ATLANTIS PRESS
Advances in Computer Science Research (ACSR), volume 76
7th International Conference on Education, Management, Information and Mechanical Engineering (EMIM 2017)

Side Channel Attacks Simulation Environment Design and Implementation for Crypto-Chip

Shigui Ma[1,a], Chaoqiong Yang[2,b], Jianbo Yao[3,c] and Zhuyu Xu[1,a]

[1]Network Technology Center, Zunyi Medical College, Zunyi Guizhou 563003, China

[2]Audit Division, Zunyi Normal College, Zunyi Guizhou 563002, China

[3]School of Electrical and Information Engineering, Guizhou Institute of Technology, Guiyang Guizhou 550003, China

[a]935620298@qq.com, [b]948893803qq.com. [c]2055164364@qq.com

Keywords: Side-channel attack; Cryptographic chips; Simulation environment; Design; Implement

Abstract. Side channel attack(SCA) is a powerful physical safety analysis method, the SCA security assessment for crypto-chip are generally in production, but with time-consuming, safety evaluation error-prone and costly wait for blemish. In order to improve the efficiency, it is necessary at design time to do SCA, but the safety evaluation needs the corresponding side channel simulation tool support. This paper presents the design scheme of SCA simulation environment. The scheme adopts the software and hardware of collaborative design thoughts, and though separating the leak simulation mechanism and safety analysis strategies, SCA simulation environment is established with component technology, can do SCA simulation analysis at design time of the crypto-chip. Compared with the existing PINPAS simulation environment, the environment has flexible and efficient characteristics.

Introduction

Side channel attack(SCA) is a safety test method can find the existing test security bugs (or cracked secret) through the leakage information of crypto-chip, but the analysis method needs corresponding side channel simulation tool support. The leakage information for side channels of the operation of crypto-chip is simulated in design time through the simulation technology.

SCA test method can be classified into two categories: one is the post-manufacture SCA analysis; the other is the design time SCA analysis.

The post-manufacture SCA analysis is relatively commonly used a method, its main characteristic is the SCA security test analysis is generally performed after chips are manufactured, the main test object is the manufactured chip. There are many practical challenges on the post-manufacture SCA analysis. One of the most important issues is the pressure of time-to-market. Another problem is a complex measurement setup and burdensome pre-process analysis on the real leakage signal [1-4].

The post-manufacture SCA analysis has become a bottleneck of R&D crypto-chip. To alleviate the contradiction, improve the efficiency, detect some security hidden danger in the early design, it is necessary the crypto-chip to do the side channel attacks the safety test analysis at design time. This paper designs and implies a side channel attacks simulation environment with soft/hardware collaborative design thinking,

This paper is organized as follows. Section 2 presents a general framework for simulation platform. Section 3 describes implements about the system configuration management module. Section 4 describes implements about leakage simulation module. Section 5 implements about strategy analysis module. Section 6 summarizes our works and gives some directions for further work.

The General Framework for Simulation Platform

SCA simulation environment can be roughly divided into three function modules from the structure: the system configuration module, simulators and analyzer.

(1) The system configuration module major unified management system parameters, safety index, the simulation data of the operation environment in simulation process.

(2) Running algorithm procedure in the virtual specific hardware platform, the simulators analyzes choose the encryption algorithm instruction from algorithms library and generates the corresponding SCA leak curve according to the established side channel information disclosure model before.

(3) analyzer is used to analysis the side channels curve, the unified format of the side channels leak data files as input, Not limit by side channel leak curve data sources; calculating the average side channel leak curve and drew the graph curve According to the chosen distinguish function diversity after pretreatment data of simulation side channel leak by Simulators produced or measured through the real physical equipment.

SCA simulation experiment environment is an important link in the whole design time of the SCA safety analysis. Considering the side channels the diversification of leakage features, through separated the leak simulation mechanism and side channel analysis strategy, can effectively do side channel information security analyses, and has strong practicability. Encapsulating different modules with the component technology, making the channel leak model with different characteristics and analysis method can flexibility to join the simulation system, and makes the module of updates, amend, and maintenance become more convenient. And compared to PINPAS power simulation analysis, has strong scalability and configurability [5-9].

Implements about the System Configuration Management Module

The system configuration management module mainly set the initial operation environment of simulator module and analyzer module according to user input parameters.

The system configuration modules respectively use two data structure to cache input configuration parameters from the user interface, and using these data to generate simulators initialization file Simulator.ini and analyzer initialization file Analyzer.ini. The key name of different simulation platform is saved different key name files. These key name documents written in advance, each key name correspond with the key value saved in the structure of SIMULATOR_PARA and ANALYZER_PARAM. System configuration module uses these data as input to generate configuration file. The advantages of this design is when to add new simulation platform or changes parameters for exist simulation platform, only modify data structure and key name file, not to modify and to recompile the code of system configuration module.

Through the user interface, can set the type for hardware platform, side channel leakage model, encryption algorithm, waiting for encryption plaintext number and Keys used by simulators simulate; can set corresponding SCA method for distinguish function using by the sub-module of selection analyzer, and can set configuration parameters about the speculation key and the judgment threshold on the difference curve peak.

Implements about Leakage Simulation Module

Power simulation module is one of the key for the design software and need to complete the following three aspects:

(1) Establish side channel leakage feature library

Side channel leakage feature library is the core of the simulation software, storage with the side channel leakage model for the instruction system of different hardware platform. There are two paths to establish side channel information leakage library: one is the use of mathematical model of the side channel leakage features, such as the execution time, power consumption, etc.; the other is by a large number of trials to test different hardware platform execution of various instruction real side channel leakage information, and form feature library though instruction corresponding with leakage characteristics. For Template Attack, mainly adopts the second kind of method to establish leakage feature library.

(2) Establish the mapping relationship of table for cryptographic algorithm instructions and leakage features

Side channel feature information leakage and machine instruction are closely related, the leakage of the information by execution different machine instructions is not the same. In addition, even the same instruction, operating different data, the leakage information is not the same. In order to establish the relation of the cryptographic algorithm and the side channels leakage, first compiled cryptographic algorithm using compile tools, generation the optimized machine instruction code; Then use the machine instructions as the index, query corresponding to the entrance of the leakage features in the feature library, as is shown in table 1: through the analysis of the machine instruction, can build the mapping relationship between instructions and the leakage.

Table 1 the mapping table between instructions and leakage feature

Chip type	Machine instruction type	Leak type	Leak feature library entrance address
AT89C51	JZ jump instructions	Power Leakage	Address 1
AT89C51	Move Transfer instructions	Electro-magnetic leak	Address 2
AT89C20	Move Transfer instructions	Execution time	Address 3

However, as the analyzed cryptographic algorithm, the instructions, which belong to need selective analysis of the operation instructions, are determined selected by side channel attacks for user. For example, Based on AT89C51 single chip, if choose data DPA attack, the user major concern is to instructions related the register and the memory and will mainly choose such as move instruction, ADD instruction. For simple energy analysis SPA attack, the operation instructions are main analysis such as the condition jump statement JZ, JNZ instructions.

(3) Draw side channel leakage curve for the entire process of cryptographic algorithm operation

The generation submodule of side channel leakage curve will be responsible for (1), (2) the result of comprehensive, generating the corresponding characteristic curve.

Strategy Analysis Module Implements

Side channel attacks strategy analysis module mainly work is as follows:

(1) Choose diversity function

Encryption algorithm is different, the corresponding distinguish function is different, so use distinction function library to save different distinction function. Curve diversity submodule according to the Settings of system configuration module, Choose designated diversity function from the distinction function library and will side channel leakage curve data assigned to two set. In order to realize the analysis about the analysis strategy and simulation mechanism, the class CselFunctions denoted virtual base classes in the diversity functions (curve diversity function) classes.

For the different analysis strategies, as simple side channel analysis, difference side channel analysis, high order difference side channel analysis, template analysis, etc, use the component technology to encapsulate choice function. For example, CaesSboxSelFunctions and CAesXorSelFunctions respectively denote the distinction function classes in allusion to AES arithmetic Sbox and exclusive or operation. Through the strategy and mechanism separation, make different attack method and distinction function can flexible to join simulation system, so as to make the simulation environment more scalable.

(2) Analysis leakage curve

On the basis of (1), calculating the average signals respectively to the different sets, and then calculating the average difference signal to the two sets.

(3) Draw analysis results curve

Use the output of steps (2) to generate the corresponding analysis curve, provide more intuitive analysis results.

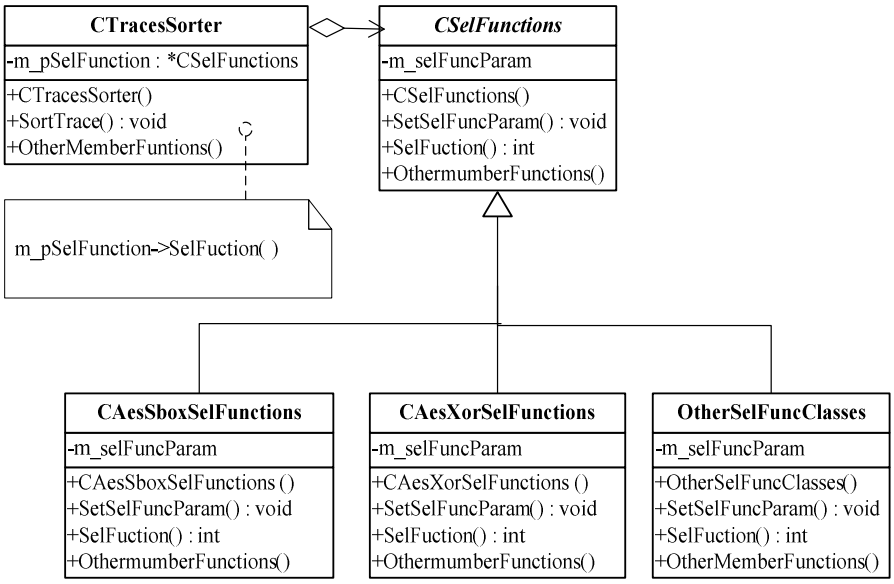

Figure 1. Finite The application about Strategy model in the curve diversity submodule

Conclusion and Further Research Work

At cryptographic chips design phase, the safety test analysis of the side of the channel attacks can overcome the shortcomings of the analysis method at production later, but need corresponding side channel simulation tools. In this paper, using the collaborative design thought about the software and hardware, gives the side channel simulation development environment and focuses on analyzing the simulation platform implementation technique. Make simulation implement and analyze implement separation, use the component technology to encapsulate the simulation development environment, so have strong flexibility. Different side channel information leakage and attack strategy can be added to the environment in the form of components, making the testers can according to the test needs to choose flexible test data and analysis strategy. This is advantage of our simulation platform than of PINPAS simulation platform.

In the further research work, we expect to join the other side channel leak model in this simulation platform, as electromagnetic leak, time leakage, etc. make the applicability of this simulation platform is stronger and extend the analysis strategies library, use new the side channels analysis methods (such as template analysis) to analyze the side channel attacks of the cryptographic chips.

Acknowledgements

This work was financially supported by the educational reform project in guizhou province department of education (SJJG 2016-05-96).

References

[1] Yongbin Zhou, QiuLiang Xv. Side channel attacks theory and technology. China cryptography development report 2008, Beijing: electronic industry press, 2009.8, 191-259.

[2] R. Anderson, M. Kuhn. Low cost attacks on tamper resistant devices. Proc of the 1997 Security Protocols Workshop, 1997, Vol.1361:125-136.

[3] C. H. Gebotys, R. J. Gebotys. Secure elliptic curve implementations: an analysis of resistance to power-attacks in DSP processor. In: proceedings of CHES 2002, 2002, Vol.2523:114-128.

[4] K. Tiri, D. Hwang, etc. A side-channel leakage free coprocessor IC in 0.18um CMOS for embedded AES-based cryptographic and biometric processing. Proc. ACM/IEEE Design Automation Conference (DAC) 2005, 2005, 222-227.

[5] Renauld M, Standaert F, Veyratcharvillon N, et al. A formal study of power variability issues and side-channel attacks for nanoscale devices. international cryptology conference, 2011: 109-128.

[6] Longo J, De Mulder E, Page D, et al. SoC It to EM: ElectroMagnetic Side-Channel Attacks on a Complex System-on-Chip. cryptographic hardware and embedded systems, 2015: 620-640.

[7] Sauvage L, Guilley S, Flament F, et al. Blind cartography for side channel attacks: cross-correlation cartography. International Journal of Reconfigurable Computing, 2012.

[8] Zhu L, Wu C, Wu L, et al. A DPA-resistant crypto engine for UHF RFID tag. International Journal of Embedded Systems, 2015.

[9] Jianbo Yao, Tao Zhang. Hardware/software co-design to secure crypto-chip from side channel analysis at design time 2010 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010, Vol.6:88-91.