Functional Locking Modules for Design Protection of Intellectual Property Cores
Brice Colombier, Lilian Bossuet

To cite this version:

HAL Id: ujm-01164036
https://hal-ujm.archives-ouvertes.fr/ujm-01164036
Submitted on 17 Jun 2015
Functional Locking Modules for Design Protection of Intellectual Property Cores

Brice Colombier, Lilian Bossuet

*Hubert Curien Laboratory, UMR CNRS 5516, University of Lyon*
42000 Saint-Étienne - France
{b.colombier, lilian.bossuet}@univ-st-etienne.fr

I. INTRODUCTION

Electronics systems design is increasingly using Intellectual Property (IP) cores. The means, however, that can render the IP core unusable if it has been obtained illegally [1] have not yet been identified. We describe lightweight locking schemes lacking in the state of the art. In Section II we identify common locking points on an IP, before describing locking schemes in Section III. Section IV concludes.

II. LOCKING-BASED PROTECTION SCHEMES

Authentication and locking schemes can be combined to fight counterfeiting and overbuilding [2], [3]. In case the IP core was illegally obtained, a locking circuitry makes it unusable. Common features can be turned into locking schemes: the FSM [2] or the CPU, the I-O ports [4], the clock manager or the address part of the memory bus.

III. DESCRIPTION OF PROPOSED LOCKING SCHEMES

*Locking a finite state machine:* The first way to achieve functional locking is to add a pseudo-randomness source for scrambling. We can be scrambled to make read data unreliable. An LFSR is used as a pseudo-randomness source for scrambling. We need to carefully chose the LFSR feedback polynomial for a lightweight implantation, so that most of its coefficients are 0s, since each coefficient equal to 1 requires a XOR gate. The $n$ bits of the LFSR are then XORed with the $n$-bit address bus. Finally, a multiplexer selects the original address bus or the scrambled one.

*Phase-locked loop (PLL) reconfiguration:* Most modern FPGAs embed reconfigurable PLLs. The reconfiguration procedure, however, is specific to each FPGA vendor, and requires a proprietary module. The overhead is high, and can not be significantly reduced without replacing this module.

*Memory bus pseudo-random scrambling:* To functionally lock the circuit, the address part of the memory bus can be scrambled to make read data unreliable. An LFSR can be scrambled to make read data unreliable. An LFSR is used as a pseudo-randomness source for scrambling. We need to carefully chose the LFSR feedback polynomial for a lightweight implantation, so that most of its coefficients are 0s, since each coefficient equal to 1 requires a XOR gate. The $n$ bits of the LFSR are then XORed with the $n$-bit address bus. Finally, a multiplexer selects the original address bus or the scrambled one.

IV. CONCLUSION

We compared features of an IP that can be leveraged for functional locking. Clock-based locking is a flexible, powerful yet lightweight option. A balance between efficiency and resources is the main point addressed by the designer.

**Acknowledgement:** The work presented in this paper was realized in the frame of the SALW ARE 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".

REFERENCES


