An open CAD flow to optimised key gate insertion in logic locking

Roselyne Chotin[1] and Lilia Zaourar[2]

[1]roselyne.chotin@lip6.fr - Sorbonne Université, CNRS, LIP6, France
[2]lilia.zaourar@cea.fr - Université Paris-Saclay, CEA, List, France

The increasing complexity of Integrated Circuits (ICs) leads to an increase in production costs. To limit this increase, parts of the design and manufacturing are delegated to third party companies. The loss of control over these steps increases the risk of threats such as theft of dedicated hardware blocks (IP), overproduction of ICs, and insertion of Hardware Trojan (HT).

To counteract these risks, methods called Desgin for Hardware Trust (DfHT) have been developed. Their goal is to guarantee the proper functioning of ICs despite the use of unreliable IP blocks and manufacturing in an unreliable foundry. In order to widly use these safety-related methods, they must be integrated into the design flow. Furthermore, to have a full control of the design phase, integrating this kind of methodology in an open Computer Aided Design (CAD) flow, can be helpfull.

Logic locking has emerged as a promising DfTr solution to counteract overproduction [1, 2]. This method adds logic gates in the circuit, connected to an unreadable memory that serves as a digital key. This allows to block any illicit use of the circuit. Thus, IC security is ensured. However it includes the counter-costs that are delay, area, and power consumption.

We propose a framework dedicated to security that can be integrated into the conventional IC design flow. To integrate our methodology, we use open source tools as Yosys for synthesis [3] and Coriolis [4] for circuit database usage. In particular, we study strong logic locking techniques to improve key-gates insertion. The aim of logic locking is to lock the functionality of the circuit by modifying the gate level netlist, obtained after logic synthesis in a conventional IC design flow, through key gates insertion. The goal of our methodology, is to take into account, as early in the design phase, both countermeasures against HTs and performance, to ensure that the System on Chip (SoC) behavior is guaranteed despite untrusted IPs vendors or foundry. Towards this objective, this work envisions to establish and evaluate security properties and then integrate them during synthesis with multi-objective optimization techniques, which are based on a mathematical modeling of the problem that takes into account both the performance and the HTs‘ effects. It is indeed necessary to find a good compromise between the level of security sought after and performance. The methodology is validated on several use cases. In this way, the SoC will enable cybercrime avoidance without a significant additional cost.

Our security mesure is calculated as in [5] which rely on the size of the cliques present in the interference graph of the circuit. In order to optimize this mesure while keeping IC performance reasonnable, we propose different approches. Our first method models the key-gates insertion problem and its exact resolution, as well as an heuristic approach. The results show that we can obtain a good solution with an Hamming distance around 40% in a computation time of less than 40 min (for the largest bench).

Our methodology is successfully integrated in a standard open CAD flow using Yosys and Coriolis. Yosys synthetizes the Register Transfert Level (RTL) description of the circuit and then Coriolis can manipulate the obtained netlist to add the key gates to the points given by the resolution of the key-gates insertion problem to produce the locked netlist.

This work is a part of the project MOOSIC ANR-18-CE39-0005, funded by The French National Research Agency.

References

[1] Jeyavijayan Rajendran et al. “Security Analysis of Logic Obfuscation”. In: *ACM/IEEE Design Automation Conference (DAC)*. 2012, pp. 83–89.

[2] Sophie Dupuis et al. “A novel hardware logic encryption technique for thwarting illegal overproduction and Hardware Trojans”. In: *IEEE 20th International On-Line Testing Symposium (IOLTS)*. July 2014, pp. 49–54.

[3] Clifford Wolf, Johann Glaser, and Johannes Kepler. “Yosys-a free Verilog synthesis suite”. In: *Proceedings of the 21st Austrian Workshop on Microelectronics (Austrochip)*. 2013.

[4] Christophe Alexandre et al. “TSUNAMI: An Integrated Timing-Driven Place And Route Research Platform”. In: *DATE 2005 - Design Automation and Test in Europe Conference*. Ed. by EDAA - European design and Automation Association. Vol. 2. Munich, Germany: IEEE, Mar. 2005, pp. 920–921.

[5] K Xiao et al. “Hardware Trojans: Lessons Learned after One Decade of Research”. In: *ACM Transactions on Design Automation of Electronic Systems* 22 (May 27, 2016), pp. 1–23.