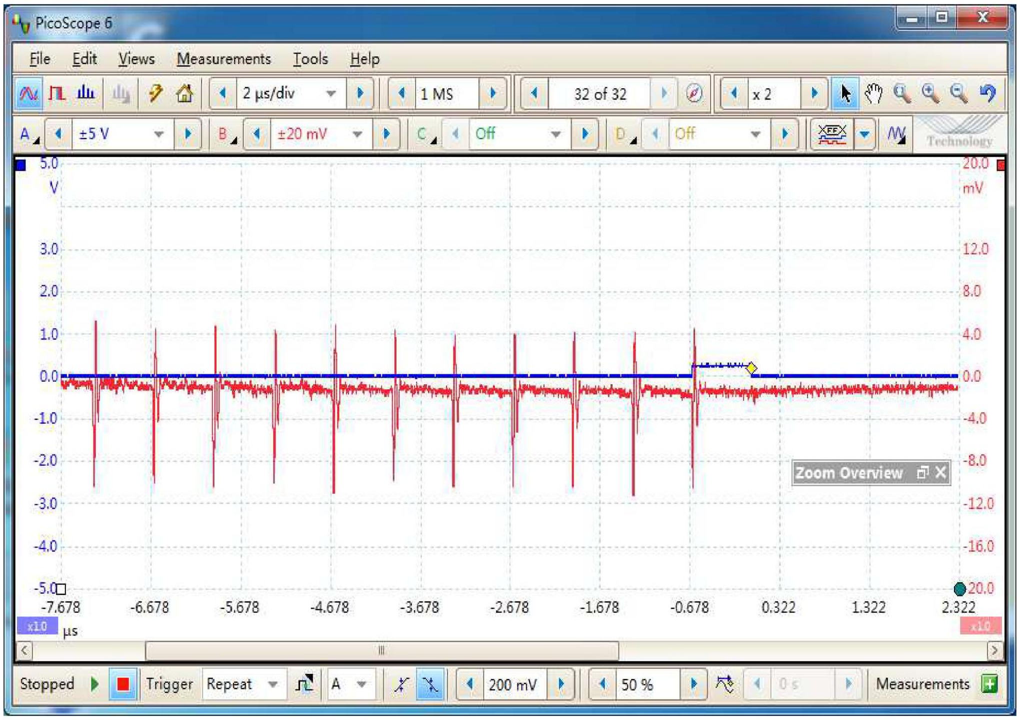

2 µs/div
1 MS
32 of 32
x 2
A ±5 V
B ±20 mV
C Off
D Off
Stopped
Trigger Repeat
A
200 mV
50 %
0 s

Figure 7. PicoScope 6 settings

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

(4) Click the "Generate key", "Change plaintext", "Change mask", "Random", can randomly generate 128 bit key, plaintext and mask.

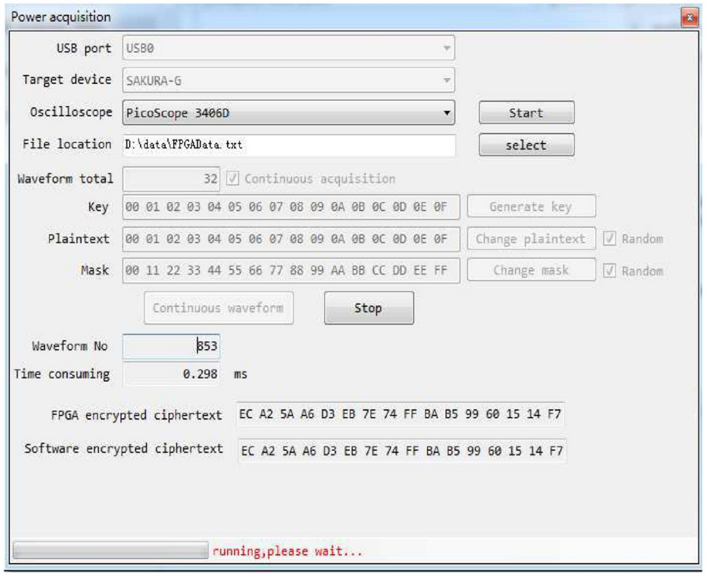
(5) Click the "Continuous waveform" can start the SAKURA-G experiment board to run AES, at the same time will see the input to the SAKURA-G experiment board through SAKURA-G experiment board plaintext encrypted ciphertext and ciphertext encrypted by AES software, which is shown in figure 8. At the same time, there are 2016 groups of data including the number, plaintext, ciphertext, mask and key to save to FPGAData.txt.

(6) At the same time, oscilloscope data acquisition, PicoScoper 3406D for the first time the number of waveforms collected for up to 32, Store in a folder, File name is: *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.

(7) Click stop to stop the SAKURA-G experiment board running AES algorithm.

3.2 Power Consumption Data Processing

Because 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}, and the 2016 waveform power files copied to the same folder, specific operations are as follows:


Power acquisition

USB port: USB0

Target device: SAKURA-G

Oscilloscope: PicoScope 3406D

File location: D:\data\FPGAData.txt

Waveform total: 32 ☑ Continuous acquisition

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

Plaintext: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F ☑ Random

Mask: 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF ☑ Random

Waveform No: 853

Time consuming: 0.298 ms

FPGA encrypted ciphertext: EC A2 5A A6 D3 EB 7E 74 FF BA B5 99 60 15 14 F7

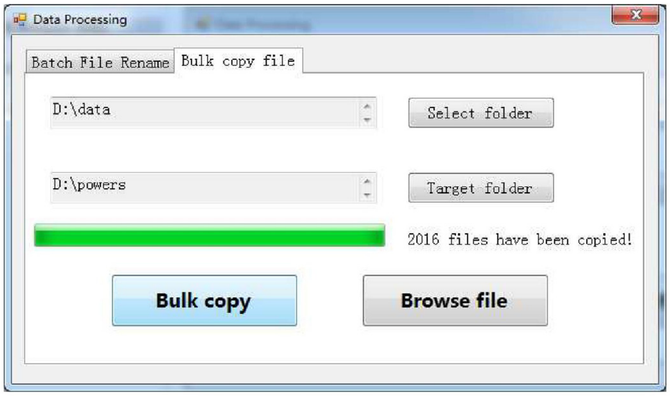
Software encrypted ciphertext: EC A2 5A A6 D3 EB 7E 74 FF BA B5 99 60 15 14 F7

running,please wait...

Figure 8. Start SAKURA-G test board interface

(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 Figure 9.

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


Data Processing

D:\data

D:\powers

2016 files have been copied!

Figure 9. Batch modify file name

(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, as shown in figure 10.

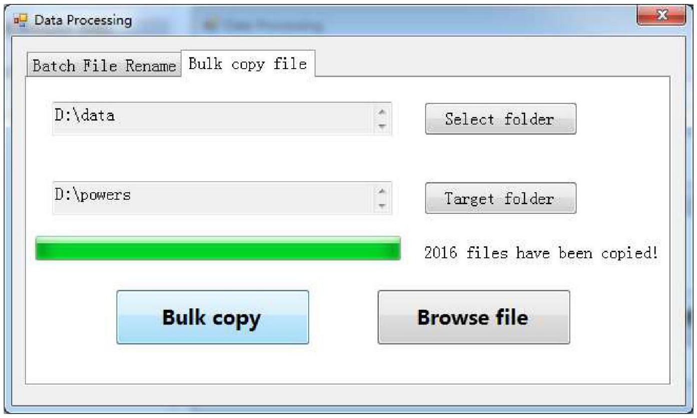
(4) Click the “Browse file” button to open the file directory, view the bulk copy of the file.

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, into the CPA attack analysis interface, as shown in figure 11.

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



D:\data

D:\powers

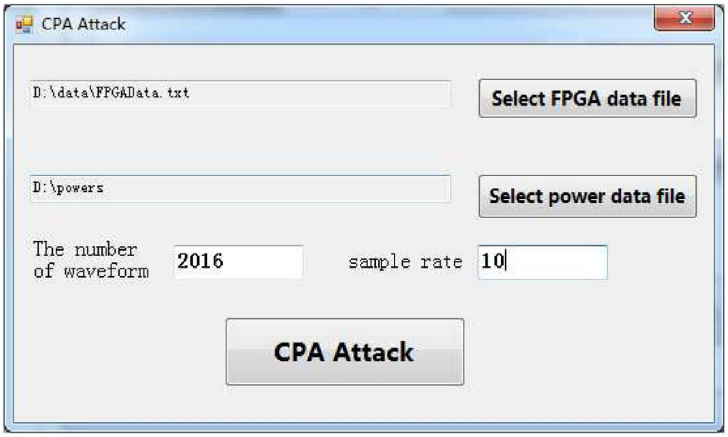
2016 files have been copied!

Figure 10. Batch Copy File

(3) Select the power consumption data file, 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.



D:\data\FPGAData.txt

D:\powers

The number of waveform 2016

sample rate 10

Figure 11. CPA attack analysis

4.2 Theoretical Power Consumption

Select the S-box of input as the point of power attacks, assuming the key value of 0 to 255, and then 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 the CMOS circuit is much better than the Hamming weight model, power and the first encrypted ciphertext and the encryption state (plaintext and key XOR) showed a linear relationship between the Hamming distance “, the Matlab program that converts the assumed intermediate result to the power data value is as follows:

```
forkeyGuess=0:255
forplaintextNo=1: 2016
midValue=bitxor(plaintext(plaintextNo,1),keyGuess);
ifplaintextNo>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

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

Click the “CPA Attack” button, will call the Matlab function (Matlab function to generate a dynamic link library), generate the corresponding waveform, the correct key is assumed to be 56 when the highest peak, the successful guess key. The results of CPA attack are shown in Figure 12.

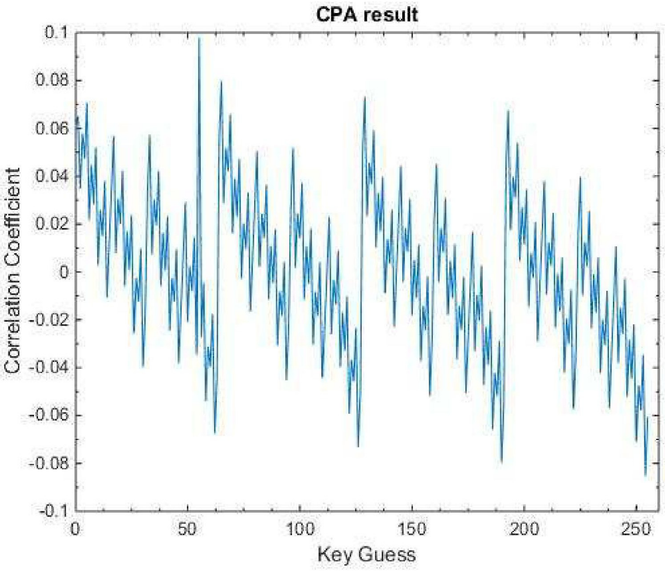


Figure 12. Result of CPA attack

5. Conclusion

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, most of the power waveform is realized by simulation software, compared with the actual hardware circuit, the energy consumption is quite different. And 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.

Acknowledgements

The author thanks the referees for their helpful and insightful comments. This work was supported by the National Natural Science Foundation of China (Grant No.61572174), Hunan Provincial Natural Science Foundation of China (Grant No.), and the Scientific Research Fund of Hunan Provincial Education Department (Grant No.16B039).

References

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

[2] Wei-dong, ZHONG., Qing-quan, MENG., ZHANGShua-wei. (2017). Implementation and optimization of S-box on AES Based on secret sharing. *Advanced Engineering Sciences*, 01, 191-196.

[3] YueDaheng. (2011). Research on circuit-level design against power analysis attack for cryptographic chip, *National university of Defense Technology*.

[4] LI Lang, LI Ken-li, JIAOGe. (2012). Research of power analysis physical experiment platform based AT89C51, *Application Research of Computers*, 07, 2681-2682.

[5] Li Zonghua. (2016). Design and implementation of differential power analysis attack platform, South China University of Technology.

[6] Bilgin, B., Gierlichs, B., Nikova, S. (2014). A more efficient AES threshold implementation. Progress in Cryptology-FRICACRYPT 2014. Switzerland: Springer, 2014 267-284.

[7] HU Wen-jing, WANGAn., Wu Li-ji. (2015). Power attack of SM4 hardware implementation based on SAKURA-G board, *Microelectronics & Computer*, 04, 15-20.