INTISARI

Rancang Bangun Rangkaian *Logic Locking* Dengan Basis *Deceptive* Multiplekser Dan Blok *Anti-Sat* Pada *Field Programmable Gate Array*

Oleh

Muhammad Rizqy Dharmawan
20/459179/PA/19840

Pengamanan perangkat keras menjadi suatu hal yang perlu dipertimbangkan. Pengamanan *intellectual property* (*IP*) menjadi salah satu bagian penting dalam pengamanan perangkat keras. *Logic locking* merupakan metode pengamanan *IP* paling mudah dilakukan. Terdapat kerentanan *logic locking* terhadap *SAT-Attack* dan *learning attack*. Blok *anti-SAT* merupakan metode paling baik dalam mengatasi *SAT-Attack* dan *D-Mux* merupakan metode yang dapat menanggulangi *learning attack*. Permasalahan utama adalah kedua metode ini tidak dapat diimplementasikan secara langsung dengan menjaga fungsionalitas kedua metode tersebut. Penelitian ini bertujuan merancang skema integrasi kedua metode tersebut dengan menghubungkan sinyal-sinyal yang diolah oleh *D-Mux* menjadi kunci dari blok *Anti-SAT*.

Pengujian yang dilakukan berupa pengujian fungsionalitas dan pengujian *overhead* untuk mengetahui karakteristik penggunaan *resource* yang digunakan oleh rankaian *logic locking* sendiri. Pengujian fungsionalitas menunjukkan implementasi rancangan *logic locking* tetap mempertahankan fungsionalitas asli rangkaian dan dapat mengamankan fungsionalitas dengan menggunakan kunci logika. Pengujian *overhead* mendapati bahwa perbandingan penggunaan *resource* dari *logic locking* sangat bergantung pada variabel kompleksitas (perbandingan *LUT* dengan *I/O*) dimana semakin kompleks rangkaian akan membuat *overhead* semakin kecil dan tren penurunannya bersifat eksponensial.

Kata kunci : *Hardware Seurity, Logic Locking, SAT-Attack, Machine Learning Attack, FPGA*

ABSTRACT

Design Of A Logic Locking Circuit Utilizing Deceptive Multiplexer Base And Anti-Sat Blocks On Field Programmable Gate Array

by

Muhammad Rizqy Dharmawan
20/459179/PA/19840

Hardware security is something that needs to be considered. Securing intellectual property (IP) is an important part of securing hardware. Logic locking is the easiest IP security method to do. There are vulnerabilities of logic locking against SAT-Attack and learning attack. Anti-SAT block is the best method to overcome SAT-Attack and D-Mux is a method that can overcome learning attack. The main problem is that these two methods cannot be implemented directly while maintaining the functionality of both methods. This research aims to design an integration scheme of the two methods by connecting the signals processed by the D-Mux to the key of the Anti-SAT block.

The tests carried out are in the form of functionality testing and overhead testing to determine the characteristics of resource usage used by the logic locking circuit itself. Functionality testing shows that the implementation of the logic locking design maintains the original functionality of the circuit and can secure the functionality by using a logic lock. Overhead testing found that the comparison of resource usage of logic locking is highly dependent on the complexity variable (ratio of LUT to I/O) where the more complex the circuit will make the overhead smaller and the downward trend is exponential.

Keywords: Hardware Security, Logic Locking, SAT-Attack, Machine Learning Attack, FPGA