Optical Side-Channel Dependency Analysis on Microcontroller Chip

Wang Hongsheng
Department of Information Engineering
Ordnance Engineering College
Shijiazhuang, China
whswzx@aliyun.com

Zhang Yang
Department of Information Engineering
Ordnance Engineering College
Shijiazhuang, China
405077949@qq.com

Ji Daogang
Department of Information Engineering
Ordnance Engineering College
Shijiazhuang, China
jidaogang@163.com

Chen Kaiyan
Department of Information Engineering
Ordnance Engineering College
Shijiazhuang, China
744188112@qq.com

Abstract-This paper analyzes the basic structure of microcontroller and researches CMOS circuit photon emission mechanism, by using single-photon detection device, builds a collection of photon emission experiments platform for microcontroller. By studying the AT89C52 microcontroller, analyzes the microcontroller photon emission information and the relationship between the perform operation and the process of data. At the same time analyzes the influence of the microcontroller photon emission by different operate voltage. Through analysis about the photon emission of microcontroller, demonstrates that the microcontroller information security exist risk.

Keywords-photon emission; dependency analysis; microcontroller; single-photon detectors; side-channel analysis

I. INTRODUCTION

Since the first paper using side-channel information to analyze cryptography chips were presented by Kocher in 1996. Using side-channel to attacks the cryptography becomes an important research area. The time side-channel [1] and power side-channel [2] were presented in 1999. Since then various side-channel analysis for cryptography chip has been developed rapidly, such as electromagnetic emission side-channel attack [3-5] and caches Time Attack [6-7], and various side-channel attacks analytical methods, such as template attack [8] and a common information analysis [9]. But most of the attacks are concentrated cryptography chip system-wide side-channel information leakage. Photon emission analysis was first proposed in 2008, it uses the running cryptography-chip emission photon for side-channel analysis [10], which allows select cryptography chip specific part to do in-depth analysis. Photon emission enables analysis sensitive information via chips single transistor attack to obtain a key, while its compare electromagnetic, power analysis for integrated circuits have a better signal to noise ratio. This paper aim at AT89C52 microcontroller MOV instruction execution, verify the relationship between photon emission and the microcontroller operation and data, to lay the foundation for the subsequent using photon emission analysis for AES, RSA algorithms.

II. BACKGROUND

A. CMOS circuit photon emission mechanism

Now most of the integrated circuit constructs on the basis of COMS structure. The majority of the COMS circuit is composed by a pair of n-MOS and p-MOS transistors. When the transistor state is switched, the current generate by the electronic transition caused a thermal effects, and thus emission photons. When the transistor changes from high state to low, the n-channel transistors of COMS circuit is emission photons, whereas the p-channel transistor of COMS circuits is emission photons. Because of n-channel in conversion process is the movement of electrons, therefore the number of n-channel photon emission to be more. Due to the different energy of electrons obtained causes a different photon radiating spectra. According to the literature [11], the emission photons in the spectral range 500nm to 1200nm, the maximum emission in the range 900nm to 1100nm. Since transistor changes emission photons of CMOS circuit is a probability event, means that not each changes must emission photon. The literature [12] gives each transistor flip probability of photon emission formula:

$$N_e=S_eBL_HI_d/(qv_s)T_s$$

Where S_e is the spectral emission density, B is the bandwidth of the emission, L_H is the length of the hot carrier region, I_d is the drain current, v_s is the saturated carrier velocity, Ts is the switching frequency. As you can see by the formula, according to the transistor technology, the probability of the transistor photon emission is about 10-2 to 10-4.

B. Single Photon Detection Technology

Today devices for single photon detection are the following: a special CCD camera, a photomultiplier tube (PMT) and avalanche photodiode (APD). Special CCD cameras usually with near-infrared microscope to observe secret chip surface area photon emission, which has high spatial resolution, easy observation cryptography chip structure, suitable for observation large area. But it implementation is relatively low accuracy, sampling rate slow cause photon capture long exposure time. For photomultiplier tube, since its large aperture detector without precise alignment cryptography chip, to cryptography chip photon emission have high acquisition rate. But its quantum efficiency is low result a longer acquisition time, also because of its larger pore size leads to a higher dark noise, it is very sensitive to external disturbance. The avalanche diode, because of the smaller of pore size, can be localized to a small area of integrated circuit for detection, more accurate detection result, greatly reduces the signal to noise ratio. But it has the high current and near-infrared region has low sensitivity. For today's high degree of integration semiconductor chips, more precise analysis in specific areas is essential. So in experiment, we use an avalanche diode as single-photon detectors.

C. dependency analysis

Cryptography chip photon emission depends on chip perform operation instruction (operation-dependent) and processed data (data dependency), both the dependency in analysis secret key information of chip is very important. By Equation 1 shows the number of photon emission depends on the number of transistors flip. So when the cryptography chip implement different instruction, the position and number of the transistor overturns is differences, then led to different occur time for photon emission. For the same instruction perform different data, different number of transistors rollover occurs, result the number of photon emission also different. Based on these differences could reflect the dependence of photon emission with operation and data, to identify this dependence can be use photon emission attacks against specific algorithm, thus can be assumed the key for cipher algorithm. Through use simple analysis, differential analysis and other analytical methods to use in specific cryptographic algorithms.

III. EXPERIMENTAL DEVICE

A. Photon System

Experiments we use silicon avalanche diode as single-photon detector to detection cryptography chip. The silicon single-photon detector can capture 400nm to 1060nm wavelength photons, which have a high collect efficiency for the visible parts. The Experimental photon system is shown in Figure 1.

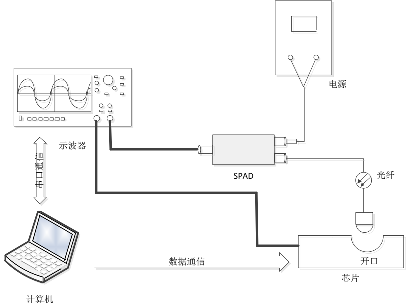

Figure1. Photon Emission photovoltaic systems

The computer control test equipment for input data, the single-photon detector to detect the device under test is connects the terminal via fiber optics. The output is connects the oscilloscope CH1 channel and the test equipment connects the oscilloscope CH2 channel to provides synchronization trigger signal. Oscilloscope obtained data is storage to the computer by Labview.

B. Device under Test

To use single-photon detectors for photon emission detection, you first need to make the cryptography chip inside exposed. Here we make ATMEL company AT89C52 microcontroller reopen, it has 8K bytes Flash program memory and 256 bytes memory SRAM. Figure 2 shows the results of the opened AT89C52 by using an optical microscope with camera obtain high-resolution image of chip surface.

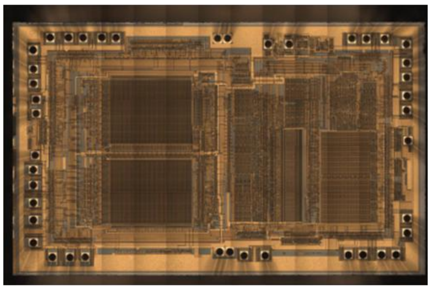

Figure2. Reopened AT89C52 microcontroller

By analysis of the basic structure of the chip, it is possible to clearly identify the function of each module, such as the SRAM, Flash memory, data bus and address bus, etc. It helps find the collection position for measurement. In this paper, the use of single-photon detectors to detection the register of the chip SRAM area, Figure 3 shows the amplified SRAM.

Figure3. The enlarged SRAM area

C. Experimental procedures and software

During the experiment, set AT89C52 microcontroller clock frequency of 12MHz. In order to verify the cryptography chip photon emission operator-dependent and data dependencies, the opened AT89C52 microcontroller performed the command shown in Figure 4, the data sent different data by the computer to the # LOW unit changes the microcontroller executed. Two assembly code front the program instructions are retrieve computer data sent to accumulator A. Program XOR instructions (XRL) and a conditional branch instruction (SJMP) each require two machine cycles to execute, and the rest all require one machine cycle instruction execution, each machine cycle is 1us, the test program cycles totaling 10us.

```
MOV    R0,#LOW
MOV    A,@R0
XRL    P1,#08H
MOV    R7,A
XRL    P1,#08H
MOV    R7,#0x00
SJMP   C0031
```

Figure 4.MOV program assembler code.

IV. EXPERIMENTAL ANALYSIS

A. The voltage of photon emission impact

During the experiment, the microcontroller chip executes the same instruction, process the same data and collecting photon emission signals in the same time interval, by changing the microcontroller operate voltage, can found the microcontroller in very different quantities of photon emission, the higher the voltage, the photon irradiation higher. AT89C52 microcontroller experiments showed that the operating voltage with the photon emission is approximately exponential rather than linear (Table 1).

TABLE1. UNDER DIFFERENT OPERATING VOLTAGE, THE AT89C52 INSTRUCTION MOV R7, A PHOTON EMISSION

	Voltage（V）			
	5.0V	5.5V	6.0V	6.5V
photons (No.)	122	406	862	1487

B. Operation dependency analysis

In experience, the microcontroller executes the instruction in Figure 4. Oscilloscope CH2 from the program given the rising trigger (corresponding program instructions is start from XRL P1, # 08H) start collecting accept single-photon detectors give photon emission information for CH1. In oscilloscope the program cycle 10us is divided into 1000 channels (record once every 10us), single-photon detector according to arrive on time distribution in these 1000 channels. The single photon detector via fiber alignment region of microcontroller SRAM registers R7, collecting two hours. The collected data is processed by the order according to Figure 4 shown the instruction. The result is in Figure 5. Found that the number of emission photons of each instruction execution is not same, indicating that photon emission relate to the chips code operate instruction.

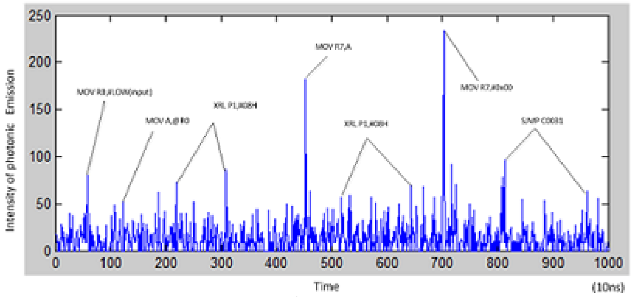

Figure 5. Single photon detector for register R7, each instruction photon emission situation

C. data dependence analysis

Cryptography chip at a time the photon emission is not only dependent on instruction, but also on processed data. To obtain the microcontroller the photon emission characteristics of processing different data, experiments on AT89C52 microcontroller register R7 to detection. Before each experiment, the value of register R7 will set 00, to ensure that each transformation is flipped from 00 to a value. Then the value of the R7 were changed to 00, 01, 03, 07, 0 F, 1F, 3F, 7F, FF, the corresponding register R7 transistor turn on flip 0-8 bits. The instruction MOV R7, A acquisition (2 hours) data analysis as shown in Table 2 (correspond the peak between 400 to 500 in Figure 5). We can observed, the more register transform, the more photons emission.

V. CONCLUSION

In this paper, by performing MOV instruction to microcontroller carried out operations and data correlation photon emission analysis, verify the photon emission associated with security chip inside information there is a certain dependence relation. To lay good foundation for subsequent specific cryptographic algorithms analysis by using photon emission, while the analysis proved that photon emission poses a serious threat to security chip.

ACKNOWLEDGMENT

The authors would like to thank Gao Yan-lei for his useful comments on the preliminary version of this article. We would also like to thank Institute of Physics Chinese Academy of Sciences to provide important experimental equipment.

This paper is supported by the National Natural Science Foundation of China (A new side-channel analysis method: pipeline electromagnetic emanation analysis. Grant No. 51377170. Research on the key techniques of hardware trojan detection based on side channel analysis. Grant No. 61271152) and the Natural Science Foundation of Heibei, China (Electromagnetic analysis against Cipher chips and practical provable security. Grant No. F2012506008).

REFERENCES

[1] *kocher P C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems[C] //Advances in Cryptology –CRYPTO'96. Springer Berlin Heidelberg, 1996:104-113*

[2] *PAUL C KOCHER, JOSHUA JAFFE, and BENJAMIN JUN. Differential Power Analysis: 19th Annual International Cryptology Conference[C]. California: Advances in Cryptology, 1999, 388–397.*

[3] *Quisquater, J.J., Samyde, D.: Electromagnetic analysis (EMA): Measures and counter-measures for smart cards. In: E-smart. pp. 2001, 200-210*

[4] *KarineGandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis: Concrete Results. In Cryptographic Hardware and Embedded Systems - CHES2001, Third International Workshop, pages 2001,251-261,*

[5] *DENG Gao-ming, ZHANG Peng, ZHAO Qiang. EM Template Analysis for Cipher Chips[J]. Microelectronics & Computer 2010，27（1）：1-4*

[6] *CHEN Cai-sen, WANG Tao, ZHENG Yuan-yuan. Timing Attacks and Defenses on RSA Public-key Algorithms[J], Computer engineering,2009,35(2): 123-125*

[7] *Bernstein, D.: Cache-timing attacks on AES Annual International Cryptology Conference, [C] Springer Berlin Heidelberg, 2005, 249-263*

[8] *Chari, S., Rao, J.R., Rohatgi, P.: Template attacks. In: Cryptographic Hardware and Embedded Systems | CHES 2002. pp. 2002,13-28*

[9] *Batina, L., Gierlichs, B., Prouff, E., Rivain, M., Standaert, F.X., Veyrat-Charvillon, N.: Mutual information analysis: a comprehensive study. J. Cryptology 24(2), 2011,269-291*

[10] *Ferrigno, J., Hlavac, M.: When AES blinks: introducing optical side channel. Information Security, IET 2(3), 2008, 94 -98*

[11] *S. Villa, A.L. Lacaita, A. Pacelli, "Photon emission from hot electrons in silicon", Physical Review B, Vol. 52, 1995, pp. 10993–10999*

[12] *F. Stellari, F. Zappa, M. Ghioni, S. Cova, "Non-invasive optical characterisation technique for fast switching CMOS circuits",*

	the data in register R7								
	0x00	0x01	0x03	0x07	0x0F	0x1F	0x3F	0x7F	0xFF
photons (No.)	766	774	789	797	809	816	822	831	836

TABLE 2.THE PHOTON EMISSION OF AT89C52 MOV R7 AT DIFFERENT DATA