UDK 004.35

P.S. EVTUKH[1], B.L. BOROWIK[2], L.M. KORKISHKO[3], V.N. KARPINSKYI[1]

[1]*Ternopil State Technical University, Ukraine*
[2]*University of Bielsko-Biala and State Higher Vocational School in Nowy Sacz, Poland*
[3]*Ternopil National Economic University, Ukraine*

THE SYSTEM MODELING OF INFORMATION LEAKAGE FROM DIGITAL DEVICES

The paper describes the creation of the system modeling of information leakage from digital devices. For this purpose side-channel analysis (SCA) attacks, which are based on gained information from the side channels (SCI) are being analyzed. Models for cryptographic attcks are based on information leakage from the side channels. Principles and methods for prevention the SCA attacks are described. The structure of system modelling of information leakage from digital devices is provided, the choice of its basic elements is made, and the main characteristics of microprocessors components are developed and created.

Key words: *side-channel analysis, attacks, digital device, microprocessor, information leakage.*

Introduction

The system modelling of information leakage from electronic digital tools that takes into account the attacks of information leakage from the side channels of SCA (Side-Channel Attacks or Side-Channel Cryptanalysis) is presented. Cryptographic applications should rely on proper implementation of cryptographic modules for their safety with respect to SCA attacks. For that we develop a method for research on different information protection algorithms for implementation in digital devices. This method allows improved design of computer components by taking into account information from information leakage modelling.

1. Structure and functioning principles of system modeling of information leakage from digital devices

Described below structure of system allows one to analyze information taken from user power consumption of digital device. The generator of clock impulses is mounted on printed circuit board. Frequency of generator of clock impulses is one of the basic parameters that determine performance of the system since every operation in the digital device is performed using a certain number of clocks.

The generator of upcast signal is presented. Special impulses of upcast produced by MCU zeroize the meter in the moment the indication time is completed. The TX\RX signals of MCU (microcomputer unit) are connected to the digital device through the transformer of levels TTL to/from RS232. The MCU has general purpose input – output ports. Port P0 is used as start signal for oscilloscope. Port P1 is used as stop signal of oscilloscope. For next analysis of saved signal the oscilloscope is connected to personal computer (PC) via Ethernet cable.

Digital device can generate the sequences of logical states, called samples on high frequency. As a result, we have to use microcontroller with high frequency of clock signal with shortest possible cycle for a command execution.

After analysis of possible choices of microprocessor, we conclude that most appropriate one should be built on RISC (Reduced Instruction Set Computer) architecture. This architecture allows microprocessor to execute almost every instruction during single clock signal.

2. Design principles and choice of components

Design principles for our system are as follows:

– Possibility to generate the logical states with the smallest possible delay.

– User-friendly displaying of the digital device states using liquid-crystal display (LCD).

– Using an enhanced microcontroller especially with Parallel Master Port module allowing to interface to LCD display, touch panel and also parallel transmission.

– Communication with the user through an intuitional interface with the touch panel.

– Opportunity of simple and fast reprogramming of device that will make it to perform other function in accordance with requirements.

– The system should communicate with a personal computer through port of RS232 or USB.

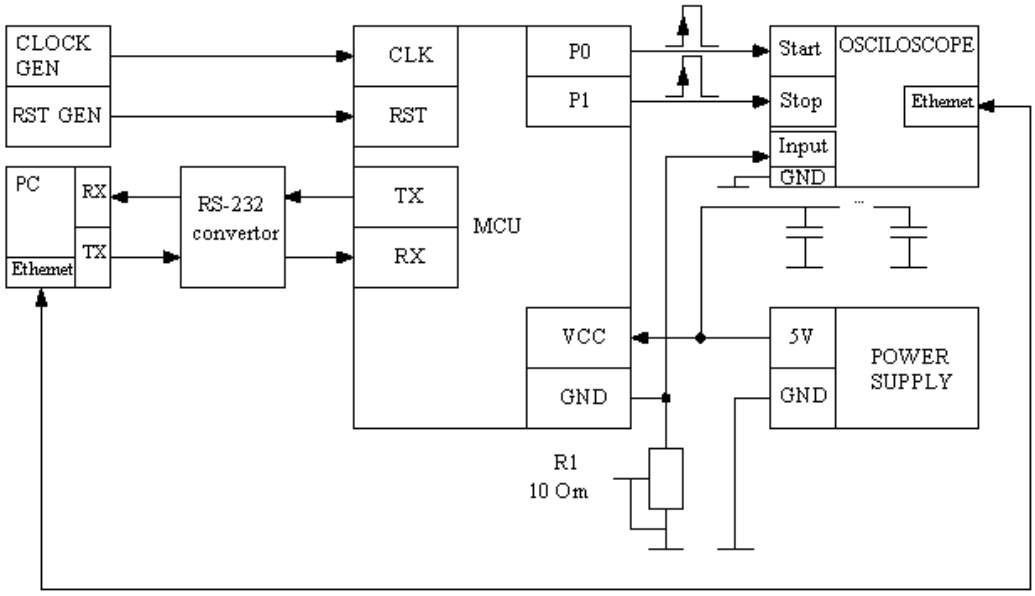

Fig. 1. A functional diagram of the source system modeling of information from microprocessor from digital device

– There should be possibility of communication with other microsystems by such highways as I²C- TWI, CAN or SPI

– LCD needs to be programmed for scrolling in order to show all necessary transmitted information.

3. Information leakage models

3.1. The model based on Hamming distance

The model based on Hamming distance relies on dependence between used power and amount of switching in combinational scheme. Therefore amount of switchings at certain time interval is utilized for the estimation of used power during it. By dividing of all burn-time of device by small intervals it is possible to evaluate the change of used power by time. To be stricter, such estimation displays change of switchings amount by time.

It's assumed that: a) a logical element consumes identical power at class transitions of $0 \to 1$ and $1 \to 0$; b) the model does not take into account parasite capacities between conductors and logical elements; c) all the logical elements bring identical contribution to the used power; d) the constituent of used power is ignored in the static mode. Hamming distance between two data v_0 and v_1 taken to the calculation of Hamming weight their sum after module of two: $HD(v_0, v_1) = HW(v_o \oplus v_1)$.

It is shown in process [1] that the model based on Hamming distance adequately describes the change of used power of internal buses and registers of cryptographic device. Necessary condition is a possession by attacker of information, which were consistently written down in a register, or passed by the buses of exchange.

3.2. The model based on Hamming weight

Quite different act is set, when an attacker possesses information only about single data, which are passed by bus, or written down in registers and attacker does not possess information about previous or next data. In that case the model based on Hamming distance is not used, as its results of modeling inadequately display the used power of device in the set time intervals. After that the model based on Hamming weight is utilized to estimate the used power.

In obedience to this model an attacker assumes that the used power of device is proportional to the amount of single bits, which are contained in processed data. From the other point of view such model approximately describes the used power of CMOS devices. In practice Hamming weight of data is not fully independent from the used power of device in processing of these data. Let's consider three main cases for the estimation of used power of device, which consistently operates the data v_0, v_1 and v_2. The aim is to get the estimations of used power using operation of v_1 without information about v_0 or v_2. v_1 is used in two class transitions, that's why $v_0 \to v_1$ and $v_1 \to v_2$. Let's consider these cases only for a transition $v_0 \to v_1$. For a transition $v_1 \to v_2$ reasoning's will be similar.

Case 1. Bits v_0 are identical and unchangeable at moments of appearance of transition $v_0 \to v_1$. Such example is the bus of data that passes always-identical

number $v_0 = 0$ before the transmission of number v_1. The Hamming weight model is then equivalent to the Hamming distance model, that is $HD(v_0, v_1) = HW(v_0 \oplus v_1) = HW(v_1)$. If all bits v_0 equals to one, than $HD(v_0, v_1) = HW(v_0 \oplus v_1) = n - HW(v_1)$. Thus, in these cases modeling results are proportional to the used power. Therefore the considered models are equivalent in relation to the conducting of attacks at identical bits v_0 before the appearance of transition $v_0 \to v_1$.

Case 2. Bits v_0 are unchangeable, however different and unknown for the attacker. Unlike the first case, here it can be possible to examine only one bit of transition $v_0 \to v_1$. Then two models of used power are considered to be equivalent, using the analogical reasonings to the first case.

However it can be possible only for one bit. Used power, caused by the change of some bit v_1, directly or not-directly proportionally depends on the value of that bit with one condition that this bit in v_0 is always set in identical value before the appearance of transition $v_0 \to v_1$. With the growth of bits amount in v_0, which remain unchangeable, dependence of Hamming weight v_1 from the amount of bit transitions grows. That's why attacker gets more completed information.

Case 3. Bits v_0 are evenly up-diffused and independent from v_1. Also bits v_0 are not permanent, but casual for every start working of cryptographic device with the purpose of algorithm of cryptographic transformation. Therefore $HW(v_1)$ is independent from $HW(v_0 \oplus v_1)$, if v_0 is independent from v_1 and possesses equable distributing of probabilities. Accordingly, results of simulation, based on these two models, are impossible to be used by the attacker.

The considered cases do not include complete list of variants of relations between bits v_0 and v_1. At the same time, unlike the theoretical model, it is known that in transitions $0 \to 1$ and $1 \to 0$ in devices the used power is different. Therefore used power in operating of data with greater Hamming weight is higher, than in operating of data with less Hamming weight - that predetermines successful application of two models mentioned in practice.

Model based on Hamming distance, unlike the model based on Hamming weight, needs information about the elements of structure of cryptographic device. That's why model based on Hamming weight is more acceptable for the attacker.

Let's consider the example of attack of N-digit operation of adding using the module of two [2]. Let the usage of power in the moment of time *j* is presented as *P[j]*. For the modeling of channel of information leakage in the signal *P[j]* we will use the following linear dependence:

$$P[j] = \varepsilon \cdot d[j] + L + n, \qquad (1)$$

where $d[j]$ – presents Hamming weight of result which achieved in the moment of time *j*;

ε – contribution to the used power of every digit of Hamming weight data;

L – permanent general used power;

N – noise with a zero average value.

Let *j* means the moment of time, when the adding operation is executed according to the module 2. Then sum S = K ⊕ P, and K – N-bit is unknown item, P is a *N*-bit plain text. Let's consider attack, offered in [2], on *N*-bit summator according to the module 2, the purpose of this attack is to determine bits *K* without information about the value of bits *S*.

Let's assume, that dependence between used power in the moment of time *j* and Hamming weight of result obtained and described in expression (1). Then the generalized algorithm of attack on realization of adding operation according to the module 2 looks as following:

For *i* and from *0* to *N-1*
{
For *b=0* to *1*
{
To calculate the average signal value of used power
Ab[j]
{
To set the *i* bit of *P* equal *b*;
To set other bits of *P* in casual values;
To collect information about the used power of device;
}
}
To calculate the differential signal of *T[j]= A0[j] – A1[j]*;
If *T[j]> 0*, *i* bit *K* is *"1"*, if *T[j]< 0* than *i* bit *K* is *"0"*;
}

Effectiveness of this attack is based on the independence of Hamming weight expected value of result of adding according to the module 2 from bit position. Differential signal will obtain positive peak for terms $k_i = 1$ and negative peak for terms $k_i = 0$.

Similar attacks are built based on statistical models of the attacked operations, which are then used for further attacks on cryptographic devices.

Attacks which are based on the information leakage from one intermediate result belong to the attacks based on analysis of used power of first-order. If at-

tacker has possibility to choose and follow up the appearance of information leakage from a few intermediate results, attacker can improve the attack results by an analysis of several intermediate results at once. If attacker simultaneously analyzes *n* intermediate results, such attack is called attack that is based on analysis of used power of *n* order.

4. Generator of logical states

Generator of the logical states is placed on one-sided printed circuit board (fig. 2).

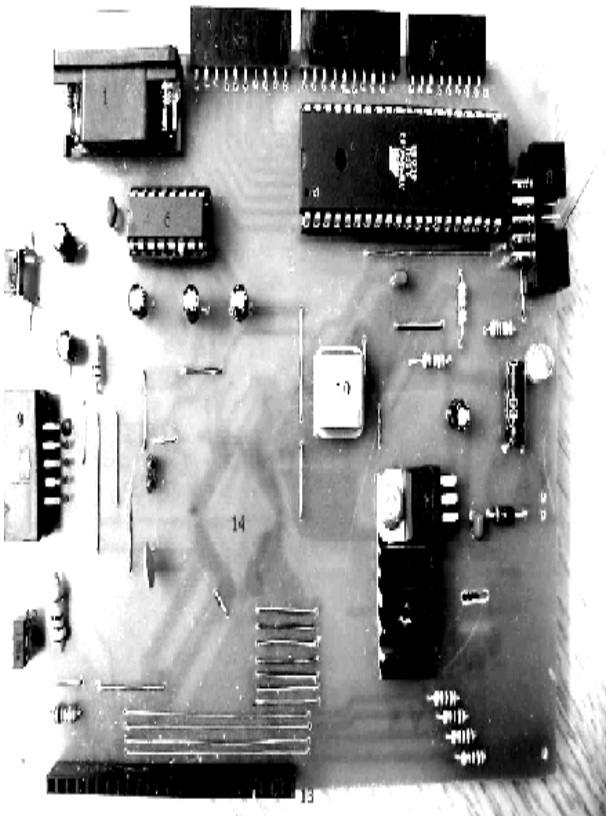

Fig. 2. Placing of elements on the generator of the logical states:
1 – connection of RS232, 2-3-4 – out-ports of microcontroller ATmega32, 5 – button RESET, 6 – converter of TTL-RS232 levels, 7 – microcontroller ATmega32, 8 – ISP port of microcontroller ATmega32, 9 – ISP port of microcontroller ATmega128, 10 – generator of time signal 16 MHz, 11 – power regulator, 12 – regulator of contrast, 13 – is connection liquid-crystal display LCD, 14 – microcontroller ATmega128 (visible from below)

Generator of the logical states was developed first in order to enable practical realization of the system. Device architecture is developed by EDA Protel software 99 SE (from Altium company). We have used following components:

– microcontroller as Atmega 128;
– microcontroller as Atmega32;
– generator of clock signal - 16 MHz;
– stabilizator of power supply together with blocking condensers;
– connection with output ports of microcontroller as Atmega32;
– converter of TTL-RS232;
– connection IDC10, which serves for flash-memory programming of microcontrollers.

Generator of the logical states includesthe liquid-crystal display LCD and touch panel. Both modules are united together via ribbon wire and modular connectors.

A Logical States Generator allows a one-byte sequence in to internal flash memory of the size 128 kB.

Further entire sequence can be sent via RS232 protocol to the encrypting circuitry. Subsequently also the not encrypted stream of data is acquired for the purpose of comparison.

5. User communication interface

An aspect which is not ignored in this paper and it has been used quite a big effort of its considering – is possibility of interaction with the user by intuitive method. A standard keyboard does not offer such intuition. It can be done by monochromatic liquid-crystal displays with a resolution of 240x128 pixels, which are based on the Toshiba controller T6963C, and also possess the integrated touch panel.

Chosen a liquid-crystal display possesses two substantial advantages. At first, its inherent component is bright illuminating and high contrast. Also it contains built-in controller and generator of signs on the Toshiba controller T6963C It predetermines substantial simplifications and facilitation for user of the system, because a liquid-crystal display with such controller does not cause the large loading of the system by generating procedures of signs or illumination of graphic. Even more, there are libraries for its operation available in almost every programming language for microcontrollers. That causes time economy for creation of controlling software. Also it is important that libraries are free of charge.

Graphic liquid-crystal display of that type gives wide possibilities to visualization, in spite of the fact that it does not possess too many colors, and possibility of giving scale of grayness, as it takes a place in monochromatic monitors. On a liquid-crystal display will appear except text, images (if to use terminology of Windows, will talk about icons). Images are compressed to the small measure of bitmap or pixmap; occupy vast enough memory of microcontroller. Therefore, it was decided to be not limited for the choice of microcontroller. Having regard, that a microcontroller as

ATmega128 possesses the volume of 128 Kbit of flash memory, it is enough for considerable amount of icons and program code.

Conclusion

Based on the models of SCA crypto attacks – models based on Hamming distance and models based on Hamming weight, – it was estimated adequacy description of used powers change of internal components of electronic digital devices. Due to that the typical correlation between bits of data and necessary conditions concerning possession of information for the conducting of crypto analysis were obtained. On a basis of the electronic digital devices operation performance peculiarities a common approaches against the attacks of SCA were generalized. Selected prevention methods against the attacks of power analysis, timing attacks and mistake attacks were appraised. The warnings which guarantee ability to resist against attacks of information leakage from the side channels to the cryptographic modules of microprocessor, and also to computer components were formulated.

Based on the offered functional scheme of the system modeling of information leakage from the digital devices, basic components for its realization were selected. In particular the microprocessor generator of the logical states with LCD and touch panel interface was designed and created. It allows also to modulate information leakage from digital devices, and to improve the protection of computer from the attacks of SCA.

References

1. Mangard S. Power Analysis Attacks: Revealing the Secrents of Smart Cards / S. Mangard, E. Oswald, T. Popp. – Berlin: Springer, 2007. – 337 p.

2. Messerges T. Using second-order power analysis to attack DPA resistant software / T. Messerges // Lecture Notes in Computer Science: Proc. of Cryptographic Hardware and Embedded Systems Workshop. CHESS-2000. – Berlin: Springer, 2000. – Vol. 1956. – P. 238-251.

Поступила в редакцию 15.01.2009

Рецензент: д-р техн. наук, проф. В.А. Заславский, Киевский национальный университет им. Т.Г. Шевченко, Киев, Украина.

СИСТЕМНЕ МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ ВИТОКІВ ІЗ ЦИФРОВИХ ПРИСТРОЇВ

П.С. Євтух, Б.Л. Боровик, Л.М. Коркішко, В.М. Карпінський

В статті описується створення системи моделювання витоку інформації з цифрових пристроїв. Для цього використовується аналіз атак з побічних каналів (side-channel analysis (SCA) attacks), котрий базується на зібраній інформації з проаналізованих побічних каналів (SCI). Представлені моделі для криптографічних атак, котрі базуються на витоку інформації з побічних каналів. Описані принципи та методи запобігання атакам SCA. Впроваджена структура системи моделювання витоку інформації з цифрових пристроїв, зроблений вибір її основних елементів, розроблені та впровадженні головні характеристики мікропроцесорних компонентів.

Ключові слова: аналіз побічних каналів, атаки, цифровий пристрій, мікропроцесор, інформаційний витік.

СИСТЕМНОЕ МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ УТЕЧЕК ИЗ ЦИФРОВЫХ УСТРОЙСТВ

П.С. Евтух, Б.Л. Боровик, Л.М. Коркишко, В.Н. Карпинский

В статье описывается создание системы моделирования истока информации с цифровых устройств. Для этого используется анализ атак с побочных каналов (side-channel analysis (SCA) attacks), который основан на собранной информации с побочных проанализированных каналов (SCI). Представлены модели для криптографических атак, которые основаны на истоке информации с побочных каналов. Описаны принципы и методы предотвращения атакам SCA. Внедрена структура системы моделирования истока информации с цифровых устройств, сделан выбор ее основных элементов, разработаны и внедрены главные характеристики микропроцессорных компонентов.

Ключевые слова: анализ побочных каналов, атаки, цифровое устройство, микропроцессор, исток информации.

Евтух Петр Сильвестрович – д-р техн. наук, проф., зав. кафедрой систем энергоснабжения и компьютерных технологий в электроэнергетике, ТГТУ им. Ивана Пулюя, Тернополь, Украина, e-mail: kaf_ee@te.edu.te.ua.

Боровик Богдан Леонович – канд. техн. наук, адъюнкт кафедры электротехники и автоматики, Университет в Бельску-Бялэй, Бельско-Бяла, Польша, e-mail: bo@borowik.info.

Коркишко Леся Мирославовна – аспирант кафедры компьютерной инженерии, ТНЭУ, Тернополь, Украина, e-mail: lesykkor@yahoo.com.

Карпинский Владимир Николаевич – аспирант кафедры систем энергоснабжения и компьютерных технологий в электроэнергетике, ТГТУ им. Ивана Пулюя, Тернополь, Украина, e-mail: vkarpinskyi@gmail.com.