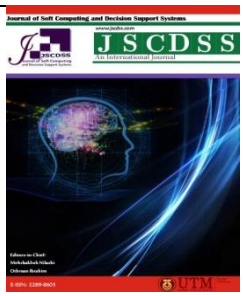
An International Journal
JSCDSS
http://www.jscdss.com
Vol.8 No.4 August 2021: 11-15
Article history:
Accepted 30 July 2021
Published online 30 July 2021

Journal of Soft Computing and Decision Support Systems



E-ISSN: 2289-8603

A Novel Circuit Level Polymorphism for Hardware Watermarking to Intellectual Property Protection

Mohsen Bagheri Zefrei [a,*], Tofigh Asbaghi [a], Mehrshad Khosraviani [a,b]
[a] Amirkabir University of Technology, Department of Computer Engineering, Tehran, Iran
[b] Institute of Higher Education MehrAlborz, Department of IT Engineering, Tehran, Iran

*** Corresponding author email address**: mohsen.baghei@aut.ac.ir

Abstract

Watermarking is a powerful approach for Intellectual Property (IP) protection is studied in this paper. The polymorphic gates are the circuit cells that provide special capabilities regarding the special input-output set which is applied to some control switches. It is known as a powerful technique to withstand reverse-engineering attacks. Using this hardware-based security approach, the attackers cannot distinguish the features of polymorphism that is created to protect the Integrated Circuits (ICs). In this paper, an area and power-efficient polygate circuit is proposed consisting of simple, moderately complex, and highly complex logic functions as a circuit output which could be altered in terms of logical functionality by applying different input control codes. This hardware encryption is set by the designer of the IC in the implementation phase. The proposed polygate circuit of this paper is very compact and complex, moreover, it provides the capability of IC break-out in untrusted uses of the IC.

Keywords: Polygate, Polymorphism, Intellectual Property Protection, Integrated Circuits, Hardware Watermarking

1. Introduction

Globalization of IC creation has driven to visit copyright encroachments and illicit possession claims on Intellectual Property (IP). The utilization of self-checking circuits is vital to different applications these days. Coordinates Circuit (IC) and chip plan have truly been recognized as a security hazard by industry and government (Sekanina, 2007). To demonstrate the possession of an IP in a court of law, the first originator can appear a subtly hidden signature or its watermark within the erroneously claimed ICs. With a blend of trusted and untrusted on-screen characters within the IC supply chain, organizations put extraordinary confidence in manufacturing smart systems since conveyed plans are vulnerable to a few security risks. This signature ought to be defended in an unambiguous way (Rai, Rupani, Nath, & Kumar, 2019).

These dangers incorporate the capacity of a noxious turnaround design to alter with the created circuit, duplicate or fake the complete designer plan, or offer the IP to interested third parties(Wang et al., 2018). Because it is assumed that fault-tolerance issues will be more vital within the period of Nan electronics, the use of this sort of circuit will certainly develop. Self-checking circuits are customarily developed by including checking rationale around an unmodified unique yield of the circuit. Assurances against malevolent invert building, cloning, and Trojan addition are shifted(Ruzicka & Simek, 2012).

Watermarking is exploited to avoid such wrong possession claims. There have been a few works on watermark (Ruzicka & Simek, 2012), but most of them bargain with including algorithmic imperatives to implant the designer's signature at different stages of rationale or physical amalgamation. Encouraged real overhead in terms of circuit parameters has not been talked about in detail (Roy, Koushanfar, & Markov, 2010).

Untrusted manufacturing facilities are studied in the literature repeatedly, and for the last-mentioned case, noxious turnaround engineers who have performed essential and adequate equipment recuperation are investigated. The ill-disposed objective, in this case, decreases to show how much data almost related to the logic plan, component arrangement, and IP of the first circuit can be recouped. Securities against pernicious turnaround building, cloning, and Trojan inclusion are changed (Zhang & Liu, 2017). Polymorphic gates and circuits are components that are planned with physical properties that can be utilized to cause the same electronic component, given the same set of inputs. Multifunction components have a wide run of applications in evolvable equipment plans that permit circuits to perform distinctive