2019 12th International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo), October 21-23, Haining, China

Side Channel Leakage Information Based on Electromagnetic Emission of STM32 Micro-controller

Xu Zhijian, Tang Qiang, Song Yanyan, Zhang Dongyao and Zhou Changlin
Strategic Support Force Information Engineering University
Zhengzhou, China
Email: Xuzhijian0@163.com, thyasher@163.com, 274739762@qq.com, 2437102553@qq.com, zhou637196@163.com

***Abstract*—This paper analyses the electromagnetic information conducted leakage mechanism of a typical single-chip micro-controller, tests and reconstructs raw information emission by micro-controllers. The direct-coupled signal detection method is used to collect the electromagnetic leakage information of the side channel to obtain the conduction coupling leakage waveform. Using the wavelet transform, feature information of the leakage signal is extracted. And the original information is reconstructed by using Support Vector Machine (SVM). The results show that the chip-level electromagnetic emission leakage is closely related to its working state, and the side channel is used to detect and analyze the leakage signal, which can reconstruct the original information and effectively know its internal working state.**

***Index Terms*—Side Channel leakage; information safety; wavelet transform; support vector machine; information reconstruction**

I. INTRODUCTION

Transient electromagnetic pulse emanation surveillance technology (TEMPEST) was one of the important research in the field of information security. The information leak caused by electromagnetic launch in the working electronic equipment.Modern electronic devices have integrated circuits inside, which generate a large number of leak signals when they are in working condition. These signals can be radiated to the surrounding space by conduction or radiation through power supplies, port lines, PCB traces, and connected external cables. In particular, the speed of microprocessor was increasing, and high-speed digital signals form an electromagnetic emission excitation source during operation. It can be generated electromagnetic emissions through the equivalent antenna of the device, component and device, and radiate electromagnetic energy to the space, thereby conductively coupling the leakage electromagnetic signal through the cable. Signal detection techniques can be used to acquire and sense leakage electromagnetic signals. Using the TEMPEST technique to analyze and decrypt leaky signals, the important information implicit in it can be obtained.

The mechanism of physical information leakage of integrated circuit chips was carried out, and an information leakage bypass analysis model based on this was established in[1]. Different measurement methods for electromagnetic leakage signals in the IC 150Hz to 1GHz range were provided in [2]. The electromagnetic leakage and information interception of keyboard input was carried out, and the mechanism of keyboard input information leakage and methods of interception and reduction and defense measures was explored [3]. The display power line signal leakage to restore the image was used in [4]. The physical model of the leakage of electromagnetic information transmitted by the power supply and the leakage of the electromagnetic information on the basis of the feasibility verification of the leakage of electromagnetic information transmitted by the power supply was estimated in[5]. Based on electromagnetic interference (EMI) theory, a new analysis of electromagnetic information leakage of cryptographic equipment was described in [6]. The literature [7] described the ability of noise on digital video signals to suppress electromagnetic leakage and restore information. The side channel attack of complex embedded systems was described. However, there were only a handful of studies on the reconstruction of raw data using chip-level electromagnetic leakage signals [8]. A neural network breath sound recognition algorithm based on SVM was proposed in [9].

This paper analyzed the conduction leakage problem of chip-level single-chip processors. The leakage coupling signal is detected by the side channel, and then the feature extraction and original information reconstruction of the conduction leakage signal are realized by the wavelet analysis and reconstruction and SVM recognition analysis method.

II. ELECTROMAGNETIC LEAKAGE MECHANISM OF MICRO-CONTROLLER

A. Typical STM32 Micro-controller Electromagnetic Function

As a typical 32-bit STM32 microprocessor, the STM32F103ZET6 incorporates the high-performance ARM Cortex-M3 32-bit RISC core operating at a 72 MHz frequency, high-speed embedded memories, and an extensive range of enhanced I/Os and peripherals connected to two APB buses. The STM32F103ZET6 has several General Purpose IO (GPIO) groups. Each GPIO group has 16 IO ports. The registers of each GPIO group are similar. The I/O port is mainly used for connection between the single chip microcontroller and an external circuit for drive control and logical digital signal transmission.

978-1-7281-4262-3/19/$31.00 ©2019 IEEE

Authorized licensed use limited to: University of Florida. Downloaded on February 10,2025 at 13:47:08 UTC from IEEE Xplore. Restrictions apply.

B. Conduction Leakage Mechanism of I/O Port

When the MCU chip is working, its pin could output a logical digital signal of 0 or 1. However, these signals were high or low switching signals. When a pin outputs a signal, nearby adjacent pins were electromagnetically coupled to it. The status information of the pins will appear on the adjacent pins in a certain form. In this way, the signal generated on adjacent pins was referred to as a conduction leakage signal. Reconstructing the working information of the original pin through the conduction leakage signal on the adjacent pin was the focus of this paper. The conduction coupling equivalent

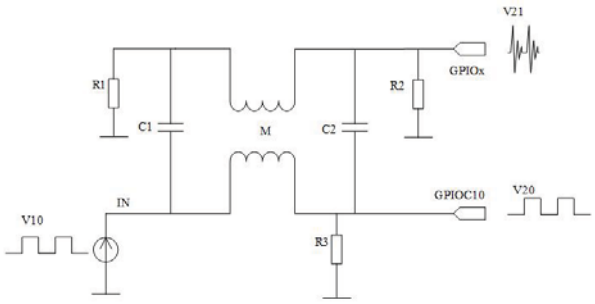


Fig. 1. Conductive coupling equivalent model between pins

model of the adjacent pins of the micro-controller chip is shown in Fig.1. When the distance between the two pins was relatively close, the induced capacitances C1, C2 and the induced inductance M were equivalent between the pins. R1 is the internal equivalent resistance of GPIOx, R2 is the load resistance of GPIOx, R3 is the load resistance of GPIOx. When a high-speed change occurs in GPIOC10, its signal was capacitance and inductance coupled into GPIOx. There is a differential relationship between the conduction leakage signal on GPIOCx and the original signal on GPIOC10,

$$V_{21} = K\frac{dV_{20}}{dt}, \tag{1}$$

where K is a constant, and its value is related to factors such as the distance between C1, C2, and M, and the length of the coupling. V20 was the signal on the target, GPIOC10, and V21 was the conduction leakage signal on the target of GPIOx.

C. Conduction Leak Test of I/O Port

In this paper, the pulse information in the conduction leakage signal on the adjacent pin was used to obtain the change of the target signal and completed the reconstruction of the original signal. This article used a high sampling rate, high depth RS ScopeRider handheld oscilloscope (bandwidth from 60MHz to 500MHz, sampling rate up to 5Gsample/s, 10-bit ADC resolution, maximum 500ksample,50Msample segmented storage) as a collection of conductive leakage signal modules. The experimental system also included a target single chip system and a data processing computer, as shown in Fig2.

When only GPIOC10 outputs pulse signals,observed by the oscilloscope, there was a distinct pulse signal in the conduction leakage signal of GPIOC11, and the moment of

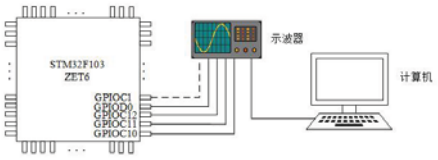


Fig. 2. Experimental system

the pulse signal appeared exactly corresponding to the edge change moment of the original signal on GPIOC10, the upper pulse corresponded to the upper edge and the lower pulse corresponded to the lower edge. When the GPIOC10 port alternately output 0 and 1 square wave level signals, a pulse-type conduction leakage signal appeared on the GPIOC11 port.

III. RESULTS ANALYSIS AND DATA RECONSTRUCTION

A. Signal Feature Extraction

Wavelet transform was suitable for in-depth analysis of complex signals. The analysis window of the wavelet transform was variable, and it was an adaptive time-frequency analysis method. When a wavelet function was selected, its window size had been fixed, but the size of the time window and the size of the frequency window can be changed. The complex signal was divided into different frequency components and analyzed by different size scales.

For high-frequency analysis of signals, it was necessary to use a small scale factor to amplify the portion of the signal with high-frequency wavelets. For low-frequency analysis of signals, a large scale factor was required, and low-frequency wavelets provided better resolution of the signal profile.

B. Automatic Recognition Classification

Support Vector Machine (SVM) was mainly used to solve data classification problems in the field of pattern recognition. It was a kind of supervised learning algorithm. The basic idea of classification learning was based on the training set in the feature space. In the training set, the researcher hopes to find an optimal division hyperplane to separate the positive and negative samples, and the SVM algorithm can be solved the problem of finding the optimal hyperplane. For SVM, in order to better distinguish data samples, finding the optimal segmentation plane was the key. The optimal hyperplane referred to the hyperplane that was the farthest from the two types of data.

C. Results Analysis and Signal Reconstruction

When there were 4 working pins, there will be 16 working states. It was difficult to distinguish the working state of the target pin directly from the difference in the amplitude of the leakage signal pulse. Therefore, machine learning algorithms were needed to automatically identify the classification.

Setting the MCU GPIOC10 GPIOC11 GPIOC12 GPIOD0 pin to work synchronously in different working states, there will be 16 working states. Figure 6 shows the output signal

Authorized licensed use limited to: University of Florida. Downloaded on February 10,2025 at 13:47:08 UTC from IEEE Xplore. Restrictions apply.

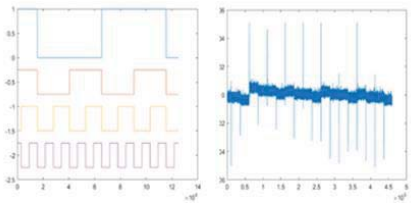


Fig. 3. Experimental system

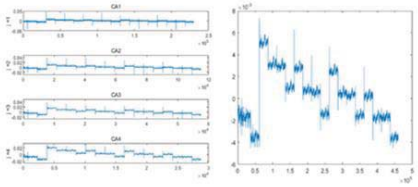


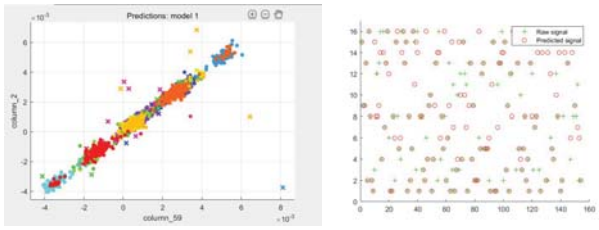
Fig. 4. Experimental system

state on the four working pins and the corresponding conduction leakage signal on the adjacent GPIOC1. As can be seen from Fig. 3, the conduction leakage signal on the GPIOC1 contains a large amount of noise signals, and most of the pulse signals containing the target pin state information in the leakage signal were flooded by noise. On the one hand, in order to suppress noise, on the other hand, in order to extract the pulse signal, the original conduction leakage signal was processed by wavelet decomposition and reconstruction. The high-frequency layer 8 wavelet decomposition coefficient is obtained for signal reconstruction, and finally a pulse signal is obtained, as shown in Fig.4. The state information is diverse, and a variety of pulse signals appear, which is difficult to distinguish and identify directly. Therefore, the SVM algorithm is selected for automatic classification and recognition.

More signals were acquired, wavelet decomposition was performed and the high frequency layer 8 wavelet coefficients were also used for reconstruction to extract useful pulse signals. The reconstructed signal was segmented and 6000 points containing the pulse signal was sliced. Each segment was numbered from 1 to 16, and the different numbers represent the different conditions of the current 4 target pin output signals. The processed segmentation signal was input into the SVM classifier for training, and the training was performed using different SVM kernel functions, and finally the training accuracy was calculated, and the result shown in Fig.5 was obtained. The training set can finally obtain an accuracy of about 89.6%, and the test data can be automatically identified by using the highest accuracy sample after training, which can achieve a correct rate of 64.29%, which proves the feasibility of the method.

IV. CONCLUSION

In this thesis, the electromagnetic conduction leakage information of the single-chip processor is studied and analyzed,



(a) Prediction model in training (b) Reconstructed results from leak signal

Fig. 5. Results of different SVM training

and then the coupling model of the side channel leakage information is established. Finally, this paper uses the pulse characteristic information in the conduction leakage signal on the adjacent pin, combined with wavelet decomposition and reconstruction and the machine learning algorithm SVM, to reconstruct the state signal of the target pin in the multi-pin working state. The results show that the electromagnetic conduction leakage signal can leak to the operational information inside the single-chip processor. Moreover, the experimental data proves that the wavelet decomposition and reconstruction combined with the machine learning algorithm SVM can effectively reconstruct the original information, which is of great significance for further research on information leakage.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under project 61271104 and 61871405.

REFERENCES

[1] Cheng Kaiyan,Zhao Qiang,Zhang Peng,Information LeakageModel for chip[J], Microcomputer Information, 2006, 22(16):74-75.
[2] Deutschmann B , Winkler G , Jungreithmair R . Measuring the electromagnetic emissions of integrated circuits with IEC 61967-4 (the measuring method and its weaknesses)[C],IEEE International Symposium on Electromagnetic Compatibility. IEEE, 2002.
[3] Zhou Yifan.Compromising electromagnetic emanations of keyboard input and information interception[D]. Beijing University of Posts and Telecommunications,2014.
[4] Zhou Changlin,Qian Zhisheng,Wang Qinmin,Yu Daojie,Cheng Junping.Recognition and reconstruction of conduction leakage signal via power line based on PSO-SVM method[J].Journal of Electronic and Information Science,2018,40(9):2206-2211.
[5] Cheng Lei,Luo Rujun,Kou Yunfeng,Liao Xiangyu,Deng Zhao,Deng Xi . Verfication of Conductive Electromagnetic Information Leakage Model Based on Power Line[J]. Communcations Technology 2018, 51(4): 941-946.
[6] Y. Hayashi et al. Analysis of Electromagnetic Information Leakage From Cryptographic Devices With Different Physical Structures[J]. IEEE Transactions on Electromagnetic Compatibility, 2013, 55(3):571-580.
[7] Song T L , Jeong Y R , Yook J G . Modeling of Leaked Digital Video Signal and Information Recovery Rate as a Function of SNR[J].IEEE Transactions on Electromagnetic Compatibility, 2015, 57(2):164-172.
[8] Dongxin Guo,Kaiyan Chen,Xiaoyang Hu,Yanhai Wei,Jianlong Li. A Survey of Prototype Side-channel Attacks Based on Machine Learning Algorithms for Cryptographic Chips[J]. Journal of Physics: Conference Series,2019,1176(3).
[9] Liu Guodong, Xu Jing. Neural network recognition algorithm of breath sounds based on SVM[J]. Journal of Communications, 2014, 35(10).

Authorized licensed use limited to: University of Florida. Downloaded on February 10,2025 at 13:47:08 UTC from IEEE Xplore. Restrictions apply.