Mathematical modelling of Logic Locking against the insertion of Hardware Trojan in an Intregated Circuit

Jonathan Fontaine, Lilia Zaourar, Roselyne Chotin

Mathematical modelling of Logic Locking against the insertion of Hardware Trojan in an Intregated Circuit.

Jonathan Fontaine, CEA LIST, LECA, France. jonathan.fontaine@cea.fr

Lilia Zaourar, CEA LIST, LECA, France. lilia.zaourar@cea.fr

Roselyne Chotin, Sorbonne Université, LIP6, France roselyne.chotin@lip6.fr

Nowadays, the increasing complexity of electronic devices has led to increase their cost. Therefore, several external agents ensure a part of the production of an Integrated Circuit (IC). A new threat has emerged from those companies. Checking that an IC works as specified by the designer and is not doing secret tasks is very difficult. In fact, it is possible to add electronic component to a malicious purpose, named Hardware Trojan (HT). This is a major security issue, especially for IC used in critical fields as transportation, health or military. It can be information leakage, material deterioration or denial of service. A solution to avoid that is to use Logic Locking. This method use a numeric key to lock the IC, which is only known from the designer. The aim is to obfuscate the logic function of the IC for untrusted party. Its purpose is to increase the security of the IC while limiting the impact on power consumption, critical path and area. The aim of this work is to model logic locking as an optimization problem. We represent the IC by a graph and express the set of constraints with a non-linear model. We first solved it exactly by linearization for small instances and we implemented a heuristic for larger ones. It compute for each pair of vertices the notion of pairwise secure. Then get all the maximum cliques. Finally, select the largest cliques, until reaching fixed keychain limit. We will present the numerical results and the prospects for improvement.