STACK BASED CONFIGURABLE LOGIC GATES TECHNOLOGY FOR IP CORES

D.Keerthana[1], K.Rajesh[2]

[1]PG scholar, SSM Institute of Engineering and Technology, Dindigul
[2]Assistant professor SSM Institute of Engineering and Technology, Dindigul

--***--

Abstract - Nowadays Logic locking is a promising proactive defense strategy against intellectual property (IP) piracy, counterfeiting, hardware Trojans, reverse engineering, and overbuilding attacks. Logic encryption is also preventing the hardware Trojans insertion which has the entire design is no longer known to an adversary and also making it more difficult to insert a Trojan without causing unintended actions which is more readily detected. To provide a method to increase IC security against a multitude of threats in combinational logic encryption, the current logic encryption techniques has a high usage of power, and area. In this paper, a novel gate level implementation of logic encryption is proposed which is significantly reduces the per-gate overhead of encrypting a gate. Logic encryption method is presented for enhancing security against such threats. In this paper, a novel stack based configurable gate level logic encryption technique is presented with reduced per-gate overheads significantly. The proposed technique also expands the search space of a key sequence and also by increasing the difficulty for an adversary to extract the key value. The proposed technique has been implemented with the comparison of benchmark circuits and also results as a minimum overhead of area and delay increment.

Key Words: Encryption, stack, key gate

1. INTRODUCTION

Due to the drastic increase of complexity in IC fabrication and/or maintaining a foundry with advanced manufacturing capabilities, many semiconductor companies are becoming fabless. Such companies designed integrated circuits (IC) and send the IC's to an advanced foundry, which is usually an off-shore manufacturing. Criticality of recent trend has forced companies to buy several IC intellectual property (IP) blocks to use it in their systems-on-chip and overall the IP blocks are distributed worldwide.

Globalization of the IC design industry has led to different kinds of hardware attacks. An attacker can reverse engineer the functionality of an IC/IP and then steal and claim ownership of the IP. Some of the unauthorized IC fabrication company may also overbuild ICs and sell the IC illegally. Finally, the unwanted circuits may insert malicious circuits into the design without the knowledge of designer. Therefore, the semiconductor industry loses $4 billion annually due to the attacks. Such attacks have led IP and IC designers to re-evaluate in hardware's trust.

Each and every IC/IP designer has an additional responsibility to protect an individual design. If a designer is able to cover the IC's functionality while it passes through the different, potentially untrustworthy design flow, these attacks can be thwarted. To overcome these issues, the logic encryption concept is proposed. Logic encryption is the process of hiding the functionality and the implementation of a hardware design by inserting some additional gates called *key-gates* into the original design. In order to find a correct functionality, the valid key has to be supplied to the encrypted design. By applying a wrong key, the encrypted design will produce wrong outputs.

In this paper, the NAND/NOR stack based logic encryption is proposed to reduces the area, power, and performance overheads of utilizing the stack-based approach. This paper is structured as follow: Section II illustrated the literature survey based on proposed approach. In section III presented a preliminaries approach based on logic locking methodology. Section IV presented the experimental results and discussions and section V concluded the paper.

II. LITERATURE SURVEY

Yingjie Lao et al [1] presented an approach to design obfuscated circuits for digital signal processing (DSP) applications using high-level transformations, a key-based obfuscating finite-state machine (FSM), and a reconfigurator.

Lannanluo et al [2] proposed a binary-oriented, obfuscation-resilient binary code similarity comparison method based on a new concept, longest common subsequence of semantically equivalent basic blocks, which combines rigorous program semantics with longest common subsequence based fuzzy matching.