Security Analysis of Cryptographical Module for FPGA

Sun Haitao[a*] Xue Deqing[c]
Department of Artillery Engineering
Ordnance Engineering College
Shijiazhuang, PRC
e-mail: sunhaitao81@sina.com

Liu Jie b
Department of Equipment Command &Management
Ordnance Engineering College
Shijiazhuang, PRC

***Abstract*—FPGA has been used abroad all fields about space, military, auto. It is the best choose of cipher protocol and arithmetic achievement. Its security has been concerned. In this article the authors design a Hardware Trojan of transmitting key information towards FPGA. It is important to realize the implement mechanism and raise the attention to IC security.**

Keywords- Hardware Trojan, FPGA life cycle, security threat model, FPGA.

I. INTRODUCTION

For the safety of FPGA, the existing two aspects: one is the FPGA of data security, which must provide FPGA to run the protection of the application. Chip internal data and peripheral circuit of communication between the data need to be protected, and the main method is in the FPGA internal integrated data encryption scheme. The second is the FPGA design safety, how to design FPGA to defend against cloning and reverse engineering, and the traditional method of attack is on intellectual property (IP) protection.

II. DESCRIPTION OF FPGA LIFE CYCLE

The life cycle of the FPGA device can be divided into three stages: manufacturing stage, the design and development stage and issue using phase, as shown in figure 1 show. In the three stages respectively password security device was described.

① The manufacturing stage, the manufacture of FPGA depends on the third party manufacturing company, usually located in Asia, to create physical device. These devices and then directly to buy system developer, to produce a final system products, or the third party company (such as Digilent, Avnet, NuHorizons) to manufacturing including FPGA and peripheral equipment development board. ② The design and development stage, design and development staff will FPGA combined into a final system, and the programming to realize its function. Designers use FPGA chip or the third party FPGA development board builds the system platform to meet the application requirements. ③ During the application of the issue, the FPGA can be widely used. Including cars, planes, wireless router, telephone, Mars plan, satellite, weapon system, camera, underwater modems, etc. Devices in the application stage weakness rely heavily on application environment. It involves physical security devices (how to easily access and protect its physical operation) and the function of the device (military device contains more valuable design, therefore, more than a student system more vulnerable to attack). That is to say, in the FPGA life cycle stages, its own security may suffer from outside threats.

III. FPGA SECURITY THREAT MODEL

The attacker wills the entire life cycle in FPGA the weakest link and the most easily to find weaknesses to attack. Chip design, manufacturing, testing in different companies, and even different countries, maintain the safety of the whole production process is very difficult.

A. Physical Attacks

Monitoring the operation of the system characteristics，Try to get the internal operation of the information system.

Threat - reveal private information, control the internal bus, and modified output address, etc.

Attack - including ① the invasion against using chemical fusion methods for equipment solution package, direct contact inside the equipment, the use of ion a observation memory unit to achieve the purpose of the read information, the typical example is the general agent against。② Half intrusion attack need to contact the equipment, but not damage equipment passivation layer, may through the unauthorized interface for electrical contact, the typical example is fault induction attack. ③ Noninvasive against the most effective is bypass attack technology: use only external observable information, usually has no intention of electromagnetic radiation, operation time, power consumption and to derive the encryption system of operation and in the operation involves secret parameter, such as power attack, collision attack, electromagnetic radiation attack, time analysis attack and error injection attack, etc.

B. Design Tool Failure

Entry point - design and development stage, the FPGA programming depending on more than one company of complicated CAD tools and IP core. To design tools and IP nuclear attack easily lead to malicious hardware chip embedded into the physical in the realization of. Such as encryption nuclear, it has a key, if the system is not fully established by you, there is no way to prove the circuit is not tamper with or be monitored. This attack can through to design tools and IP core of manipulation to achieve, as Ken

Published by Atlantis Press, Paris, France.

Thompson in Turing said, "you can never fully believe not you create your own code".

Threat - information leakage, hardware tamper with.

Attack - hardware Trojan.

C. *Steal Design*

Entry point - hardware bit stream contains on FPGA programming of all the information to accomplish a specific work. It is usually private information; it is design personnel's work. Therefore, protect the bit stream is the main to eliminate intellectual property stealing. In addition, the bit stream internal may contain sensitive information, such as. Encryption key, etc.

Threat - design lost information leakage.

Attack - mainly include ① cloning: The SRAM type FPGA, configuration data is stored in external a nonvolatile device (such as PROM), in power on configure into FPGA, the attacker can monitor configuration process, to get the configuration file. ② The reverse engineering: not all cloning, it is to point to the data flow code into and original design function the same functional unit. On FPGA speaking, it means that the bit data flow reverse recovery become HDL description or net list. ③ To read attack: directly from the device read bit stream. Some FPGA allows the JTAG, ICAP or etc bit stream program interface configuration data from the device will be in direct reading, the attacker provides convenient attack.

This paper studies the FPGA chip hardware Trojan attacks to realize, the main idea is to a PC running encryption program FPGA module, the development of hardware Trojans, realize the Trojan horse.

IV. FPGA CHIP HARDWARE TROJAN ATTACKS

Hardware Trojans, is through the integrated circuit design, manufacturing or secondary development in the process of human to create some illegal circuit, thus leaving "electronic back door", for the subsequent attack opened the door. This new type of hardware attacks can easily around very strong hardware such as password security barriers, the current hardware constitutes a major threat to the security model.

Hardware Trojan horse is a small horse, in the key stage of large-scale and visa circuit just dozens or hundreds of gate can realize functions, not easy to be noticed and found that is installed a time bomb, once the trigger activated, it is possible to control to the enemy. There is no stop hardware Trojan appear effective way, this is the IC design and manufacturing process of the decision.

The implementation of the Hardware Trojan presented in this Report will be covered in this chapter. First, we give an overview of the used hardware, the architecture and in the end a test setup to verify the functional correctness of the Trojan.The Trojan presented in this report was developed on a XUPV5-LX110T DES is running on the FPGA board. Cleartext is sent from PC to FPGA. Ciphertext which encrypted by FPGA is transmited back to PC. Development System by Xilinx Inc. This development board hosts a Spantan3 FPGA, which supplies more than enough resources to implement necessary components. Therefore the majority of the design, such as the communication control blocks, the data encoding module, CRC modules, and the system monitor instances for A/D conversion are implemented on this FPGA.

In order to manage testing conveniently, we used the RS232 port to connect the FPGA to the PC. A Graphical User Interface (GUI) was designed with MATLAB to handle UART communication. The testing parameters, such as Baud rate, number of packets and packet size can be easily controlled with this user interface.

V. CONCLUSION

In this article the authors descript the life cycle towards FPGA，establishes FPGA security threat model， and depicts the chip hardware Trojan attacks. It is important to realize the implement mechanism and raise the attention to IC security.

REFERENCES

[1] Mohammad Tehranipoor, Farinaz Koushanfar. A Survey of Hardware Trojan Taxonomy and Detection. IEEE Design and Test of Computers.

[2] Harrini Bhamidipati. Single Trojan Injection Model Generation And Detection. Case Western Reserve University.

[3] Miodrag Potkonjak, Ramesh Karri. Special Issue on Integrated Circuit and System Security. IEEE Transactions on Information Forensics and Security

[4] Thomas Feller, Aziz Demirezen. HARDWARE TROJANS: Data Leakage Using General Purpose LEDs. Technical Report - TUD-CS-2010-2384.

[5] Zhang Peng，Zou Cheng. Hardware Trojans design of correlation analysis based on electric.
Journal of Huazhong University of Science and Technology(Natural Science Edition).

Published by Atlantis Press, Paris, France.

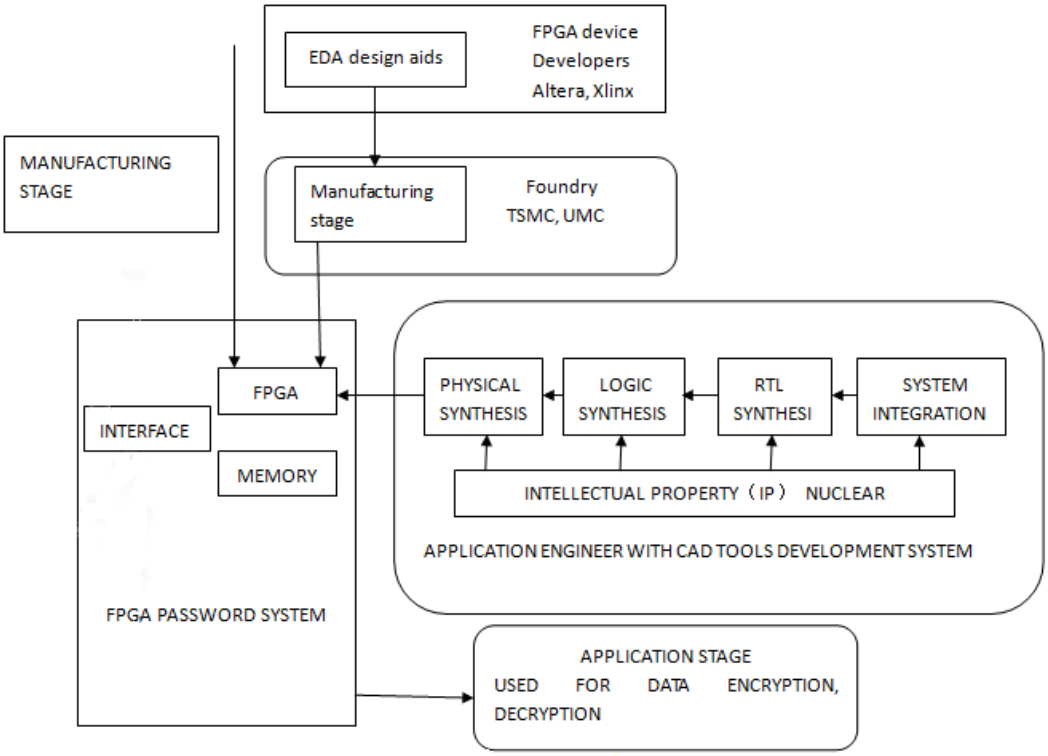

Figure 1 The life cycle of FPGA

Published by Atlantis Press, Paris, France.