ITR/NGS: Toward Autonomous Computing Platforms: System-Wide Hardware/Software Performance Monitoring and Adaptation

School of Electrical and Computer Engineering
Georgia Institute of Technology, Atlanta, GA 30332
2008 NSF Annual Report for Cornell University
Project Number: 21066PH

Co-Principal Investigator: Hsien-Hsin Sean Lee
Project site: Georgia Institute of Technology
leehs@gatech.edu Tel: (404) 894-9483

Brief Statement

As this project was approved for one-year no-cost extension by both Cornell University and their sponsor National Science Foundation, the original scheduled "Final technical report" will be extended for one more year. Therefore, the required upload of the originally scheduled final report is identical to the Annual technical report submitted in August 2008.

1 Activities and Findings

The objective of this research of this year is to develop novel techniques for FPGA to protect the intellectual property (IP) of a digital design based on array-based FPGA, which follows the similar line of monitoring/security work we had conducted for the last few years on this project at Georgia Tech. This issue is increasingly becoming critical as we have seen more and more digital systems are being deployed using array-based FPGA for its fast time-to-market and flexibility. The potential issue of IP theft, however, has not been addressed with any effective measure. Toward this goal, we have developed an effective post-processing algorithm which can be transparently integrated into array-based FPGA synthesis process to imprint watermark onto a digital design. The additional process can be added seamlessly as part of the logic synthesis within any automatic FPGA CAD tool chain, the overheads in terms of routing area and timing are minimal.

1.1 Motivation

As the physicals design tools become more stable and mature, designing a complex circuit with billions of transistors using automatic standard cell based design flow is receiving more popularity. At the same time, system-on-chip (SoC) designers advocate the concept of IP reuse to accelerate the design and delivery time for fulfilling the time-to-market constraint for applications in this field. Most of the companies would purchase IP designs from IP vendor companies or create their own IP macros for reducing their overall system design effort. The fast evolution path of Field Programming Gate Array (FPGA) makes the task of designing an IP or an entire system using automatic synthesis design flow highly feasible. It offers an advantage of a low cost and a faster design turnaround time and elevates the ability of competition. More significantly, the designers targeting for FPGA do not need to be a circuit expert but can rely mostly on a synthesis-based CAD tool chain provided by the FPGA vendors. However, for an industry toward this direction to be successful and profitable, it is a necessity to address a variety of

issues in security to safeguard the original designers' copyright to the IP on the FPGA. The legal means of IP protection such as patents and license agreement are a deterrent to illegal IP circulation. Unfortunately, they are insufficient to detect an IP protection breach. In the absence of security check, an adversary can easily circumvent and illegally sell a copy of a design with the original designers' consent. One way to address this pirate issue is to encrypt the FPGA bitstream and store the encryption key inside the internal SRAM on the FPGA. Even though such a mechanism could deter adversaries from using it illegally to certain degree, it is by no means sufficient to detect illegal distribution of designs by a licensed customer. Another higher level solution is to protect the IP with unique, embedded watermark to a design to provide certain identification of ownership of the synthesized IP. The second approach is what we believe a more effective approach. We perform our research to seek viable solutions in this direction. Our overall objective is to realize a low-cost while effective watermarking scheme used in synthesizing circuits onto FPGA.

1.2 Research and Education

An effective watermarking technique provides guarantee for detecting any security breach. Traditionally, watermarking embeds a unique signature (either a secret word or a logo) into a design by the authors or designers. Once distributed, the authors or legitimate users/licensees can verify the authenticity of a design by checking the embedded watermark. A digital watermarked design has exactly the same purpose, i.e., to protect the intellectual property and guarantee the security of a given design. In particular, in this research, we focus on the IP protection for FPGA-based design. Due to its versatility and portability, an array-based FPGA synthesis design, once obtained, can be easily copied and used with commercially available tools without any license agreement binding from the vendors. Our premise in this work is that watermarking can be applied to protect a design by embedding certain, unique circuit patterns during the synthesis. The watermarked bitstream can further be optionally protected with conventional encryption techniques. With these techniques, any theft of an HDL-based design can be identified by comparing the circuit-level watermark. A good digital watermarking scheme must provide the following characteristics: (1) difficult to remove without damaging the IP design; (2) resistance to any tampering attempt; (3) low area and critical timing overhead; (4) transparency; (5) strong indication of authorship; (6) low false positive rate.

To achieve our objectives, we investigated the FPGA design flow and identified the key parts of the procedure where we can insert watermark. Another consideration is that this extra task should be non-invasive, i.e., incurring no or little extra design time and cost without any impact on the final circuit performance. From CAD design flow, routing is the most flexible part of the process which one can modify for embedding a unique pattern without affecting the original functionality. Our idea is to manipulate the routing algorithm and integrate our watermarking mechanism as part of the routing process. The design flow we proposed is shown in Figure 1. In addition to the circuits-level description, we need to add a signature text provided by the designer (or the customer) as part of the input to the FPGA synthesis tool. This signature is meant to be used when a design is being authenticated and verified. The final routing tool is enhanced with the capability of digital watermarking. The resulting FPGA routing will be watermarked using the signature input. The verification process is depicted in Figure 2.

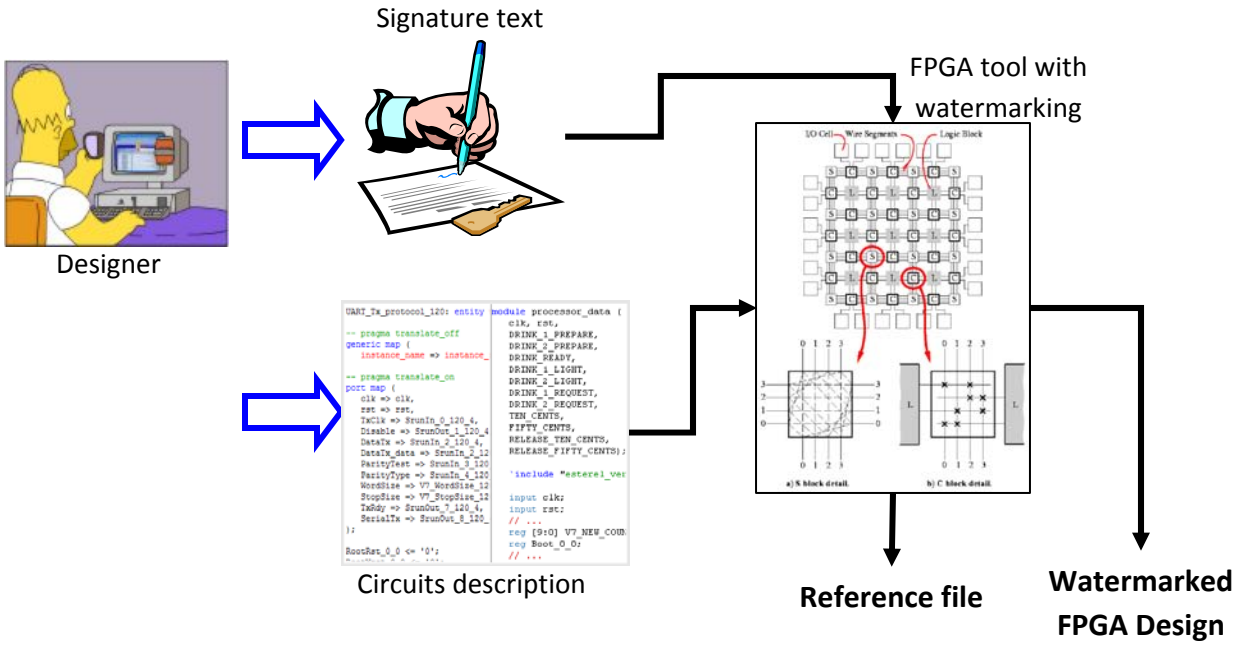

Figure 1. Watermarking based design

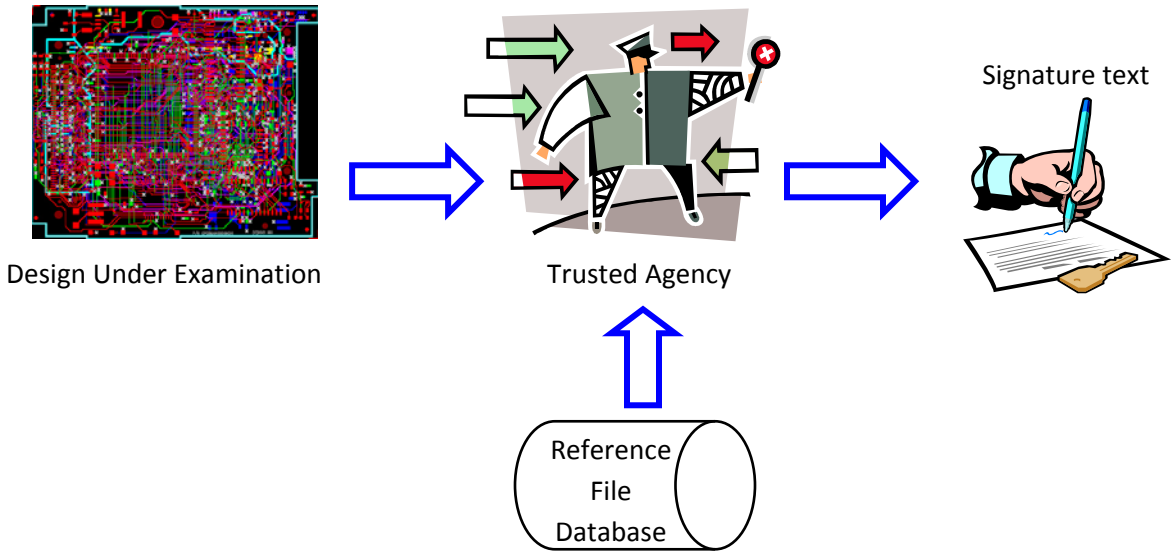

Figure 2. Verification Process

Basically, our technique can be classified with a set of constraint-based watermarking techniques. We specify the routing constraints that are directly correlated to the signature text given by the designer. The routing generated under these constraints is a function for generating the signature bitstream. The watermark, if added during the early stage of the FPGA CAD flow, may be removed or distorted due to several design optimizations being applied by the automated tool chain. To address this shortcoming, we integrated the watermarking technique during the last stage of the CAD flow. Using the pattern of the

signature text, we modify the routing cost function for each tile in the FPGA to detour the default routing pattern used by the CAD tool. The cost function is an exponential function itself, thus the routing decision may be procrastinated to some certain extent.

1.3 Major Findings

In this study, we implemented our new cost function and the routing algorithm in the open-source VPR placement and routing tool. The analysis we performed mainly focuses on the final quality of the generated (re-routed) FPGA circuits including the following: false positive rate, synthesis time impact, critical path impact, and extra wire overhead to fulfill our routing requirement.

With respect to the false positive rates, an ideal watermarked design should have a zero false positive probability. False positive occurs during the verification process when two different designs were categorized into the same one, leading to a failure of identifying an illegally cloned design. Apparently, such coincidence is a function of the circuits complexity and routing quality. We have analyzed this probability using an analytical model based on our algorithm and found that the likelihood of a commercial product circuits to encounter false positive is extremely low. Since our watermarking based cost function is tightly integrated into the original cost function of the routing algorithm, the time to perform FPGA routing will be almost identical to the original algorithm as our cost function does not involve any overly complex calculation. We performed a detailed analysis on the critical path delay using different signature files under different FPGA architecture assumptions for the MCNC benchmark circuits. On average, 70% of the circuits could be watermarked with the same channel width provided by a reasonable sized FPGA. In other words, the watermarked design did not further complicate the routability and will be able to fit the watermarked design onto the same FPGA chip as the original design. However, there were a couple of cases where the critical path delays were increased by more than 15%. Depending on the applications, this may or may not be acceptable. We could limit this delay penalty by increasing the channel width on the FPGA architecture. For the routing area overhead, we found the difference between a non-watermarked design and a watermarked design is not substantial. In some cases, the watermarked design actually consumed less wire area.

2 Product and Progress

In this research, we investigate the IP protection problem in an array-based FPGA design, which is receiving more popularity due to its fast time-to-market, reconfigurability, and the continuously increasing gate counts in commercial FPGA. Also due to the same fact, it is rather easy to duplicate such a design and compromise its IP copyright. We approach this problem by using a watermarking technique which will embed a hidden, unique routing pattern inside the design being protected by modifying the routing cost function using an input signature given by the designer. Later on, the designer or provider will be able to check the authenticity of the design by reversing the signature. We have completed the following tasks:

- We analyzed an open-source placement and routing tool (VPR) for array-based FPGA.
- We designed a new cost function which takes a given signature into account. This function will be used to guide the routing process.
- We integrated the watermarking-based cost function into the routing process of the VPR tool and performed different experiments to evaluate the effectiveness, the false positives, the timing impact, and the area / wire overheads.
- Most of the benchmark circuits we experimented did not incur any area overhead. However, critical path delay could be increased depending on the routability (i.e., an indirect consequence of circuit complexity), the capacity of the FPGA used (i.e., the channel width provided), and the input signature used.

- Note that, VLSI routing is an NP hard problem. Under certain circumstances, our watermarking based routing algorithm may fail to complete as we observed even though they accounted for a very small portion in our experiments. The reason has been that it does not have enough nets to modify. This problem could be worked around by trying different signatures or modifying the constraints in other cost functions such as performance or area objectives.

3 Research and Teaching Skills and Experience

During this research thrust, the students require to learn multiple industry and academic tools to have our proposed technology carried out successfully. Most of these tools are new to computer architecture researchers. It is also rather complex to analyze the code in order to implement our proposed routing mechanism for watermarking. The multifaceted tools include the following

- VPR (Versatile Place and Route) --- an automated placement and routing tool for array-based FPGA. The code is an open-source available in the public domain. Therefore, we can modify the routing algorithm with our proposed watermarking technique. VPR has also been included as one of the benchmark programs in the SPEC CPU2000 integer benchmark suite.
- MCNC (Microelectronics Center of North Carolina) benchmark --- this suite contains a collection of netlists (20 circutis) commonly used in CAD community for floorplanning studies. We used it to evaluate the quality and performance of our proposed watermarking technique.
- Xilinx ISE Foundation Software --- this is the complete tool provided by Xilinx for developing logic circuits on their FPGA and CLD products. It includes the entire integrated development environment and simulation infrastructure.

Among these tools, we spent the majority of the time in tracing and analyzing the source code of the VPR tool. We modified the portion related to routing algorithm to integrate our watermarking technique, which was done by adding our proposed signature cost function to the original routing cost function. A digital signature is generated in the post-processing stage using the rout file. As we demonstrated in our experiments, the extra steps to embed a watermark signature are insignificant from the performance standpoint. At our current stage, the critical path delays, in most of the cases, are not affected by our watermarking technique. Nonetheless, certain MCNC circuit benchmark was affected by as much as 15%. This drawback can be addressed by increasing the channel width on the FPGA architecture.