QR Pattern Driven Hardware Obfuscation and High-Level Transformations

Y.Nisha, S. Sangeetha, V.Kishore Kumar,
1, 2UG Students, 3Assistant Professor, Department Of ECE Apollo Engineering College, Poonamalle.

Abstract: In Recent Years Piracy Over Digital System Is Emerging And Hardware Security Is Aim To Thwart, Overbuilding. And Reverse Engineering (RE) By Obfuscating And/Or Camouflaging. However, These Techniques Incur High Complexity And Power Overheads, And Structural Changes Cannot Provide Any Protection For The Gate-Level Netlist Of The Third Party Intellectual Property (IP) Core Or The Single Large Monolithic IC. In Order To Circumvent These Weaknesses, In This Work We Carried Out QR Code Pattern Driven Functional Obfuscation And Elaborately Analyzes Security Levels And Proposes A Practical Logic Obfuscation Method Over FIR DSP Digital Design With Low Overheads Which Prevents An Adversary From RE Both The Gate-Level Netlist And The Layout-Level Geometry Of IP/IC And Protect IP/IC From Piracy And Overbuilding. Experimental Evaluations Demonstrate The Low Area, Power, And Zero Performance Overhead Of The Proposed Obfuscation Technique.

Keywords: Finite State Machine (FSM), Register Transfer Level (RTL), Intellectual Property (IP) Etc.

I. INTRODUCTION

II. HIGH LEVEL TRANSFORMATION

A Supply Chain Adversary is an insider who is involved in the design and manufacturing of a hardware device. The tamper capability is based on his role in the supply chain, specifically, his read and write permission in the design and the manufacturing process of a specific device. An IP provider [4] or a designer for a specific module may have limited access to the design, while a foundry or a chip-level integration designer has access to the whole device design. The general lack of access control in today's supply chain further facilitates an adversary to gain knowledge of a design and launch attacks. Besides based on his role in the supply chain, a supply chain adversary may gain further knowledge of a design by probing, testing, side-channel analysis, or reverse engineering. The state-of-the-art VLSI Logic Encryption/Locking techniques [2] include combinational logic locking and finite-state machine (FSM) locking. Combinational logic locking augments a combinational logic network [3] with an additional group of lock inputs such that the augmented combinational logic network has the same function as the original combinational logic network only if a specific vector (aka a valid key) is applied to the lock inputs. The simplest combinational logic locking technique is to insert XOR and XNOR gates into a combinational logic network. An adversary knows which inputs are functional inputs and which inputs are lock inputs. He can then identify the lock gates connected to the lock inputs. If a total of M lock gates are inserted in a combinational logic network, the complexity for an adversary to find the correct logic may not be 2^M. If a lock input is connected to a lock gate that is not a XOR or XNOR gate, the key to the lock input is implied to be the non-controlling logic value of the lock gate. An adversary may then easily obtain the key, unless the lock input is connected to multiple lock gates and is implied to have conflicting logic values. For example, the lock input is connected to a group of AND gates and a OR gate which have the same function as a XOR or XNOR gate.

2.1 DSP CIRCUIT OBFUSCATION APPROACH

A novel DSP hardware protection methodology through obfuscation by hiding functionality via high-level transformations. This approach helps the designer to protect the DSP design [5] against piracy by controlling the circuit configuration among the generated variation modes. Figure 1 shows a reconfigurator reset re-set state MUX. Select signal connection 1 connection 2 connection K. Obfuscating configuration FSM key (switch instances).

Fig 1. FSM Based Confusion Metrics Architecture

Fig 2. Functional Block Diagram
2.2 Obfuscation Steps Involved

Step 1: DSP Algorithm. This step generates the DSP algorithm based on the DSP application [3].

Step 2: High-Level Transformation Selection. Based on the specific application, appropriate high-level transformations should be chosen according to the performance requirement (e.g., area, speed, power or energy).

Step 3: Obfuscation Via High-Level Transformation. Selected high-level transformations are applied simultaneously with obfuscation where variation modes and different configurations of the switch instances are designed.

Step 4: Secure Switch Design. The secure switch is designed based on the variations of high-level transformations. Note that different configuration data could be mapped into the same mode, which only involves simple combinational logic synthesis.

Step 5: Two-Level FSM Generation. The reconfigurator and the obfuscating FSM are incorporated into the DSP design as shown in Fig. 2. The configuration key is generated at this step.

Step 6: Design Specification. This step includes the HDL and netlist generation and synthesis of the DSP system. The proposed design methodology does not require significant changes to established verification and testing flows. In fact, the obfuscated DSP circuit with the correct key behaves just like the original circuit.

2.3 COLOR QR Code Generation

QUICK Response (QR) Codes [1], [2] have rapidly emerged as a widely used inventory tracking and identification method in transport, manufacturing, and retail industries [3]. Each QR code symbol consists of an encoding region, alignment patterns, and function patterns, as shown in Fig. 1. Function patterns include finder, separator, and these are not used for encoding the data. These are detected with several versions from version 1 to version 40.

The encode steps of QR code are shown below. Firstly, input data is encoded in a formatted bit stream in an efficient mode. The bit streams which are obtained by encoding the data are divided into code words. These code words are again divided into sets of blocks, and error correction level is added to all the set of blocks.

Step 1.1 — Transform Message M into a bit stream B of codes;

Step 1.2 — Transform every three bits of B into four bits and represent them by a binary pattern block, resulting in a pattern image IP;

Step 1.3 — Modulate each pattern block Ti of IP by two representative values calculated from the Y-channel values of the corresponding block Bi of target image IT, yielding a modulated pattern image IP';

Step 1.4 — Replace the Y-channel of target image IT with IP' to get a signal-rich-art code image IC as the output. In the second phase, given a camera-captured version IC of a paper or display copy of the signal-rich-art code image IC, a message M', which is supposed to be identical to M, is extracted from IC' by four major steps:

```
Fig. 3 Color QR Code Generation
```

International Conference On Progressive Research In Applied Sciences, Engineering And Technology (ICPRASET 2K18)
III. IMPLEMENTATION

High-Level Transformations Also Allow Design Of Circuits Using Same Data Path But Different Control Circuits. For Example, A Data Path May Implement A 3rd-Order Or A 6th-order Digital Filter, Or In General A (3l) Th-Order Filter, Where L Is A Positive Integer. These Correspond To Different Modes. While These Modes Generate Outputs That Are Functionally Incorrect, These May Represent Correct Outputs Under Different Situations, Since The Output Is Meaningful From A Signal Processing Point Of View. Finally, Other Modes Lead To Non-Meaningful Outputs. The Initialization Key And The Configure Data Must Be Known For The Circuit To Work Properly. Consequently, The Circuit Behaves As An Obfuscated Circuit.

![Color QR Code](Fig. 4: Color QR Code)

![FSM States](Fig. 5: FSM States)

![RTL Viewer](Fig. 6: RTL Viewer)

### Table 1 Hardware Complexity Report Comparison Using Cyclone III Family Devices

<table>
<thead>
<tr>
<th>Type</th>
<th>AREA</th>
<th>SPEED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type_1 (state: off)</td>
<td>513</td>
<td>317.16MHz</td>
</tr>
<tr>
<td>Type_2 (state: optimal)</td>
<td>512</td>
<td>59.66MHz</td>
</tr>
</tbody>
</table>

IV. CONCLUSION

In This Work, We Proved The Efficiency Of Structural And Functional Obfuscation By Utilizing High-Level Transformation Techniques With Variation In Modes. Here We Construct The Secure Reconfigurable Switch Design Which Will Increases Hardware Complexity Slightly As The As Compared To Existing Method. Compared With All Other Existing Obfuscation Methods, In Our Proposed Methodology, The Generation Of QR Code Followed By Multi Key Extraction Will Give Non-Meaningful Variation Modes In Levels. We Analyze The Complexity Trade-Off Between Numbers Of States In FSM Over Complexity. Finally In Order
To Reduce The Hardware Complexity Without Compromising Speed And Area QR Code Were Used And Its Efficiency Is Proved Through Hardware Synthesis.

REFERENCES


