Complete activation scheme for FPGA-oriented IP cores design protection

Brice Colombier, Ugo Mureddu, Marek Laban, Oto Petura, Lilian Bossuet, Viktor Fischer

Complete activation scheme for FPGA-oriented IP cores design protection

Brice Colombier[1], Ugo Mureddu[1], Marek Laban[2], Oto Petura[1], Lilian Bossuet[1], Viktor Fischer[1]
[1]Hubert Curien Laboratory, UMR CNRS 5516, University of Lyon, 42000 Saint-Étienne - France
{b.colombier, ugo.mureddu, oto.petura, lilian.bossuet, fischer}@univ-st-etienne.fr
[2]Department of Electronics and Multimedia Communications, Technical University of Košice, Park Komenskho 13
04120 Košice, Slovak Republic,
MICRONIC, Sliačska 2/C, 83102, Bratislava, Slovak Republic
laban@micronic.sk

***Abstract*—Intellectual Property (IP) illegal copying is a major threat in today's integrated circuits industry which is massively based on a design-and-reuse paradigm. In order to fight this threat, a designer must track how many times an IP has been instantiated. Moreover, illegal copies of an IP must be unusable. We propose a hardware/software scheme which allows a designer to remotely activate an IP with minimal area overhead. The software modifies the IP efficiently and can handle very large netlists. Unique identification of hardware instances is achieved by integrating a TERO-PUF along with a lightweight key reconciliation module. A cryptographic core guarantees security and triggers a logic locking/masking module which makes the IP unusable unless the correct encrypted activation word is applied.**

I. Graphical user interface

A user interface allows one to perform the following actions:

- Modify the IP, using logic masking [1] or logic locking [2] to make it controllably unusable. Several parameters can be tuned, as well as the area overhead.
- Obtain the reference response from the TERO-PUF [3].
- Reconcile the key with `CASCADE` [4] and activate the IP.

II. Demo scenario and observables

The typical demo scenario is the following. First, an IP in the form of a netlist is modified and the associated activation word (AW) is stored. The motherboard is then connected to the PC and the daughterboard is enrolled by obtaining a response from a PUF instantiated at a known location. This response is used to encrypt AW. The protected IP is instantiated on the enrolled daughterboard. Before activation, the IP does not operate correctly. When the activation phase starts, the key reconciliation procedure is conducted to ensure that the PUF response generated on the daughterboard is identical to the one obtained during enrollment. Then, AW is encrypted and sent to the board. It is then internally decrypted and sent to the logic masking/locking module, to make the IP fully operational. If the IP is instantiated on a different daughterboard, it does not operate correctly since the PUF response is different. Each IP is securely bound to a trusted hardware target.

Acknowledgments

The work presented in this paper was realized in the frame of the SALWARE project number ANR-13-JS03-0003 supported by the French "Agence Nationale de la Recherche" and by the French "Fondation de Recherche pour l'Aéronautique et l'Espace", funding for this project was also provided by a grant from "La Région Rhône-Alpes".

This project has also received funding from the European Unions Horizon 2020 research and innovation program under grant agreement no. 644052.

References

[1] J. A. Roy, F. Koushanfar, and I. Markov, "Epic: Ending piracy of integrated circuits," in *Design, Automation and Test in Europe*, 2008, pp. 1069–1074.

[2] B. Colombier, L. Bossuet, and D. Hély, "Reversible denial-of-service by locking gates insertion for IP cores design protection," in *IEEE Computer Society Annual Symposium on VLSI*, Montpellier, France, Jul. 2015, pp. 210–215.

[3] A. Cherkaoui, L. Bossuet, and C. Marchand, "Design, evaluation and optimization of physical unclonable functions based on transient effect ring oscillators," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1291–1305, 2016.

[4] B. Colombier, L. Bossuet, D. Hély, and V. Fischer, "Key reconciliation protocols for error correction of silicon PUF responses," *IEEE Transactions on Information Forensics and Security*, 2017.

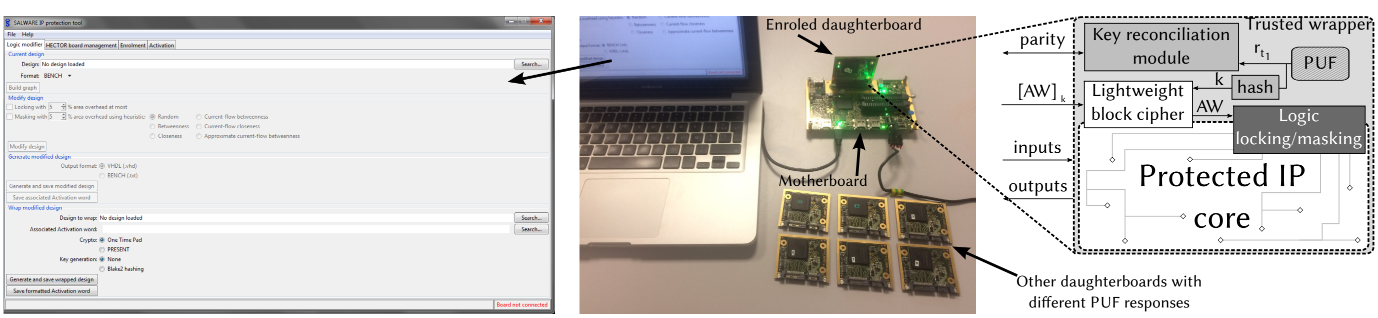

Fig. 1. Experimental setup showing the software user interface and the hardware wrapper added to the IP.