Novel Approach for Power Analysis in Microcontrollers

P. Muthu Subramanian and A. Rajeswari

Abstract Security showcases a major breakthrough in the history of the embedded systems, as the connections move beyond computing devices, from intelligent traffic management systems to missile control system. The drift of Internet protocol from version 4 to version 6 has greatly expanded the number of devices that could be connected over the Internet and it is estimated that it could accommodate three times the number of devices currently existing in the world. With this growing pace in embedded systems, security issues are an area of great concern. Objective of this approach examines the vulnerability of the commonly used ARM processor to a simple distributive embedded security—power analysis attack for difference and also making the role of service provider active by modifying the conventional security model.

Keywords Microcontrollers · Security · Embedded systems · Power analysis · Cryptography

1 Introduction

Nowadays security plays a major roll in embedded systems. This security system is expected to continue for decades. The security range required for embedded systems is from smallest RFID to satellites which are orbiting the earth. The below chapter will explain few types of security requirements and their attacks on embedded systems. In embedded systems, embedding security into devices is not a direct process. Requirement of security functionality must be determined before embedding into a device. Security requirements mainly depend upon threat models or attacks which may be fully known at that time. It has been already said that prevention is the most viable course of action when it comes to fraud. Security is an important layer to avoid fraudulent. In the embedded world, detection is an equally important layer to mitigating stolen codes. Consideration is shown on the various attacks developed

P. Muthu Subramanian · A. Rajeswari (✉)
Department of Electronics and Communication Engineering, Coimbatore Institute of Technology, Coimbatore, India

V. Bindhu et al. (eds.), *International Conference on Communication, Computing and Electronics Systems*, Lecture Notes in Electrical Engineering 637,
https://doi.org/10.1007/978-981-15-2612-1_50

to take out the secret information of the cryptographic methods (cores) by analyzing the leaked information of the hardware. In the proposed technique, analysis of the attacks by means of power is said to be one of the efficient and most powerful methods for pilfering the data from the ARM processor and it is said to be a most important threat to the processor security. A simple analysis is made to compare the leaked information with the actual data to prove the ownership. Also in this proposed system, we investigate the PAA on ARM processor by means of processed data and to analyze the graphical trace for very few instructions.

2 Related Work

In the case of erroneous (faulty) attacks, the attacker attempts to takeout the secret information by applying some erroneous running in the device. Ecological parameters are influenced to generate the erroneous behavior. Non-invasive fault attacks will be based on the various parameters which influence the temperature, the voltage source, generation of clock signals and by injecting electromagnetic pulses [1–3]. Programming modifications are not required for these attacks since all these attacks are induced by means of various hardware signals. Semi-invasive fault attacks will be based on inducing faults by means of laser light. Here in this technique IC packaging to be altered for implementing the attacks. During the past years, cryptographic primitives have been reported for a large number of invasive fault attacks. Normally, attacks are common to both software (RSA and block cipher algorithms) and hardware. Fault can be identified based on either the control logic or the data path of the controller by making changes in the algorithm.

3 Methods of Fault Attacks

Following section is regarding the mechanisms of the fault injection and the types of attacks.

3.1 Fault Attack—Non-invasive

To induce the fault, modification is not required in the equipment or in the attacked device. Victim cannot recognize the chance of identifying the attack. Applying methods like sending spikes, EM and clock pulses are the distinctive methods [1]. Here, the attacked device is influenced by making some changes in the timing. Temperature and the pulses which are working externally may direct to the faults in the memory section.

3.2 Fault Attack—Semi-invasive

To induce the fault, modification is required in the chip. Here, IC is de-packaged to modify the changes in the passive layer which cannot be damaged. Laser and flashlight will be the source for inducing the attacks. Memory bits and the registers will be targeted by laser light where the flashlight covers the overall structure of the chip.

3.3 Invasive Fault Attacks

To induce the fault, bus line of the IC is modified by getting the access to the metal layer; here, the access to the metal layer is achieved by removing the passive coating of the de-packaged IC and metal layer is observed using miniprobes [4]. Quite a few analyses have been undergone earlier to identify the incorrect outputs produced in the cryptographic operations.

4 Power Analysis

Analysis on differential and correlation power is considered to be the major concern and threat to the devices operating under cryptographic conditions. Generally, devices will seep out its information on the processed records by means of power dissipated through the ground or supply channel. Gate circuit will absorb the current when there is a change in the state of the logical conditions. When the logic is 0 now the state is defined as 0 V and when the logic is 1 it will be the maximum voltage point and normally current dissipation will happen when there is a transition from maximum to minimum and this will help in recording the analysis of the power with more accuracy. [5] Thus, differential method is one of the advanced techniques compared to correlation analysis.

4.1 Fault Injection Attack

Procedure to induce an error maliciously in a computing device in order to alter the software execution behavior is defined as the fault injection attack. After fault injection, two effects are possible, i.e., execution of an instruction can be avoided and the second, corrupt the data at which the processor is working with. These effects are used to compromise the embedded device security by bypassing the security checks or leaking the private keys.

Among the several types of glitching such as optical, heat or radiation glitching, the most common glitching is the clock and voltage glitching.

4.2 Clock Glitchıng Attack

For a very short moment, a sudden increase of the system clock frequency is referred as the clock glitch. Due to the difference in the distribution paths like length, capacitance in traces and transistor gates, etc., the clock signal is not evenly distributed and does not reach every point at same time in a digital integrated circuit such as microcontroller or processor, FPGA. Based on the clock frequency specified by the manufacturer, the clock signal will be able to reach every register in average processing time. If it is beyond the specified limit, it would make the IC not to operate effectively. Therefore, if we force the IC to work beyond the set limit for a particular time period then the instruction will not be processed efficiently and it will retain back to the normal frequency. While clock glitching the entire instruction execution is avoided in the processor.

5 Proposed System

Supply voltage is connected with a resistor in the ARM processor and it is used for observing the power variation (current) of the circuit. Supply voltage should be greater than the normal voltage supplied to the ARM processor since resistance is connected across the VDD of the processor. Thus, the supply voltage should be greater than 3.3 V. Frequency with higher clock rate will have some changes in the analysis of current, and electrical signals are measured in terms of microvolt using digital oscilloscope. Bits of the controllers are varied with different logics (i.e., 0 and 1) in the ARM processor. Changes will make variations in the power pattern. Spartan 3 is enough to attack most of the microcontroller, as the Spartan 3 would produce the clock frequency of 150 MHz by modifying the signal path and it is possible to add some delay to alter the clock phase as needed. In Spartan 3, digital clock manager allows to produce different clock frequencies. To generate the clock cycle by the host microcontroller, it needs two instructions: One is to set 1, and the other is to set 0. Host microcontroller operating frequency/2 is applied to the target system to get the maximum clock frequency. To inject a clock fault, we need to generate the clock frequency much faster than the maximum operating frequency of the target system. Sometimes it is required that there is a need to generate at least 40 MHz clock signal, and for that high-speed processors like ARM series are used to achieve the required traces (Fig. 1).

When an external clock is applied to the processor, the clock rate frequency (Fmax) is defined.

No abnormal behavior can be observed if,

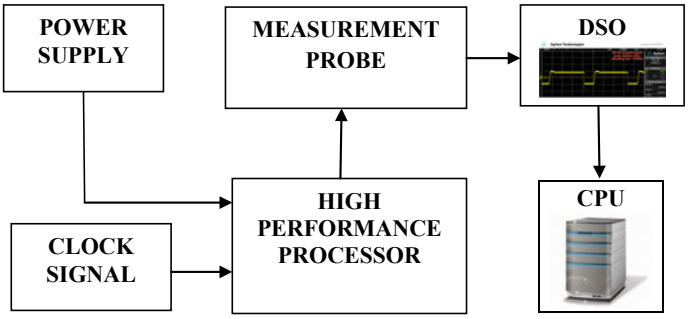

Fig. 1 Setup for power analysis

$$T\text{glitch} \geq T\text{min} \tag{1}$$

Possibility of abnormal behavior increases when,

$$T\text{glitch} < T\text{min} \tag{2}$$

While running the program, timing violation will be the major reason for the abnormal behavior.

6 Experimental Results

6.1 Power Analysis for Addition Operation

Impact of power consumption by the controller is observed from the arithmetic operation. Power variations are observed from the ARM processor while doing the arithmetic operations. One of the ports from the microcontroller is extracted with the addition output. Repeated pattern was observed from the power traces for the various instructions as shown in Figs. 2, 3 and 4.

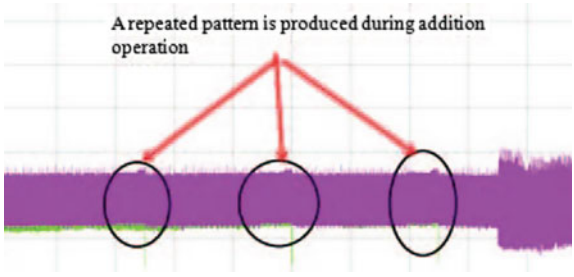

Fig. 2 Addition operation power analysis

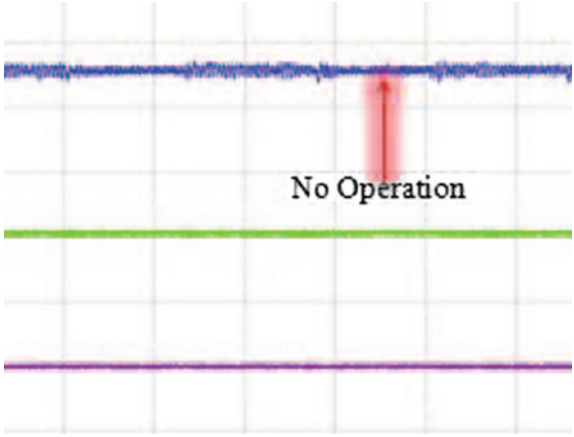

Fig. 3 NOOP power analysis

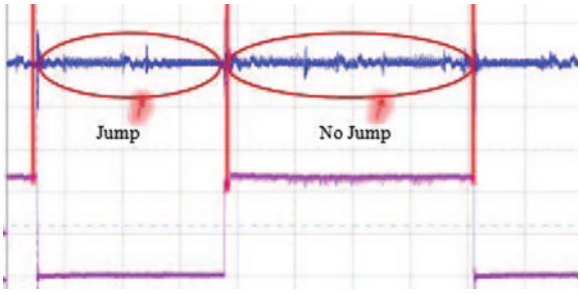

Fig. 4 JUMP and NOJUMP power analysis

It is observed from the power investigation that there is a unique correlation between the processor power utilization and the power pattern. This study is further extended into the next step as the power analysis.

7 Conclusion

Embedded security has been achieved through the power analysis. Based on the clock signal and using simple alteration to the target system by applying glitches, it is proved and tested that processors are vulnerable to power analysis attack and various instructions were tested for different data sets for the power trace correlation.

References

1. Balasch, J., Gierlichs, B., Verbauwhede, I.: An in-depth and black-box characterization of the effects of clock glitches on 8-bit MCUs. In: FDTC, 2011, pp. 105–114. IEEE (2011)
2. Hutter, M., Schmidt, J.M.: The temperature side-channel and heating fault attacks. In: CARDIS. Springer (2013)
3. Moro, N., Dehbaoui, A., Heydemann, K., Robisson, B., Encrenaz, E.: Electromagnetic fault injection: towards a fault model on a 32-bit microcontroller. In: FDTC, pp. 77–88. IEEE (2013)
4. Skorobogatov, S.P.: Semi-invasive attacks—a new approach to hardware security analysis. PhD thesis, University of Cambridge, Computer Laboratory (2005)
5. Zhai, X., Appiah, K., Ehsan, S., Howells, G., Hu, H., Gu, D., McDonald-Maier, K.D.: A method for detecting abnormal program behavior on embedded devices. IEEE Trans. Inf. Forensics Secur. **10**(8), 327–345 (2015)