Mixed-Signal IP Protection Against Piracy Based on Logic Locking
Julian Leonhard, Marie-Minerve Louërât, Hassan Aboushady, Ozgur Sinanoglu, Haralampos-G. Stratigopoulos

To cite this version:
Julian Leonhard, Marie-Minerve Louërât, Hassan Aboushady, Ozgur Sinanoglu, Haralampos-G. Stratigopoulos. Mixed-Signal IP Protection Against Piracy Based on Logic Locking. 32. GI / GMM / ITG - Workshop Testmethoden und Zuverlässigkeit von Schaltungen und Systemen, Feb 2020, Ludwigsburg, Germany. hal-02465996

HAL Id: hal-02465996
https://hal.archives-ouvertes.fr/hal-02465996
Submitted on 4 Feb 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Mixed-Signal IP Protection Against Piracy Based on Logic Locking
Julian Leonhard*, Marie-Minerve Louërât*, Hassan Aboushady*, Ozgur Sinanoglu‡, Haralampos-G. Stratigopoulos*
Sorbonne Université, CNRS, LIP6, Paris, France
New York University Abu Dhabi, Abu Dhabi, UAE

I. INTRODUCTION

During its lifetime an integrated circuit (IC) may be subjected to various types of attacks. Threats can be categorized into Hardware Trojans, reverse engineering, counterfeiting, and side-channel attacks [1]. Hardware security aims at understanding security breaches in ICs and developing mechanisms for detecting attacks or preventing them by implementing countermeasures for on-chip resilience. Hardware security has been studied extensively for digital ICs recently, but for analog, mixed-signal, and RF ICs the solution space is still largely unexplored [2].

In this work, we focus on the problem of IC/IP piracy, which includes reverse engineering and counterfeiting. In particular, we develop a countermeasure for mixed-signal IC/IP piracy that is based on design locking. Locking aims at modifying the design, in order to introduce \( k \) key bits. There is only one valid combination of key bits, i.e. the secret key, that can result in correct functionality for any input. Otherwise, if an invalid key is applied, then the functionality will be corrupted for some or all inputs.

There are various techniques for locking digital ICs, known as logic locking techniques. The earliest logic locking techniques aimed at inserting key-gates into the design [3], i.e. XOR and XNOR gates, controlled by the key bits. Researchers are working in parallel trying to show the vulnerabilities of existing logic locking techniques, proposing attacks that can break them: (i) The brute-force attack sequentially applies keys until the valid one is found; (ii) The SAT attack, the most lethal attack based on a Boolean satisfiability solver, can recover the secret key with very reasonable effort [4]; (iii) Removal attacks aim at identifying and removing the added protection logic; (iv) Approximate attacks aim at extracting a key that establishes an incorrect yet approximate functionality. The most recent state-of-the-art logic locking technique is Stripped-Functionality Logic Locking (SFLL) [5] and provides quantifiable resilience against these attacks.

Locking analog ICs is very challenging as the key bits need to be introduced in a way that nominal performance is not degraded. Techniques for locking of analog ICs are proposed in [6]–[8], [10], [11] and are illustrated in Fig. 1. Specifically, in [6], a locking technique for sense amplifiers is proposed based on locking the body biasing of the transistor input pair. The locking mechanism is based on an architecture that comprises memristor crossbars. In [7], it is proposed to replace transistors within the biasing circuit with parallel-connected transistors whose gates are controlled by key-bits. The key-bits enable transistors whose aggregate width equals that of the original transistor. In [8], it is shown how to redesign the current mirrors providing the biasing so as to insert key-bits. In [10], it is proposed to lock the calibration feedback loop via logic locking of the digital optimizer that is part of the loop, such that it generates the wrong tuning settings unless the valid key is applied. In [11], it is proposed to add on-chip a neural network that is trained to map the secret analog key, which is in the form of analog DC voltages presented as inputs to the neural network, to the correct biases.

The secret key management scheme is common for all locking techniques and includes storing the secret key on-chip or generating it on-chip; in the latter case, a Physical Unclonable Function (PUF) can be utilized to even produce chip-unique keys.

In this work, we propose a technique called MixLock that is based on locking a mixed-signal circuit via logic locking of its digital section [9].

II. MIXLOCK

MixLock aims at securing mixed-signal IPs against piracy through a logic locking mechanism applied to the circuit’s digital section, as illustrated in Fig. 1(d). Only when the valid key is provided the mixed-signal circuit performs its intended function. Otherwise, for invalid keys the mixed-signal performances are pushed outside of their specification, i.e., they are locked.

![Fig. 1. Locking techniques for analog ICs: (a) locking biases based on memristor crossbars [6]; (b) obfuscating biasing transistors [7]; (c) locking of current mirrors [8]; (d) locking mixed-signal circuits via logic locking of their digital section [9]; (e) logic locking of the digital optimizer in the calibration feedback loop [10]; (f) locking through neural network-based biasing [11].]
MixLock presents several appealing properties. It is non-intrusive since it does not alter the analog section, which is key for its wide adoption by designers. Modifications in the digital section do not affect mixed-signal performance either. It incurs low area and power overheads since area and power are dominated by the analog section which is left intact. It is fully-automated since logic locking adds only one extra synthesis step. Finally, this concept is applicable to a wide range of mixed-signal circuits such as PLLs, RF transceivers, data converters, etc.

Breaking Mixlock will require either recovering the secret key via a logic locking attack or trying to unlock directly mixed-signal performances by applying an iterative multi-objective optimization algorithm. The latter is unlikely to succeed since mixed-signal performances do not show a smooth monotonic relationship with the key bits. Regarding the former attack, Mixlock is independent of the underlying logic locking technique, but to achieve strong digital security Mixlock uses the state-of-the-art SFLl logic locking mechanism [5].

III. RESULTS AND DEMONSTRATOR

To demonstrate MixLock, we used as case study a bandpass (BP) Σ∆ ADC whose block-level schematic is shown in Fig. 2. A Σ∆ ADC is decomposed into a Σ∆ modulator, which is the analog section, and a decimation filter, which is the digital section. In this case, Mixlock naturally locks the decimation filter. SFLL was used to guarantee strong digital security; in particular, a 64-bit resilience against the SAT attack was obtained. By simulating thousands of randomly chosen invalid keys we confirmed that Mixlock achieves strong analog security; in particular, the main Signal-to-Noise Ratio (SNR) performance was degraded dramatically below its specification. Fig. 3 considers an arbitrarily selected incorrect key and compares the transient and frequency responses of the unlocked and a locked Σ∆ ADC. The locked Σ∆ ADC presents a large amount of glitches in its transient response, which translate to a high noise floor in the frequency response, resulting in corrupted SNR.

In addition, we demonstrated Mixlock in an audio application [12]. The demonstrator, illustrated in Fig. 4, emulates a microphone for capturing a sound source, signal processing for digitizing the input audio, and a speaker for listening back the sound source. MixLock is used to lock the Σ∆ ADC in the signal processing chain. The effect of locking on audio quality can be measured by the glitches introduced from the locking operation that can be heard as noisy “cracks”. This demonstrator helps us in essence to listen to the effect of locking. Audio samples include speech recordings in German and English and professional music recordings of various genres. The interested reader can download and listen to the output audio samples from this link: https://nuage.lip6.fr/s/CYowe89aXBe6rP. The downloadable archive includes the output audio samples in the case of the unlocked design, where the valid key is applied, and locked designs where a random invalid key is applied.

ACKNOWLEDGMENTS

This work has been carried out in the framework of the ANR STEALTH project with No ANR-17-CE24-0022-01. J. Leonhard has a fellowship from the doctoral school EDITE de Paris.

REFERENCES