Anti-Counterfeiting Secured Design of a Bandgap Reference Circuit

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

Anti-Counterfeiting Secured Design of a Bandgap Reference Circuit

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

***Abstract*—Integrated circuit (IC) piracy and counterfeiting are a major preoccupation threat for IC designers. A powerful defense is IC locking which consists in making the IC functionality dependent on a digital key. In this work, we propose to simultaneously lock indirectly all analog and mixed-signal blocks of an IC via locking the bandgap reference (BGR) circuits that provide their biasing or reference currents or voltages. We demonstrate an obfuscated BGR in the 22nm FDSOI technology by GlobalFoundries featuring a 24-bit single secret key. Obfuscation shows no performance penalty for the valid key and less than 10% area overhead compared to the unsecured design, while guaranteeing high functionality corruption for invalid keys. The proposed obfuscation shows strong resilience against all known counter-attacks in the analog domain.**

***Index Terms*—Hardware security and trust, piracy, counterfeiting, locking, analog and mixed-signal circuits, bandgap reference circuits.**

I. Introduction

As semiconductor supply chains become more globalized, integrated circuit (IC) cloning and insertion of counterfeit chips have increased significantly [1]. The intellectual property (IP) and ownership of the IC may be lost in seconds while the design is a multi-person effort spanning several months or years. Adversaries can be a third-party that purchases a licence to use the IP block into a larger design, i.e., a system-on-chip (SoC), and the foundry that receives the blueprint of the chip for fabrication. These scenarios are very threatening as with today's globalized IC supply chain many companies depend on third-party IP providers and/or are fabless. Nowadays, IP/IC ownership protection is typically a contractual confidentiality agreement between the two parties often reinforced by security audits. However, this approach does not offer strong security guarantees and the IP/IC is in fact left unprotected with the design owner having no means to verify that the design is not unauthorizedly re-used. Piracy and counterfeiting can also be the target of a reverse-engineer [2].

Adding protection into IPs/ICs against piracy and counterfeiting becomes unavoidably a design goal. Especially for analog and mixed-signal (AMS) circuits, design and security are entangled and adding security is no longer an afterthought once the design is completed. The protection mechanism needs to conform to competing objectives, such as low area and power overhead, zero performance penalty, and proven security against counter-attacks that aim at breaking the defense with reasonable effort.

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.

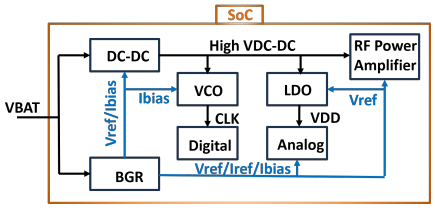

Fig. 1: BGR circuit in SoC.

IP/IC locking is a strong protection mechanism, safeguarding against adversaries throughout the supply chain [3], [4]. It aims at embedding a keying mechanism inside the circuit such that its functionality is controlled by a key in the form of a bit-string. Loading an invalid key makes the circuit non-functional. The valid key is the secret of the designer and is not shared with any untrusted third-party. The circuit is securely activated by loading the secret key after fabrication into a tamper-proof memory which is resistant to probing.

In this work, we propose to simultaneously lock all AMS blocks of an IC via locking the bandgap reference (BGR) circuits. The purpose of a BGR is to generate a stable bias or reference current or voltage that is largely independent of process, voltage, and temperature (PVT) variations [5]. A single BGR can supply more than one AMS blocks inside the SoC, as illustrated in Fig. 1. By locking the BGRs, we erroneously set the operating point of all AMS blocks, rendering them non-functional. Therefore, to unlock the AMS functionality of the chip, an adversary will first need to unlock the BGRs which, as we will show, boils down to re-designing the BGRs that is beyond what an attacker is willing to do.

One AMS circuit locking method it to secure its digital section using logic locking [6]–[10]. A second method treats the digital calibration word as a secret key [11]–[14]. However, BGRs lack both a digital section and a digital calibration mechanism, making these methods inapplicable. A third method targets locking simple biasing circuits, e.g. a current mirror [15], or replacing the biasing circuit with an alternative key-controlled structure, such as a neural network [16] or memristor-crossbar [17]. However, these alternative biasing structures are not adopted by analog designers because of area overhead concerns and because of low bias stability. Besides locking, there also exist key-less obfuscation approaches for analog circuits [18]–[20], but these can defend only against reverse-engineering [18], [19] or an untrusted foundry [20].

To lock a BGR, we require a locking technique that applies to purely analog circuits, such as the ones proposed in [21]–[23]. In [21], a transistor is obfuscated by replacing it with parallel-connected transistors of different widths, where each transistor has a switch placed in series with it controlled by a key-bit. The key sets on the right combination of transistors to establish the correct effective width. In [23], the technique is enhanced by obfuscating, in addition, the device ratings, thus the chip is likely to be damaged if trying an incorrect key. The technique in [22] leverages layout-dependent effects (LDEs). A transistor is augmented with extra parallel-connected transistors displaying different LDEs and the key sets on only the original transistor.

Herein, we adopt and extend the technique in [21]. In addition to transistors, we obfuscate passive components, which adds more flexibility for enlarging the key size and induces circuit instability for a large fraction of invalid keys. Furthermore, we integrate obfuscation into the design plan balancing the aforementioned competing objectives. We demonstrate a 24-bit, $<$10% area overhead, counter-attack resilient locked version of a BGR designed in the 22nm FDSOI technology by GlobalFoundries. In [21], 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 $1.57\times$. A similar large overhead was reported for an op-amp in [22].

The rest of this article is structured as follows. In Section II, we present the proposed obfuscation methodology. In Section III, we present the obfuscated BGR design and the results. In Section IV, we show that the locked BGR is resilient against all known counter-attacks in the analog domain. Section V concludes this article.

II. Obfuscation Strategy

The designer first completes and verifies the non-obfuscated design at netlist-level. Then, components are obfuscated one by one until we reach a minimum key size n that makes a brute-force attack impracticable. In a brute-force attack, the attacker uses a trial and error tactic to identify a working key. The average cost is $2^n * T_s/2$, where T_s is the circuit simulation time including all performance test benches.

Any component can be subject to obfuscation. Obfuscation replaces the component with a key-controlled version, as illustrated in Fig. 2. The section of the key controlling a component is called sub-key. Transistors are obfuscated by replacing them with parallel-connected transistors of different widths. Every transistor is made on/off thanks to a switch that is placed in series with the drain/source and is controlled by a key-bit of the sub-key. The sub-key defines which transistors are on and the correct sub-key sets the correct effective width $W_{eff} = \sum b_i * W_i$, where W_i is the width of the i-th transistor and b_i is the key-bit controlling it. Capacitors are obfuscated in a similar way by replacing them with a parallel-connected capacitor bank, i.e., $C_{eff} = \sum b_i * C_i$, while resistors are obfuscated by replacing them with series resistors, i.e., $R_{eff} = \sum b_i * R_i$.

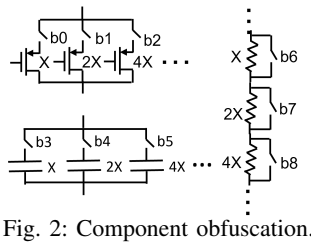

Fig. 2: Component obfuscation.

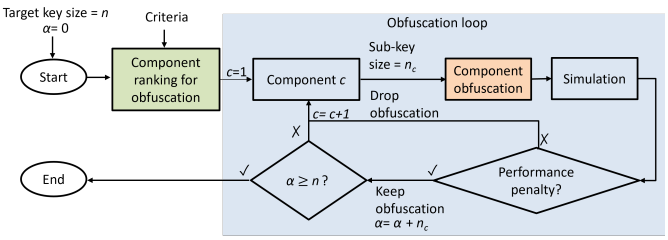

Fig. 3: Obfuscation methodology.

When obfuscating a component, there should be a single correct sub-key that sets its correct value, and any other incorrect sub-key should result in significant performance degradation a set percentage away from the specification. To meet these objectives, the guidelines are to use: (a) binary weighted obfuscation components, as shown in Fig. 2, so as to impose a large performance shift per one key-bit step; and (b) a correct sub-key with at least two "1"s so as to avoid a linear search of n trials. For example, suppose that we want to obfuscate a transistor with weight W using four obfuscation transistors. The four transistors are assigned widths $U, 2\times U, 4\times U, 8\times U$. For correct key "0110" we use $U = W/6$, for correct key "1011" we use $U = W/13$, etc.

The obfuscation steps, illustrated in Fig. 3, are as follows:

- *Step 1: Component ranking for obfuscation*. Components for which the circuit response is very sensitive to their variations are the best candidates for obfuscation since incorrect keys will produce high performance corruption. However, sensitivity alone is not the only criterion. Performance penalty for the correct key should be considered and can conflict with the sensitivity criterion. Another criterion is the size of the component. Obfuscating large components will inevitably result in a larger area overhead. Combining all these objectives, the designer makes an initial ranking of obfuscated components.
- *Step 2: Obfuscation loop*. The designer starts from the top of the list and obfuscates components one at a time so as to have control over the performance penalty and area overhead. For each component c, a sub-key size n_c is determined, such that $\sum_{i=1}^{N}(n_c) \geq n$, where N is the final number of obfuscated components. A component is obfuscated as shown in Fig. 2, verifying through simulation that for the correct key the intent performance trade-off is unchanged or minimally affected across PVT variations. Otherwise, the obfuscation is dropped and we move on to the next candidate in the list. To examine functionality corruption, simulations can be performed for incorrect sub-keys while setting correct key-bits for all previously obfuscated

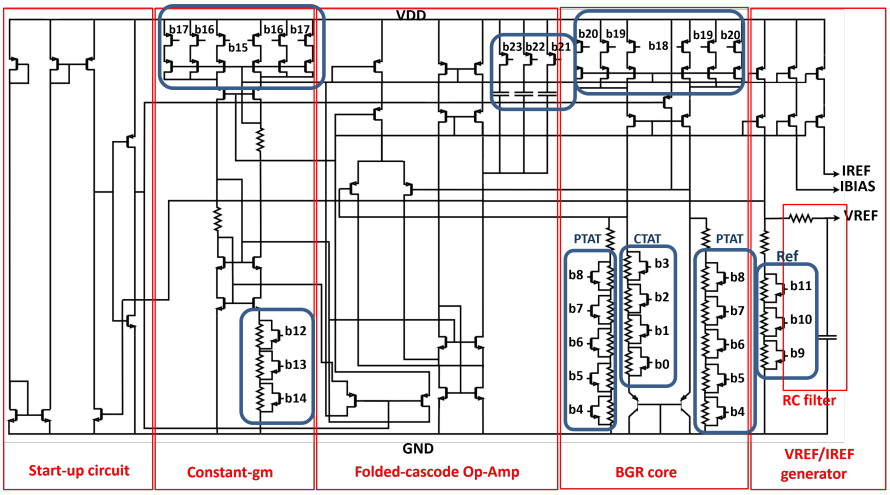

Fig. 4: Obfuscated BGR circuit design.

components. During the obfuscation loop we keep track of the key size with a parameter α. We exit the obfuscation loop when we meet the target key size n.

III. BGR Obfuscation

We use a fractional BGR [24]–[27] as a case study for obfuscation. Fig. 4 shows the obfuscated BGR design with a 24-bit key, highlighting the different sub-circuits with red rectangles and the obfuscated components with blue rectangles. The design was made in the 22nm FDSOI technology by GlobalFoundries.

The bias or reference current or voltage values generated by the BGR, i.e., IBIAS, IREF, and VREF, depend on the mirroring ratios and resistor values. They are constant with temperature variation because the BGR core current is a summation of a weighted proportional to absolute temperature (PTAT) current in the resistors and a weighted complementary to absolute temperature (CTAT) current in the BJT. This current is mirrored through the PMOS mirrors to generate IBIAS and IREF or is dumped into a reference resistor to generate VREF. A high-gain folded-cascode amplifier is used in a feedback loop to set its two inputs equal for a proper loop operation and for biasing the BGR core's main PMOS mirrors. A constant-gm circuit is used to bias the amplifier's NMOS and PMOS load devices and the BGR core's cascode PMOS devices. It has the advantage of self-biasing and constant gm across temperature ranges. A capacitor is used between the amplifier's output and the supply to improve the loop stability and the high-frequency power supply rejection (PSR) at VREF. A low-pass filter is used as a soft start circuit to remove any overshoot on the VREF signal during start-up. It senses VREF which is zero before the BGR starts. At this time, the start-up output becomes zero, opening the PMOS start-up device in the BGR core, and pushing current into the BJTs. Also, it connects the bias voltages of the constant-gm circuit to start it up. Once the constant-gm circuit and the amplifier start, the loop starts operating normally generating VREF, which, in turn, turns the start-up circuit off and isolates it.

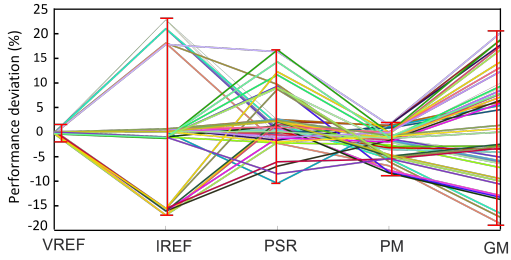

Fig. 5: Variation of BGR performances across PVT using correct key.

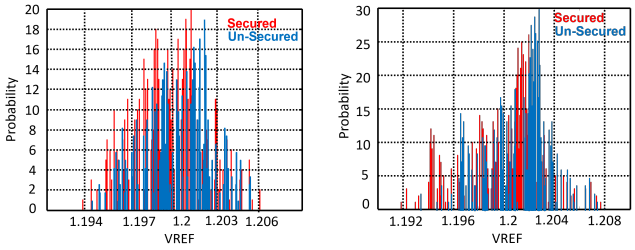

Fig. 6: Monte Carlo VREF simulation for (a) maximum and (b) minimum temperature and power supply.

The un-secured non-locked BGR was characterized across PVT. The supply is typically 1.8V with +/- 10% variation. The temperature range is from -40°C to 125°C. We considered FS, SF, SS, and FF process corners for MOSFETs, FF and SS for capacitors, and max and min for resistors and BJTs. VREF is 1.2 V typically and has 1.196 V minimum and 1.204 V maximum values across PVT. IBIAS/IREF is 1 µA typically with 0.83 µA minimum and 1.23 µA maximum values across PVT. The PSR results across PVT show a DC PSR of -45 dB and a high-frequency PSR of -25dB typically. The minimum PSR is -38 dB at DC and -18 dB at high frequency. The minimum loop gain is 60 dB, the minimum phase margin (PM) is 60 degrees, and the minimum gain margin (GM) is 20 dB. The quiescent current of the un-secured BGR shows 8.5 µA typical and 14 µA maximum values. For the secured version, these values change only for incorrect keys, thus for the correct key there is zero power consumption overhead.

Fig. 5 shows PVT simulations of the obfuscated BGR when

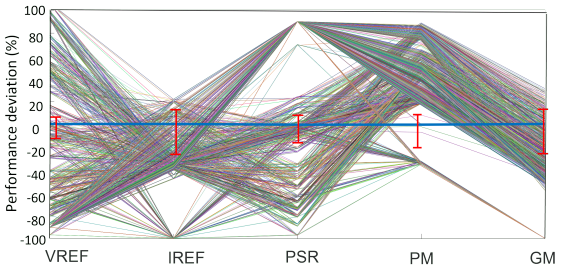

Fig. 7: Variation of BGR performances across different incorrect keys.

using the correct key. The above lower and upper bounds of the un-secured BGR performances simulated across PVT are used as specifications and are indicated in Fig. 5 with the red box plots, where the whiskers extend to the specifications. Each piecewise line corresponds to a different PVT simulation and connects the percentage deviation values of performances. As it can be seen, variations are confined within the specifications, proving that the keying mechanism has minimal effect on the performance trade-off. Another illustration that obfuscation incurs no penalty is shown in Fig. 6, which plots the histogram of the Monte Carlo variation of VREF at maximum and minimum temperature and supply conditions for the un-secured (blue) and the secured design (red) using the correct key. As it can be seen, the VREF variation is similar for both designs.

Fig. 7 shows the resultant BGR performance variation using the correct key and 2000 random incorrect keys. Each piecewise line corresponds to using a different key. The blue thick nearly straight line around 0% variation corresponds to the correct key. In contrast, for all incorrect keys, the corresponding lines exceed the specification bounds for at least 2 performances. Few of them result in a maximum of 2 or 3 performances being within the specifications. After 2 weeks of key trials, only the correct key showed the correct operation.

Finally, Fig. 8 shows the layout of the secured BGR, designed using matching techniques and parasitic optimization. The new BGR area is 99 μm $\times$ 50 μm, incurring less than 10% area overhead compared to the un-secured BGR which has an area of 90 μm $\times$ 50 μm.

IV. Security Analysis

An attacker will try to de-obfuscate the circuit to extract the correct key. Herein, we discuss the resilience against all known counter-attacks in the analog domain.

- *Brute-force attack*: For the obfuscated BGR, n=24 and T_s=5 sec, thus on average the attack will take approximately 485 days to complete. This time is unreasonable and the attacker will soon be discouraged and will give up.
- *Attacks on biasing locking*: A number of attacks have been developed to de-obfuscate locked biasing circuits [28]–[30]. The focus is on current mirrors and these attacks do not generalize for more complex biasing circuits such as a BGR. More specifically, the attack in [28] is based on developing circuit equations that link known currents and performances with the unknown obfuscated component values, which are then solved with a satisfiability modulo theories (SMT) solver. It is not applicable as the internal branch currents of the BGR are unknown to the attacker. The attack in [29] uses the circuit at simulation level and an oracle chip that has the correct key loaded into the TPM. A Genetic Algorithm (GA) is used to search in the space of keys at simulation level using as fitness function the difference between the simulated and oracle chip responses. This attack is too time-consuming for a 24-bit key. Besides, the optimization is likely to "zigzag" endlessly as the performance trade-off behaves as a delta function on the single correct key. In [30], the locked biasing circuit is replaced with a fresh non-locked version that is sized using a GA to explore the design space. This boils down to re-sizing the complete BGR and will require also re-designing the layout afterwards, which is beyond what the attacker is willing to do.
- *Monotonic attack [31]*: Finding the key can be quick if there is a monotonic dependency between the performance and the key. This attack would be applicable if the components could be de-obfuscated independently. It is not the case for the obfuscated BGR because the performance trade-off jointly depends on all obfuscated components.
- *Key spacing attack [31]*: Considering an obfuscated transistor, this attack points out that if attention is not paid to how the obfuscation is done, likely the nominal width W_{cor} for the correct key will have a large exclusion zone around it, i.e., the width W_{incor} for any incorrect key will satisfy $|W_{incor} - W_{cor}| > \epsilon$. 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 to the isolated obfuscated components. However, by using binary weighted obfuscation components, the keys produce widths of large and equal spacing, thus thwarting this attack.

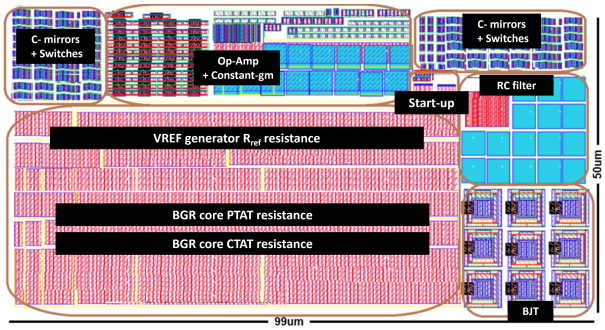

Fig. 8: Layout of the secured BGR.

V. Conclusion

By locking the BGRs of a chip, we indirectly simultaneously lock the functionality of all AMS blocks inside it. We presented an obfuscated BGR featuring a 24-bit key that is robust against all known counter-attacks. There is a single key that restores the BGR functionality, while any other incorrect key results in drastic performance deviation. The obfuscated BGR shows an area overhead of less than 10% compared to the original un-secured BGR, while there is no performance or power overhead when using the correct key.

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

[5] B. Razavi, "The bandgap reference [a circuit for all seasons]," *IEEE Solid State Circuits Mag.*, vol. 8, no. 3, pp. 9–12, Sep. 2016.

[6] 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.

[7] J. Leonhard *et al.*, "MixLock: Securing mixed-signal circuits via logic locking," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar. 2019, p. 84–89.

[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] 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.

[16] G. Volanis, Y. Lu, S. Govinda, R. Nimmalapudi, A. Antonopoulos, A. Marshall, and Y. Makris, "Analog performance locking through neural network-based biasing," in *Proc. IEEE VLSI Test Symp. (VTS)*, Apr. 2019.

[17] D. H. K. Hoe, J. Rajendran, and R. Karri, "Towards secure analog designs: A secure sense amplifier using memristors," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI*, Jul. 2014, pp. 516–521.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] H. H. Hammam, H. Aboushady, and H.-G. Stratigopoulos, "Analog circuit anti-piracy security by exploiting device ratings," in *Proc. Design, Automat. Test Eur. Conf. Exhib. (DATE)*, Mar./Apr. 2025.

[24] H. H. Hammam, H. A. Omran, and S. A. Ibrahim, "Ultra-low-power low drop-out (LDO) voltage regulator with improved power supply rejection," in *Proc. 38th Nat. Radio Sci. Conf. (NRSC)*, Jul. 2021, pp. 177–185.

[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.

[26] H. Banba, H. Shiga, A. Umezawa, T. Miyaba, T. Tanzawa, S. Atsumi, and K. Sakui, "A CMOS bandgap reference circuit with sub-1-V operation," *IEEE J. Solid-State Circuits*, vol. 34, no. 5, pp. 670–674, May 1999.

[27] H. H. Hammam, K. M. Hassan, and S. A. Ibrahim, "An ultra-low-power process-and-temperature compensated ring oscillator," in *Proc. 9th Int. Conf. Electr. Electron. Eng. (ICEEE)*, Mar. 2022.

[28] 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.

[29] 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.

[30] 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.

[31] 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.