Optical Side-Channel Dependency Analysis on Microcontroller Chip

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

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:

\[ N_e = S_e B I_d (q v_s) T_s \]

Where \( S_e \) is the spectral emission density, \( B \) is the bandwidth of the emission, \( I_d \) is the length of the hot carrier region, \( I_d \) is the drain current, \( v_s \) is the saturated carrier velocity, \( T_s \) 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

© 2014. The authors - Published by Atlantis Press
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.

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.

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.

1. MOV R0, #LOW
2. MOV A, @R0
3. XRL P1, #08H
4. MOV R7, A
5. XRL P1, #08H
6. MOV R7, #0x00
7. 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 operation with the photon emission is approximately exponential rather than linear (Table 1).

<table>
<thead>
<tr>
<th>Voltage (V)</th>
<th>5.0V</th>
<th>5.5V</th>
<th>6.0V</th>
<th>6.5V</th>
</tr>
</thead>
<tbody>
<tr>
<td>photons (No.)</td>
<td>122</td>
<td>406</td>
<td>862</td>
<td>1487</td>
</tr>
</tbody>
</table>

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 is not same, indicating that photon emission relate to the number of emission photons of each instruction execution detector via fiber alignment region of microcontroller the instruction. The result is in Figure 5. Found that the distribution in these 1000 channels. The single photon chips code operate instruction. The voltage of photon emission impact

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 to 0, 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 Hebei, China (Electromagnetic analysis against Cipher chips and practical provable security. Grant No. F20125060008).

REFERENCES


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

Figure 4. MOV program assembler code.
the data in register R7

<table>
<thead>
<tr>
<th></th>
<th>0x00</th>
<th>0x01</th>
<th>0x03</th>
<th>0x07</th>
<th>0x0F</th>
<th>0x1F</th>
<th>0x3F</th>
<th>0x7F</th>
<th>0xFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>photons (No.)</td>
<td>766</td>
<td>774</td>
<td>789</td>
<td>797</td>
<td>809</td>
<td>816</td>
<td>822</td>
<td>831</td>
<td>836</td>
</tr>
</tbody>
</table>

Table 2. The photon emission of AT89C52 MOV R7 at different data