A new key-gate insertion strategy for logic locking with high output corruption

Quang-Linh Nguyen, Sophie Dupuis, Marie-Lise Flottes

A new key-gate insertion strategy for logic locking with high output corruption

Quang-Linh Nguyen, Sophie Dupuis, Marie-Lise Flottes
LIRMM (Université de Montpellier – CNRS), Montpellier, France

***Abstract*— The outsourcing business model currently dominates the semiconductor industry. Ever-shrinking technologies have indeed raised the cost of manufacturing Integrated Circuits (ICs). Currently, constructing a fabrication plan with advanced technologies (5 nm to 3 nm) costs more than $10 Billions [1]. Therefore, outsourcing the fabrication process to offshore, but possibly unreliable, foundries has become a major trend [2]. This leads to possible security threats on hardware, such as IP piracy, Hardware Trojan insertion and IC overproduction [3].**

Logic locking has emerged as a solution to protect ICs against overproduction – An untrusted foundry fabricating more ICs than the required/ordered number in order to sell the excess on the black market. Logic locking consists in modifying the circuit structure with additional logic gates, driven by an added input pin: a key with a secret value, required for the IC to function properly [4]. For the past decade, logic locking has garnered tremendous attention from the research community [5]. Early research in logic locking focused on solutions based on key-gate insertion. One of the main goals of these techniques was to attain significant output corruption, so that a locked IC is unusable. In 2015, an oracle guided attack broke all previously proposed solutions [6], by discovering the value of the secret key thanks to a SAT solver and comparison of the outputs with the ones of an unlocked IC (the oracle). Subsequent locking methods therefore focused on thwarting this so-called SAT attack, often to the detriment of output corruption [5]. The computation time of this type of attacks indeed increases as corruption decreases. Most recent solutions have recently begun to propose a satisfactory compromise between output corruption and protection against the attack, making gate insertion algorithms aimed at maximizing corruption interesting once again [7].

In this presentation, we will present a scalable insertion strategy in which nets for insertion are chosen according to their *output corruption score*, computed by measuring the change in primary outputs' probabilities to be logic 0 or logic 1, upon the insertion of a key gate onto the net or not. Experimental results show that this insertion strategy achieves optimal results in the three output corruptions metrics evaluated – output corruption rate (the percentage of input vectors leading to errors at the output of a locked circuit), output corruption coverage (the maximum number of outputs bit that can be corrupted) and output corruptibility (the average Hamming distance between the output on applying any wrong key and the correct key) – while requiring much less execution time than FLL [8], the initial most effective key gate insertion strategy strategy in terms of output corruption.

Keywords—Logic Locking, Oracle Guided Attacks, Output Corruption, Overproduction.

ACKNOWLEDGMENT

This work has been funded by the French National Research Agency (ANR) under the project MOOSIC ANR-18-CE39-0005.

REFERENCES

[1] A. Shilov, Samsung Foundry: New $17 Billion Fab in the USA by Late 2023, https://www.anandtech.com/show/16483/samsung-in-the-usa-a-17-billion-usd-fab-by-late-2023.

[2] R. Kumar, "Simply Fabless!", IEEE Solid-State Circuits Magazine, vol.3, no. 4, pp. 8–14, 2011, ISSN: 1943-0590.

[3] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", Proceedings of the IEEE, vol. 102, no. 8, pp. 1207–1228, 2014.

[4] J. Roy, F. Koushanfar, I. Markov, "EPIC: Ending Pircay of Integrated Circuits", Design, Automation & Test in Europe (DATE), pp. 1069-1074, 2008.

[5] S. Dupuis, M.-L. FLottes, "Logic Locking: A survey of proposed methods and evaluation metrics", Journal of Electronic Testing, vol. 35, no.3, pp. 273-291, 2019.

[6] P. Subramanya, S. Ray, S. Malik, "Evaluating the security of logic encryption algorithms", IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 137-143, 2015.

[7] Q.-L. Nguyen, M.-L. Flottes, S. Dupuis, B. Rouzeyre, "On preventing SAT attack with decoy key-inputs", IEEE Computer Annual Symposium on VLSI (ISVLSI), pp. 114-119, 2021.

[8] J. Rajendra, H. Zhang, C. Zhang, G. S. Rose, Y. Pino, O. Sinanoglu, R. Karry, "Fault-anamysis-based logic encryption", IEEE Transactions on Computers, vol. 64, no. 2, pp. 410-424, 2015.