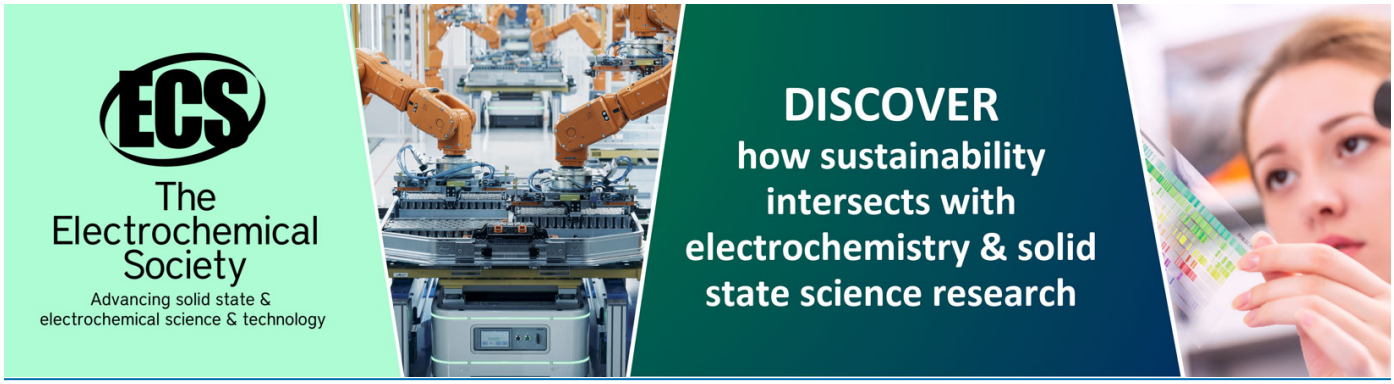
Research on security attack technology and detection method of RFID tag chip in intelligent electric meter



Research on security attack technology and detection method of RFID tag chip in intelligent electric meter

Rui Wang[1], Qiujing Gong[2], Ke Zhen[1], Xing Zhe Hou[2], Min He[1] and Ling Yu Wang[1]

[1] State Grid Chongqing Electric Power Company Marketing Service Center (Metrology Center), Chong Qing, China

[2] State Grid Chongqing Electric Power Research Institute (Chongqing Key Laboratory of Energy Internet Advanced Metrology and Measurement Technology), Chong Qing, China

[*]Corresponding author's e-mail: wangrui8@cq.sgcc.com.cn

Abstract. This paper introduces the security threats faced by RFID chips of intelligent electric meters firstly, and then focuses on the attack principle and security detection methods of Side-Channel Attack, which are elaborated from four aspects: non-contact RFID card test, fault-injection test, software and hardware cooperative detection and physical detection.

1. Foreword

In order to meet the needs of intelligent management of electric meters, and achieve scientific, efficient, anti-counterfeiting, anti-theft, etc., RFID technology is selected in electric meters now, and the RFID electric meter based on the Internet of things conforms to the development trend of national power grid construction. RFID tags are used as the media to realize the management of the whole period process of electric meters. By reducing staff and working intensity, the work efficiency is improved, and the intelligent, information-based and refined management of electric meters is further realized. However, RFID technology also has some security issues, including data overflow, data duplication, false event and tag reading rate. Through physical attacks, modification of configuration files, and data eavesdropping, product information may be stolen by people outside the physical system, resulting in product information leakage. The related technologies and methods of security attack and detection of intelligent electric meter RFID products chip are introduced in detail below. [1].

2. Chip security attack technology

Power consumption attack, time attack and electromagnetic attack are three typical kinds of Side-Channel Attack. Their attack idea is to plan channel attacks by measuring power consumption, execution time and electromagnetic field. In addition, Side-Channel Attack is not only a non-active intrusion attack, but also an active intrusion attack. When the IC cover is not unlocked, the IC can be attacked by injecting faults. The methods of injecting faults include: adjusting and changing ambient temperature, power/clock jitter. The effectiveness of this new type of attack is much higher than that of the mathematical method of cryptographic analysis, so it poses a serious threat to cryptographic devices. [2-3].

2.1. Side-Channel Attack method

Side-Channel Attack technology involves multiple disciplines and there are many kinds of attack methods, even the attack methods published in academic papers are numerous. According to different attack requirements and targets, the purpose, objectives, specific principles and methods of Side-Channel Attack are not consistent or even different. Therefore, Side-Channel Attack is not only aimed at a certain algorithm or chip, and it may need to be considered in a broader context of systems. At the same time, cryptographic system is not only the object of running cryptographic algorithms and security protocols, but also has a broader category. Generally speaking, there are some common things in the basic principles and methods of Side-Channel Attack. The basic principle of any attack using side channel is to first mine the side information related to confidential data from the cryptographic system, and then use the dependency relationship between confidential data and side information to acquire confidential information through analysis and derivation. According to different attacked objects, the confidential information to be obtained may be keys and passwords, or even the contents of confidential information. According to the implementation details of Side-Channel Attack, considering from the broad system category, the process of implementing a Side-Channel Attack on a cryptosystem can be summarized as follows: firstly, according to the attack purpose, the characteristics of the attacked object (cryptosystem) and the development status of existing Side-Channel Attack technology, determine the appropriate attack target; Secondly, according to the attack target, the basic operation of the electronic part and software part of the target is investigated; investigate which of the leaked side information may have data dependence when the system works, and whether these are consistent with the target of attack are investigated. According to the attack target, determine whether you need to know the cryptographic algorithm and security protocol in detail. According to the attack target, propose a Side-Channel Attack method with strong implementability and high attack efficiency. Then, according to the proposed Side-Channel Attack method, determine whether special stimulus (such as fault import, etc.) is needed for side channel data collection. According to the proposed Side-Channel Attack method, process and analyze side channel data and mine confidential information.

According to the result of Side-Channel Attack, confirm whether the attack is successful and whether the intended attack purpose is achieved. If it is not successful, according to the attack results, further study the problems in each step, correct to return to the above related steps to repeat the attack. For example, determine whether it is necessary to improve the side information data collection scheme, signal processing method, or improve the Side-Channel Attack method, and whether it is necessary to use other attacks of side information, whether it is necessary to combine Side-Channel Attack with traditional cryptanalysis, whether it is necessary to combine multiple Side-Channel Attack methods, and so on, it may even need to adjust the target or aim of attack. For example, someone need to get confidential information on a computer in an organization, but it cannot be known. According to the attack purpose, if the target is to invade the computer system, but the computer is not connected to the network, it can not be penetrated through the network. For the artificial intrusion into the computer system, the first may have to pass through the stringent security monitoring, biometric access control system, and so on to access the computer. Then there is the challenge of cracking passwords, even if the attack is successful, it still needs to leave no trace, which is almost always a series of difficult problems. According to the existing Side-Channel Attack technology and the surrounding environment of the computer, use the electromagnetic radiation emitted by the computer monitor or the monitor light leaking through curtains as the attack target. When the internal personnel of an institution browse the confidential information normally on the computer, they can read it directly and quietly in the distance without leaving any trace, thus achieving the attack purpose without knowing and deciphering its cryptographic algorithm and security protocol. Therefore, according to the comprehensive situation of attack purpose and demand, choosing the appropriate attack target will get twice the result with half the effort, which is also one of the key factors for the success of Side-Channel Attack. Some whimsical Side-Channel Attack ideas may make people feel incredible, even though these ideas have not been involved in general industrial technology research, but they can be implemented under the existing technical conditions, even easy to implement, and can play an unexpected role.

2.2. c and test equipment

The side channel detection equipment we use is shown in Figure 2-1, which can quickly analyze and process power consumption (SPA/DPA/CPA), electromagnetic (SEMA/DEMA/EMA-RF) and non-contact (RFA) testing methods. It also supports first-order and second-order attacks on all major encryption algorithms (such as SEED, MISTY1, DSA, ECDSA, HMAC&Camellia supported by 3DES, AES, RSA&ECC standards and national designated algorithms).

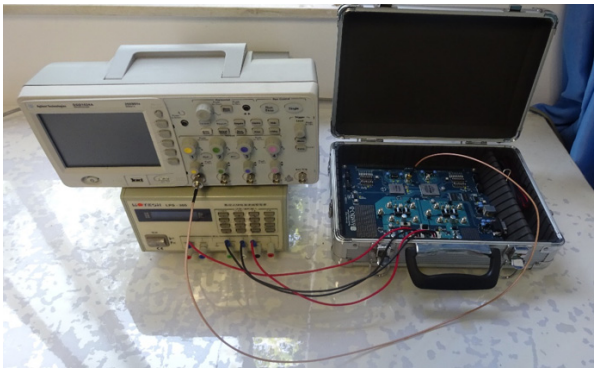


Figure1. diagram of Side-Channel Attack equipment.

3. Chip security detection method

Without considering the security problems caused by the imperfect design, there are usually three ways to embed backdoors and make security vulnerabilities in integrated circuits: the first is to implement it completely in hardware, and to design special control units in the circuit to work with the normal functions of the circuit, occupying the chip area and logic circuit resources, which can be realized in a simple circuit. The second is to implement the control information and algorithm completely in software, and trigger it by specific signals or timing when necessary. This method is generally used in advanced circuits. The third method is the combination of software and hardware, in which the processing of control information is realized partly by hardware and partly by software. This method is the most difficult to be detected, and usually has the highest cost[4].

In view of these means of generating circuit security risks, the corresponding chip security detection methods can also be divided into three categories: physical detection, electrical detection and protocol detection. The core of physical detection is to obtain the layout of integrated circuits by reverse engineering, and master the circuit topology related to security through analysis, and then find the circuit parts related to potential safety hazards. In electrical testing, the chip can be placed in abnormal state to find out the logic flaws in the chip design and determine their types, or trace and analyze the tiny electrical performance differences caused by each action of the integrated circuit chip, so as to know the possible abnormal functional circuits inside the chip. Protocol detection is a detection method which is analyzed and attempted by experts or professionals who are familiar with this technology after obtaining some information of security control algorithm structures.

The method of protocol detection needs a deep understanding of information control and algorithm, which generally belongs to the field of cryptography and needs experts in signal processing and communication. At the same time, it also needs a deep understanding of the internal logic structure of integrated circuits, which makes it difficult to implement. In view of the current equipment conditions and technical capabilities, it is a feasible scheme to use more physical detection and electrical detection methods to detect potential safety hazards of electronic components.

3.1 Non-contact RFID card test

Non-contact radio frequency card (RFID card) is widely used in most countries in the world because of its advantages of high reliability, convenient operation, anti-collision and good encryption performance. Among them, Mifare Classic card is the most widely used and popular card. According to the statistics

of the research team of Radboud University in the Netherlands, more than 1 billion Mifare Classic cards have been sold worldwide, and more than 200 million people are using the cards (this data does not include China), and occupy 80% of the contactless smart card market. In China, Mifare Classic card is widely used in medical treatment (medical card), transportation (bus card) and other aspects, including the campus card of most schools and the access card used by property.

Non-contact RFID card test is to compare the password in the known default password book with the key on the card to confirm whether there is a default key. If the card does not have a default key, change the ID of the probe card to the ID of the card to be cracked, and use the probe card to swipe it through the corresponding card reader for 2~3 times. The probe card will record the authentication data between it and the card reader (using parity and PRNG vulnerabilities). Using Sniffer software and NFC card reader, we obtained a key of the card, and then calculated the remaining 31 keys through nested authentication vulnerabilities according to the obtained key. Use the acquired 32 keys to read the card information. Finally, the storage location of the key data is analyzed according to the card information.

3.2 Fault injection test (fault Injection)

The reason of fault injection is that the smart card chip is made of silicon wafer, and the electrical properties of silicon wafer will vary with different environmental parameters. For example, the electrical properties of silicon wafers will change with different voltages, frequencies, temperatures, light, ionizing radiation and surrounding electromagnetic fields. Usually, the attacker will force the chip to make a wrong decision (for example, receiving the wrong input authentication code), allowing access to the confidential data in the memory[5].

Fault injection testing refers to introducing some wrong behaviors by changing voltage and frequency parameters, or using external light radiation, including introducing errors into the program flow of smart card chip, and analyzing its operation to test its anti-attack ability.

3.3 Software and hardware collaborative detection

For circuits with embedded software, the hardware and software co-testing is needed. Using the rapid prototyping system, the circuit is placed in the system simulation and verification environment, and each functional module of the circuit is tested and verified in isolation by the complete set of system tests related to it, and the special modules, especially the modules for controlling data flow and signal transmission, are identified and compared with the conventional control modules. At the same time, software and hardware co-testing is beneficial to distinguish the functions of circuit control instructions and determine the working state of circuits at various stages. In the process of chip detection, single-step tracking and breakpoint are the most fundamental technologies.

3.4 Physical detection

Physical detection also means layout analysis. The reverse engineering method is used to analyze the chip layout in detail using unpacking, sample preparation, photographing, puzzles, scanning electron microscopy, and electronic probes , etc. The corresponding circuit structure is detected and extracted, and the parts exceeding the functional requirements are analyzed and judged to determine whether there are potential safety hazards such as back door circuits and redundant circuits. The function of structural analysis in chip security inspection is mainly reflected in that the logic circuit diagram of the chip can be re-established by layout reconstruction technology, and the functions of different circuit modules can be analyzed from the physical level to find out whether there are abnormal circuit modules which may be a security risk.

4. Conclusion

This paper first introduces the chip security attack technologies of RFID products, including Side-Channel Attack technology, contactless RFID card test technology and fault injection test technology, and then expounds the detection methods of chip security from three aspects: electrical detection, hardware and software collaborative detection and physical detection.

References

[1] Juels A, Minimalist Cryptography for Low-Cost RFID Tags[C]// Security in Communication Networks, International Conference, Scn, Amalfi, Italy, September, Revised Selected Papers. DBLP, 2005.
[2] Zhang Hongzhuang. Security and privacy issues and policy analysis in RFID, Microcomputer information, 2008. 24- 6:48~49.
[3] Gwo-ChingChang, A Feasible Seeurity Mechanism for Low Cost RFID Tags， IEEE Proeeedings of the International Conference on Mobile Business(ICMB'05).
[4] Sun C.H, Research and implementation of side channel attack and defense[D]. Xi'an University of Electronic Science and technology, 2012
[5] Alavi, Seyed Mohammad, et al. "Traceability Analysis of Recent RFID Authentication Protocols." Wireless Personal Communications (2015).