FPGA Design Duplication based on the Bitstream Extraction

Soyeon Choi
Dept. of Electronics Engineering
Chungnam National University
Daejeon, South Korea
soyeonchoi@cnu.ac.kr

Nari Im
Dept. of Electronics Engineering
Chungnam National University
Daejeon, South Korea
nrim.cas@gmail.com

Hoyoung Yoo
Dept. of Electronics Engineering
Chungnam National University
Daejeon, South Korea
hyyoo@cnu.ac.kr

Abstract— **Due to fast design process, SRAM-based Field Programmable Gate Array (FPGA) is widely used for various industrial applications. Since the netlist stored in external non-volatile memory is transferred in the form of bitstream whenever FPGA powers on, the netlist on FPGA is vulnerable for malicious attacks. In this paper, we present how the attackers duplicate the original FPGA design using FPGA bitstream extraction, and emphasize the need for countermeasure to prevent such malicious duplication. Xilinx Spartan-6 evaluation board is used, which includes XC6SLX9 FPGA and XCF04S flash memory. According to the experiments, the described method is succeeded in replicating the original design on the other FPGA.**

FPGA; Bitsteram analysis; FPGA Duplication

I. INTRODUCTION

Among various FPGA types, SRAM-based Field Programmable Gate Arrays (FPGAs) are most widely used, and there are many companies that manufacture SRAM-based FPGA chips such as Xilinx, Intel Altera, Lattice, and etc. [1]. Since SRAM is a type of volatile memory, SRAM-based FPGA inevitably necessitates external non-volatile memory that stores the netlist information to prepare the moment when the power turns off. Therefore, a typical SRAM-based FPGA board always includes both a FPGA device and an external non-volatile memory as shown in Fig. 1 [2].

In general, EDA tools such as ISE and Vivado design suites are provided from FPGA vendors in order to synthesize and implement circuit design on FPGAs. The generated netlist is converted into a bitstream format and stored in a non-volatile memory in the FPGA board. When power is applied to the FPGA board, the bitstream is transferred from the DO (Data Out) pin of the non-volatile memory to the DI (Data In) pin of FPGA device as shown in Fig. 1. Given the bitstream, FPGA device is reconfigured to operate FPGA as the circuit design. Since the circuit implemented on the FPGA board can be easily duplicated to another FPGA board when the bitstream is extracted completely, the design on FPGA is vulnerable for malicious attacks.

In this paper, we present how the attackers duplicate the original FPGA design using FPGA bitstream extraction. To bring a practical example, the proposed duplication method is exemplified using FPGA evaluation board that includes XC6LX9 Xilinx Spartan-6 FPGA and XCF04S flash memory.

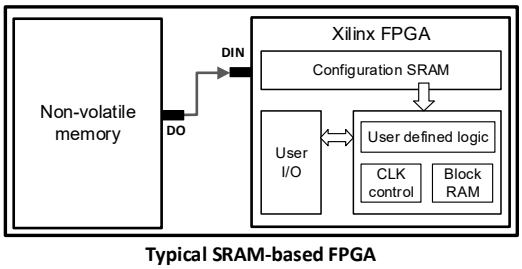

Figure 1. Configuraiton of a typical SRAM-based FPGA.

II. FPGA DUPLICATION METHOD

In order to replicate the Xilinx FPGA using bitstream extraction, it is necessary to analyze the file structure used to configure FPGAs. Xilinx Design Suites provides two types of file formats; RBT and MCS file. Although RBT and MCS file formats are the same in that they represent netlist information, they are slightly different for usages and contents. More precisely, RBT file format is used when Xilinx design suite directly programs a FPGA without going through an external non-volatile memory, but MCS file format is used when Xilinx design suite programs an external non-volatile memory. Furthermore, RBT file is written in binary number, but MCS file is written in hexadecimal number. This is because the FPGA is connected to the host PC with serial line whereas the external memory is connected to the host PC with parallel lines. Lastly, MCS file contains not only netlist information but also an additional information including byte count, address, record type, and check sum. One example of RBT and MCS files are depicted in Fig. 2.

Based on file format analysis, the process of the circuit duplication on FPGA can be summarized as follows;

STEP 1) Extract the bitstream from FPGA board

STEP 2) Restore MCS file from the extract RBT file

STEP 3) Program the other FPGA using the restored MCS file

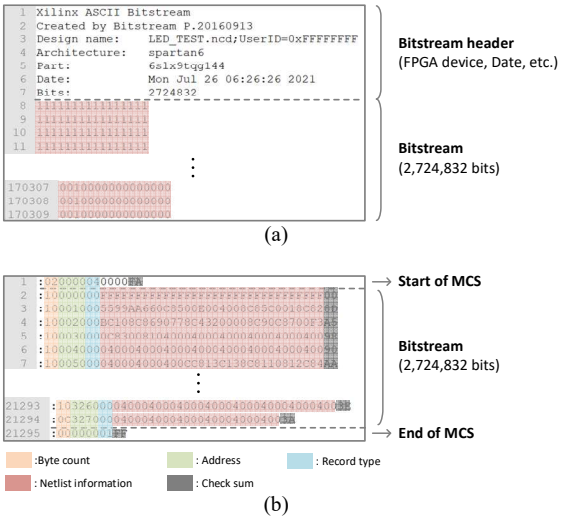

Figure 2. (a) RBT file format and (b) MCS file format.

First, when power turns on, the transferring bitstream from non-volatile memory to FPGA device is extracted using measurement instrument such as logic analyzer or oscilloscope. Note that the bitstream file stored on the non-volatile memory is MCS file format, but the bitstream extracted from the non-volatile memory is measured in RBT file format. Next, it is necessary to insert additional information and convert number representation to rebuild the measured bitstream in the form of a complete MCS file format. Since EDA tool accepts only MCS file format to program an external non-volatile memory, it is highly needed to follow the MCS file format designed from the FPGA vendor. After converting the file format successfully, the regenerated MCS file format is finally loaded to another FPGA board to duplicate the circuit design.

III. Experimental Results

As an example, Xilinx Spartan-6 evaluation board is tested, which consists of Xilinx Spartan-6 XC6LX9 device and 4M-bit flash memory XCF04S. ISE Design Suite 14.7 on Windows10 is used to program the test design to Xilinx Spartan-6 XC6LX9. A simple design is implemented, which performs logical AND and XOR operations with two inputs of 4-bit IN_A and IN_B and two outputs of 4-bit O_AND and O_XOR. Two inputs IN_A and IN_B are assigned to DIP switches, and two outputs O_AND and O_XOR are assigned to LEDs, respectively.

Figure 3 shows the process of the circuit duplication in more detail. First, we extract a bitstream that transferring through the DO pin of XCF04S to the DI pin of XC6LX9 FPGA device at the speed of 1.7 Mbps using a logic analyzer keysight 16861A at sampling rate 100 MS/s. After extracting the bitstream, we generate MCS file by inserting byte count, address, record type, and check sum, and converting binary numbers to hexadecimal numbers in order to follow Xilinx's MCS file format. At last, the recovered MCS file is loaded into the other FPGA board as a normal MCS file is loaded. As shown in Fig. 3, it is successfully verified that the circuit can be perfectly duplicated from the original FPGA board to the other one. We checked all the cases of inputs and outputs for complete verification. It is also important to note that this

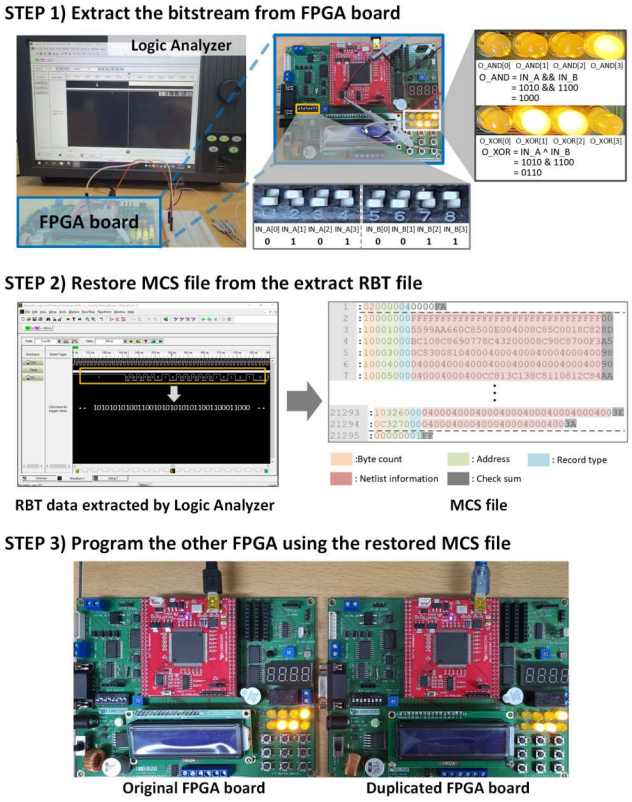

Figure 3. FPGA duplication process.

method can be applied to other types of FPGAs not limited to XC6LX9 chips.

IV. Conclusion

This paper describes a method to duplicate circuit on SRAM-based FPGAs using the bitstream extraction. Xilinx Spartan-6 XC6LX9 is exemplified, and we show that a simple logic design can be successfully replicated from one to another one. Since this duplication can be performed by malicious attackers, it is highly needed to study countermeasures to protect circuit design on FPGAs.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2021R1I1A3055806).

References

[1] P. Swierczynski, M. Fyrbiak, P. Koppe and C. Paar, "FPGA Trojans Through Detecting and Weakening of Cryptographic Primitives," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 8, pp. 1236-1249, Aug. 2015

[2] O. Heron, T. Arnaout and H. -. Wunderlich, "On the reliability evaluation of SRAM-based FPGA designs," International Conference on Field Programmable Logic and Applications, 2005., 2005, pp. 403-408.

[3] Xilinx, "Spartan-6 FPGA Coonfiguraiton User Guide," CA, Xilinx, 2009.