Leveraging Layout-based Effects for Locking Analog ICs

Muayad J. Aljafar
Tallinn University of Technology
Tallinn, Estonia
muayad.al-jafar@taltech.ee

Marie-Lise Flottes
Université de Montpellier (UM) - CNRS
Montpellier, France
marie-lise.flottes@lirmm.fr

Florence Azais
Université de Montpellier (UM) - CNRS
Montpellier, France
florence.azais@lirmm.fr

Samuel Pagliarini
Tallinn University of Technology
Tallinn, Estonia
samuel.pagliarini@taltech.ee

ABSTRACT

While various obfuscation methods exist in the digital domain, techniques for protecting Intellectual Property (IP) in the analog domain are mostly overlooked. Understandably, analog components have a small footprint as most of the surface of an Integrated Circuit (IC) is digital. Yet, since they are challenging to design and tune, they constitute a valuable IP that ought to be protected. This paper is the first to show a method to secure analog IP by exploiting layout-based effects that are typically seen as undesirable detractors in IC design. Specifically, we make use of the effects of Length of Oxide Diffusion and Well Proximity Effect on transistors for tuning the devices’ critical parameters (e.g., $g_m$ and $V_{th}$). Such parameters are hidden behind key inputs, akin to the logic locking approach for digital ICs. The proposed technique is applied for locking an Operational Transconductance Amplifier. In order to showcase the robustness of the achieved obfuscation, the case studied circuit is simulated for a large number of key sets, i.e., >50K and >300K, and the results show a wide range of degradation in open-loop gain (up to 130dB), phase margin (up to 50 deg), 3dB bandwidth ($\approx$2.5MHz), and power ($\approx$1mW) of the locked circuit when incorrect keys are applied. Our results show the benefit of the technique and the incurred overheads. We also justify the non-effectiveness of reverse engineering efforts for attacking the proposed approach. More importantly, our technique employs only regular transistors and requires neither changes to the IC fabrication process nor any foundry-level coordination or trust.

CCS CONCEPTS
- Hardware → Analog and mixed-signal circuits; - Security and privacy → Hardware security implementation; Hardware reverse engineering.

KEYWORDS
Analog Obfuscation; Layout-based effects; Logic Locking; Hardware Security

ACM Reference Format:
Muayad J. Aljafar, Florence Azais, Marie-Lise Flottes, and Samuel Pagliarini. 2022. Leveraging Layout-based Effects for Locking Analog ICs. In Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security (ASHES ’22), November 11, 2022, Los Angeles, CA, USA. 9 pages. https://doi.org/10.1145/3560834.3563826

1 INTRODUCTION

The semiconductor supply chain has been exposed to various security threats as a result of fabrication outsourcing. These threats are integrated circuit (IC) piracy, counterfeiting, overproduction, and hardware Trojans [2, 4, 9, 12], causing a huge annual loss that was estimated a decade ago to be $4 billion [22]. These security threats have been countered by design-for-trust (DfTr) techniques, mostly applicable to digital ICs [3, 17]. Logic locking is a prime example of a DfTr technique [20].

However, the research effort for securing analog ICs or analog intellectual property (IP) is relatively small. Analog ICs are vulnerable to security threats as they have a small footprint and a wide range of use in nearly every application domain. Arguably, it is much easier to pirate analog ICs with a few hundred transistors than digital ICs with millions of transistors. Previous works on analog logic locking aim at locking the circuits by key provisioning techniques[21] and tuning circuits functionalities[5] by either hiding the proper voltage or current bias, the transistor sizing, or the voltage thresholds of devices[1, 6, 7, 15, 19, 24, 25]. There are also other techniques used for locking analog mixed-signal (AMS) circuits where digital logic locking techniques have been applied for locking the digital part of the circuits [10, 14]. In addition, vulnerabilities of obfuscated analog circuits have been evaluated [18], and attacks based on satisfiability modulo theories (SMT) and bias locking have been proposed [11, 13]. However, the technique we put forward in this paper relies on a completely different approach for analog obfuscation: layout-based effects are leveraged to establish a key-based lock. This is the first work to utilize this approach.

We propose a technique for locking analog ICs that protects against counterfeiting and reverse-engineering (RE) attacks. Counterfeiting means illegally selling cloned ICs as original ones or selling illegitimately overproduced ICs in the aftermarket. RE techniques, on the other hand, are applied to derive IC proprietary
information such as its netlist and layout. The goal here is either to counterfeit the ICs (by extracting the information necessary for producing similar or identical ICs) or to steal secret information that an adversary should not be privy to. In RE techniques, the adversary needs to de-pack the IC, de-layer it, “take pictures” of the layers, and stitch the images together (likely by using specialized image processing tools) to obtain a netlist. While there are difficulties in this process (e.g., the number of individual images is rarely tractable), the pictures clearly show the metal lines, vias, and even contacts. However, the features shrink as the delayering process gets closer and closer to the device’s layers that form the transistors. Finally, at the device level, doping gradients and other low-level properties are not trivial to obtain by delayering alone.

A graphic notion of the difficulty in RE a complex metal stack is depicted in Fig. 1.

In this work, we perform obfuscation by manipulating two of such low-level properties in the diffusion layer: these are layout-based effects termed well proximity effect (WPE) and length of diffusion (LOD). This class of effects is often referred to as local layout effects or layout-dependent effects (LDEs), depending on the vendor. Surely, it is much harder to identify/characterize these effects than identifying the size of a transistor. To date, no RE attack has demonstrated this capability. In addition, extracting this level of detail is seemingly very expensive and time-consuming [8]. That being said, these effects have a direct impact on the transistors’ behavior such as the threshold voltage ($V_{th}$) and transconductance ($g_m$), which in turn affect the characteristics of an analog circuit. For example, for an operational transconductance amplifier (OTA), the effects would influence the power, gain, phase, and transconductance parameters.

The following contributions are made in this paper:

- It is shown, for the first time, how to capitalize on undesirable layout-based effects for locking analog circuits
- The effectiveness of the proposed technique is shown via a design example of an OTA
- We evaluate the effectiveness of our approach against RE efforts

The remainder of the paper is organized as follows. In Section II, the proposed technique is introduced and explained. Section III shows a case study for the proposed locking technique and its results. Section IV discusses possible attack models and security analysis. Section V concludes the paper.

2 BACKGROUND AND PROPOSED LOCKING TECHNIQUE

2.1 Layout-Dependent Effects

LDEs are a result of reducing the process geometries in lithography. WPE and LOD are examples of layout-dependent effects that appear in sub-100nm CMOS technology. However, we clarify that WPE and LOD effects are even more pronounced in technology nodes under 65nm. WPE relates to the device’s proximity to the well edge. A transistor that is close to the well edge will show a different performance (voltage threshold and drain current) from that of a device located far from the well edge (see X in Fig. 2a). This is due to the implant ions scattering off the resist side-well, even if the transistors are drawn with identical dimensions. LOD corresponds to different mechanical stress induced by a different OD length (i.e., poly to OD distances in Fig. 2a, marked as A and B), which affects the carrier mobility, hence the current in the devices.

Fig. 3 shows the effects of LOD and combined LOD and WPE on the absolute values of voltage threshold and transconductance of a PMOS transistor with standard (SVT-), high (HVT-), and low (LVT-) voltage thresholds at $v_{gs} = 1\text{V}$. For very small or very large B (Fig. 3), where the poly is close to the sides of the OD (Fig. 2b), the device shows different $V_{th}$ and $g_m$ compared to other values for B. This will be exploited in this work for obfuscating analog ICs. These layout-dependent effects similarly impact the performance of an NMOS transistor. They also give rise to the device mismatch in analog circuits.

In this work, our goal is to exploit these layout effects for locking analog circuits. To do so, we consider three arrangements for a transistor, namely baseline (BL), side-poly (SP), and short-OD
Leveraging Layout-based Effects for Locking Analog ICs

Figure 3: Effects of LOD and both LOD and WPE on the absolute values of voltage threshold and transconductance of PMOS transistors with a minimum length and representative width. B is shown in Fig. 2.

Figure 4: Effects of PMOS width, WPE and LOD on the absolute values of voltage thresholds for all arrangements.

Table 1: Variations (%) in Voltage Threshold and Transconductance with respect to BL (the baseline)

| $A_i$ | Device | $V_{th}$ | $g_m$ |
|-------|--------|----------|-------|
|       | PMOS   | 2.85     | 3.7   |
|       | NMOS   | 4.05     | 4.38  |
|       | PMOS   | 6.08     | 7.9   |
|       | NMOS   | 8.33     | 9.28  |
|       | PMOS   | 4.76     | 4.72  |
|       | NMOS   | 1.72     | 2.54  |
|       | PMOS   | 10.4     | 10.19 |
|       | NMOS   | 3.7      | 3.41  |

Values were obtained from corner analysis for typical corner for devices with a minimum length and representative width. $A_i$ is an arrangement as defined in Fig. 2.

(SOD), as shown in Fig. 2. BL corresponds to a nominal LDE case, whereas SP and SOD are utilized to further exploit WPE and LOD effects. With these arrangements, variations of up to $\approx 10\%$ in $V_{th}$ and $g_m$ with respect to the BL can be obtained, as shown in Table 1. The voltage threshold variations in NMOS are larger than in PMOS, while transconductance variations in NMOS are smaller than in PMOS. The statistical variations (due to both process and mismatch) for all arrangements were also simulated. Table 2 shows the standard deviations (SD) of $V_{th}$ and $g_m$ with respect to their mean values. The numbers reported in Table 1 and Table 2 demonstrate that the layout-based effects are deterministic, i.e., they still present themselves no matter where the fabricated IC fares in the process variation spectrum.

The effect of transistor width $W$ along with the layout-dependent effects on the voltage thresholds for all arrangements is shown in Fig. 4 where the PMOS transistors have minimum length. Note that the margin between the lines BL-SP and BL-SOD is nearly constant, indicating that transistors of any size are potential candidates for obfuscation. In this example, the increase of $W$ in SOD can change the voltage threshold variations from 6.8% to 8.7% compared to BL.

We propose designing analog circuits with different arrangements of transistors from which the ‘correct’ arrangement is selected via keys. In principle, there are three possible arrangements for each NMOS or PMOS transistor where the order of these arrangements in a layout is arbitrary (e.g., SOD-BL-SP or SP-BL-SOD), where different orders lead to different correct key values. The three arrangements are controlled by three key bits (see Fig. 5). This procedure is the same for NMOS and PMOS transistors. Therefore, for a circuit with $N$ devices, the keylength for the entire circuit is $N \times 3$. In principle, there are a total of $2^{3N}$ possible combinations of arrangements or keys when assuming the keys are binary signals.

However, it is observed that some of the ‘wrong’ combinations lead to desirable performance, while others may produce nearly correct or completely incorrect performance/behavior. To explore this space and efficiently obfuscate an analog IP, we first propose a very simple three-step procedure as follows:
(1) Design a circuit with a combination of BL/SP/SOD transistors
(2) Examine, for each transistor, the effect of the other 2 arrangements that have not been employed originally
(3) Maintain only the arrangements that result in incorrect performance and thus promote obfuscation

The three-step process described above can be improved if certain configurations of transistors are prioritized. First, it is beneficial to convert transistors with multiple fingers to a single finger wherever possible. This step magnifies performance shifts in transistors due to layout-based effects. Second, we do not need to examine all transistors exhaustively. One can examine transistors by randomly selecting a transistor, choosing an alternative arrangement for it, and assessing the effect on performance. This can be further improved if, as a starting point, one uses a combination of the designer’s experience and circuit symmetry analysis for selecting transistors.

Finally, the third step can be modified to stop maintaining arrangements that lead to incorrect performance that is too close to the desired performance. We term the keys that create such scenario as undesirable keys. In Section 3, we consider an OTA as a case study and implement the three-step procedure for locking it.

3 CASE STUDY: OPERATIONAL TRANSCONDUCTANCE AMPLIFIER

We apply the proposed technique to lock an OTA as shown in Fig. 6. The specs of the OTA for the chosen arrangements are given in Table 3. Note that, in this case study, we only use transistors with a standard voltage threshold. This is, by no means, a limitation of our technique. Then, we examine the effect of unused arrangements on the OTA performance. The number of transistors in the circuit is 36, hence our initial search space is $2^{36 \times 3}$. In practice, we cannot examine all the arrangements for all transistors, but we can explore those with a potential effect on the input differential pairs, summing circuit, floating class-AB control, bias block, and class-AB output (see Fig. 6 for details). This type of reasoning is what we previously alluded to when referring to a designer’s expertise and symmetry.

![Figure 5: Principle of locking analog circuit. The order of these arrangements in the layout design is arbitrary. The figure shows only 3 out of 6 possible orders.](image)

![Figure 6: Schematic of OTA circuit. Multiple subcircuits such as input differential pairs (P1, P2, N1, N2), summing circuit (P7-P10, N7-N10), bias circuit (P13-P17, N13-N17), and class-AB output (P18, N18) are used for applying the layout-based effects. Red, blue, and black transistors represent arrangements SOD, SP, and BL, respectively.](image)

Table 3: OTA Specs for utilized arrangements in Fig. 6

| Spec | \( \text{gm} \) | Power* | Gain* | Phase | 3dB Bandwidth |
|------|--------------|--------|-------|-------|---------------|
| Spec1 | 1.32mS | 1.1mW | 73.6dB | 90deg | 641KHz |

*Power is the DC power, and gain is the open-loop gain.

Simulation results: In this work, all simulations are performed by using the Virtuoso Spectre circuit simulator and a commercial
65nm technology. We start with selecting the following 13 transistors from different subcircuits for obfuscating the circuit: P1, P2, P7-P10, N7-N10, N17, N18, and P18. At this point, the keyspace has $2^{13 \times 3}$ possible keys. However, not every key is desirable for obfuscating the circuit performance and should be discarded. We shrink the keyspace by applying our three-step procedure as well as controlling a symmetrical pair of transistors, instead of an individual transistor, to balance the layout-dependent effects. The latter technique requires tying together the control bits of the symmetrical pair of transistors. In principle, each symmetrical pair of transistors in the base design can be a couple of arrangements shown in Fig. 7, which in turn can be hidden among other 8 couples of arrangements. In other words, each transistor pair can be obfuscated by at most 8 couples of arrangements. The 13 selected transistors for obfuscation form 6 pairs of transistors plus a singular transistor. We use different number of couples of arrangements for obfuscating these pairs. In total, we added a sum of 28 random couples of arrangements (i.e., 3, 4, 6, 4, 8, 3) to hide the 6 pairs of transistors. In addition, we added 1 single arrangement to obfuscate 1 transistor. In this experiment, the keylength is 36 bits (i.e., $28 + 6 + 1 + 1$) made by adding 57 arrangements (i.e., $28 \times 2 + 1$) to the design. At this point, the size of keyspace is 50400.

To show the robustness of the achieved obfuscation, we simulated the impact of all different keys on the gain, phase margin, 3dB bandwidth (BW), and DC power of the OTA. Fig. 8 shows the impact of the keys on the gain. This impact manifests itself as a wide range of degradation in the gain (i.e., up to $130\, \text{dB}$). The desired keys, which generate a gain of $\geq 70\, \text{dB}$, may satisfy the design specs. In this experiment, the rate of the correct keys, which is adjustable, forms 0.66% of the overall keys. In Fig. 8, there is a gap of $8\, \text{dB}$ between the plots caused by eliminating the nearly correct keys. This is achieved by updating some of the added pairs of arrangements to the circuit. We can further remove the nearly correct keys that produce gain values between $67\, \text{dB}$ and $70\, \text{dB}$. However, these latter keys correspond to less than 0.14% of the overall keys.

It should be evident that here we establish a trade-off space between keylength and output/behavior “corruption”, which is a dimension also explored in digital logic locking [16]. Fig. 8 also shows the impact of the applied keys on the phase. This impact manifests itself as degradation of up to $50\, \text{deg}$ in the phase margin. Fig. 9 and Fig. 10 show the 3dB bandwidth and the DC power consumption for the applied keys, respectively. The range of power consumption in the circuit for the correct keys is between $1.143\, \text{mW}$ and $1.188\, \text{mW}$. Interestingly, 1702 keys cause a power consumption within this range, but only 266 keys of which are the correct keys. The simulation time for assessing gain and power parameters was nearly 55 hours long. The area increase as a result of 57 added arrangements is 158%. In addition, power variations of up to 77% compared to that consumed by the initial circuit were noticed.

As an attempt to protect the correct keys, we apply the following three techniques (and fourth one comes later on):

![Figure 7: Coupled arrangements. One couple of arrangements is used in the based design as a pair of transistors that can be obfuscated by the other 8 couples of arrangements.](image)

![Figure 8: Layout-based effects on (a) the OTA gain and (b) phase simulated for 50K keys. The gap marked in the graph is the result of purposefully removing nearly correct keys.](image)
(1) Balance the effect of arrangements
(2) Eliminate keys that result in nearly correct performance
(3) Remove couples of arrangements with a relatively large impact on performance

Let us explain the third technique by an example as the first two techniques have already been discussed. Selecting non-identical couples of arrangements (such as BL-SP or SOD-BL) for N7 and N8 in Fig. 6 results in a negative gain, disregarding other arrangements used in the circuit. In other words, there are only three identical couples of arrangements for N7 and N8 to make the gain positive. We eliminate the other six couples of arrangements to remove their alarming effects on the circuit performance. Note that these techniques can result in an uneven number of coupled arrangements for pairs of transistors and raise questions. One attempt to solve this problem is to equalize the number of coupled arrangements for each transistor pair. This solution would shrink the keyspace, but it would regularize the layout and reveal less structural information. We expanded the keyspace by selecting five more transistors: P16-P17 and N13-N15. Now, the locked design has 31 couples of arrangements (i.e., 28 minus 6 removed couples of arrangements from the previous experiment plus 9 added couples of arrangements in current experiment) to hide 8 pairs of transistors from the base design. We also kept the single arrangement added to the original design in the previous experiment. Now, the keylength is 41 bits made by adding 63 arrangements. We simulated the circuit for the entire keyspace, which has 340200 keys. Fig. 11 shows the impact of these keys on the gain. The target keys form less than 2% of the overall keys. In addition, all gains are positive, and the minimum target gain value is 70 dB. The simulation time for gain, 3dB bandwidth and power evaluation was nearly 22 days. The area is increased by 175% as a result of adding 63 arrangements. In addition, power variations of up to 73% compared to that consumed in the base circuit were noticed. All simulations were run on a server powered by an Intel (R) Xeon (R) Gold 5122 CPU with 32 cores @3.60GHz.

The proposed locking scheme can be used for a larger analog circuit than the representative OTA block. In fact, there might not be necessary to apply the locking scheme to all analog blocks. As soon as one of the block is locked, it is very likely that the alteration of the performance of this specific block will affect the performance of the entire circuit. Recall that from the point of view of a single obfuscated transistor in isolation, the overhead is 300%. For an analogue circuit, however, only in the absolute worst case would the overhead be 300%. We emphasize that not all transistors are obfuscated: some are not satisfactory candidates and some pairs of transistors are jointly obfuscated by fewer combinations of arrangements. State-of-the-art approaches [19, 25] have displayed smaller overheads while being susceptible to the SMT-based attack [11]. Our approach establishes a trade-off between overhead and security where we favor higher security. Section 4 elaborates the security aspect of the locking scheme.

4 DISCUSSIONS

First, we clarify that in our threat model we assume that both foundry and end-user can be untrusted. We assume that the foundry knows every detail about the IP but the correct keys. We assume that a malicious end-user has the required expertise and tools for RE the IP. For example, he/she has access to high-precision optical imaging equipment, circuit simulators, and copies of the functional IP to use as an oracle. However, he/she does not enjoy LDE-level visibility as it is not a current practice in RE efforts. We also assume he/she has no access to a detailed transistor model that takes into account LDEs. In addition, he/she knows to select only one arrangement for each transistor and not more than one. Further, we justify the inefficiency of the brute-force attack, SMT-based attack, and removal attack on the proposed approach. Here we consider the following scenarios for attacking the proposed approach.

4.1 Untrusted foundry

Everything about the design including LDE-level details is known to the foundry except for the correct keys. As an attempt to further protect the keys, we apply the fourth technique in addition to the three techniques discussed in Section 3:
An adversary would try different combinations of arrangements. The SMT-based attack has been applied to analog ICs with locked circuits. The parameters in this equation can be found in the circuit specifications or the PDK (process design kit) documentation. The SMT solver can alone solve this equation without any need for a circuit simulator. This attack has also been applied to a camouflaged analog IP [1] on the same basis (Table 4).

In our approach, however, the layout-based effects are applied to all sub-circuits (e.g., input differential pairs and summing circuit in Fig. 6) and not only to the bias circuit. Therefore, using SMT-based attacks which solve for bias circuits is not sufficient for our approach. Specifically, equations that link the undesirable layout-based effects to circuit performance must be solved by a circuit simulator, and this requirement is not scalable.

Fig. 12 shows a wide range of current variations in one branch of the OTA circuit. The SMT solver should know the desirable range of current in each branch to solve the equations. This cannot be done without extensive simulations. This problem does not exist in the circuits used to apply the SMT-based attack as the currents in those circuit equations are functions of fixed reference currents. Therefore, the existing SMT-based attack cannot be directly applied to our proposed technique. Recently, another attack has been developed for analog biasing locking techniques [13]. This attack searches for a correct bias instead of the key and is not applicable to our proposed technique which obfuscates not only the bias circuit but also other parts of the circuit.

Is the removal attack applicable to the proposed approach? No. The removal attack is mounted to retrieve the base design by identifying and removing the protection circuitry [26]. In our locking scheme, the protecting parts cannot be distinguished from the original design. Since our method obfuscates multiple blocks (and not only the biasing block) removing the key-bit transistors would mean redesigning the circuit from the scratch. Specifically, removing the ‘key-bit transistors’ from the OTA would remove \( \approx 50\% \) of the original design. In contrast to our method, the state-of-the-art techniques which act on biasing blocks [7, 19, 24, 25] are vulnerable to a removal attack because the attacker only needs to recover biasing blocks, which typically have a small number of transistors. Although additional steps might be required. In addition, locked AMS designs in [10, 14] are vulnerable to a removal attack. In fact, the digital lock of the circuits can be removed and the small biasing blocks can be redesigned. Table 4 summarizes the aforementioned discussion and shows the security-overhead trade-off established by our approach. The area overhead in our approach can be reduced to \( \sim 30\% \) by selecting 2 (instead of 3) arrangements per obfuscated transistor at the cost of lowering the security level of the locked circuit.

4.2 Untrusted End-user

Assuming that the netlist is obtained via a RE effort, the IP will not work at the desired performance without knowing the correct key. We assume an adversary can see the metal lines, vias, and even bias circuits, where current mirrors or voltage dividers are obfuscated [19, 25]. The correct key in these circuits is a selection of the mirrored branches, each with a different transistor size, that results in a desirable sum of current. To find the selection, what needs to be done is to write a simple equation, which links the current of the reference branch to the currents of mirrored branches, and assign this task to the SMT solver. The area overhead in our approach can be reduced to \( \sim 30\% \) by selecting 2 (instead of 3) arrangements per obfuscated transistor at the cost of lowering the security level of the locked circuit.
Table 4: Vulnerability of state-of-the-art DfTr methods to SMT-based attack

| DfTr technique                          | Susceptible to SMT-based attack | Susceptible to removal attack | Purely analog | Area overhead (%) |
|-----------------------------------------|---------------------------------|-------------------------------|---------------|-------------------|
| Memristor-based protection [7]          | Yes                             | Yes                           | No            | –                 |
| Parameter biasing obfuscation [19]      | Yes                             | Yes                           | Yes           | 6.3               |
| Combinational lock [25]                 | Yes                             | Yes                           | Yes           | 6.64              |
| Analog Camouflaging [1]                 | Yes                             | No                            | Yes           | up to 48*         |
| Neural Net. Biasing [24]                | Yes                             | Yes                           | Yes           | –                 |
| AMS lock [10]                           | No                              | Yes                           | No            | 0 ~ 171.3**       |
| Mix lock [14]                           | No                              | Yes                           | No            | 6.7 ~ 24.4**      |
| This work                               | No                              | No                            | Yes           | 30.6 ~ 175***     |

*This is not a key-based technique, thus the relatively low overhead.

**These values vary depending on the obfuscated circuit and parameters of the locking scheme.

***Depending on the number of arrangements per transistors selected for obfuscation, which is either 2 or 3, the area overhead varies as shown above.

5 CONCLUSIONS

This paper shows a novel approach for locking analog ICs. It exploits otherwise undesirable layout-based effects such as WPE and LOD for locking the circuits. This approach is applied to an OTA circuit for a large number of keys to show the robustness of achieved obfuscation. The layout-based effects on gain, phase margin, 3dB bandwidth, and power show the effectiveness of the proposed approach for locking analog ICs. This work demonstrates the potential of the proposed approach for protecting analog circuits against counterfeiting and RE-based attacks.

As a future work, we intend to validate our design in silicon by utilizing a commercial foundry service to achieve a realistic scenario of outsourcing.

6 ACKNOWLEDGMENTS

This work has been partially conducted in the project “ICT programme” which was supported by the European Union through the European Social Fund. It was also partially supported by European Union’s Horizon 2020 research and innovation programme under grant agreement No 952252 (SAFEST).

REFERENCES

[1] Abdullah Ash-Saki and Swaroop Ghosh. 2018. How multi-threshold designs can protect analog IPs. In 2018 IEEE 36th International Conference on Computer Design (ICCD) IEEE, 464–471.

[2] Shivam Bhasin and Francesco Regazzoni. 2015. A survey on hardware trojan detection techniques. In 2015 IEEE International Symposium on Circuits and Systems (ISCAS). 2021–2024. https://doi.org/10.1109/ISCAS.2015.7169073

[3] Brice Colombier and Lilian Bossuet. 2014. Survey of hardware protection of design data for integrated circuits and intellectual properties. IET Computers & Digital Techniques 8, 6 (2014), 274–287.

[4] Sophie Dupuis, Papa-Sidi Ba, Giorgio Di Natale, Marie-Lise Flottes, and Bruno Rouzeure. 2014. A novel hardware logic encryption technique for thwarting illegal overproduction and Hardware Trojans. In 2014 IEEE 20th International On-Line Testing Symposium (IOLTS) 49–54. https://doi.org/10.1109/IOLTS.2014.6873671

[5] Mohamed Elshamy, Alhasan Sayed, Marie-Minerve Louarat, Amine Rhouani, Hassan Aboushady, and Haralampos-G Stratigopoulos. 2020. Securing programmable analog ICs against piracy. In 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE) IEEE, 61–66.

[6] Mohamed Elshamy, Alhasan Sayed, Marie-Minerve Louarat, Amine Rhouani, Hassan Aboushady, and Haralampos-G Stratigopoulos. 2020. Securing programmable analog ICs against piracy. In 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE) IEEE, 61–66.
[7] David HK Hoe, Jeyavijayan Rajendran, and Ramesh Karri. 2014. Towards secure analog designs: A secure sense amplifier using memristors. In 2014 IEEE Computer Society Annual Symposium on VLSI. IEEE, 516–521.

[8] Intelligence Advanced Research Projects Activity (IARPA). 2016. Rapid Analysis of Various Emerging Nanoelectronics (RAVEN). Retrieved June 17, 2022 from https://www.iarpa.gov/index.php/research-programs/raeven

[9] Nisha Jacob, Dominik Merli, Johann Heyzal, and Georg Sigl. 2014. Hardware Trojans: current challenges and approaches. IET Computers & Digital Techniques 8, 6 (2014), 264–273.

[10] Nithyashankari Gummidipoondi Jayasankaran, Adriana Sanabria-Borbon, Edgar Sánchez-Sinencio, Jiang Hu, and Jeyavijayan Rajendran. 2018. Towards provably-secure analog and mixed-signal locking against overproduction. In Proceedings of the International Conference on Computer-Aided Design. 1–8.

[11] Nithyashankari Gummidipoondi Jayasankaran, Adriana Sanabria-Borbon, Amr Abuellil, Edgar Sánchez-Sinencio, Jiang Hu, and Jeyavijayan Rajendran. 2020. Breaking analog locking techniques. IEEE Transactions on Very Large Scale Integration (VLSI) Systems 28, 10 (2020), 2157–2170.

[12] Shahrzad Keshavarz, Cunxi Yu, Samaneh Ghandali, Xiaolin Xu, and Daniel Holcomb. 2018. Survey on applications of formal methods in reverse engineering and intellectual property protection. Journal of Hardware and Systems Security 2, 3 (2018), 214–224.

[13] Julian Leonhard, Mohamed Elishamy, Marie-Minerve Louërat, and Haralampos-G Stratigopoulos. 2021. Breaking analog biasing locking techniques via re-synthesis. In Proceedings of the 26th Asia and South Pacific Design Automation Conference. 555–560.

[14] Julian Leonhard, Muhammad Yasin, Shadi Turk, Mohammed Thari Naheel, Marie-Minerve Louërat, Roselyne Chotin-Avot, Hassan Aboushady, Oezgur Sinanoglu, and Haralampos-G Stratigopoulos. 2019. MixLock: Securing mixed-signal circuits via logic locking. In 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 84–89.

[15] Sai Govinda Rao Nimmalapudi, Georgios Volanis, Yichuan Lu, Angelos Antonopoulos, Andrew Marshall, and Yiorgos Makris. 2020. Range-controlled floating-gate transistors: A unified solution for unlocking and calibrating analog ICs. In 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 286–289.

[16] Jeyavijayan Rajendran, Youngok Pino, Oezgur Sinanoglu, and Ramesh Karri. 2012. Logic encryption: A fault analysis perspective. In 2012 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 953–958.

[17] Jeyavijayan Rajendran, Oezgur Sinanoglu, and Ramesh Karri. 2014. Regaining trust in VLSI design: Design-for-trust techniques. Proc. IEEE 102, 8 (2014), 1266–1282.

[18] Vaibhav Venugopal Rao, Kyle Juretus, and Ioannis Samavides. 2020. Security vulnerabilities of obfuscated analog circuits. In 2020 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 1–5.

[19] Vaibhav Venugopal Rao and Ioannis Samavides. 2017. Protecting analog circuits with parameter biasing obfuscation. In 2017 18th IEEE Latin American Test Symposium (LATS). IEEE, 1–6.

[20] Jarrod A Roy, Farinaz Koushanfar, and Igor L Markov. 2010. Ending piracy of integrated circuits. Computer 43, 10 (2010), 30–38.

[21] A Sanabria-Borbon, Nithyashankari Gummidipoondi Jayasankaran, S Lee, Edgar Sánchez-Sinencio, J Hu, and J Rajendran. 2020. Schmitt trigger-based key provisioning for locking analog/RF integrated circuits. In 2020 IEEE International Test Conference (ITC). IEEE, 1–10.

[22] SEMI. 2008. Innovation Is at Risk: Losses of up to $4 Billion Annually due to IP Infringement. Retrieved June 17, 2022 from https://www.edn.com/semi-semi-equipment-industry-stands-to-lose-up-to-4b-annually-due-to-ip-infringement

[23] Pramod Subramanyan, Sayak Ray, and Sharad Malik. 2015. Evaluating the security of logic encryption algorithms. In 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 137–143.

[24] Georgios Volanis, Yichuan Lu, Sai Govinda Rao Nimmalapudi, Angelos Antonopoulos, Andrew Marshall, and Yiorgos Makris. 2019. Analog performance locking through neural network-based biasing. In 2019 IEEE 37th VLSI Test Symposium (VTS). IEEE, 1–6.

[25] Jiafan Wang, Congyin Shi, Adriana Sanabria-Borbon, Edgar Sánchez-Sinencio, and Jiang Hu. 2017. Thwarting analog IC piracy via combinational locking. In 2017 IEEE International Test Conference (ITC). IEEE, 1–10.

[26] Muhammad Yasin, Rodhatsawa Mazumdar, Oezgur Sinanoglu, and Jeyavijayan Rajendran. 2017. Removal attacks on logic locking and camouflaging techniques. IEEE Transactions on Emerging Topics in Computing 8, 2 (2017), 517–532.