# Anti-Piracy of Analog and Mixed-Signal Circuits in FD-SOI

Mariam Tlili, Alhassan Sayed, Doaa Mahmoud, Marie-Minerve Louërat, Hassan Aboushady, Haralampos-G. Stratigopoulos

▶ **To cite this version:**

Mariam Tlili, Alhassan Sayed, Doaa Mahmoud, Marie-Minerve Louërat, Hassan Aboushady, et al.. Anti-Piracy of Analog and Mixed-Signal Circuits in FD-SOI. 27th Asia and South Pacific Design Automation Conference (ASP-DAC), Jan 2022, Virtual, Taiwan. pp.423-428, 10.1109/ASP-DAC52403.2022.9712547 . hal-03416062v1

**HAL Id: hal-03416062**
**https://hal.science/hal-03416062v1**

Submitted on 5 Nov 2021 (v1), last revised 14 Jan 2023 (v2)

**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.

# Anti-Piracy of Analog and Mixed-Signal Circuits in FD-SOI

Mariam Tlili
Sorbonne Université, CNRS, LIP6
Paris, France
e-mail: Mariam.Tlili@lip6.fr

Alhassan Sayed
Minia University
Minia, Egypt
e-mail: Alhassan.Sayed@mu.edu.eg

Doaa Mahmoud
Sorbonne Université, CNRS, LIP6
Paris, France
e-mail: doaa.mahmoud@lip6.fr

Marie-Minerve Louërat
Sorbonne Université, CNRS, LIP6
Paris, France
e-mail: Marie-Minerve.Louerat@lip6.fr

Hassan Aboushady
Sorbonne Université, CNRS, LIP6
Paris, France
e-mail: Hassan.Aboushady@lip6.fr

Haralampos-G. Stratigopoulos
Sorbonne Université, CNRS, LIP6
Paris, France
e-mail: Haralampos.Stratigopoulos@lip6.fr

**Abstract— We propose an anti-piracy security technique based on locking for analog and mixed-signal circuits designed in FD-SOI. We show that obfuscating the body-bias voltages of tunable transistors is an effective way for inducing high functionality corruption. The obfuscation is achieved by constituting a secret key from the concatenation of the input digital codes of the body-bias generators that produce the correct body-bias voltages. We also propose a slight modification of the body-bias generator that increases prohibitively the time complexity of counter-attacks aiming at finding an approximate key. The proposed locking scheme is demonstrated on a $\Sigma\Delta$ modulator used in highly-digitized RF receiver architectures.**

## I. Introduction

The fabless business model and the outsourcing of portions of a design to third parties have given rise to the Intellectual Property (IP)/Integrated Circuit (IC) piracy threat [1]. An embodiment of IP/IC piracy is cloning a design or portions of it without the consent or the design owner, and illegitimately using it to build counterfeit chips. Cloning can be performed by a System-on-Chip (SoC) intergrator who buys an IP licence, by a foundry that receives the design blueprint, or by an end-user via chip reverse engineering [2]. Cloning reduces the competitive disadvantage of the attacker, while it has significant repercussions for the design owner, i.e., loss of financial revenue, know-how, and brand name. Other forms of piracy include chip overbuilding, remarking of out-of-spec chips, and chip recycling [1].

Protecting against IP/IC piracy has become a major preoccupation for design houses. Efforts have concentrated primarily on digital designs with countermeasures such as locking [3], split manufacturing [4], and camouflaging [5]. For analog and mixed-signal (AMS) designs the first defenses have appeared only recently [6]–[8]. Similar countermeasure principles are adapted for AMS designs, including locking [9]–[17], split manufacturing [18], and camouflaging [19], [20].

Locking has been shown to be one of the strongest defenses to thwart IP/IC piracy. The idea is to insert within the design a lock circuit that is controlled with a digital key. Correct functionality is established only upon application of the correct key, while applying incorrect keys results in corrupted functionality. The correct key is kept secret from any potential malicious entity and after fabrication is stored in an on-chip tamper-proof memory (TPM). Locking techniques have been proposed for digital ICs (a.k.a logic locking) [3] and recently for AMS ICs too [9]–[17]. The prior art on AMS IC locking will be discussed in more detail in Section II.

In this paper, we propose a locking technique for AMS ICs designed in Fully Depleted Silicon on Insulator (FD-SOI) technology. The locking technique exploits the existence of multiple domains of body-bias voltages. For each domain one Digital-to-Analog Converter (DAC) is typically used to generate the desired body-bias. We propose to form the key by concatenating the input codes of the DACs, thus obfuscating the intent body-biases that are required for establishing correct functionality. We also propose to make a small modification within the DAC switching structure for achieving resilience against counter-attacks aiming at finding an approximate key. The proposed locking technique can effectively thwart cloning, it is generally applicable, it is non-intrusive which is vital for its wide adoption by AMS IC designers, and it incurs minimal area and power overhead. We demonstrate it on a $\Sigma\Delta$ modulator in the context of multi-standard, highly-digitized RF receivers designed in 28nm FD-SOI from STMicroelectronics.

The rest of the paper is structured as follows. In Section II, we provide an overview of prior art on AMS IC locking. In Section III, we provide an overview of body-biasing of transistors in FD-SOI technology. In Section IV, we discuss the proposed locking methodology and its properties. In Section V, we present our case study. In Section VI, we present results that prove the locking efficiency. Finally, Section VII concludes the paper pointing also to future work ideas.

## II. Prior Art in AMS IC locking

Inserting a lock circuit into an AMS IC is challenging from both design and security points of view. AMS IC designers are reluctant to make any circuit topology alternations since this adds parasitics and perturbs the performances. This is conflicting with the two main security requirements, namely inserting: (a) a multiple-bit digital key, typically larger than 64 bits; and (b) a lock circuit that "blends" well with the design such that it cannot be straightforwardly removed. To

date, three categories of AMS IC locking have been proposed, namely biasing, calibration, and mixed-signal locking.

Biasing locking consists in controlling the circuit biases with a key. Existing techniques include expanding the biasing circuit, i.e., a current source [9] or a current mirror [10], to embed a lock or re-designing new biasing circuits with locking capability, i.e., using memristor crossbars [11] or on-chip neural networks [12]. Recent works have shown that such biasing locking defenses can be easily broken by an attacker [21]–[23].

Calibration locking consists in controlling the setting of the tuning knobs with a key. Existing techniques include performing logic locking of the digital optimizer inside the calibration feedback loop [13], limiting the calibration range of Analog Floating-Gate Transistors (AFGTs) when used as tuning knobs [14], and using the programming bits of highly-digitized AMS ICs directly as a key [15].

Finally, mixed-signal locking consists in performing logic locking of digital blocks within the signal processing path [16], [17]. The technique in [13] can be placed in this category too.

All these locking techniques are generally applicable to AMS ICs including designs in FD-SOI. However, in this paper we exploit a specific property of the FD-SOI technology, in particular the use of body-bias, to perform a natural lock-less locking without needing to modify or re-design the core of the circuit. Slight modifications are only performed in the DACs generating the body-biases so as to decelerate the time of counter-attacks. Thus, performance penalty and overheads are minimized and design-for-security is simplified. Furthermore, the lock-less aspect makes the attacks in the analog domain [21]–[23] non-applicable since they all assume the existence of an obfuscated component. Conceptually, our approach is similar to the one in [15]; however, in [15] the secret is the digital control of current sources at the programming interface, while in this work the secret is the body-bias voltage levels of internal transistors.

## III. Body-biasing of transistors in FD-SOI

Body-biasing refers to altering the transistor's bulk connection from the source terminal to a controlled voltage so as to adjust the transistor's threshold voltage. Body-biasing of transistors in FD-SOI [24] offers extensive capabilities to AMS IC designers. It allows improving the trade-off between performance and power consumption, reducing noise, improving matching of small-size devices, and implementing a wide tuning range for variability compensation and performance adaptation [25].

The solutions to avoid power and area overhead associated with generating multiple body-bias voltage levels are: (a) limiting the body-bias control only to critical parts of the design; and (b) partitioning the design into independent body-bias domains, also called body-bias islands or clusters. Each domain is composed of body terminals sharing the same bias voltage and voltage generator, which is typically a DAC. The collection of the DACs constitutes the body-biases driver unit. The simplest partitioning scheme is into two domains in accordance to transistor types, i.e., NMOS and PMOS, where each transistor type is uniformly biased to one of two reference

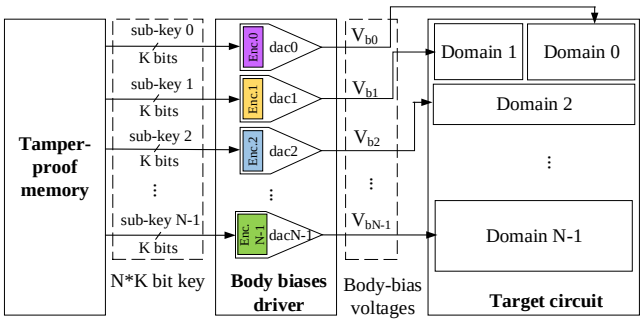



Fig. 1: Illustration of locking principle.

voltages, typically $Vss$ or $Vdd$. In the general case, several domains can take an intermediate voltage value and there exist also mono-transistor domains.

## IV. Locking Methodology

### A. Locking principle

The locking principle is illustrated in Fig. 1. Let us denote by $N$ the number of body-bias domains. Each $i$-th DAC in the body-biases driver, denoted by dac$i$, $i = 0, \cdots, N-1$, maps a $K$-bit input digital code to the required body-bias voltage $V_{bi}$ of the $i$-th domain. Each input digital code is treated as a $K$-bit secret sub-key. Combining the individual $N$ secret sub-keys in series generates a global secret key of $N * K$ bits. This key is stored in the TPM whose output is directly mapped to the body-biases driver establishing correct body-bias voltage levels, which is a prerequisite for achieving the intent performances. Applying an incorrect key will generate incorrect body-bias voltage levels, which leads to functionality corruption, i.e., the performance trade-off of the circuit is degraded and some or all of the specifications are no longer met.

In practice, it may not be necessary to obfuscate all body-bias voltages as indicated in Fig. 1. It suffices to select to obfuscate a subset such that: (a) the global key has a large size to thwart attacks aiming at extracting an approximate key, e.g., brute-force attacks that aim at randomly searching in the key space until a key is found that establishes approximately correct functionality; and (b) random incorrect keys result in high functionality corruption.

It should be noted that invalid keys that are "close" to the correct key may establish approximately correct body-biases which, in turn, yields performances that may be degraded but still lie within the specification limits. The effective key size becomes $N * K - m$, where $m$ is the number of such approximate keys, and it is typically required that is larger than 64-bits such that approximate keys represent a tiny fraction of the key space.

So far no modifications have been made in the body-biases driver and the only hardware overhead is the addition of the TPM for storing the secret key, which is the minimum hardware overhead for implementing any IC locking scheme.

The defender may choose to make additional transistors tunable via their body-bias so as to increase the functionality corruption and security level if needed. The defender can

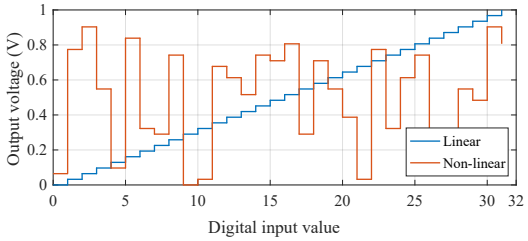



Fig. 2: Linear versus non-linear transfer function of a 5-bit DAC.

choose to: (a) create new mono-transistor domains by performing a sensitivity analysis to identify transistors that are the most influential on the performance-trade-off; and (b) group transistors with body-bias equal to a specific voltage, i.e., reference or intermediate, and create a new multi-transistor domain. For each new voltage domain the key size increases by $K$ bits and one DAC is added to the area and power overhead. Although not necessary, option (a) is also explored in our case study.

Although a large key size is a prerequisite for defending against brute-force attacks, this locking scheme remains vulnerable against optimization-based attacks [22] which aim at searching in the key space towards optimizing the performance trade-off. More specifically, the attacker can formulate an optimization problem $\min_{key} |f(key) - s|$ to approximate a "close" key, where $f(key)$ is the function relating the performance with the key and $s$ denotes the specification of the performance. Such an optimization will converge after a number of iterations denoted by $\ell$. In every iteration, the circuit simulator is evoked to compute $f(key)$ using appropriate test benches. Analog simulation can be very time-consuming. If we denote the simulation time to compute all performances by $T$, then the optimization-based attack time is $\ell * T$.

Typically, linear DACs are used establishing a linear relationship between the key and performances. Thus, despite the long analog simulation time, the attack can still terminate in reasonable time, within the time budget of the attacker. For this reason, we propose to convert linear DACs to non-linear ones, in order to provoke an intricate relationship between key-bits and circuit response. This will force the optimization to converge much slower, thus making the optimization attack time-inefficient. Moreover, the approximate keys will now be non-consecutively distributed in the key space.

Fig. 2 illustrates an example of linear versus non-linear transfer function of a 5-bit DAC. As it can be seen, the non-linear DAC response approaches a random noise making the relationship between key-bits and body-bias voltage highly non-linear. The difference between two successive output voltages is not necessarily equal to one quantization step, denoted by $q$, but can be any value between $q$ and $(2^K - 1) * q$, where in this example $K = 5$.

Fig. 1 shows that a non-linear encoder, denoted by Enc$i$, is added within the linear dac$i$, in order to transform it to non-linear. This non-linear DAC transformation is described in Section IV-B in more detail. It should be noted that: (a) the non-linear transformation incurs zero performance penalty for the target circuit; and (b) the resulting area and

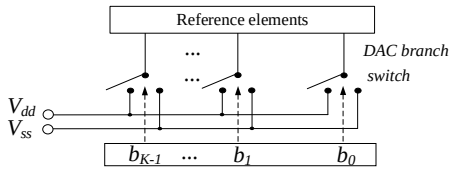
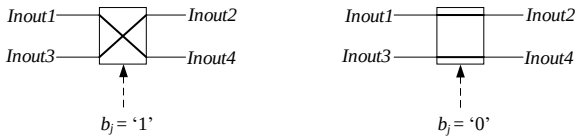



Fig. 3: High-level description of a binary-weighted DAC.




(a) Cross connection. (b) Parallel connection.

Fig. 4: Replacement switches.

power overhead compared to a linear DAC is very small and justifiable for equipping the design with anti-piracy capability.

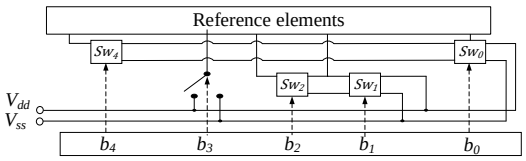
The non-linear DAC transformation offers an important auxiliary benefit. Some domains may utilize the reference voltages $Vss$ or $Vdd$. In the case of a linear DAC, the first and last codes '00...0000' and '11...1111' correspond to $Vss$ and $Vdd$, respectively. Thus, for these domains the attacker has a binary choice to make which reduces the effective key size. In contrast, for a non-linear DAC, the codes that generate the reference voltages are intermediate codes and cannot be guessed, thus retaining the effective key size.

### *B. Non-linear DAC transformation*

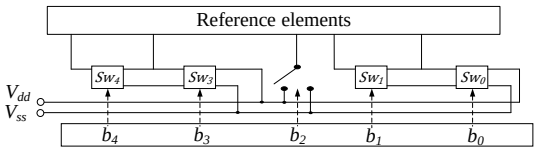
Binary-weighted DACs are popular topologies for voltage generation and are typically the preferred solution for the body-biases driver. A binary-weighted DAC architecture comprises reference elements, e.g., resistors or capacitors, connected to a switching network as shown in Fig. 3. Each branch of the network is controlled by one input bit $b_i$, which in our case is a sub-key-bit, and depending on the value of $b_i$ it connects the reference element of the branch to one of two different reference voltages, typically $Vss$ or $Vdd$.

We propose to transform a linear DAC to a non-linear DAC by modifying the switching network structure to embed into it an encoder. The role of the encoder is to create the non-linear, non-monotonic DAC transfer function shown in Fig. 2. The proposed modification relies on replacing some of the conventional switches with the 4-port dual-input/dual-output switch structure shown in Fig. 4. When the value of the control bit $b_j$ is high, the terminals are cross-connected as shown in Fig. 4a, whereas when the value of the control bit $b_j$ is low, the terminals are parallel-connected as shown in Fig. 4b.

Two example topologies of 5-bit DACs using this switch type are shown in Fig. 5. One pair of such switches $Sw_i$ and $Sw_j$ is inserted at a time in the $i$-th and $j$-th branches, where $i, j \in \{0, \cdots, N-1\}$, $i \neq j$, controlled by input bits $b_i$ and $b_j$, respectively, replacing the two conventional switches in these two branches. The two inputs of switch $Sw_j$ are the reference voltages where the two outputs drive the two inputs of switch $Sw_i$ and one output also connects to the reference element in the $j$-th branch. Only one output of switch $Sw_i$ is used and is




(a) Example 1.




(b) Example 2.

Fig. 5: Two examples of switches placement in the DAC's network.

TABLE I: Examples of transformed input codes

| Original code | Equivalent code in example 1 | Equivalent code in example 2 |
|---|---|---|
| 00000 | 10100 | 10010 |
| 01101 | 11011 | 11111 |
| 10001 | 00100 | 01011 |
| 11111 | 01000 | 00100 |

connected to the corresponding reference element in the $i$-th branch.

This strategy of switches placement inside the DAC switching network is equivalent to a transformation of the original input codes to a different encoding. The encoding is determined by the position of the switches. Increasing the number of inserted pairs of switches generalizes the coding transformation to more bits, i.e., the Hamming Distance (HD) between the original and the transformed code is increased. Furthermore, a large choice of configurations is possible allowing the design of DACs with different encoders, i.e., different non-linear transfer functions and different possibilities to encode the same voltage level. For example, Table I shows the code transformation for the two example 5-bit DACs of Fig. 5.

The non-linear DAC transformation has three important implications that increase the security level:

- Using different encoders in each DAC, the same body-bias voltage level is generated by using different input digital codes, i.e., sub-keys.
- The voltage references $Vss$ and $Vdd$ are generated by intermediate input digital codes.
- The resulting non-linear, non-monotonic transfer function significantly slows down the convergence of the optimization-based attack making it behave like a randomized brute-force attack.

### C. Locking properties

The proposed locking scheme has the following properties:

- *Threat model and attack resilience:* We assume the most pessimistic threat model where the attacker possesses the circuit netlist and an oracle chip. The attacker has a non-functional netlist as the body-biases which are defined during design and are required for correct functionality are kept secret. The key that generates the correct body-biases is stored in the TPM in the oracle chip and any attempt to read it results in irreversible key loss. Therefore, the proposed locking thwarts IP/IC piracy. The key has a large size, which, combined with the long analog simulation time, thwarts counter-attacks to extract the key based on brute-force or optimization [22]. The non-linear DAC transformation further slows down the optimization convergence and, in addition, protects body-bias domains that are fixed to the reference voltages. It is important also to stress that all attacks in the digital domain [3], e.g., oracle-based Boolean satisfiability (SAT) attacks, are non-applicable in this context.
- *Wide applicability:* It is generic and can be used for any AMS IC design in FD-SOI.
- *Non-intrusiveness:* It is non intrusive as the locking mechanism acts on the peripheral body-biases driver and does not alter the core circuit topology. No design modifications are required within the circuit and the analog design flow is not affected. The body-biases driver is already part of the design and the DAC switching network modification does not affect the matching of the reference elements of the DAC. The required body-bias voltages can be generated with the same accuracy using the non-linear DAC transformation.
- *Low-overhead:* Apart from the addition of the TPM, which is a requirement for all IC locking schemes and can be shared for locking different IP blocks within a SoC, the area overhead is minimal and stems only from replacing part of the DAC switching network. This replacement results also in minimal power overhead.
- *Body-biasing type:* It applies to static body-biasing where pre-specified body-biases are used. For more sophisticated dynamic body-biasing schemes where body-biases are adapted on-the-fly based on different criteria, i.e., active or idle state of operation, temperature, etc., one can envision performing logic locking of the digital engine that controls the adaptation. This approach is inspired from the locking techniques in [13], [16], [17].

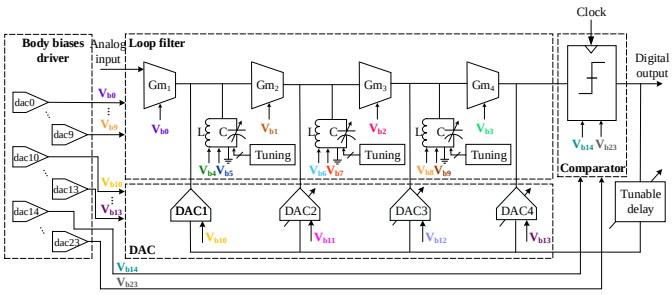



Fig. 6: Block diagram of the configurable $\Sigma\Delta$ modulator.

## V. Case Study

Our case study is a 6-th order, continuous time, band-pass, 1-V $\Sigma\Delta$ modulator designed in 28nm FD-SOI from STMicroelectronics. The circuit is re-configurable in the frequency range of 1-4GHz with a variable sampling rate of 4-16 GHz. It is intended for use in highly-digitized, multi-standard RF receiver architectures. The architecture, shown in Fig. 6, includes a loop filter with three Gm-LC type band-pass filters, a single-bit comparator with a tunable delay and a feedback current-steering DAC. Setting the center frequency is done

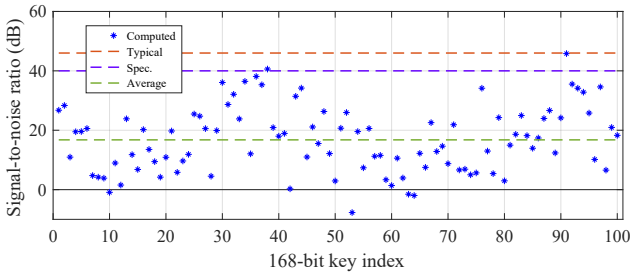



Fig. 7: SNR of 100 random keys.

TABLE II: SNR metrics for 100 random keys.

| Evaluation metric | "Natural" 168-bit key | Enhanced 175-bit key |
|---|---|---|
| Average (in dB) | 16.74 | 4.2 |
| MAE (in dB) | 29.26 | 41.8 |
| ME (in dB) | 2.6 | 17.3 |

by means of tuning the capacitors of the band-pass filters. In addition, static body-biasing is utilized as the trimming technique to compensate against process variations. In total, 24 transistors with controlled body-bias are placed in all three main blocks of the circuit, as depicted in Fig. 6, thus the body-biasing scheme is divided into 24 mono-transistor voltage domains. A body-biases driver composed of 24 7-bit binary-weighted linear DACs is used in the original design. Therefore, the key size is $7 * 24 = 168$ bits. The DACs are transformed to non-linear using the technique described in Section IV-B where each DAC uses a different encoder.

For the purpose of our experiment, without loss of generality, we consider a single configuration corresponding to a center frequency of 3GHz with sampling rate 12GHz. Unlocked, the $\Sigma\Delta$ modulator has a typical Signal-to-Noise Ratio (SNR) equal to 46dB in a 90MHz bandwidth. The minimum SNR specification is set to 40dB.

## VI. Results

Simulating the circuit with a medium precision and performing Fast Fourier Transform (FFT) to compute SNR requires at least 30 minutes. This long simulation time also points to a prohibitive time complexity of brute-force or optimization-based attacks. We simulated the circuit for 100 randomly generated keys for a total simulation time of approximately 2 days, which is a reasonable simulation budget.

The SNR is plotted versus the 168-bit key index in Fig. 7. Different SNR metrics computed on these 100 random keys are summarized in the second column of Table II, including the average SNR, the minimum error (ME), defined as the difference between typical SNR and the highest computed SNR, and the mean absolute error (MAE), defined as the difference between average and typical SNR values. As it can be seen, 98% of the random keys lead to a non-acceptable functionality corruption, that is, the SNR is less than the specification of 40dB. However, 2 random keys, namely keys with indexes #38 and #91, result in an acceptable SNR within the 6dB tolerance window.

The attacker may believe that 2 approximate keys are found, but this is misleading. The reason is that SNR is not the only

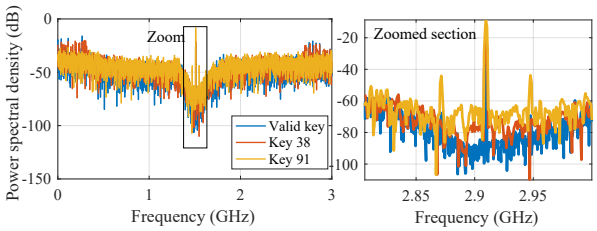



Fig. 8: PSD for the correct key and keys #38 and #91.

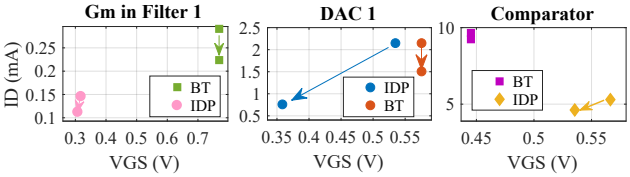



Fig. 9: DC operating point analysis for key #38.

performance and, in fact, it turns out that other performance specifications are violated.

For example, let us consider two more performances, namely the Power Spectral Density (PSD) and the Spurious-Free Dynamic Range (SFDR), which require an extra simulation time of over 1 hour per key. Fig. 8 shows the PSD for the correct key and keys #38 and #91. As it can be seen, lower orders of noise shaping are achieved with the random keys. The quantization noise level around the signal bandwidth is less attenuated. This can be seen as a degradation in the effective $\Sigma\Delta$ modulator's order. SFDR for the correct key is 31.39dB, while for key #38 is 24.97dB and for key #91 is 20.02dB, thus locking significantly degrades the SFDR.

We also performed DC analysis to investigate the variations of the operating points of some transistors in the comparator, DAC, and Gm part of the first band-pass filter. Fig. 9 shows for key#38 two transistor examples per block, namely an input differential-pair (IDP) transistor and a biasing transistor (BT). Some of these transistors do not have their body-bias tuned. In all cases, the operating points deviate, which shows that a deviation in the expected body-bias of the tunable transistors impacts the operating point of several other non-tunable transistors due to the strong dependencies within the circuit. This proves that obfuscating body-bias voltages is an excellent choice for spreading errors into the circuit and inducing high functionality corruption.

So far we considered the natural 168-bit key offered by the design, thus locking incurs a very small area and power overhead only due to the non-linear DAC transformations. As explained in Section IV-A, the designer can choose to make more transistors tunable so as to intensify functionality corruption at the expense of some area and power overhead. We explored the option of adding a single new mono-transistor domain for a critical transistor. To select this transistor, first a candidate shortlist of likely critical transistors is defined based on designer expertise, then the final choice is reinforced by sensitivity simulations to quantify SNR degradation. The sensitivity analysis consists in varying the input digital code for one new mono-transistor domain at a time, which is equivalent to varying the corresponding transistor's body-bias

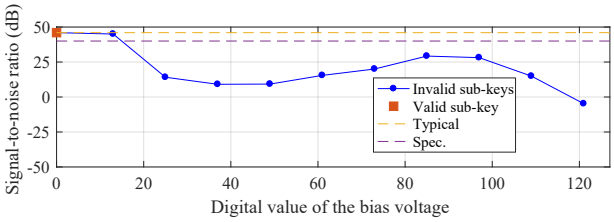



Fig. 10: SNR variation versus the digital value of the body-bias voltage of the top ranked transistor in terms of SNR sensitivity.

voltage, and examining the SNR variation. The transistors in the shortlist are ranked based on descending SNR scores, then the transistor at the top of the list is picked. The picked transistor is a current source transistor located inside the comparator's pre-amplifier, responsible for biasing its input differential pair. This transistor has a body-bias voltage set equal to 0V. Fig. 10 shows the SNR variation versus the digital value of the body-bias voltage. For illustration purposes, a linear DAC is used in the simulation such that the first code '00...0000' corresponds to the correct sub-key. As it can be seen, only for the first 16 "close" sub-keys the SNR stays above 40dB.

Finally, the third column of Table II shows the SNR metrics computed on 100 random keys now considering the enhanced $168+7 = 175$-bits key. As it can be seen, a significantly higher functionality corruption is achieved. The ME is now 17.3dB, that is, the best random key has a SNR of $64-17.3 = 28.7$dB, which is well below the SNR specification of 40dB.

## VII. Conclusions

We proposed a locking scheme for AMS ICs in FD-SOI serving as an anti-piracy security mechanism. The key results from the concatenation of the digital codes of the DACs that generate the body-biases of transistors. A slight modification in the switching network of the DACs is proposed so as to make the dependence of the body-biases on the key non-linear. This low-overhead re-design increases prohibitively the convergence time of optimization-based attacks making them behave like randomized brute-force attacks. The locking scheme is demonstrated on a $\Sigma\Delta$ modulator showing drastic SNR degradation upon application of invalid keys. Rendering an additional critical transistor tunable degrades SNR further. In terms of future work, we plan to generalize the proposed locking scheme for dynamic body-biasing, for other types of body-biases drivers, and for digital ICs.

## Acknowledgments

This work was supported in part by the ANR STEALTH Project under Grant ANR-17-CE24-0022-01 and in part by the RAPID FLEXyRADIO Project.

## 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] T. D. Perez and S. Pagliarini, "A survey on split manufacturing: Attacks, defenses, and challenges," *IEEE Access*, vol. 8, pp. 184013–184035, Oct. 2020.

[5] R. P. Cocchi, J. P. Baukus, L. W. Chow, and B. J. Wang, "Circuit camouflage integration for hardware IP protection," in *Proc. 51st Design Automat. Conf. (DAC)*, 2014.

[6] A. Antonopoulos, C. Kapatsori, and Y. Makris, "Trusted analog/mixed-signal/RF ICs: A survey and a perspective," *IEEE Design Test*, vol. 34, no. 6, pp. 63–76, Jul. 2017.

[7] M. M. Alam, S. Chowdhury, B. Park, D. Munzer, N. Maghari, M. Tehranipoor, and D. Forte, "Challenges and Opportunities in Analog and Mixed Signal (AMS) Integrated Circuit (IC) Security," *J. Hardw. Syst. Secur.*, vol. 2, no. 1, pp. 15–32, Mar. 2018.

[8] A. Sanabria-Borbón, N. G. Jayasankaran, J. Hu, J. Rajendran, and E. Sánchez-Sinencio, "Analog/RF IP protection: Attack models, defense techniques, and challenges," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 1, pp. 36–41, Jan. 2021.

[9] V. V. Rao and I. Savidis, "Mesh based obfuscation of analog circuit properties," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2019.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] Leonhard *et al.*, "Digitally-assisted mixed-signal circuit security," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, 2021, early access.

[18] Y. Bi, J. S. Yuan, and Y. Jin, "Beyond the interconnections: split manufacturing in RF designs," *Electronics*, vol. 4, no. 3, pp. 541–564, Aug. 2015.

[19] 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.

[20] 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.

[21] N. G. Jayasankaran, A. Sanabria-Borbón, A. Abuellil, E. Sánchez-Sinencio, J. Hu, and J. Rajendran, "Breaking analog locking techniques," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, Oct. 2020.

[22] 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.

[23] 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.

[24] N. Planes *et al.*, "28nm FDSOI technology platform for high-speed low-voltage digital applications," in *Proc. IEEE Symp. VLSI Technology (VLSIT)*, Jun. 2012.

[25] G. de Streel, F. Stas, T. Gurné, F. Durant, C. Frenkel, A. Cathelin, and D. Bol, "Sleeptalker: A ULV 802.15. 4a IR-UWB transmitter SoC in 28-nm FDSOI achieving 14 pJ/b at 27 Mb/s with channel selection based on adaptive FBB and digitally programmable pulse shaping," *IEEE J. Solid-State Circuits*, vol. 52, no. 4, pp. 1163–1177, Jan. 2017.