Efficient Protection of Design IP: Disguising the Interconnects

Satwik Patnaik, Mohammed Ashraf, Johann Knechtel, and Ozgur Sinanoglu

†Tandon School of Engineering, New York University, New York, USA
‡New York University Abu Dhabi, Abu Dhabi, United Arab Emirates
{sp4012, ma199, johann, ozgursin}@nyu.edu

Abstract—Ensuring the trustworthiness and security of electronics has become an urgent challenge in recent years. Among various concerns, the protection of design intellectual property (IP) is to be addressed, due to outsourcing trends for the manufacturing supply chain and malicious end-user. In other words, adversaries either residing in the off-shore fab or in the field may want to obtain and pirate your design IP. As classical design tools do not consider such threats, there is clearly a need for security-aware EDA techniques. Here we present novel but proven techniques for efficient protection of design IP, embedded in an industrial-level design flow using Cadence Innovus. The key idea in our work is that disguising the interconnects is supremely suitable to protect design IP, while inducing only little additional cost and providing strong resilience. We share our customized libraries with the community, and we demonstrate our design flow and its security measures.

I. BACKGROUND AND MOTIVATION

Design IP may be duplicated without consent, resulting in financial loss for the IP owner—it is estimated that several billions of dollars are lost each year owing to IP piracy [1]. The tools and know-how for reverse engineering (RE) are becoming more widely available, thus rendering the scenario of malicious end-user obtaining chip design IP a practical threat. Besides, adversaries in the fab can readily obtain the underlying IP from the design files given to them.

Different countermeasures have been proposed against IP piracy. To mitigate RE attacks, layout camouflaging (LC) seeks to alter the appearance of a chip such that it is arduous for the attacker to infer the chip’s real functionality [2]. The notion of split manufacturing (SM) is to split a layout into multiple parts (typically into FEOL and BEOL), and outsource only one part (typically the FEOL) [3], [4]. There are various shortcomings with prior art, limiting their practical value. Most LC schemes are costly, customized, ambiguous gates incur high PPA overheads, and adapting the FEOL manufacturing processes incurs commercial cost on top [2]. As for SM into FEOL and BEOL, there is a cost-security trade-off: the higher the split layer, the lower the commercial cost, but also the lower the resilience [3].

II. CONCEPTS AND METHODOLOGY

To advance both SM and LC, we developed novel techniques for judicious and well-controlled disguising of interconnects. As for SM, we implement three different strategies: lifting of nets to the BEOL, controlling the distances between open pin pairs, and addition of dummy nets (Fig. 1). Further, we promote a new metric, percentage controlling the distances between open pin pairs, and addition of nets, at least once higher PPA budgets are considered as acceptable. As for lifting and disguising nets further during SM, we demonstrate our scheme is more effective than naive lifting, both in terms of security and PPA cost [3]. We also found that our scheme excels prior art; a state-of-the-art attack experiences 0% correct connections (CCR), which is a first in the literature. Besides 0% CCR, we obtain a PNR that is 31% on average [3]. This translates to much better IP protection than prior art (with ≥ 89% PNR). Note that we may further reduce the PNR by lifting and disguising more nets, at least once higher PPA budgets are considered as acceptable.

In short, the objectives we addressed here are (i) splitting after higher metal layers, reducing the commercial cost of SM, (ii) generic and low-cost LC without the need to alter the FEOL, (iii) superior resilience against FEOL-fab-based adversaries and malicious end-user, and (iv) reasonable and controllable PPA cost. We believe that schemes like ours are essential to expedite IP protection in practice.

ACKNOWLEDGEMENTS

This work was supported in part by the Army Research Office (ARO) under Grant 65513-CS, and the Center for Cyber Security (CCS) at New York University NY/Abu Dhabi (NYU/NYUAD).

REFERENCES