

Centrality Indicators For Efficient And Scalable Logic Masking

Brice Colombier, Lilian Bossuet
Univ Lyon, UJM-Saint-Étienne, CNRS
Laboratoire Hubert Curien UMR 5516
F-42023, Saint-Étienne, France

`{b.colombier,lilian.bossuet}@univ-st-etienne.fr`

David Hély
Univ. Grenoble Alpes, LCIS
F-26000, Valence - France
`david.hely@lcis.grenoble-inp.fr`

Abstract

Modifying the logic at register transfer level can help to protect a circuit against counterfeiting or illegal copying. By adding extra gates, the outputs can be controllably corrupted. Then the circuit operates correctly only if the right value is applied to the extra gates. The main challenge is to select the best position for these gates, to alter the circuit's behaviour as much as possible. However, another major point is the computational efficiency of the selection process, which should be as good as possible for integration in EDA tools. State-of-the-art methods, based on fault analysis, are very demanding and cannot cope with large netlists in a reasonable runtime. We propose to use centrality indicators instead. Centrality is used to identify the most significant vertices of a graph. We show that, when used to select the nodes to modify, they lead to low correlation between original and altered outputs while being computationally efficient. We give experimental results on combinational benchmarks and compare to other previously proposed heuristics. We show that this method is the only efficient selection heuristic that is able to handle large netlists and integrate smoothly into EDA tools.