Utilizing layout effects for analog logic locking

Muayad J. Aljafar, Florence Azaïs, Marie-Lise Flottes, Samuel Pagliarini

▶ **To cite this version:**

Muayad J. Aljafar, Florence Azaïs, Marie-Lise Flottes, Samuel Pagliarini. Utilizing layout effects for analog logic locking. Journal of Cryptographic Engineering, 2024, 14 (2), pp.311-324. 10.1007/s13389-024-00350-8 . lirmm-04658699

HAL Id: lirmm-04658699

https://hal-lirmm.ccsd.cnrs.fr/lirmm-04658699

Submitted on 22 Jul 2024

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.

Journal of Cryptographic Engineering (2024) 14:311–324
https://doi.org/10.1007/s13389-024-00350-8

RESEARCH ARTICLE

Utilizing layout effects for analog logic locking

Muayad J. Aljafar[1] · Florence Azais[2] · Marie-Lise Flottes[2] · Samuel Pagliarini[1,3]

Received: 16 June 2023 / Accepted: 4 March 2024 / Published online: 6 April 2024
© The Author(s) 2024

Abstract

While numerous obfuscation techniques are available for securing digital assets in the digital domain, there has been a notable lack of focus on protecting intellectual property (IP) in the analog domain. This is primarily due to the relatively smaller footprint of analog components within an integrated circuit (IC), with the majority of the surface dedicated to digital elements. However, despite their smaller nature, analog components are highly valuable IP and warrant effective protection. In this paper, we present a groundbreaking method for safeguarding analog IP by harnessing layout-based effects that are typically considered undesirable in IC design. Specifically, we exploit the impact of length of oxide diffusion and well proximity effect on transistors to fine-tune critical parameters such as transconductance (g_m) and threshold voltage (V_{th}). These parameters remain concealed behind key inputs, akin to the logic locking approach employed in digital ICs. Our research explores the application of layout-based effects in two commercial CMOS technologies, namely a 28 nm and a 65 nm node. To demonstrate the efficacy of our proposed technique, we implement it for locking an operational transconductance amplifier. Extensive simulations are performed, evaluating the obfuscation strength by applying a large number of key sets (over 50,000 and 300,000). The results exhibit a significant degradation in performance metrics, such as open-loop gain (up to 130 dB), phase margin (up to 50°), 3 dB bandwidth (approximately 2.5 MHz), and power consumption (around 1 mW) when incorrect keys are employed. Our findings highlight the advantages of our approach as well as the associated overhead.

Keywords Analog obfuscation · Layout-based effects · Logic locking · Hardware security

1 Introduction

The outsourcing of fabrication in the semiconductor supply chain has exposed it to numerous security threats, including integrated circuit (IC) piracy, counterfeiting, overproduction, and hardware Trojans [1–4]. These threats have resulted in significant annual losses, estimated at $4 billion a decade ago [5]. To mitigate these security risks, design-for-trust (DfTr) techniques have been developed, primarily focused on digital ICs [6, 7]. One prominent example of a DfTr technique is logic locking [8].

However, the research efforts to secure analog ICs or analog intellectual property (IP) have been relatively limited. Analog ICs are susceptible to security threats due to their small footprint and widespread use across various application domains. In fact, pirating analog ICs, which typically consist of a few hundred transistors, is often easier compared to digital ICs with millions of transistors. It should also be noted that in digital design the transistor are often sized with the minimum allowed length and width parameters, which is not necessarily true for analog designs. Previous studies on analog logic locking have explored techniques such as key provisioning [9] and tuning circuit functionalities [10], involving the concealment of voltage or current biases, transistor sizing, or voltage thresholds of devices [11–18]. Additionally, some techniques have been applied to lock the digital portion of analog mixed-signal (AMS) circuits using digital logic locking methods [19, 20]. Vulner-

✉ Samuel Pagliarini
pagliarini@cmu.edu

Muayad J. Aljafar
muayad.al-jafar@taltech.ee

Florence Azais
florence.azais@lirmm.fr

Marie-Lise Flottes
marie-lise.flottes@lirmm.fr

1 Department of Computer Systems, Tallinn University of Technology, Tallinn, Estonia

2 LIRMM, Université de Montpellier (UM) - CNRS, Montpellier, France

3 Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, USA

ability assessments of obfuscated analog circuits have been conducted [21], and attacks utilizing satisfiability modulo theories (SMT), bias locking, and genetic algorithm have been proposed [22–24]. However, the approach presented in this paper, which is an extension of our previous research work [25], introduces a completely novel method for analog obfuscation by leveraging layout-based effects to establish a key-based lock. Our method is the first to utilize this unconventional approach.

We propose a novel technique for securing analog ICs against counterfeiting and reverse engineering (RE) attacks, which aim to clone ICs or extract proprietary information such as netlists and layouts. Counterfeiting involves selling cloned or illegitimately overproduced ICs in the aftermarket, while RE attacks aim to derive confidential information from ICs. In RE attacks, the adversary undergoes a process of depackaging the IC, delayering it, capturing images of the layers, and reconstructing the netlist using specialized image processing tools. While this process has its challenges, such as handling a large number of images, it still successfully reveals the metal lines, vias, and contacts. However, as the delayering process approaches the transistor layers, the features become increasingly difficult to obtain. Obtaining low-level properties like doping gradients at the device level solely through delayering and imaging is non-trivial. Figure 1 illustrates the complexity involved in RE of a complex metal stack. In this research, we introduce obfuscation by manipulating two low-level properties in the diffusion layer, specifically the *Well Proximity Effect* (WPE) and the *Length of Diffusion* (LOD). These properties, also known as local layout effects or layout-dependent effects (LDEs), are challenging to identify or characterize compared to transistor size. To date, no RE attack has demonstrated the capability to extract this level of detail, and the process of obtaining such information is deemed costly and time-consuming [26]. However, these effects directly impact transistor behavior, including parameters such as threshold voltage (V_{th}) and transconductance (g_m), which in turn affect the performance of analog circuits. For instance, in an operational transconductance amplifier (OTA), these effects would influence power consumption, gain, phase, and transconductance parameters.

This work presents several significant contributions, which are outlined below:

- *Introduction of a novel approach* the paper demonstrates, for the first time, how to leverage undesirable layout-based effects to effectively lock analog circuits. This innovative technique adds a new dimension to analog circuit protection.
- *Scalability and adaptability of the proposed technique across different process technologies* the validation results obtained from 28nm and 65nm technology nodes confirm that the locking mechanism can be implemented effectively in various manufacturing processes, enhancing the security of analog circuits in different technology generations.
- Demonstrating the deterministic nature of LDEs, even in the presence of parasitics and process variation.

The remaining sections of the paper are organized as follows: Sect. 2 introduces and explains the proposed technique in detail. Section 3 presents a comprehensive case study, demonstrating the application of the locking technique and providing the corresponding results. Section 4 discusses potential attack models and conducts a security analysis. Finally, Sect. 5 concludes the paper, summarizing the findings and emphasizing the contributions of this research.

2 Background and proposed locking technique

2.1 Layout-dependent effects

Layout-dependent effects emerge as a consequence of the reduction in process geometries during lithography. Among these effects in sub-100 nm CMOS technologies, it is known that the electrical behavior of a device (i.e., a transistor) depends on its well proximity and on its length of diffusion. However, it is important to note that WPE and LOD are not the only LDE effects that exist. More advanced nodes have many other effects such as poly and poly-cut related issues.

WPE is closely related to the proximity of a device to the well edge. Transistors located near the well edge exhibit different performance characteristics, such as voltage threshold and drain current, compared to those positioned farther from the well edge (represented as X in Fig. 2). This discrepancy arises from the scattering of implant ions off the resist sidewell, even when the transistors have identical dimensions. LOD, on the other hand, arises from the mechanical stress induced by different lengths of oxide (illustrated as A and B in Fig. 2). These variations in OD length affect carrier mobility, thereby impacting the current flow within the devices.

Figure 3 illustrates the impact of LOD and the combined effects of LOD and WPE on the absolute values of voltage threshold and transconductance for a 65 nm PMOS transistor with standard (SVT-), high (HVT-), and low (LVT-) voltage thresholds at a V_{gs} of 1 V. In Fig. 3, when the value of B (as shown in Fig. 2) is very small or very large, indicating that the poly is in close proximity to the sides of the OD, the transistor exhibits distinct V_{th} and g_m values compared to other B values. This observation forms the basis of leveraging layout-dependent effects for the obfuscation of analog ICs in this study. These layout-dependent effects have a sim-

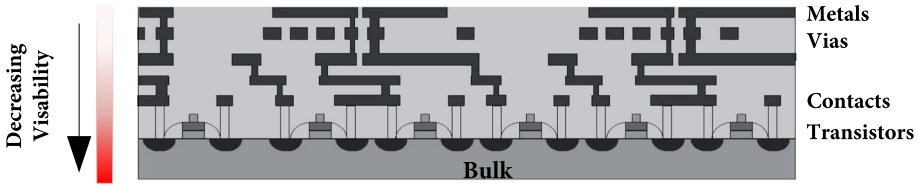


Fig. 1 Cross section of the metal stack in an IC. Moving towards the base layer, the visibility decreases and the effort to reverse engineer increases

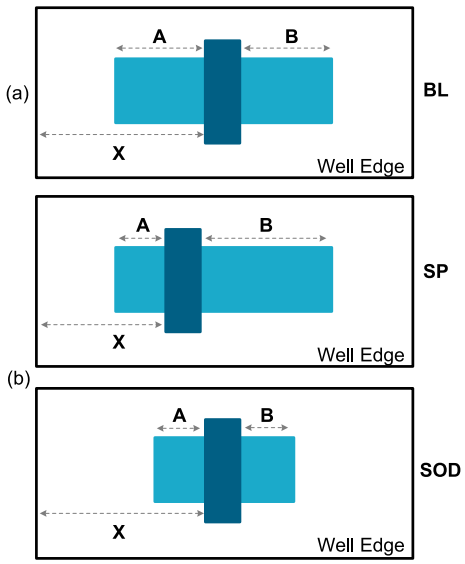


Fig. 2 Layout-dependent effects. **a** Simplified transistor layout, baseline. **b** Different transistor arrangements, used for obfuscating analog circuits. OD is the oxide diffusion, and PO is the poly (gate). A and B are the distances between the poly and the OD edges, and X is the distance between the poly and the well edges. X relates to WPE, and A and B relate to LOD

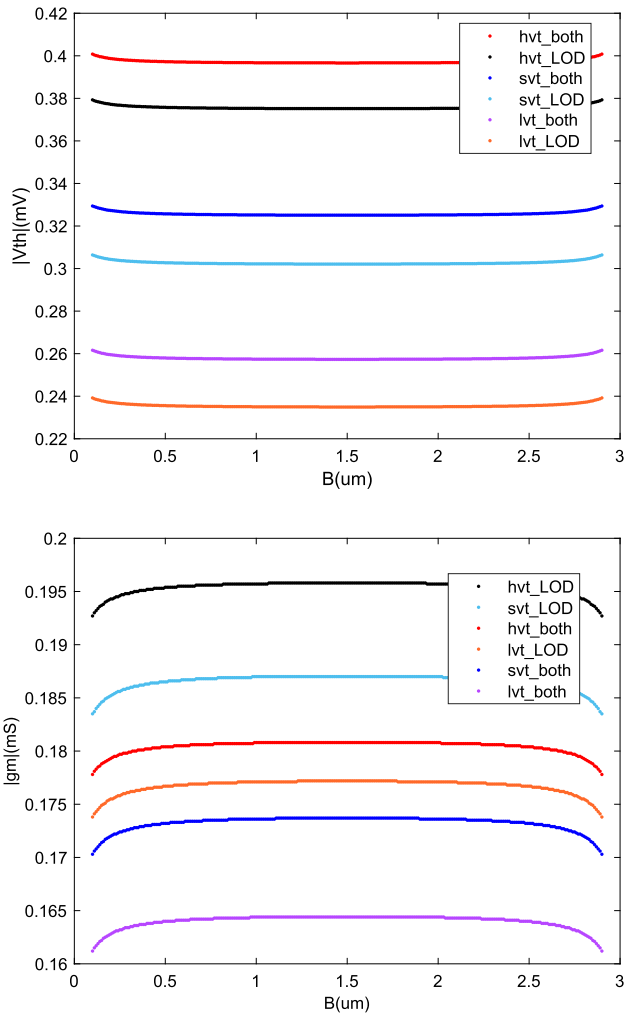


Fig. 3 Effects of LOD and both LOD and WPE on the absolute values of voltage threshold and transconductance of PMOS transistors with a minimum length and representative width. B is shown in Fig. 2

ilar impact on the performance of an NMOS transistor and contribute to device mismatch in analog circuits.

In this study, our objective is to leverage these layout effects to implement a locking mechanism for analog circuits. We consider three different **arrangements or configurations** for a transistor: baseline (BL), side-poly (SP), and short-OD (SOD), as illustrated in Fig. 2. The baseline configuration represents the nominal case of layout-dependent effects, while SP and SOD configurations are utilized to further exploit WPE and LOD effects. By employing these different arrangements, we can achieve variations of approximately 10% in voltage threshold and transconductance compared to the baseline case. The magnitude of voltage threshold variations is larger for NMOS transistors compared to PMOS transistors, whereas the transconductance variations are smaller for NMOS transistors compared to PMOS transistors (Table 1). Statistical variations due to both process variations and mismatch were also simulated for all configurations. Table 2 presents the standard deviations (SD) of V_{th} and gm with respect to their mean values. The results reported in Tables 1 and 2 demonstrate the deterministic nature of layout-based effects. Regardless of where the fabricated IC falls within the process variation spectrum, these effects consistently manifest themselves. In essence, the statistical variations arising from both process variations and mismatch, simulated across all layout configurations, consistently reveal the presence of LDEs.

Figure 4 illustrates the impact of transistor width (W) in conjunction with the layout-dependent effects on the voltage thresholds for all transistor arrangements. In this plot, PMOS transistors with minimum length are considered. It is noteworthy that the margin between the lines represent-

Table 1 Variations (%) in voltage threshold and transconductance with respect to BL (the baseline)

		A_i	Device	Variations		
				hvt (%)	svt (%)	lvt (%)
Parameter	V_{th}	SP	pmos	2.85	3.7	4.59
			nmos	4.05	4.38	5
		SOD	pmos	6.08	7.9	9.79
			nmos	8.53	9.28	10.61
	gm	SP	pmos	4.76	4.72	4.68
			nmos	1.72	2.54	2.42
		SOD	pmos	10.4	10.19	10.16
			nmos	3.7	5.41	5.09

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

Table 2 Process and mismatch of the arrangements

		A_i	Device	Variations in SD*		
				hvt (%)	svt (%)	lvt (%)
Parameter	V_{th}	BL	pmos	9.78	10.64	12.95
			nmos	15.34	12.29	9.73
		SP	pmos	9.38	10.12	12.17
			nmos	14.07	11.28	9.16
		SOD	pmos	8.97	9.58	11.37
			nmos	12.88	10.34	8.61
	gm	BL	pmos	3.55	3.98	2.90
			nmos	3.78	2.85	5.93
		SP	pmos	3.35	3.94	2.83
			nmos	3.63	2.84	5.98
		SOD	pmos	3.17	3.91	2.75
			nmos	3.45	2.85	6.05

*SD means standard deviation

ing the BL–SP and BL–SOD configurations remains nearly constant, indicating that transistors of any size can be potentially used for obfuscation. In the specific example shown, increasing the W in the SOD configuration leads to a change in voltage threshold variations from 6.8 to 8.7% compared to the BL configuration. This demonstrates that altering the transistor width can further enhance the effectiveness of the layout-based effects for obfuscation purposes.

2.2 LDEs in sub-100 nm technologies

We now demonstrate the influence of well proximity effects and length of diffusion on key parameters of transistors in both 28 nm and 65 nm technologies, considering parasitic effects. Additionally, we highlight the impact of these LDEs on digital circuits, specifically on the behavior of CMOS inverters. Figure 5 presents the drain current variations of an

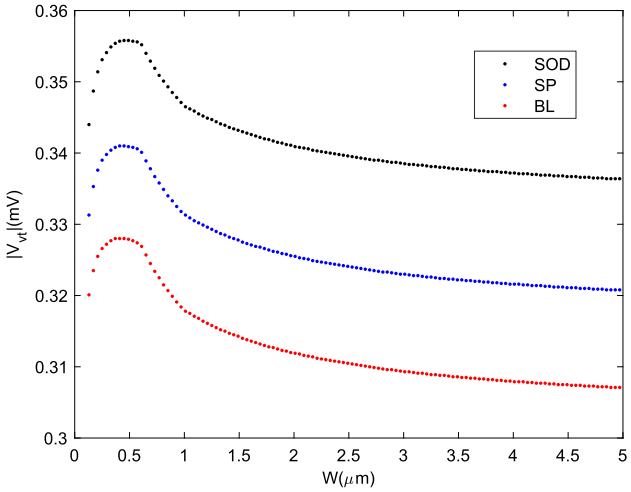


Fig. 4 Effects of PMOS width, WPE and LOD on the absolute values of voltage thresholds for all arrangements

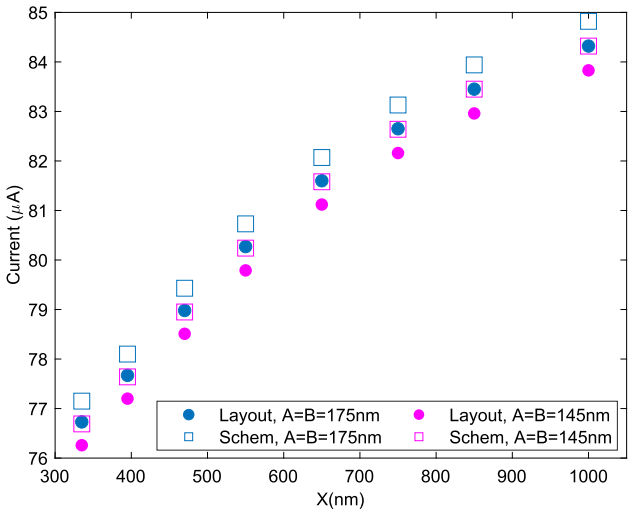


Fig. 5 Impact of layout-dependent effects on an LVT PMOS drain current in 65 nm technology

LVT PMOS transistor in 65 nm technology due to LDEs. Schematic and layout simulations are conducted for different values of A, B, X, and an applied v_{gs} of 1V. The results indicate a consistent trendline, showing an increase in drain current with higher values of X (and A and B). Similarly, Fig. 6 illustrates the impact of LDEs on the drain current of an LVT PMOS transistor in 28 nm technology. Layout simulations are performed for different values of X and an applied v_{gs} of 0.9 V. The obtained results align with those observed in the 65 nm technology simulations.

Furthermore, LDEs can impact the specifications of digital circuits, as demonstrated by their effect on the transient response of CMOS inverters. In Fig. 7, the transient response of two inverters with different variants of SP for PMOS transistors is shown. The inverter with the SP1 arrangement exhibits a slightly faster transient response (V_{SP1}) compared

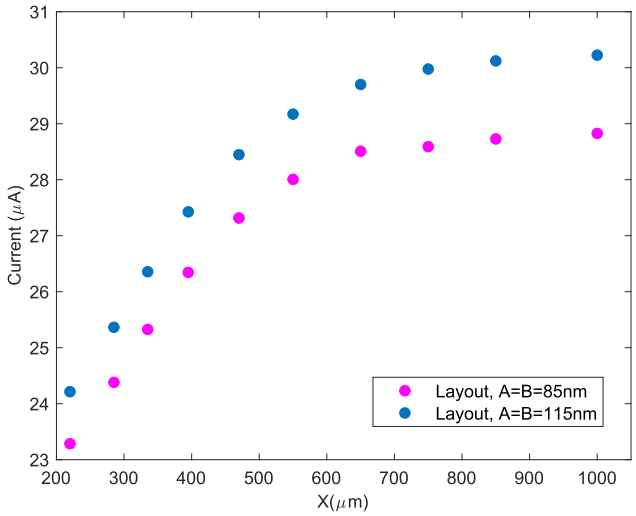


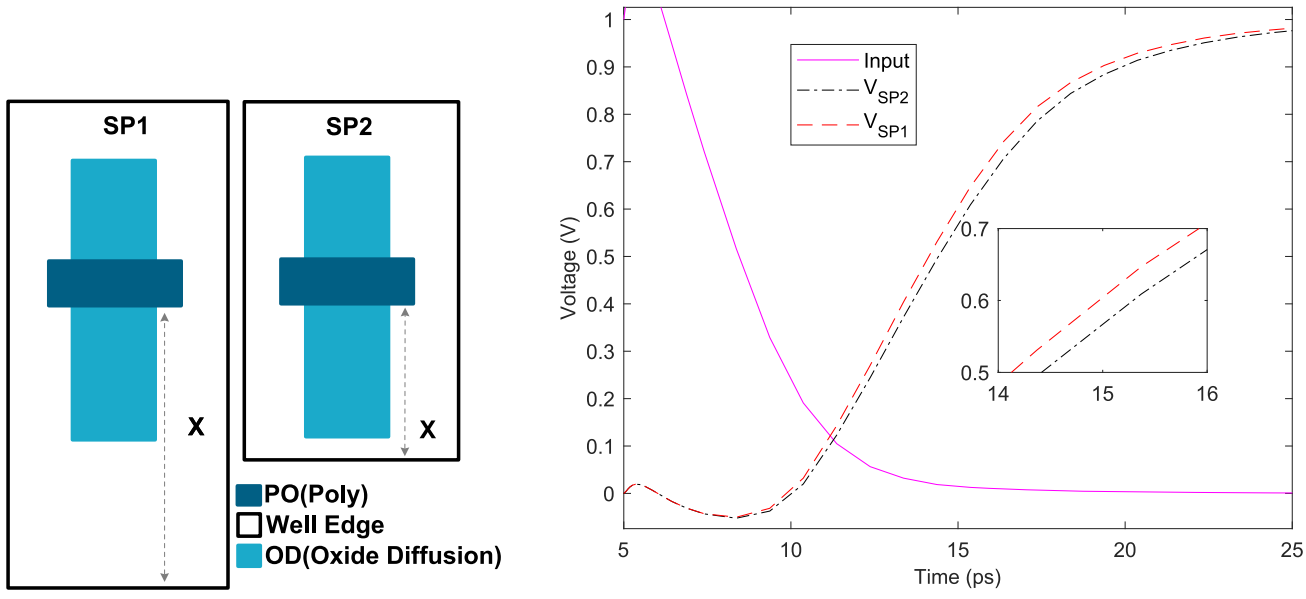
Fig. 6 Impact of layout-dependent effects on an LVT PMOS drain current in 28 nm technology

to the inverter with the SP2 arrangement (V_{SP2}). This difference in transient response indicates that the SP arrangements introduce variations in the propagation delay and rise/fall times of the inverters. When these manipulated inverters are used to replace the original inverters in a 7-stage ring oscillator, the frequency of the oscillator deviates accordingly, as shown in Fig. 8. Specifically, when inverters with the SP2 arrangement for PMOS transistors are utilized, the oscillator's frequency decreases. This decrease in frequency can be attributed to the slower transient response and longer propagation delay introduced by the SP2 arrangement. On the other hand, replacing each of these inverters one by one with the variant inverters featuring the SP1 arrangement for PMOS transistors gradually increases the oscillator's frequency. This increase in frequency is due to the faster transient response and shorter propagation delay associated with the SP1 arrangement. The observed frequency variations, in the range of a few MHz, highlight the significant impact of LDEs on the specifications of the 7-stage ring oscillator. These variations demonstrate that the layout configurations and arrangements of transistors can have a substantial influence on the performance of digital circuits.

2.3 Applied technique for obfuscating analog circuits

We propose a method for designing analog circuits using different arrangements of transistors, with the correct arrangement determined by a set of key bits. Each NMOS or PMOS transistor can have three possible arrangements, and the order of these arrangements in the layout can be arbitrary (Fig. 9). Therefore, the correct key values correspond to a specific order of the arrangements. The key length for the entire circuit is determined by the number of devices, with each device requiring three key bits. This results in a total of 2^{3N} possible keys, assuming binary key signals.

However, it has been observed that some of the 'wrong' keys can still result in desirable performance, while others may lead to nearly correct or completely incorrect behavior.



(a) Layouts (b) Transient Response

Fig. 7 Transistor layouts with different variants of the SP arrangement. The impact of WPEs on transient response of inverters with these layouts for PMOS transistors

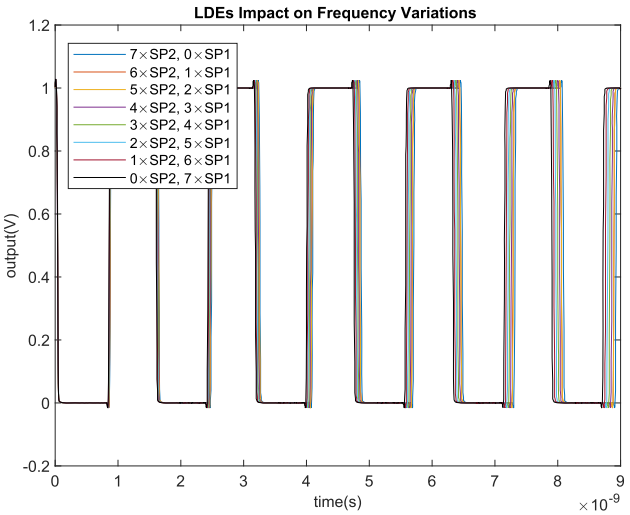


Fig. 8 Impact of LDEs on a 7-stage ring oscillator's frequency

To efficiently obfuscate an analog IP, we propose a simple three-step procedure:

1. Design the circuit using a combination of BL, SP, and SOD transistors.
2. Evaluate the impact of the two alternative arrangements for each transistor that were not originally employed.
3. Retain only the arrangements that result in incorrect performance, thereby promoting obfuscation.

This three-step process can be enhanced by prioritizing certain configurations of transistors. Specifically, it is advantageous to convert transistors with multiple fingers into single-finger transistors whenever possible. This amplifies the performance shifts caused by layout-based effects. Additionally, exhaustive examination of all transistors is not necessary. Transistors can be randomly selected, and alternative arrangements can be chosen for evaluation. Circuit symmetry analysis and the designer's experience can be leveraged to identify a starting point for transistor selection. Finally, the third step can be modified to discard arrangements that result in performance too close to the desired performance. If such "undesirable"arrangements are identified, they can be eliminated. In Sect. 3, we provide a case study involving an OTA and implement the three-step procedure to lock the circuit.

3 Case study: operational transconductance amplifier

We utilize the proposed technique to lock an operational transconductance amplifier as depicted in Fig. 10. The specifications of the OTA for the chosen transistor arrangements

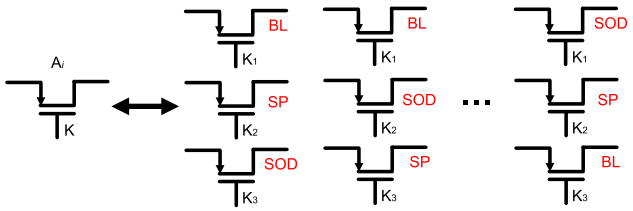


Fig. 9 Principle of locking analog circuit. The order of these arrangements in the layout design is arbitrary. The figure shows only 3 out of 6 possible orders

are provided in Table 3. It is important to note that, for this specific case study, we exclusively employ transistors with a standard voltage threshold. However, this does not imply a limitation of our technique, as it can be applied to transistors with different voltage thresholds as well. Next, we investigate the impact of unused transistor arrangements on the performance of the OTA. The circuit comprises a total of 36 transistors, resulting in a search space of $2^{36\times3}$ possible arrangements. In practice, it is not feasible to examine all arrangements for every transistor. However, we can focus on those arrangements that are likely to affect the input differential pairs, summing circuit, floating class-AB control, bias block, and class-AB output, as indicated in Fig. 10. This approach aligns with our earlier observation of leveraging the designer's expertise and considering circuit symmetry when selecting transistors for examination.

Simulation results in our simulations, we utilize the virtuoso spectre circuit simulator in conjunction with a commercial 65 nm technology. To initiate the obfuscation process, we select a set of 13 transistors from various parts within the circuit. These transistors are chosen arbitrarily and include P1, P2, P7, P8, P9, P10, N7, N8, N9, N10, N17, N18, and P18. After selecting the transistors for obfuscation, the initial keyspace consists of $2^{13\times3}$ possible keys. However, not all of these keys are suitable for effectively obfuscating circuit performance, so we apply our three-step procedure to improve the obfuscation at a cost of shrinking the keyspace. One important observation is that certain transistors can have varying degrees of impact on circuit performance and performance deviation caused by LDEs. To achieve a more balanced performance deviation, we have devised a strategy. Rather than obfuscating individual transistors, we choose to obfuscate a pair of transistors by tying together their select bits. This approach results in a more balanced LDE-induced performance deviation in a pair of transistors and enhances the overall effectiveness of the obfuscation technique.

In the obfuscation process, each pair of transistors in the base design can be hidden among other pairs of arrangements, providing multiple possibilities for obfuscation (Fig. 11). In this particular case, the 13 selected transistors for obfuscation form 6 pairs of transistors and one individual transistor. To obfuscate these 6 pairs, we introduce a different number

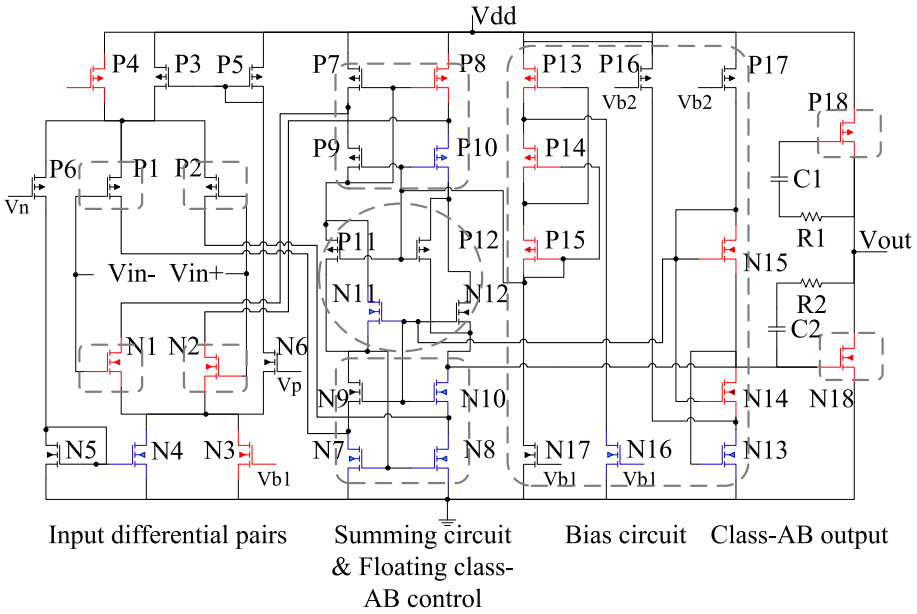


Fig. 10 Schematic of OTA circuit. Multiple subcircuits such as input differential pairs (P1, P2, N1, N2), summing circuit (P7-P10, N7-N10), bias circuit (P13-P17, N13-N17), and class-AB output (P18, N18) are used for applying the layout-based effects. Red, blue, and black transistors represent arrangements SOD, SP, and BL, respectively

Table 3 OTA specs for utilized arrangements in Fig. 10

Specs				
gm	Power*	Gain*	Phase	3 dB Bandwidth
1.32 mS	1.1 mW	73.6 dB	90°	641 KHz

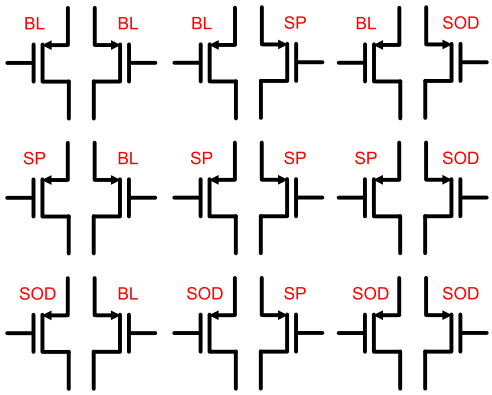
*Power is the DC power, and gain is the open-loop gain

of pairs of arrangements. Specifically, we add a total of 28 random pairs of arrangements to hide the pairs of transistors, along with an additional single arrangement to obfuscate the individual transistor. Consequently, the key length for this experiment is 36 bits (i.e., $28 + 6 + 1 + 1$), achieved by adding 57 arrangements (i.e., $28 \times 2 + 1$) to the original design.

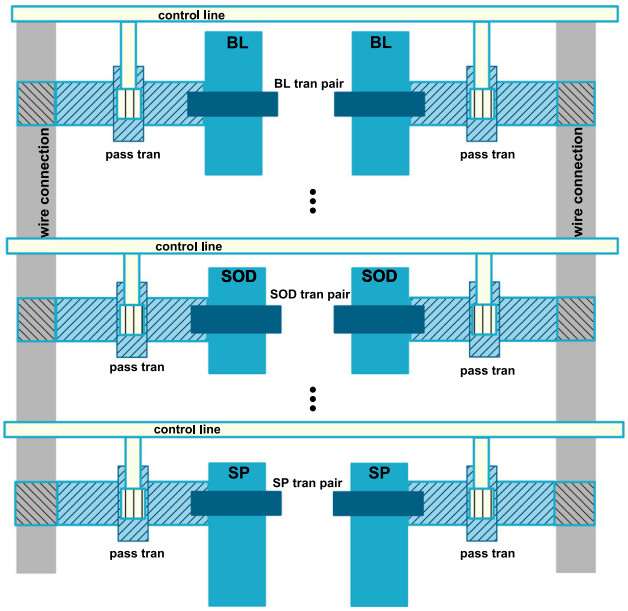
Figure 12 presents a conceptual representation of an obfuscated analog design featuring a tamper-proof memory responsible for storing key bits essential for unlocking the IC. The diagram illustrates three instances of obfuscation in an analog design. In the first scenario, depicted in Fig. 12a, a pair of PMOS transistors is obfuscated alongside two additional pairs of transistors. The second scenario, represented by Fig. 12b, involves obfuscating two adjacent transistors among other pair. The third scenario mirrors the first, focusing on obfuscating a pair of NMOS transistors, as illustrated by Fig. 12c. Pass transistors serve to connect the obfuscated transistors to the circuit, and the selection of these pass transistors is determined by control bits stored in tamper-proof memory. This memory is loaded with secret keys by a trusted party post-IC fabrication.

To demonstrate the robustness of the obfuscation achieved, we conducted simulations to evaluate the impact of 50,400 keys on the gain, phase, 3 dB bandwidth (BW), and DC power of the OTA. Figure 13 illustrates the effect of the keys on the gain, showing a wide range of degradation (up to 130 dB) due to different obfuscation arrangements. It can be observed that some keys result in a gain of $\geq$ 70 dB, which meets the design specifications. In this experiment, the rate of correct keys, which can be adjusted, accounts for 0.66% of the total keys. Figure 13 also displays a gap of 8 dB between the plots, which is achieved by eliminating the nearly correct keys. This is accomplished by updating certain pairs of arrangements in the circuit. Furthermore, it is possible to remove the nearly correct keys that yield gain values between 67 and 70 dB. However, these keys constitute less than 0.14% of the total keys, indicating their negligible presence. Overall, these simulation results highlight the effectiveness of the obfuscation technique in introducing significant variations in circuit performance across different keys, ensuring the robustness of the achieved obfuscation. Figure 13 illustrates the impact of the applied keys on the phase, showing a degradation of up to 50° in the phase margin. Additionally, Figs. 14 and 15 present the impact of the applied keys on the 3 dB bandwidth and DC power consumption, respectively.

The power consumption in the circuit for the correct keys falls within the range of 1.143–1.188 mW. Interestingly, out of 1702 keys that result in power consumption within this range, only 266 of them are the correct keys. In other words, observing power consumption as a proxy for correctness might mislead an adversary. It is important to note that the simulation time for evaluating gain and power was approximately 55 h, highlighting the extensive computational effort involved in this analysis. Furthermore, the introduction of 57 added arrangements in the obfuscation process leads to a 158% increase in circuit area. Moreover, power variations of up to 77% were observed compared to the power con-



(a)



(b)

Fig. 11 Pairs of arrangements. **a** One pair of arrangements in the based design can be hidden among a subset of 8 pairs of arrangements. **b** Illustration of the layout for three pairs of transistors connected to the circuit via pass transistors. Control lines convey select bits stored in a tamper-resistant memory

sumed by the initial circuit, indicating the significant impact of obfuscation on power consumption. These observations highlight the trade-offs and considerations involved in the obfuscation technique, including the impact on circuit performance, power consumption, and area overhead.

In summary, we apply the following three techniques (and fourth one is discussed later on) to protect the correct keys and enhance the obfuscation process:

1. Balance the effect of arrangements
2. Remove pairs of arrangements producing a nearly correct performance

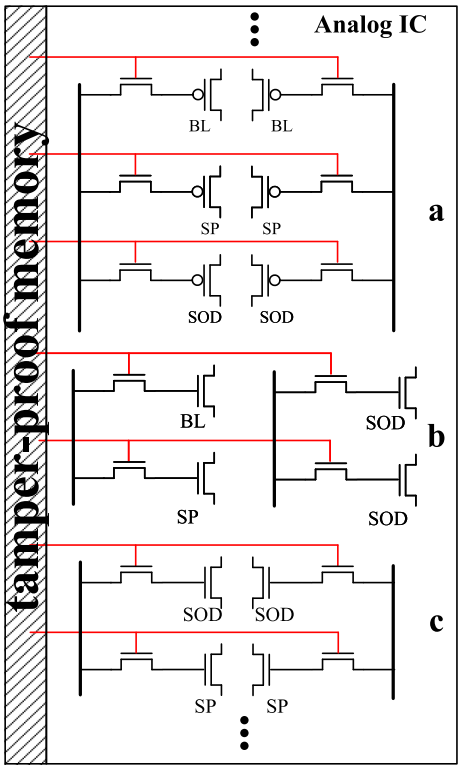


Fig. 12 Conceptual representation of an obfuscated analog design showcasing a tamper-proof memory. The figure depicts three scenarios for obfuscating a pair of transistors

3. Remove pairs of arrangements with a relatively large impact on performance

The third technique involves the elimination of pairs of arrangements that have a significant impact on the performance of the circuit. To better understand this technique, let us examine the circuit depicted in Fig. 10 and focus on transistors N7 and N8. When we choose non-symmetrical pairs of arrangements, such as BL–SP or SOD–BL, for N7 and N8, the circuit exhibits a negative gain, regardless of the other arrangements used. However, when we select symmetrical pairs of arrangements, such as SP–SP, BL–BL, or SOD–SOD, for N7 and N8, the gain becomes positive. We remove the non-symmetrical pairs of arrangements to eliminate the alarming effects on the circuit's performance and improve the quality of the obfuscation. A point worth considering is that the application of these techniques may result in an uneven distribution of pairs of arrangements among different transistors, which can potentially raise concerns about the regularity of the circuit layout and unveil structural information. To address this issue, a possible solution is to equalize the number of pairs of arrangements for each transistor. Although this approach would reduce the keyspace, it would promote a more uniform layout and limit the Conflict of interest of structural details. Indeed, the obfuscation tech-

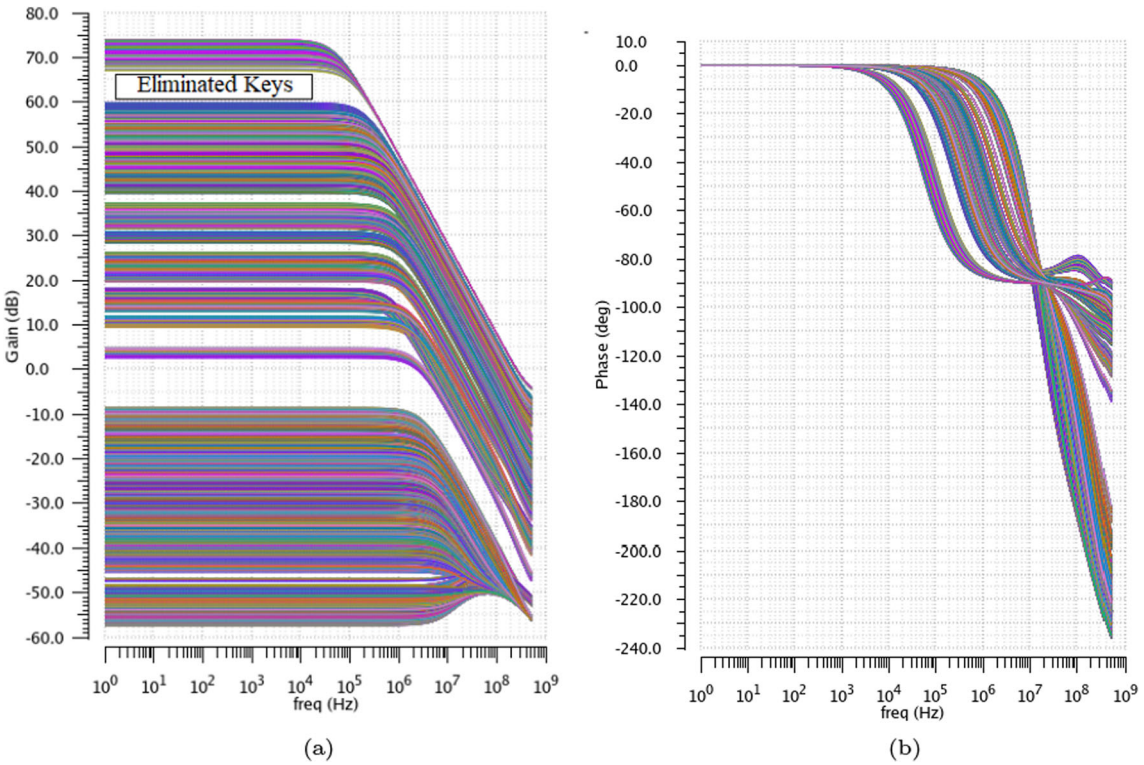


Fig. 13 Layout-based effects on **a** the OTA gain and **b** phase simulated for 50 K keys. The gap marked in the graph is the result of purposefully removing nearly correct keys

nique employed in this work involves a trade-off between the key length and the level of output/behavior "corruption"in the circuit, a concept also explored in digital logic locking [27]. In order to expand the keyspace and address the issue of uneven pairs of arrangements, we consider five additional transistors: P16, P17, N13, N14, and N15. These transistors are specifically chosen to create additional pairs, enhancing the obfuscation of the circuit. By incorporating additional pairs of arrangements, the locked design now consists of a total of 31 pairs of arrangements. This is achieved by subtracting the six removed pairs from the original 28 pairs and adding nine new pairs. These 31 pairs of arrangements serve to hide eight pairs of transistors from the original base design. Furthermore, the single arrangement that was added in the previous experiment is still present in the locked design. As a result, the keylength is now 41 bits, achieved by adding 63 arrangements to the original design. We simulated the circuit for 340,200 keys. Figure 16 demonstrates the impact of these keys on gain. The desired target keys account for less than 2% of the overall keys. Importantly, all gains are now positive, with a minimum target value of 70 dB. The simulation time for evaluating gain, 3 dB bandwidth, and power consumption was approximately 22 days. The circuit's area increased by 175% due to 63 added arrangements, and power variations of up to 73% compared to the base circuit were observed. These simulations were performed on a server equipped with

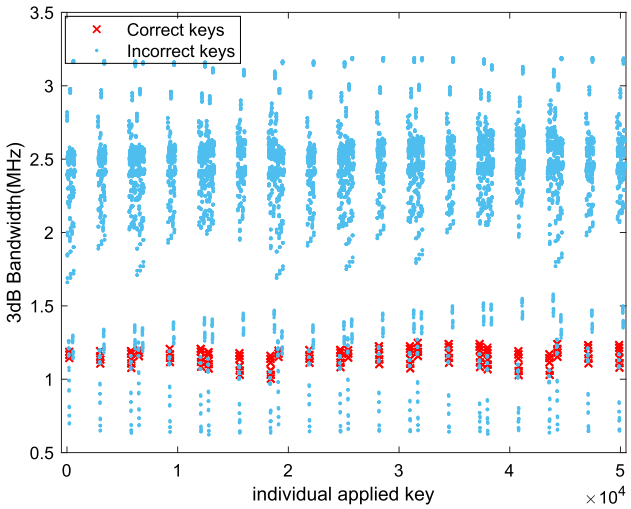


Fig. 14 Variation in the 3 dB bandwidth of the OTA for the applied keys

an Intel Xeon Gold 5122 CPU with 32 cores running @ 3.60 GHz.

The proposed locking scheme can be applied to larger analog circuits beyond the representative OTA block. It may not be necessary to apply the locking scheme to all analog blocks in a circuit. Once one block is locked, altering its performance is likely to affect the overall circuit performance,

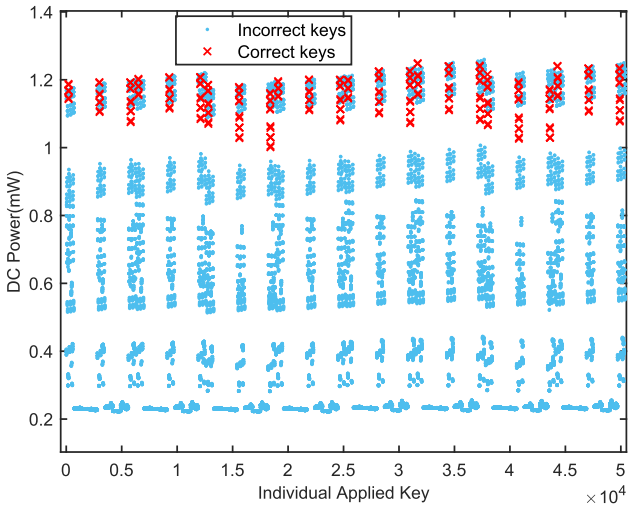


Fig. 15 DC power consumption for the applied keys

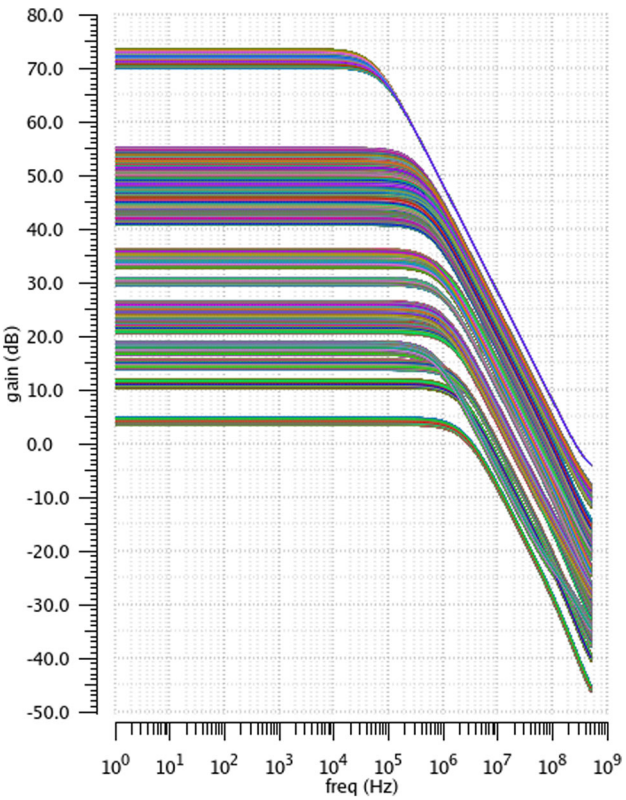


Fig. 16 Layout-based effects on the OTA simulated for 300 K keys

especially in multi-stage circuits. It should be noted that the overhead of the locking scheme for a single obfuscated transistor, in isolation, is 300%. However, for an entire circuit, the overhead will not be as significant since obfuscation can be applied selectively: it is important to highlight that not all transistors are obfuscated, as some may not be suitable candidates, and certain pairs of transistors are jointly obfuscated by fewer combinations of arrangements. While state-of-the-art approaches [12, 13] have achieved smaller overheads, they are also susceptible to SMT-based attacks [22]. In our approach, we strike a balance between overhead and security, prioritizing higher security. The security aspect of the locking scheme is further elaborated in Sect. 4.

4 Discussions

Applying digital logic locking to analog designs presents challenges, primarily in that it does not completely prevent the theft of the analog component. We strongly advocate for prioritizing analog obfuscation over digital methods when safeguarding valuable analog intellectual property.

This being said, in our threat model, we consider both the foundry and the end-user as potentially untrusted entities. We assume that the foundry has complete knowledge/visibility over the IP except for the correct key(s). The malicious end-user is assumed to possess the necessary expertise and tools for reverse engineering the IP, including high-precision optical imaging equipment, circuit simulators, and functional copies of the IP as an oracle. However, the end-user does not have the level of visibility into the layout-dependent effects as it is typically not a current practice in RE efforts. It is also assumed that the end-user does not have access to a detailed transistor model that accounts for LDEs. Moreover, the end-user is aware of selecting only one arrangement for each transistor and not more than one. In addition, we justify the inefficiency of several attack scenarios on the proposed approach, namely brute-force attack, SMT-based attack, and removal attack. 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 key(s). To enhance the protection of the keys, we employ an additional technique, referred to as the fourth technique, in addition to the three techniques previously described in Sect. 3:

4.1.1 Making the order of the arrangements in the layout design arbitrary

To further enhance the security of the keys, we applied an additional technique, which involves making the order of the arrangements in the layout design arbitrary. This means that the specific arrangement of the transistors in the layout is randomized, adding an extra layer of obfuscation to the design. By introducing this randomness, it becomes more difficult for an attacker, such as the foundry, to determine the correct arrangement and infer the corresponding keys. This method

aims to thwart simple guesses made by the attacker, such as assuming that all arrangements follow a specific pattern (e.g., all arrangements are of a certain type, like BL). The arbitrary order of the arrangements introduces further complexity and unpredictability, making it harder for an attacker to reverse engineer the correct keys and compromise the security of the locked design. Given these considerations, we now address the following questions:

Can a brute force attack compromise the design? The key sizes used in the examples discussed are, technically, susceptible to brute force attacks, especially when the attack is mounted on a real device by observing its performance. However, it is important to note that the simulation time for evaluating the keys in the mentioned example was already significant, taking 22 consecutive days to evaluate only 300 K keys, which represents a very small subset of the potential keyspace. For larger circuits and longer keylengths, the computational requirements for a brute force attack become impractical and infeasible. Therefore, while the considered key sizes may be vulnerable to brute force attacks in certain scenarios, the time and resources required for such attacks increase significantly as the keylength and complexity of the circuit increase.

Do partial simulations help to obtain the keys? *Or, in other words, can an adversary decompose the problem into smaller ones and apply a divide and conquer strategy*? Consider the input differential pairs in the OTA as an example. If an adversary attempts different combinations of arrangements for the transistors P1, P2, N1, and N2 to find a correct g_m, they may indeed find multiple combinations that yield the desired g_m value. However, it is important to note that achieving the correct g_m alone is not sufficient to unlock the circuit. The circuit specifications involve multiple performance parameters beyond just g_m. While the adversary may find combinations that satisfy g_m, it is highly likely that most of these combinations will not meet the other required specifications of the circuit. To successfully unlock the circuit, the adversary would need to find keys that simultaneously satisfy all the desired specifications. Expanding the search space to find keys that satisfy multiple specifications simultaneously significantly increases the complexity of the problem. It could easily lead to exploring a substantial portion, if not the entire keyspace. Moreover, the value of g_m is dependent on the bias circuit, which is also obfuscated. Therefore, there might be incorrect bias values that still result in the desired g_m value, further complicating the search for the correct key. In summary, finding a key that deterministically satisfies multiple specifications at the same time is highly challenging. The search space is vast and the interdependencies between different specifications, as well as the obfuscation techniques employed, make it extremely difficult for an adversary to find the correct key solely by exploring different combinations of arrangements.

Is the SMT-based attack applicable to the proposed approach? No. The SMT-based attack has been employed on analog ICs with locked bias circuits, where obfuscated current mirrors or voltage dividers are involved [12, 13]. In these cases, the correct key corresponds to a selection of mirrored branches with different transistor sizes, resulting in the desired sum of current. To find this selection, a simple equation is formulated, connecting the current of the reference branch to the currents of the mirrored branches, and the task is delegated to an SMT solver. The parameters necessary for this equation can be obtained from circuit specifications or the process design kit (PDK) documentation. The SMT solver can solve this equation without relying on a circuit simulator. This type of attack has also been applied to camouflaged analog IP [15] based on the same principle (Table 4). However, in our approach, the layout-based effects are applied to multiple parts of the circuit, not just the bias circuit. Consequently, utilizing SMT-based attacks that target the bias circuit alone is insufficient for overcoming our approach. The equations that establish the link between the undesirable layout-based effects and circuit performance must be solved using a circuit simulator. This requirement presents **scalability challenges**, as the computational burden increases with the complexity and size of the circuit. In summary, while SMT-based attacks have been successfully applied to certain analog ICs with locked bias circuits, our approach extends beyond the bias circuit and introduces layout-based effects to multiple parts of the circuit, including input differential pairs and summing circuit, as illustrated in Fig. 10. Solving the equations that capture the impact of these effects on circuit performance necessitates the use of a circuit simulator, making the approach less scalable compared to the SMT-based attack. In Fig. 17, it is evident that there is a wide range of current variations observed in one branch of the OTA circuit. To effectively solve the equations using an SMT solver, the solver needs to be aware of the desirable range of currents in each branch. This information can only be obtained through extensive simulations. This poses a challenge as the existing SMT-based attack does not require such extensive simulations because the currents in those circuit equations are functions of fixed reference currents.

Furthermore, it is worth noting that a recent attack has been developed specifically targeting analog biasing locking techniques [23]. However, this attack focuses on searching for a correct bias instead of determining the key itself. Consequently, this attack is not applicable to our proposed technique, which obfuscates not only the bias circuit but also other parts of the circuit. By extending the obfuscation to multiple circuit components, our approach adds an extra layer of security and complexity, making it more challenging for attackers to extract the correct keys.

Is the removal attack applicable to the proposed approach? No. The removal attack aims to retrieve the base design by

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 (%)
Hoe et al. [11]	Yes	Yes	No	–
Rao and Savidis [12]	Yes	Yes	Yes	6.3
Wang et al. [13]	Yes	Yes	Yes	6.64
Ash-Saki and Ghosh [15]	Yes	No	Yes	Up to 48*
Volanis et al. [16]	Yes	Yes	Yes	–
Jayasankaran et al. [19]	No	Yes	No	0 ∼ 171.3**
Leonhard et al. [20]	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

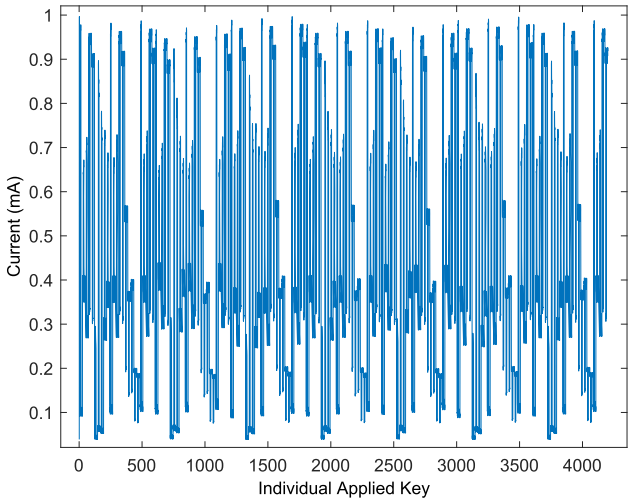


Fig. 17 Current variations in an OTA branch for 4 K different keys

identifying and removing the protection circuitry [28]. However, in our locking scheme, the protected parts cannot be immediately distinguished from the original design, making it challenging to mount a successful removal attack. Since our method obfuscates multiple blocks, not just the biasing block, removing the key-bit transistors would require redesigning the entire circuit from scratch. In the case of the OTA, removing the key-bit transistors would eliminate approximately 50% of the original design, rendering the attack ineffective. In contrast, state-of-the-art techniques that focus solely on biasing blocks are vulnerable to removal attacks [11–13, 16]. In such cases, the attacker only needs to recover the biasing blocks, which typically consist of a small number of transistors. Similarly, locked AMS designs in other approaches can also be vulnerable to removal attacks by removing the digital lock and redesigning the small biasing blocks [19, 20]. Table 4 summarizes the security-overhead trade-off achieved by our approach compared to other techniques. Our approach establishes a balance between security and overhead, with the ability to reduce the area overhead to approximately 30% by selecting two arrangements per obfuscated transistor instead of three. However, it is important to note that lowering the number of arrangements per transistor would also lower the security level of the locked circuit.

4.2 Untrusted end-user

In the scenario where the netlist of the locked circuit is obtained through reverse engineering efforts, the adversary will have access to the metal lines, vias, contacts, and poly lines of the circuit. However, it is important to note that the adversary does not have access to LDE-level visibility, which means they cannot observe the detailed characteristics and behavior of the transistors. Upon obtaining the locked netlist, the adversary will observe groups of transistors with identical sizes, representing the arrangements used in our locking scheme. However, since we do not manipulate the transistor's width (W) or length (L), the adversary's model will not capture the layout-dependent effects that were originally designed to exploit. Therefore, simulating the obtained netlist with different keys will result in the same behavior, which is incorrect if the circuit was specifically designed to utilize LDEs. Even if the adversary has access to an oracle that can confirm that different keys lead to different performance, they have no means to map these performance variations back to the circuit's design. This lack of detailed knowledge about the LDEs prevents the adversary from establishing useful distinguishing input patterns, similar to the SAT attack [29]. Consequently, the adversary's chances of unlocking the circuit are not higher than those of a malicious foundry, even when they possess an oracle.

Along similar lines, the genetic algorithm-based attack [24], which relies on oracle and locked netlist, is unlikely to be effective against the proposed approach. The genetic algorithm-based attack utilizes evolutionary search techniques to explore the design space and find potential keys that unlock the circuit. However, since our threat model does not provide access to the detailed locked netlist, the adversary lacks the necessary information to conduct such an attack. Without access to the detailed locked netlist, the adversary is unable to accurately model the circuit's behavior and the impact of different keys on its performance. This lack of detailed information about the circuit's design and layout-dependent effects makes it extremely challenging for the adversary to successfully apply the genetic algorithm-based attack to reverse engineer or unlock the locked analog ICs.

In summary, the absence of LDE-awareness in the netlist obtained through reverse engineering makes it extremely challenging for the adversary to accurately understand and exploit the design's key-dependent performance variations, thus impeding their ability to unlock the circuit.

5 Conclusion

This paper presents a novel approach for locking analog integrated circuits by leveraging layout-based effects such as well proximity effect and length of oxide diffusion. The proposed approach is demonstrated on an operational transconductance amplifier circuit using a large number of keys to showcase the effectiveness of the obfuscation achieved. By applying the layout-based effects to the circuit, we show that the gain, phase margin, 3 dB bandwidth, and power characteristics are significantly altered, thereby enhancing the security of the locked circuit. These layout-based effects serve as a form of obfuscation, making it difficult for adversaries to reverse engineer or counterfeit the circuit. The results of this work demonstrate the potential of the proposed approach in protecting analog circuits against counterfeiting and reverse engineering attacks, which are common threats in the semiconductor industry.

As a future direction, we plan to validate the methodology in silicon by utilizing a commercial foundry service. This step will provide a realistic scenario of outsourcing, where the circuit is fabricated by a third-party foundry. By implementing the proposed approach in silicon, the authors can evaluate its practicality, performance, and effectiveness in a real-world setting.

Acknowledgements This work has received partial funding from the European Union through the European Social Fund as part of the "ICT programme". Additionally, it has also been supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 952252 (SAFEST).

Funding Open Access funding provided by Carnegie Mellon University

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Bhasin, S., Regazzoni, F.: A survey on hardware trojan detection techniques. In: 2015 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 2021–2024 (2015). https://doi.org/10.1109/ISCAS.2015.7169073
2. Dupuis, S., Ba, P.-S., Di Natale, G., Flottes, M.-L., Rouzeyre, B.: A novel hardware logic encryption technique for thwarting illegal overproduction and hardware trojans. In: 2014 IEEE 20th International On-Line Testing Symposium (IOLTS), pp. 49–54 (2014). https://doi.org/10.1109/IOLTS.2014.6873671
3. Jacob, N., Merli, D., Heyszl, J., Sigl, G.: Hardware trojans: current challenges and approaches. IET Comput. Digit. Tech. **8**(6), 264–273 (2014)
4. Keshavarz, S., Yu, C., Ghandali, S., Xu, X., Holcomb, D.: Survey on applications of formal methods in reverse engineering and intellectual property protection. J. Hardw. Syst. Secur. **2**(3), 214–224 (2018)
5. SEMI: White paper: innovation at risk–intellectual property challenges and opportunities. Technical report (2008)
6. Colombier, B., Bossuet, L.: Survey of hardware protection of design data for integrated circuits and intellectual properties. IET Comput. Digit. Tech. **8**(6), 274–287 (2014)
7. Rajendran, J., Sinanoglu, O., Karri, R.: Regaining trust in VLSI design: design-for-trust techniques. Proc. IEEE **102**(8), 1266–1282 (2014)
8. Roy, J.A., Koushanfar, F., Markov, I.L.: Ending piracy of integrated circuits. Computer **43**(10), 30–38 (2010)
9. Sanabria-Borbon, A., Jayasankaran, N.G., Lee, S., Sánchez-Sinencio, E., Hu, J., Rajendran, J.: Schmitt trigger-based key provisioning for locking analog/RF integrated circuits. In: 2020 IEEE International Test Conference (ITC), pp. 1–10. IEEE (2020)
10. Elshamy, M., Sayed, A., Louërat, M.-M., Rhouni, A., Aboushady, H., Stratigopoulos, H.-G.: Securing programmable analog ICs against piracy. In: 2020 Design, Automation and Test in Europe Conference and Exhibition (DATE), pp. 61–66. IEEE (2020)
11. Hoe, D.H., Rajendran, J., Karri, R.: Towards secure analog designs: a secure sense amplifier using memristors. In: 2014 IEEE Computer Society Annual Symposium on VLSI, pp. 516–521. IEEE (2014)
12. Rao, V.V., Savidis, I.: Protecting analog circuits with parameter biasing obfuscation. In: 2017 18th IEEE Latin American Test Symposium (LATS),pp. 1–6. IEEE (2017)
13. Wang, J., Shi, C., Sanabria-Borbon, A., Sánchez-Sinencio, E., Hu, J.: Thwarting analog IC piracy via combinational locking. In: 2017 IEEE International Test Conference (ITC), pp. 1–10. IEEE (2017)
14. Nimmalapudi, S.G.R., Volanis, G., Lu, Y., Antonopoulos, A., Marshall, A., Makris, Y.: Range-controlled floating-gate transistors: a

unified solution for unlocking and calibrating analog ICs. In: 2020 Design, Automation and Test in Europe Conference and Exhibition (DATE), pp. 286–289. IEEE (2020)
15. Ash-Saki, A., Ghosh, S.: How multi-threshold designs can protect analog IPs. In: 2018 IEEE 36th International Conference on Computer Design (ICCD), pp. 464–471. IEEE (2018)
16. Volanis, G., Lu, Y., Nimmalapudi, S.G.R., Antonopoulos, A., Marshall, A., Makris, Y.: Analog performance locking through neural network-based biasing. In: 2019 IEEE 37th VLSI Test Symposium (VTS), pp. 1–6. IEEE (2019)
17. Elshamy, M., Sayed, A., Louërat, M.-M., Rhouni, A., Aboushady, H., Stratigopoulos, H.-G.: Securing programmable analog ICs against piracy. In: 2020 Design, Automation and Test in Europe Conference and Exhibition (DATE), pp. 61–66. IEEE (2020)
18. Tlili, M., Sayed, A., Mahmoud, D., Louërat, M.-M., Aboushady, H., Stratigopoulos, H.-G.: Anti-piracy of analog and mixed-signal circuits in FD-SOI. In: 2022 27th Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 423–428. IEEE (2022)
19. Jayasankaran, N.G., Borbon, A.S., Sanchez-Sinencio, E., Hu, J., Rajendran, J.: Towards provably-secure analog and mixed-signal locking against overproduction. In: Proceedings of the International Conference on Computer-Aided Design, 1–8 (2018)
20. Leonhard, J., Yasin, M., Turk, S., Nabeel, M.T., Louërat, M.-M., Chotin-Avot, R., Aboushady, H., Sinanoglu, O., Stratigopoulos, H.-G.: Mixlock: securing mixed-signal circuits via logic locking. In: 2019 Design, Automation and Test in Europe Conference and Exhibition (DATE), pp. 84–89. IEEE (2019)
21. Rao, V.V., Juretus, K., Savidis, I.: Security vulnerabilities of obfuscated analog circuits. In: 2020 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1–5. IEEE (2020)
22. Jayasankaran, N.G., Sanabria-Borbón, A., Abuellil, A., Sánchez-Sinencio, E., Hu, J., Rajendran, J.: Breaking analog locking techniques. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **28**(10), 2157–2170 (2020)
23. Leonhard, J., Elshamy, M., Louërat, M.-M., Stratigopoulos, H.-G.: Breaking analog biasing locking techniques via re-synthesis. In: Proceedings of the 26th Asia and South Pacific Design Automation Conference, pp. 555–560 (2021)
24. Acharya, R.Y., Chowdhury, S., Ganji, F., Forte, D.: Attack of the genes: finding keys and parameters of locked analog ICs using genetic algorithm. In: 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 284–294. IEEE (2020)
25. Aljafar, M.J., Azaïs, F., Flottes, M.-L., Pagliarini, S.: Leveraging layout-based effects for locking analog ICs. In: Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security. ASHES'22, pp. 5–13. Association for Computing Machinery, New York, NY, USA (2022). https://doi.org/10.1145/3560834.3563826
26. Intelligence Advanced Research Projects Activity (IARPA): Rapid Analysis of Various Emerging Nanoelectronics (RAVEN). https://www.iarpa.gov/index.php/research-programs/raven
27. Rajendran, J., Pino, Y., Sinanoglu, O., Karri, R.: Logic encryption: a fault analysis perspective. In: 2012 Design, Automation and Test in Europe Conference and Exhibition (DATE), pp. 953–958. IEEE (2012)
28. Yasin, M., Mazumdar, B., Sinanoglu, O., Rajendran, J.: Removal attacks on logic locking and camouflaging techniques. IEEE Trans. Emerg. Top. Comput. **8**(2), 517–532 (2017)
29. Subramanyan, P., Ray, S., Malik, S.: Evaluating the security of logic encryption algorithms. In: 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 137–143. IEEE (2015)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.