

# Trustworthy Reconfigurable System-on-Chip Computing

JULIAN L. RRUSHI

University of Illinois at Urbana-Champaign

---

The migration offshore of a large number of foundries that fabricate FPGAs for use in U.S. military, intelligence, and industry, has raised concerns within the U.S. defense and national security organizations. An adversary nation or state with modern semiconductor capabilities, talented people, financial resources, and motivation could use dirty tricks, namely manipulate computer chips in offshore foundries, to cause serious harm to U.S. Such an adversary may also target software tools used to transform application designs into FPGA configurations. The proposed research aims at devising algorithms for detection of malicious alterations of FPGA chips and FPGA configurations. The detection capability of devised algorithms will be quantified via receiver operating characteristic curve analysis based on metrics such as probability of detection and probability of false alarms. The proposed research is relevant to the I3P core research area titled Discovery and Analysis of Security Properties and Vulnerabilities.

Categories and Subject Descriptors: B. Hardware [**B.7 INTEGRATED CIRCUITS**]: B.7.1 Types and Design Styles

General Terms: I3P Core Research Area: Discovery and Analysis of Security Properties and Vulnerabilities

Additional Key Words and Phrases: Field Programmable Gate Arrays, Trust Validation

---

## 1. INTRODUCTION

In U.S. field programmable gate arrays (FPGAs), i.e. computer chips which can be programmed to perform user defined logic functions, are used to implement a large number of highly sophisticated system-on-chip (SoC) designs for critical military, intelligence, and industrial applications. FPGAs are proposed as an alternative to application specific integrated circuits (ASICs) due to their flexibility in reprogrammability and currently lower engineering costs. Although ASICs have the capability of reaching extremely high execution speeds through employment of parallel computation, the logical functions that they implement are hard wired into them. Therefore ASICs do not allow for modifying the implementation of logical functions which potentially are supposed to change over time for reasons such as upgrading algorithms to a recent version or eliminating security vulnerabilities identified after device deployment. These two factors are relevant for maintaining persistent military and intelligence stealth technology to preserve superiority over potential adversaries, and for preventing cyber attack damage to controlled physical infrastructures (when applicable), respectively.

SRAM FPGAs, which are currently the dominant type of programmable logic devices, allow for fast in-circuit reprogramming. While other types of FPGAs such as those based on EPROM, EEPROM, or FLASH, are reprogrammable via ultraviolet radiation. A typical SRAM FPGA chip consists of a two-dimensional array of circuit element sets referred to as configurable logic blocks (CLB). CLBs are interconnected among themselves with horizontal and vertical routing wires according

to a programmable routing architecture. Since a computation can be represented as a Boolean equation, and a Boolean equation in turn can be represented as a truth table, truth tables are core computational units of FPGAs. Truth tables are implemented in each CLB by the means of look-up tables (LUTs), which are one-dimensional one bit wide memory arrays. Inputs of a CLB serve as address lines for such memory arrays, while bits addressed by these address lines represent LUT output. LUTs can be used in combination with each-other. In addition to LUTs, CLBs also contain bit storage elements, such as for example D flip-flops, and multiplexers to select a result either from functions implemented by LUTs or from bits stored in D flip-flops.

CLBs are generally surrounded by programmable I/O blocks. In fact modern FPGAs in general contain a large number of macro blocks such as embedded memories, digital signal processing blocks, embedded processors, high-speed I/O blocks, clock distribution circuits, etc. System developers code designs of a system to be implemented on chip in a hardware description language (HDL) such as VHDL or Verilog. These designs are eventually combined with intellectual property (IP) cores, i.e. ready-made designs of defined logical functions developed and provided by third parties, also coded in HDL. Synthesis tools, which in principal are comparable with traditional compilers, process HDL code and assemble it into netlists for a given FPGA architecture. Netlists are descriptions of primitives, i.e. LUTs, D flip-flops, multiplexers, etc., in a defined FPGA architecture and interconnections between them. Some IP cores are provided as netlists rather than HDL code, in which case they are integrated with the netlists generated by synthesis tools. A software tool is then used to map the content of a netlist to specific primitives of a defined FPGA architecture.

This software tool generates a placelist, which is a description of the physical placement of each primitive and their interconnection routes. A placelist is then encoded into a bit stream via a proprietary encoding scheme. As of this writing the details of these encoding schemes are generally kept secret by FPGA vendors. A bit stream produced by such an encoding scheme is referred to as the configuration or programming of a FPGA. When a bit stream is loaded on a FPGA it defines all primitives and their routing architecture.

## 2. THREAT MODEL

Due to economic factors a large number of fabrication facilities which produce FPGAs, ASICs, integrated circuits in general, have been migrating offshore. This fact has raised concerns in U.S. defense and national security organizations that an adversary nation or state with modern semiconductor capabilities, talented human resources, financial resources, and motivation could use dirty tricks to cause serious harm to U.S. The danger lies in the feasibility for such adversaries to maliciously manipulate computer chips produced and assembled in offshore foundries and packaging facilities, respectively. Malicious manipulation of computer chips includes insertion of backdoor features into chip designs, weakening or total neutralization of security mechanisms, insertion of chip primitives carrying resident malicious code such as worms and trojan horses, etc. Since computer chips are widely used in microelectronics-based weapons, navigation, space, and battle management, an ad-

versary could cause disruption of U.S. warfare capabilities in moments of military engagement. Such dirty tricks could also provide an adversary with huge espionage advantages as computer chips form the basis of intelligence and military communications.

One of the principal objectives of attacks on FPGAs and ASICs is the acquisition of application designs implemented in them. Modern FPGAs and ASICs employ a variety of security mechanisms to prevent theft of the algorithmic capabilities implemented in them. FPGAs for example employ bit stream encryption, tamper proofing, and watermarking. Protection of application design is quite relevant to U.S. military in order to preserve ownership of stealth technology embedded in reconnaissance aircrafts, missiles, etc. Malicious manipulations of computer chips facilitates the extraction of application designs from FPGAs and ASICs, hence provide an adversary with advanced technological knowledge. Although the issues discussed in this section have been raised by U.S. defense and national security organizations, manipulation of computer chips represents a serious danger also for an industry such as nuclear power. Monitoring and control functions in nuclear power plants traditionally have been carried out via analog control systems. Nevertheless, generation III+ and IV reactors are equipped with digital control systems, and in older reactors analog control systems are being replaced with digital control systems due to aging factors.

A digital system type under consideration for monitoring and controlling nuclear power plants in U.S. is the FPGA. U.S. nuclear regulatory commission (NRC) has identified FPGAs as an emerging technology, and has implemented research projects to confirm the viability of FPGAs and their compliance with NRC standards. By modifying FPGA designs an adversary could on one hand neutralize reactor safety systems, hence leave reactors without automatic protection, and on the other hand disrupt their operation. In addition to intervening on computer chips, and adversary nation or state may target the software flow used to transform an application design from HDL code into a bit stream. An adversary may manipulate FPGAs by introducing into the software flow in question trojan horse IP cores as HDL code and/or netlists, trojan horse synthesis tools, trojanized versions of the software tool used to generate placelists from netlists, or trojan horse implementations of encoding schemes.

### 3. PROPOSED RESEARCH

The proposed research project aims at devising algorithms to detect malicious manipulations of FPGA chips by a scientifically highly advanced, highly motivated, and financially well-endowed adversary such as a nation, state, or large organization, which possesses or acquires the opportunity to intervene on FPGAs at fabrication facilities, packaging facilities, or software tools through which bit streams are produced. The proposed work won't focus on electrical testing and reverse engineering as earlier research results have shown that these techniques are unreliable when used to detect malicious modifications of integrated circuits in general. Given a FPGA chip associated with a defined FPGA chip design. The proposed work will develop algorithms to establish whether the FPGA chip under analysis does nothing more and nothing less than what is defined by its corresponding design. These

algorithms will check for additional behavior inserted during FPGA chip fabrication, and for alterations or complete lack of implementation of architectural aspects and operations required by the FPGA chip design.

Examples of additional behavior include stealth FPGA chip features which under a given set of conditions at defined points in time generate side-channels such as power consumption, data-dependent timing regularities, and electromagnetic radiation. Thus, additional behavior which facilitates side-channel attacks on cryptographic protocols implemented in manipulated FPGAs. An example of additional behavior may also be the insertion of predictability in the initial content of LUTs if LUTs are used as a source of entropy for random number generator functions, which in turn are used to feed the generation of cryptographic keys. An adversary may also insert extra CLBs and routing network interconnections for on-the-fly generation of mutated worm code. Thus, there is a myriad of attack options which are implementable via malicious FPGA chip alterations and which are to be checked via detection algorithms. The proposed work will investigate on whether, and how, obfuscation techniques could be used to hide bits and additional behavior in a FPGA chip.

As research projects in general on establishing trust in FPGAs and ASICs produce algorithms capable of detecting malicious alterations in corresponding chips, it is likely that potential adversaries work on the other side, namely how to conceal malicious FPGA chip alterations. The proposed work will also develop algorithms to determine the behavior of circuits in a FPGA chip which are found not to be part of the associated FPGA chip design. Given a configured FPGA and the design in HDL of a user-defined application which is supposed to be implemented in the FPGA under consideration. The proposed work will develop algorithms to establish whether the bit stream loaded on the FPGA in question entirely meets the specification of the user-defined application, and whether this bit stream does not implement any additional features with respect to such specification. These algorithms will check for potential trojan horse synthesis tools which may implement the injection of backdoors, worms, or other malware into the final bit stream during the assembling of HDL code into netlists.

These algorithms will also focus on detection of trojanized tools responsible for the generation of placelists from netlists, and on detection of trojanized implementations of bit stream encoding schemes. The proposed work will cover the detection of malicious IP cores in HDL or netlist forms. Most popular user-defined functions, including softcore processors and elliptic curve cryptography, are implemented and provided as IP cores by third parties. A softcore processor, i.e. a microprocessor specified via software in HDL and implemented in FPGA, for example, could be constructed to support hidden instructions as part of its instruction set. Such a malicious softcore processor then could interpret preliminarily defined data as indications to execute a series of hidden instructions, hence create a backdoor into FPGAs for knowledgeable adversaries. The proposed research project is currently at its very beginning, therefore potential areas to be explored are still under analysis.

Nevertheless, a direction which could be explored in the proposed work could comprise hidden, potentially mathematical, schemes which aim at facilitating detection

of malicious alterations of FPGA chips and their configurations. The idea is to try to define a series of factors in FPGA chip designs and application designs with the following characteristics. These factors are supposed to be hidden from untrusted parties with access to FPGA fabrication facilities, FPGA packaging facilities, or FPGA software tools. That is, untrusted parties who can read FPGA chip designs and application designs should not be able to identify neither the form of these factors nor their existence in the aforementioned designs. Further, in the case of FPGA chip designs these factors are supposed not to have any negative affects on the correct functioning of the fabricated FPGA chip. These factors should be such that, if any malicious alterations of FPGA chips and their configurations take place, they generate symptoms which are unidentifiable by untrusted third parties but recognizable by who developed the hidden mathematical sensors scheme.

Another idea could be to examine FPGA chip designs and application designs in order to derive conditions that must be met by FPGA chips and FPGA configurations, respectively, for their trustworthiness to be validated. This project will develop quantifications of the performance of proposed detection algorithms via receiver operating characteristic (ROC) curve analysis based on metrics such as probability of detection and probability of false alarms. It will also demonstrate a discrimination curve that will provide the relationship between these two detection performance metrics. The planned deliverables of the proposed research project comprise technical papers providing detailed descriptions of devised algorithms along with quantification of their detection performance, implementations of these algorithms in the form of security analysis tools, and a book of research on detection of malicious alterations of computer chips and reconfigurable device configurations. The technical papers will be submitted for publication to peer reviewed conferences and journals, while the analysis tools will be made available to the research community.

The proposed research project is relevant to the I3P core research area titled Discovery and Analysis of Security Properties and Vulnerabilities, as it addresses issues such as proposals of new approaches and tools to determine whether exploitable defects have been introduced, capabilities to analyze hardware and software systems to identify vulnerabilities before the systems are used operationally, and determination whether hardware and software components from multiple sources include vulnerabilities, trapdoors, or malicious code. Establishing trust in computer chips and hardware representations of application designs has been an issue for U.S. DoD and U.S. intelligence community even before integrated circuit fabrication facilities migrated offshore. It is the candidate's aspiration that the proposed research project will contribute to the assurance of U.S. information infrastructures.