Analog Circuit Anti-Piracy Security by Exploiting Device Ratings

Hazem H. Hammam, Hassan Aboushady, Haralampos-G. Stratigopoulos

Analog Circuit Anti-Piracy Security by Exploiting Device Ratings

Hazem H. Hammam, Hassan Aboushady and Haralampos-G. Stratigopoulos
Sorbonne Université, CNRS, LIP6, Paris, France

***Abstract*—We propose a novel anti-piracy security technique for analog and mixed-signal (AMS) circuits. The circuit is re-designed by obfuscating transistors and capacitors with key-controlled versions. We obfuscate both the device geometries and their ratings, which define the maximum allowable current, voltage, and power dissipation. The circuit is designed to function correctly only with a specific key. Loading any other incorrect key degrades performance and for the vast majority of these keys the chip is damaged because of electrical over-stress. This prevents counter-attacks that employ a chip to search for the correct key. The methodology is demonstrated on a low-dropout regulator (LDO) designed in the 22nm FDSOI technology by GlobalFoundries. By locking the LDO, the entire chip functionality breaks unless the LDO is unlocked first. The secured LDO shows no performance penalty and area overhead is justifiable and less than 25%, while it is protected against all known counter-attacks in the AMS domain.**

***Index Terms*—Hardware security and trust, IC piracy, locking, analog and mixed-signal ICs, low-dropout regulator.**

I. Introduction

In today's globalized Integrated Circuit (IC) supply chain, an IC design is shared with third parties that are potentially untrusted. Consequently, IC designers are largely preoccupied with preserving the ownership of their IC [1]. In particular, a common type of business model in IC industry is the design of specialized and high performance intellectual property (IP) blocks which are licensed to other companies to be integrated in larger designs. Once the IP has been transferred to another company, the ownership is practically lost instantly, albeit the design is a several months to years effort demanding high expertise. In addition, most IC companies are fabless outsourcing chip fabrication to a foundry that is often offshore. Again, the design ownership is lost instantly when the GDSII file is sent to the foundry. In both scenarios, the IP/IC can be pirated and reused without the IP/IC owner knowing it and without being remunerated. Nowadays, ownership protection is a contractual confidentiality agreement between the two parties often reinforced by security audits. In fact, the risk of piracy is even greater considering the increased capability of chip reverse-engineers [2]. An attacker can legally purchase a chip from the market and via reverse engineering can extract the circuit netlist. Therefore, there is a pressing demand for IP/IC designers to incorporate a rigorous and systematic method to effectively secure the design ownership.

This work was funded by the Chips JU project Resilient Trust of the EU's Horizon Europe research and innovation programme under Grant agreement N^{o} 101112282.

The most promising anti-piracy technique is locking as it provides an end-to-end protection across the supply chain [3]–[5]. Locking renders the behavior of the circuit key-dependent, where the key K is a bit-string. Given a circuit with input I and output O such that $O = f(I)$, locking embeds into the circuit a keying mechanism, making internal nodes controlled by key-bits, i.e., $O = f(I, K)$. The correct key K_{cor} must be applied to set the correct functionality, i.e., for any incorrect key $K_{incor} \neq K_{cor}$ we have $f(I, K_{cor}) \neq f(I, K_{incor})$ for some inputs I. The correct key becomes the secret of the designer and is not shared with any untrusted third party. Then, the chip is securely activated by storing the correct key in a tamper-resistant non-volatile memory.

This work focuses on locking analog and mixed-signal (AMS) ICs. The vast majority of locking approaches for AMS ICs do not attempt to lock the core of purely analog blocks so as to avoid putting any burden on the analog designer. This is because analog blocks are sensitive to any modification and meeting the zero performance penalty objective becomes a challenging task. More specifically, the keying mechanism is inserted into the biasing circuitry [6], into a digital section [7]–[10], or it acts on the calibration [11]–[14]. Locking digital sections enables locking only at the system-level, thus leaving the analog blocks unprotected and vulnerable to piracy. Calibration locking uses the digital tuning as secret key, thus it requires multi-bit programmability and assumes that the calibration algorithm is unknown to the attacker, which are conditions that are rarely met. Biasing locking, on the other hand, does not offer strong security as several counter-attacks exist [15]–[18] (see Section VI).

Inevitably, inserting a keying mechanism into analog cores becomes a design objective. Two analog core locking approaches can be found in the literature [19], [20]. In [19], transistor geometry obfuscation is proposed by replacing a transistor with parallel connected transistors of different widths. Each transistor is controlled by a switch driven by a key-bit. The key defines which transistors are on and the correct key sets the correct effective width. Alternatively, a transistor can be replaced by a mesh structure of parallel and serially connected transistors to obfuscate both length and width. However, this geometry obfuscation strategy requires more significant design effort to meet the intent performances. In [20], it is proposed to leverage layout-dependent effects (LDEs). Three transistors are used in parallel with different layout arrangements, each displaying different LDEs. The key sets on the transistor with which the circuit is being designed. In both approaches, an

incorrect key results in performance variations and ideally one or more specifications should be violated. For N obfuscated transistors, the key size is $2^{\sum(n_i+1)}$ for geometry obfuscation, where n_i is the number of extra obfuscation transistors for the i-th obfuscated transistor, and $2^{3\times N}$ for LDE obfuscation.

Note that there also exist key-less obfuscation approaches [21]–[23], but these can defend only against reverse-engineering [21], [22] or an untrusted foundry [23].

In this work, we propose a novel analog core locking methodology having the comparative advantage with respect to [19], [20] that an incorrect key trial is very likely to break down a device and damage the chip. In this way, the method offers an innate defense against any count-attack that performs key trials on a chip. This property is achieved by obfuscating, in addition to the geometry, the rating of the devices. Furthermore, while [19], [20] focus on transistor obfuscation, we also obfuscate capacitors. In analog feedback loops, the capacitor is typically used to control the loop stability and high-frequency response. Thus, by obfuscating capacitors, not only adds more flexibility for enlarging the key size, but an incorrect key may render the circuit unstable having a catastrophic effect.

The idea is demonstrated by designing a locked version of a low dropout voltage regulator (LDO) circuit in the 22nm FDSOI technology by GlobalFoundries. Locking an LDO is an excellent choice as all circuits in the chip supplied by the LDO are non-functional unless the LDO is unlocked first.

In [19], the case studies are a bandpass filter and an op-amp demonstrating obfuscation with small key sizes of 10-bits and 12-bits in the reach of a brute-force attack. The circuit area increased by $2.2\times$ and $1.57\times$ for parallel transistor obfuscation and by $2.7\times$ and $2.24\times$ for mesh transistor obfuscation. A similar large overhead was reported for an op-amp in [20]. Herein, we show a 18-bits key secured LDO with zero performance penalty across process, voltage, and temperature (PVT) corners and only 25% area overhead.

The rest of this article is structured as follows. In Section II, we present the proposed locking methodology. In Section III, we argue why locking an LDO is an excellent choice for global chip security. In Section, IV, we present the un-secured LDO design. In Section V, we present its locked version and the results. In Section VI, we discuss known counter-attacks in the AMS domain and we demonstrate the robustness of the proposed methodology. Section VII concludes this article.

II. Proposed Analog Obfuscation Methodology

A. IC design with device ratings

AMS circuits are generally supplied by different voltages depending on the application and the circuit type. Low-power applications, low-speed designs, and digital circuits are commonly supplied by a low-voltage. On the other hand, high-power, high-frequency applications and automotive circuits require high voltages. Thus, most of the Process Design Kits (PDKs) have different device ratings to support different ranges of power supply without any electrical over-stress issues. For example, in the PDK of the 22nm FDSOI technology by GlobalFoundries which is used for our LDO case study, 6.5V, 5V, 2.5V, and 1.8V rated transistors and MOM capacitors are available.

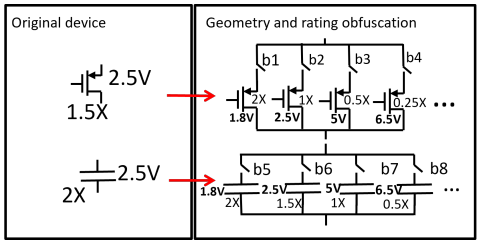

Fig. 1: Principle of geometry and rating obfuscation.

B. Principle of obfuscation

The proposed methodology exploits the ratings of transistors and capacitors that define the maximum allowable current and voltage across their terminals, as well as the maximum power dissipation. A device (transistor or capacitor) is replaced with parallel-connected devices that have different geometries and ratings, as illustrated in Fig. 1. Each device i is made on/off thanks to a switch controlled by a key-bit b_i. A key-bit "1" enables the device, whereas a key-bit "0" disconnects it. There is only one key-bit combination that is correct, setting the correct effective geometry $X_{eff} = \sum b_i * X_i$, where for transistors X is the width and for capacitors X is the capacitance. The circuit is designed with this combination to meet the intent performances. An invalid key will set an erroneous geometry, thus the circuit performances will deviate. An invalid key may also lead to one or more activated devices experiencing electrical over-stress (EOS), i.e., the voltage across the terminals will exceed the rating, which will break down the device and damage the chip metals and layers. This is a desired and sought-after property from a security perspective as it defers an attacker from performing a counter-attack to extract the secret key using a "virgin" chip that does not have the key provisioned yet. Incorrect key trials will sooner or later break the chip and the attack will fail.

Fig. 1 shows an example of obfuscating a PMOS transistor of 2.5V rating, width 1.5X, and nominal source-to-drain voltage V_{sd} 2.5V, and a MOM capacitor of 2.5V rating and value 2X, where X denotes a unit value. The transistor is obfuscated by adding 3 extra parallel sub-transistors with 1.8V rating and 2X width, 5V rating and 0.5X width, and 6.5V rating and 0.25X width. The correct key $b1b2b3b4$=0110 enables the 2.5V and 5V rating transistors of overall 1.5X width. It is easy to confirm that there is a single correct key as any other key will result in a width in the ranges $[0.25\text{X}, \cdots, 1.25\text{X}]$ or $[1.75\text{X}, \cdots, 3.75\text{X}]$ with a 0.25X step. An incorrect key alters the operating point of all devices in the circuit and, therefore, will alter the V_{sd} of the obfuscated transistor as well. If for an incorrect key the obfuscated transistor experiences $V_{sd}^{'}$, then any sub-transistor with rating $V_{sd,max}$ such that $V_{sd} > V_{sd,max}$ will suffer EOS. For example, if for an incorrect key $b1b2b3b4$=1XXX the new V_{sd} value is 2.1V, then the sub-transistor with 1.8V rating will suffer EOS. Regarding

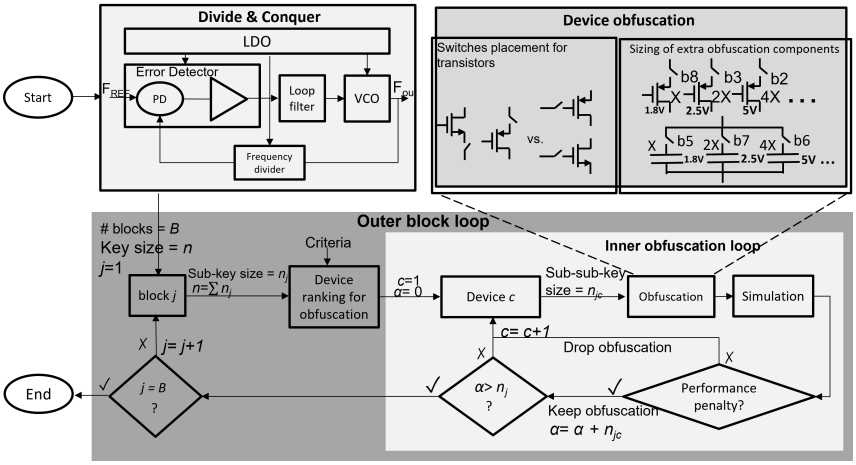

Fig. 2: Analog design using the proposed locking approach.

the MOM capacitor, the correct key is $b5b6b7b8$=0101, but there is a second key $b5b6b7b8$=1000 which also correctly sets the capacitance value to 2X. However, it may be the case that for the key $b5b6b7b8$=1000 the voltage across the capacitor will be larger than 1.8V, making the left-hand "on" sub-capacitor suffering EOS. In summary, unless the correct key is set, the devices are erroneously sized resulting in a shifted performance trade-off and/or suffering EOS.

C. Threat model

We consider the most pessimistic threat model for the circuit owner. In particular, we assume that the adversary possesses the circuit netlist and an oracle chip, and knows the rating of each device. However, without knowing the secret key, the adversary does not know the nominal voltage across the devices' terminals and, thereby, cannot pre-set some key-bits to prune down the key space based on the ratings of devices. The nominal voltage may as well be smaller than the minimum rating and the sub-device with the smallest rating may need to be "on" to set the correct geometry. Selecting devices with maximum rating to avoid EOS will set incorrect effective geometries. Incorrect key trials on a chip will eventually damage it due to device EOS.

D. Methodology steps

We integrate obfuscation into the design plan, balancing competing objectives such as large key-size, low obfuscation overhead, and zero performance penalty. Next, we explain the different steps, illustrated also in Fig. 2, and provide guidelines for the analog designer.

- *Step 1: Divide & Conquer*. A large design is decomposed into its main blocks and obfuscation is performed on a block-by-block basis. For example, Fig. 2 shows a phase-locked loop (PLL) with its error detector and voltage-controlled oscillator (VCO) biased by an LDO. Obfuscating every individual block forces the attacker to de-obfuscate the circuit altogether rather than block-by-block thanks to feedback loops and block inter-dependencies. This makes the implementation of an attack harder and the attack convergence time longer.
- *Step 2: Key size*. The objective is to introduce for the entire circuit a key size n that provides the desired security level. At this stage the security level is determined by the average cost for a brute-force attack to succeed and the objective is to set a key size that makes the attack impracticable (see Section VI). The designer can pre-assign a sub-key size budget per block such that $n = \sum_{j=1}^{B} n_j$, where n_j is the sub-key size for block j and B is the number of blocks.
- *Step 3: Device ranking for obfuscation*. Given a block, the designer ranks device candidates for obfuscation based on different criteria: (a) output sensitivity to component variations (the highest the sensitivity is, the highest the functionality corruption is for incorrect keys); (b) obfuscation effect (i.e., performance variation, circuit instability); (c) performance penalty for the correct key (ideally zero); (d) obfuscation area overhead (the larger the layout of the device is, the larger the obfuscation area overhead will be).
- *Step 4: Obfuscation loop*. The designer starts from the top of the list and obfuscates devices one at a time so as to have control over the performance penalty and area overhead. For each device c, a sub-sub-key size n_{jc} is determined based on the device layout size and a rough calculation of the area overhead so as to stay within the area overhead budget. The device is obfuscated (see *Step 5*) and simulation is carried out to verify that for the correct key the intent performance trade-off is unchanged or minimally affected across PVT variations. Whenever the performance penalty cannot be confined, the device is dropped from the candidate list and we move on to the next device. To examine functionality corruption, simulations can be performed for incorrect sub-sub-keys while setting correct key-bits for all previously obfuscated devices within all blocks. This simulation effort is tractable compared to trying full-dimensional keys. During the obfuscation loop we keep track of the current block sub-key size with a parameter α. We exit the obfuscation loop when we meet the target sub-key size n_j for the block.
- *Step 5: Device obfuscation*. Devices are obfuscated by replacing them with parallel-connected devices of different ge-

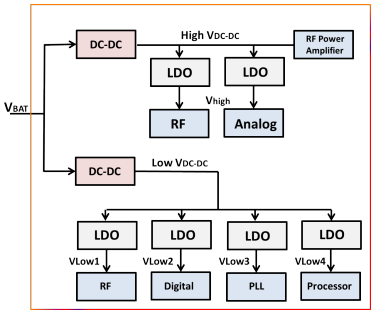

Fig. 3: LDO utilization in chip design.

ometries and ratings, as described in Section II-B. Switches should have minimum sizing towards zero performance penalty and low area overhead. They can be connected to the gate or placed in series with the drain or source. The best placement choice depends on the headroom, dropout, and sensitivity of the loop stability or power supply rejection (PSR) on the gate capacitance. The placement decision should be made per transistor. When obfuscating a device, ideally there should be a single correct sub-key and any incorrect sub-key should result in significant performance degradation a set percentage away from the specification. To meet this objective, the guideline is to use sub-devices with binary-weighted geometries, i.e., each key-bit adds or removes a $\pm$ 2×, 4×, 8×,$\cdots$ of a unit size component, so as to impose a large performance shift per one key-bit step. Finally, sub-devices should have a mixture of ratings so as to inflict EOS for incorrect sub-keys.

In the end, incorrect full-dimensional keys can be randomly selected and simulated in a brute-force fashion for a time that is considered reasonable for an attacker before the attacker is discouraged and gives up.

III. LDO Locking

Locking an LDO offers auxiliary security beyond the protection of the LDO itself. As shown in Fig. 3, this is because the LDO is widely used in any IC with its purpose being to provide a regulated supply voltage to the analog and digital blocks. This regulated supply voltage is noise-free with minimal variation under manufacturing process variations, temperature fluctuations, and electrical disturbances such as battery voltage variation. Therefore, locking the LDOs indirectly locks the entire IC and unlocking the IC requires first unlocking the LDOs. As we will show, with the proposed locking methodology, the unlocking effort boils down to redesigning the LDO, which is beyond what an attacker is willing to do.

IV. LDO Design

Fig. 4 shows the schematic of the original un-secured LDO designed in the 22nm FDSOI technology by GlobalFoundries. The pass device (MPT) provides a specific dropout at a given load current range and generates the output voltage (VOUT). The error amplifier in the loop is a 5-transistor operational transconductance amplifier (OTA) biased by a biasing current (IBIAS) from a bandgap reference circuit (BGR), not shown

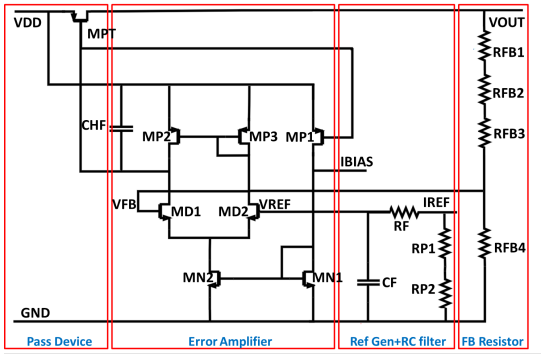

Fig. 4: Original un-secured LDO circuit.

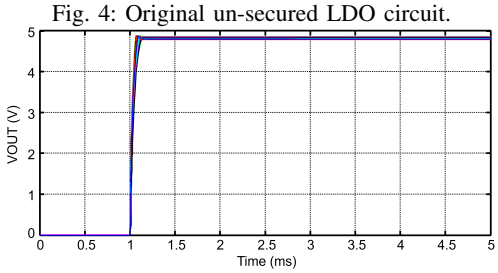

Fig. 5: LDO output voltage across PVT.

in Fig. 4, in addition to a load-dependent bias current mirrored from MPT [24]. The OTA sets its two inputs to be equal and its output biases MPT controlling its dropout. The reference voltage (VREF) at the negative input of the error amplifier is generated from the same BGR with a soft start low pass filter (RF and RC). Also, there is a feedback resistive divider (RFB1, RFB2, RFB3, and RFB4) that sends a feedback divided ratio (VFB) of the output to the error amplifier's positive input. A capacitor CHF is added between the error amplifier output and the supply to couple the high-frequency noise from the supply to the gate of MPT. This improves the high-frequency PSR of the LDO output [25].

The LDO is designed to have a typical pass device dropout of 200 mV at 10 mA load current. Figs. 5, 6, and 7 show the simulated VOUT, output PSR, and loop stability, i.e., gain margin (GM) and phase margin (PM), across PVT variations. The supply is typically 5V with +/- 10% variation. The temperature range is from -40°C to 125°C. The output voltage has typical, minimum, and maximum values of 4.8V, 4.754V, and 4.824V, respectively, i.e., less than 1% variation. The PSR shows a typical DC value of -35 dB and a typical high-frequency value of -33 dB up to 100 MHz. The minimum DC PSR is -32 dB and the minimum high-frequency PSR is -30 dB, i.e., less than 10% variation. The minimum loop gain is 50 dB, the minimum PM is 58 degrees, and the minimum GM is 18 dB, corresponding to less than 20% variation from their typical values. The typical quiescent current of the whole LDO is 7.5 μA and the maximum value across PVT is 12 μA.

V. LDO Obfuscation and Results

Fig. 8 shows the modified LDO design to embed the keying mechanism. Seven devices are obfuscated, each replaced with three parallel-connected sub-devices. A knowledgeable attacker understands that MP2 and MP3 in the OTA should

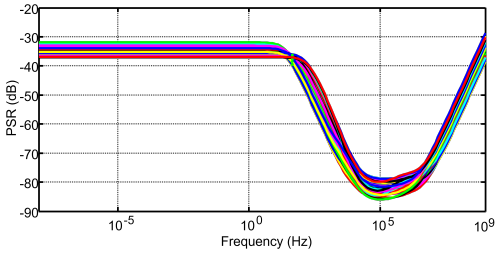

Fig. 6: LDO output PSR across PVT.

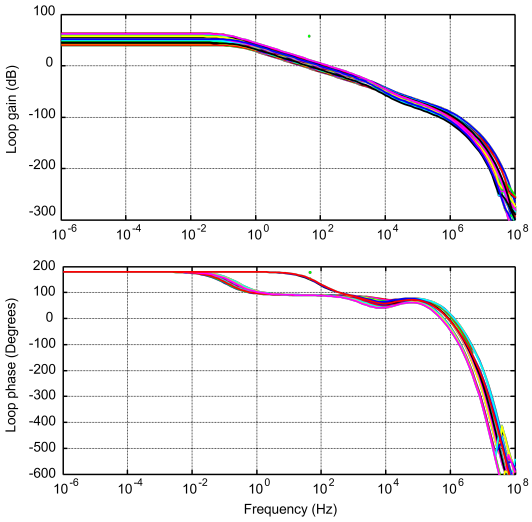

Fig. 7: LDO loop stability across PVT.

be identical and, thereby, they should be driven by the same sub-key. Thus, the effective key size is $6 * 3 = 18$ bits. The obfuscation is done following the steps and guidelines of Section II-D. There is a single correct key and sub-devices have varying ratings.

The switches are designed with maximum rating and are placed in series for all devices except MPT. This is because the branch currents are very low in the μA range, so the switches' dropout voltages are low. Connecting them to the gates would have a non-negligible effect on the PSR and loop stability. In contrast, for the MPT, the least invasive option is to connect the switches to the gates of its sub-devices. This is because the MPT handles the large load current, so adding switches in series would require large switches for minimal dropout, which would increase the area overhead of the keying mechanism. Also, adding them in series would affect the output resistance of the MPT and, thereby, the loop gain.

Fig. 9 shows the resultant LDO performances variation when using the correct key and 4000 random incorrect keys. Each piecewise line corresponds to using a different key and connects the performance deviation values resulting from using this key. Fig. 9 also shows the specification bounds for each performance, derived from the PVT analysis in Section IV. The thick nearly straight line around 0% variation corresponds to the correct key. In contrast, for all incorrect keys the line exceeds the specification bounds for at least one performance. Few incorrect keys result in a maximum of 2 or 3 performances being within the specifications. After 2 weeks

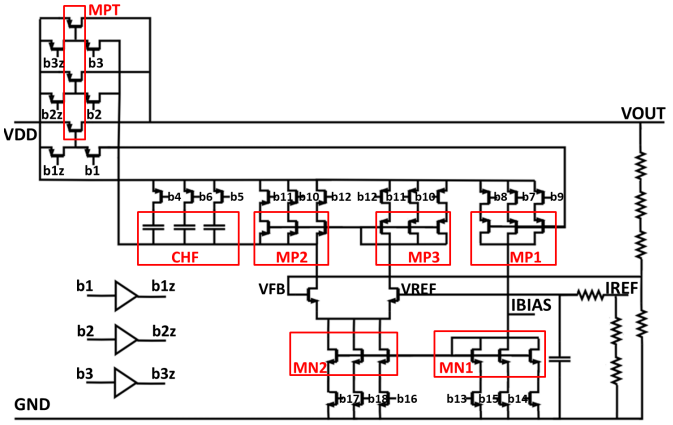

Fig. 8: Secured LDO with embedded keying mechanism.

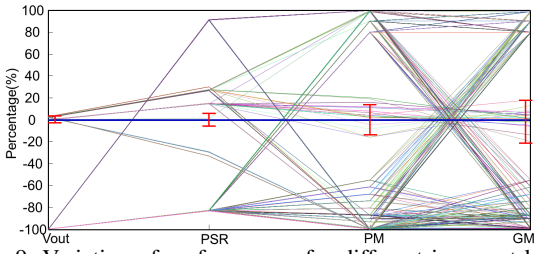

Fig. 9: Variation of performances for different incorrect keys.

of different possible key trials, only the correct key showed the correct performance. 90% of incorrect keys resulted in larger than 100% variation for all performances and 80% in EOS warnings during simulations.

Fig. 10 shows the four performances across PVT variations using the correct key. As it can be seen, performance variations are confined within the specification bounds, thus adding the keying mechanism has minimal effect, guaranteeing no performance penalty across PVT variations. Note that the typical quiescent current changes only for incorrect keys, thus for the correct key there is zero power consumption overhead. Another illustration that device obfuscation incurs no performance penalty is shown in Fig. 11, which plots the histogram of the Monte Carlo variation of VOUT at maximum and minimum temperature and supply conditions for the un-secured design and the secured design using the correct key. As it can be seen, the VOUT variation is similar and below 0.85%.

Finally, Fig. 12 shows the layout of the secured LDO. The added obfuscation devices are highlighted with yellow rectangles. The new LDO area is 225 μm $\times$ 150 μm, incurring less than 25% area overhead compared to the un-secured design.

VI. Security Analysis

The proposed technique is by design resilient to any attack that employs chip measurements thanks to device rating obfuscation. The chip will be damaged no later than after a few incorrect key trials. At simulation level, devices that undergo EOS due to incorrect key may be simulated with errors with the simulator giving a warning. In general, simulation time for AMS ICs can be very long. For example, simulating all

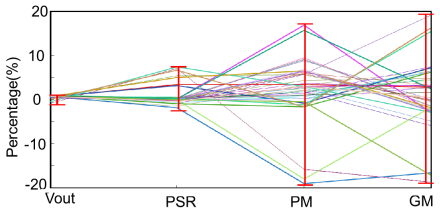

Fig. 10: Performance variation across PVT using the correct key.

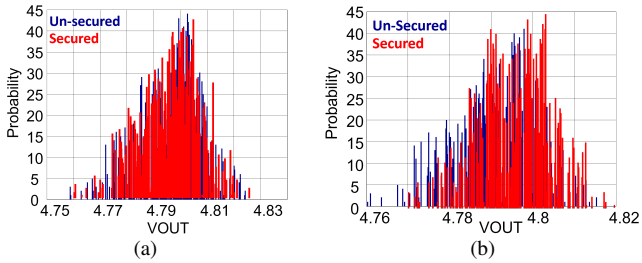

Fig. 11: Monte Carlo VOUT simulation for (a) maximum and (b) minimum temperature and supply.

test benches of a PLL shown in Fig. 2 takes hours. For the LDO, the key size is $n = 18$ bits and the simulation time is about 30 sec. Next, we discuss the resilience against all known counter-attacks in the AMS domain.

- *Brute-force attack*: The attacker uses a trial and error tactic to identify a working key. The attack is more practical by trying keys on an actual chip, thus the proposed technique is inherently resilient. At simulation level, the cost is $2^{18} * 30\,sec \approx 91$ days, which is prohibitive for an attacker.
- *Monotonic attack [18]*: Finding the key can be quick if there is a monotonic relationship between the performances and key, which, in general, holds true for a single obfuscated device. In the case of multiple device obfuscation, an incorrect key sets erroneously the operating point of the devices and the performances. As a result, the relationships between sub-keys and performances are not the right ones to query them individually and sequentially to identify the correct sub-keys. The devices will need to be de-obfuscated simultaneously.
- *SMT attack [15]*: The attacker develops circuit equations and solves them using satisfiability modulo theory (SMT). For example, for biasing locking, circuit equations include: $I_i^{'} = \psi(K_i)$ that expresses the biasing current $I_i^{'}$ generated by the i-th locked biasing circuit as a function of its key K_i, $i = 1, \cdots, M$, M is the number of obfuscated biasing circuits, and $P = \theta(I_1, \cdots, I_M)$ that expresses the performance vector as a function of the specified biasing currents $I = [I_1, \cdots, I_M]$. The attacker also sets a range for the biasing currents $I_i^{min} < I_i < I_i^{max}$. An SMT-solver is used to find a set of keys that satisfies the combined equation $P = \theta(\psi(K_1), \cdots, \psi(K_M))$ such that $I_i^{'} = I_i$ or $I_i^{min} < I_i^{'} < I_i^{max}$ $\forall i$. This attack requires knowing I_i. Projecting it to our proposed technique, it is not applicable as the attacker does not know the nominal values of the internal branches' currents. Besides, deriving the equation $P = \theta(I)$ is not trivial even for simple circuits, and even when a simplified Spice level 1 transistor model is used.

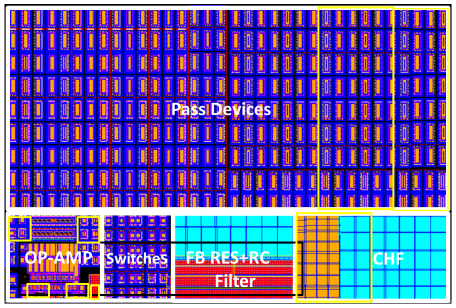

Fig. 12: Layout of secured LDO.

- *Optimization attacks*: In [17], a genetic algorithm (GA) is employed to search in the space of keys. The fitness function is the matching between the simulated response and the measured response on an oracle chip with the correct key stored. For the LDO obfuscation, given the single correct key and the binary-weighted geometries of the sub-devices, the fitness behaves as a delta function on the correct key, thus the optimization will "zigzag" endlessly or convergence will be very slow approximating the brute-force effort. In [16], the counter-attack is on a locked current mirror that provides the bias current. First, the current mirror is replaced with a fresh non-locked version. Then, a circuit sizing tool is used to meet the intent performances where the core of the circuit is fixed and the only unknown parameters in the optimization are those of the current mirror. As in the secured LDO design multiple devices are obfuscated, this attack boils down to resizing the entire circuit. Thus, the attacker will have thereafter to redesign the layout, which is beyond the capabilities we assume for an attacker.
- *Key spacing attack [18]*: If attention is not paid on how the transistor obfuscation is done, the nominal width W_{cor} may have a large exclusion zone around it, i.e., the width W_{incor} for any incorrect key satisfies $|W_{incor} - W_{cor}| > \epsilon$. In this case, the attack consists of searching in the space of keys and ruling them out if the resultant width falls close to the resultant width for a previously tried key. This attack can be fast as it is applied on the isolated obfuscated devices. However, in our approach, given the binary-weighted geometries of the sub-devices, the keys produce widths of equal spacing, thus thwarting this attack.

VII. Conclusion

We presented a locking methodology for AMS ICs that can be applied even to purely analog blocks. Locking is based on obfuscating both the geometry and the rating of devices. By obfuscating the rating, we nullify any counter-attack that performs key trials on a chip. The methodology is demonstrated on an LDO. Locking the LDOs in a chip makes the entire chip fail unless the correct LDO keys are uploaded. The secured LDO design has a single 18-bit correct key, shows no performance penalty for the correct key and high functionality corruption or chip damage for incorrect keys, and is resilient to any known counter-attack, having a 25% area overhead compared to the original un-secured design.

REFERENCES

[1] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug. 2014.

[2] B. Lippmann *et al.*, "Integrated flow for reverse engineering of nanoscale technologies," in *Proc. 24th Asia and South Pacific Design Automat. Conf.*, Jan. 2019, p. 82–89.

[3] A. Chakraborty *et al.*, "Keynote: A disquisition on logic locking," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 39, no. 10, pp. 1952–1972, Oct. 2020.

[4] M. Yasin, J. Rajendran, and O. Sinanoglu, *Trustworthy Hardware Design: Combinational Logic Locking Techniques*, Springer, 2020.

[5] K. Z. Azar, H. M. Kamali, F. Farahmandi, and M. Tehranipoor, *Understanding Logic Locking*, Springer, 2023.

[6] J. Wang, C. Shi, A. Sanabria-Borbon, E. Sánchez-Sinencio, and J. Hu, "Thwarting analog IC piracy via combinational locking," in *Proc. IEEE Int. Test Conf. (ITC)*, Oct. 2017.

[7] N. G. Jayasankaran, A. S. Borbon, E. Sanchez-Sinencio, J. Hu, and J. Rajendran, "Towards provably-secure analog and mixed-signal locking against overproduction," in *Proc. 18th Int. Conf. Comput.-Aided Design (ICCAD)*, Nov. 2018.

[8] J. Leonhard *et al.*, "Digitally-assisted mixed-signal circuit security," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 41, no. 8, pp. 2449–2462, Aug. 2021.

[9] A. R. Díaz-Rizo, J. Leonhard, H. Aboushady, and H. Stratigopoulos, "RF transceiver security against piracy attacks," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 69, no. 7, pp. 3169–3173, Jul. 2022.

[10] A. R. Díaz-Rizo, H. Aboushady, and H.-G. Stratigopoulos, "Anti-piracy design of RF transceivers," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 70, no. 1, pp. 492–505, Jan. 2023.

[11] M. Elshamy, A. Sayed, M.-M. Louërat, A. Rhouni, H. Aboushady, and H.-G. Stratigopoulos, "Securing programmable analog ICs against piracy," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2020, pp. 61–66.

[12] S. G. Rao Nimmalapudi, G. Volanis, Y. Lu, A. Antonopoulos, A. Marshall, and Y. Makris, "Range-controlled floating-gate transistors: A unified solution for unlocking and calibrating analog ICs," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar 2020.

[13] M. Elshamy, A. Sayed, M.-M. Louërat, H. Aboushady, and H.-G. Stratigopoulos, "Locking by untuning: A lock-less approach for analog and mixed-signal IC security," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 29, no. 12, pp. 2130–2142, Dec. 2021.

[14] M. Tlili, A. Sayed, D. Mahmoud, M.-M. Louërat, H. Aboushady, and H.-G. Stratigopoulos, "Anti-piracy of analog and mixed-signal circuits in FD-SOI," in *Proc. Asia South Pac. Design Autom. Conf. (ASP-DAC)*, Jan. 2022, pp. 423–428.

[15] N. G. Jayasankaran, A. Sanabria Borbon, A. Abuellil, E. Sánchez-Sinencio, J. Hu, and J. Rajendran, "Breaking analog locking techniques via satisfiability modulo theories," in *Proc. IEEE Int. Test Conf. (ITC)*, Nov. 2019, Paper 9.1.

[16] J. Leonhard, M. Elshamy, M.-M. Louërat, and H.-G. Stratigopoulos, "Breaking analog biasing locking techniques via re-synthesis," in *Proc. 26th Asia South Pacific Design Automat. Conf.*, Jan. 2021, p. 555–560.

[17] R. Y. Acharya, S. Chowdhury, F. Ganji, and D. Forte, "Attack of the genes: Finding keys and parameters of locked analog ICs using genetic algorithm," in *Proc. IEEE Int. Symp.Hardw. Oriented Secur. Trust (HOST)*, Dec. 2020, pp. 284–294.

[18] V. V. Rao, K. Juretus, and I. Savidis, "Security vulnerabilities of obfuscated analog circuits," in *Proc. IEEE Int. Symp. Circuits and Syst. (ISCAS)*, Oct. 2020.

[19] V. Rao and I. Savidis, "Performance and security analysis of parameter-obfuscated analog circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 29, no. 12, pp. 2013–2026, Dec. 2021.

[20] M. J. Aljafar, F. Azaïs, M.-L. Flottes, and S. Pagliarini, "Leveraging layout-based effects for locking analog ICs," in *Proc. Workshop on Attacks and Solutions in Hardware Security (ASHES)*, Nov. 2022.

[21] A. Ash-Saki and S. Ghosh, "How multi-threshold designs can protect analog IPs," in *Proc. IEEE Int. Conf. Comput. Design (ICCD)*, Oct. 2018, pp. 464–471.

[22] J. Leonhard, A. Sayed, M.-M. Louërat, H. Aboushady, and H.-G. Stratigopoulos, "Analog and mixed-signal IC security via sizing camouflaging," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 5, pp. 822–835, Jul. 2021.

[23] M. R. Muttaki, H. M. Kamali, M. Tehranipoor, and F. Farahmandi, "PALLET: Protecting analog devices using a last-level edit technique," in *Proc. IEEE Phys. Assurance Inspection Electron. (PAINE)*, Oct. 2023.

[24] H. H. Hammam, M. A. Hosny, H. A. Omran, and S. A. Ibrahim, "A low power low inrush current LDO with different techniques for PSR and stability improvement," *Eng*, vol. 4, no. 3, pp. 2110–2121, Aug. 2023.

[25] H. H. Hammam, H. A. Omran, and S. A. Ibrahim, "A low power high PSR wide load LDO with load-dependent feedforward cancellation technique," in *Proc. IEEE Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2021, pp. 216–219.